Quest® Stat® 7.0.3

System Administration Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, Stat, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Stat System Administration Guide
Updated - April 2026
Software Version - 7.0.3

Contents

Overview of Stat Administration 10
Stat Architecture and Components 10
Windows Client / Web Browser 10
Stat Central Agent / App Web Server 10
Database Tier 11
Application Environments 11
Stat Administrator Responsibilities 12
Manage Stat Maintenance Tables 12
Administer Security 12
Manage the Stat Central Agent 12
Provide End-User Support 13
Perform Application Upgrades 13
Perform Database Maintenance 13
The Stat SYSTEM User Account 13
Standard Maintenance Windows 14
Buttons and Controls 14
The Record List 15
Field Types 16
Adding and Deleting Records 17
Using the Color Selection Dialog Box 17
Importing and Exporting Maintenance Tables 18
Exporting Data 18
Importing Data 18
Limitations 19

Administrative Utilities 20
Stat INI Editor 20
The Database Tab 21
The Options Tab 24
Encryption Key Update 24
Data Replicator 25
Table Dump Utility 26
PeopleSoft Object Mover Instruction Update Utility 27
Configuration Guide for New Installations 28

Stat Security 29
Stat Security Layers 29
Login Security 29
Internal Security 30
Changing the Database Password 30
Defining User Classes 31
Editing User Class Rights 32
Defining Stat Users 32
Copying User Definitions 34

Resetting Passwords . . . 35
The User Access Information Window . . . 35
User Password Security Settings . . . 41
LDAP Connection Maintenance . . . 42
Defining LDAP Connections . . . 43
Assigning LDAP Connections to Users . . . 44
Connection Manager . . . 45
The Current Tab . . . 45
The History Tab . . . 46

General Maintenance Tables . . . 47
System Maintenance . . . 47
General Tab . . . 47
License Tab . . . 48
Users Tab . . . 49
Other Options Tab . . . 49
Parameters Tab . . . 51
DB Scripts Tab . . . 53
CSR History Tab . . . 53
Approvals Tab . . . 54
Service Domain Maintenance . . . 54
Department Maintenance . . . 55
Issue Tracking Maintenance . . . 56
Custom Label Fields . . . 56
Issue Statuses . . . 57
Country Maintenance . . . 57
Updating PeopleSoft Country and Department Definitions . . . 58
Customer Maintenance . . . 59
Object Type Maintenance . . . 60
File Types . . . 61
Setup Object Types for Oracle Applications . . . 68
File Servers . . . 71
PT Servers . . . 77
User Default Directories . . . 78
Oracle Apps Base Directories . . . 79
Testing File Locations, Servers, and Default Directory Locations . . . 79
PeopleSoft Environment Connection Maintenance . . . 80
Testing Environment Connections . . . 83
Inactivating PeopleSoft Environments . . . 84
Managing File Locations by Environment . . . 84
PeopleSoft Options . . . 84
Copying PeopleSoft Environments . . . 88
Pre/Post Migration Steps Parameters . . . 88
Oracle Applications Configuration . . . 90
Patch Types . . . 90
Product Families . . . 90
Platforms . . . 91

Updating Products 91
Languages 91
Patch Prerequisites 92
Oracle Applications Connection Maintenance 92
Testing Environment Connections 93
Defining Oracle Applications Servers 94
Start/Stop Oracle Applications Agents 96
Inactivating Oracle Applications Environments 96
Setting Up Migration and Patch Approval Lists 96
Updating Products per Environment 100
Copying Oracle Applications Environments 100
Generic Application Connection Maintenance 100
Testing Environment Connections 102
Inactivating Generic Application Environments 102
Managing Source File Locations by Environment 102
Setting Up Migration Approval Lists 103
Copying Generic Application Environments 106
Schema Object Parameters Maintenance 106
Data Object Maintenance 106
Defining Application Version Numbers 107
Defining Data Objects 107
Data Object Example 109
PeopleSoft Search Configurations 111
Creating Tables and Views 112
Exclusions 115
Stat Report Definition Maintenance 115
Editing Reports 116
Adding Custom Reports 116
Turning off the Emailing of Blank Reports 117
Version Control Management Connection Maintenance 117

Service Domain-Specific Maintenance 122
Working With Service Domains 122
Activity Code Maintenance 123
Application Maintenance 123
Application Environment Maintenance 124
Auto Task Maintenance 125
Business Rule Maintenance 126
Defining Business Rules 127
Viewing Rule History 133
CSR Log Topics Maintenance 133
CSR Priority Maintenance 133
CSR Type and Status Maintenance 134
Customer Priority Maintenance 136
Generic Application Migration Path Maintenance 136
Migration Path Diagram 137
Defining Distribution Environments 138

Updating CSR Migration Paths with Additional Environments . . . 139
PeopleSoft Migration Path Maintenance . . . 140
Migration Path Diagram . . . 141
Defining Distribution Environments . . . 141
Updating CSR Migration Paths with Additional Environments . . . 142
Oracle Application Migration Path Maintenance . . . 143
Migration Path Diagram . . . 144
Defining Distribution Environments . . . 145
Updating CSR Migration Paths with Additional Environments . . . 146
Pre and Post Migration Steps . . . 146
Step Types . . . 147
Predefined Steps . . . 147
Defining a Custom Command . . . 148
Release Management Maintenance . . . 150
Template Maintenance . . . 151
Queue Maintenance . . . 152
Workflow Maintenance . . . 153
Template Diagrams . . . 154
Workflow Rules . . . 155
Copying Workflows . . . 161

Configuring the Stat Central Agent . . . 163
Starting and Stopping the Stat Central Agent . . . 163
Starting the Stat Central Agent . . . 163
Stopping the Stat Central Agent . . . 163
Defining Agent Jobs . . . 164
Error Notification . . . 164
Job Maintenance . . . 165
Job Classes . . . 165
The Schedule Tab . . . 168
The Error Notification Tab . . . 169
Stat Central Agent Printers . . . 169
Monitoring the Stat Central Agent . . . 169
Accessing the Job Monitor . . . 170
Schedule Tab . . . 170
Jobs Tab . . . 170
Logs Tab . . . 170
Filtering and Sorting . . . 171
Showing Job and Log Details . . . 171
Customizing the What's New Tab in Stat Web . . . 172
Customizing Field Labels for the Stat Web Client . . . 173

Email Configuration . . . 174
Configuring the Stat Central Agent for Email . . . 174
Outbound Mail Configuration . . . 176
Object Lock . . . 177
Request for Info . . . 177

Approval Notification . . . 178
Resetting Password Message . . . 178
Inbound Mail Configuration . . . 178
Default Values Tab . . . 178
Special Processing Tab . . . 180
Advanced Customer Identification and Tracking # Tabs . . . 182
Field-Specific Tabs . . . 186
Reply Tabs . . . 187

Object Security . . . 189
PeopleSoft Proprietary Object Security . . . 189
PeopleSoft Object Security Setup Instructions . . . 189
Frequently Asked Questions . . . 194
File Object Security . . . 196

Enabling Web Client to perform PeopleSoft migrations . . . 197
Overview . . . 197
Present architecture . . . 197
Compatibility issues with the current implementation . . . 198
Goals of an alternate approach . . . 198
Alternate Architecture . . . 198
How to inform Stat about the available PT servers . . . 199
How does the test connection of PT servers work? . . . 199
How to map PT servers with individual users . . . 199
Using same PT server for migration of multiple PT environments . . . 200

Enable Windows Client to use ODBC for SQL Server . . . 202
Overview . . . 202
Configuring ODBC DataSource in Windows . . . 202
Using editini to create ODBC SQL connections . . . 206

Appendix: Sample Service Domain Configuration . . . 207

Appendix: User Class Rights . . . 209
Notes on User Class Rights . . . 209
CSR Edit Rights . . . 210
CSR Tabs Rights . . . 211
CSR Tasks Rights . . . 212
Generic Application Migration Management Rights . . . 213
Generic Application Object Management Rights . . . 214
Maintenance - File Object Rights . . . 214
Maintenance - General Rights . . . 215
Maintenance - Service Domain Rights . . . 218
Oracle Apps Migration Rights . . . 220
Oracle Apps Object Management Rights . . . 221
Oracle Apps Patch Management Rights . . . 222
PeopleSoft Migration Management Rights . . . 223
PeopleSoft Object Management Rights . . . 224

Project Rights . . . 225
Security Rights . . . 225
Stat Central Agent Rights . . . 226
Tool Rights . . . 226
Wizard Rights . . . 227

Appendix: Creating a Staging Database . . . 229
PeopleSoft on Oracle . . . 229
PeopleSoft on SQL Server . . . 230

Appendix: Database Tuning . . . 231
Oracle Database Instance Tuning . . . 231
MSS SQL Server Database Tuning . . . 231

Appendix: Oracle Applications File Type Directory . . . 232

Appendix: Ports and Firewalls . . . 246
Resolving port and firewall conflicts . . . 246

Appendix: REST Web Services API . . . 249
Authentication . . . 249
URI Structure . . . 249
REST API Resources . . . 249

Appendix: SOAP-Based Web Services API . . . 284
Services and Exposed Methods . . . 284
Login Service . . . 284
CSR Service . . . 285
Approval Service . . . 295
Class Definitions . . . 297
RecordType Bean . . . 297
AttachmentType Bean . . . 298
CSRType Bean . . . 298
CSRLogType Bean . . . 298
CSRTaskType Bean . . . 298
CSRTimeType Bean . . . 299
CSRWorkflowType Bean . . . 299
CSRWorkflowStatusType Bean . . . 299
CSRWorkflowStatusQueueType Bean . . . 300
CSRWorkflowStatusQueueMemberType Bean . . . 300

Appendix: Troubleshooting Chart . . . 301
Stat Database . . . 302
Stat Central Agent . . . 302
Stat Oracle Agent . . . 303
Login/Connection . . . 304
Administrative Utilities . . . 304
CSRs . . . 305
Stat Web . . . 306

Archiving and Migrating 306
Printing 307
Miscellaneous 307

Appendix: Oracle Agent: Stat.conf and log4j2.xml configuration 308

Appendix: Custom Report Files 319
About Stat Report Files 319
Define Data Adapter for Stat Datasource 319
Report Parameters 320
Watermarks 321
Copyright 322
Report Variables 322
Text Field Expressions 322

About us 324

Glossary 325

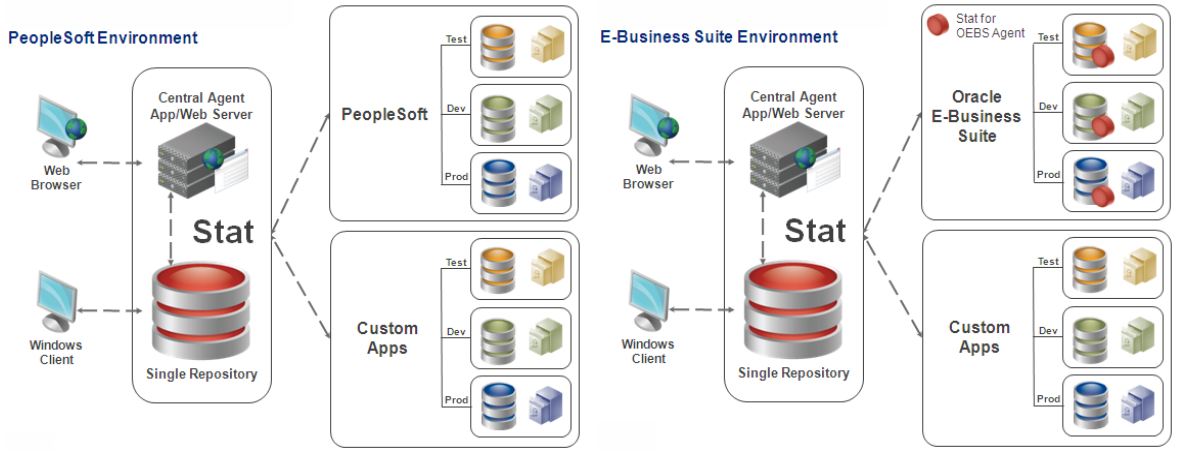
Index 329

Overview of Stat Administration

- Stat Architecture and Components
- Stat Administrator Responsibilities
- The Stat SYSTEM User Account
- Standard Maintenance Windows
- Importing and Exporting Maintenance Tables

Stat Architecture and Components

Stat is based on a four-tier architectural model consisting of a client tier, a web tier, a business logic tier, and a database tier. The components within each tier work together to provide a complete change management solution for PeopleSoft and Oracle Applications, as well as other application environments.



Windows Client / Web Browser

Users interact directly with Stat through the client application installed on their Windows-based workstation. They interact with Stat Web through a browser window.

You can install the Stat Windows Client either locally or on a network. It connects with the Stat Database through various native environment interfaces. You may also install Stat Windows Client on a single network drive accessible by all Stat users.

Stat Central Agent / App Web Server

The Stat Central Agent is a Java-based application that contains the business logic for Stat and the UI for the Stat Web Client.

The Stat Central Agent interacts directly with the Stat Database and the application environments to automate such tasks as generating and printing reports, sending email messages, archiving objects, and maintaining database parameters.

Database Tier

The Stat Database contains activity data and configuration information for the Stat Windows Client and the Stat Central Agent.

The database engine or Database Management System (DBMS) is not a component provided by Stat. Because Stat supports several different database platforms, the DBMS is purchased and implemented independently of Stat.

The management and maintenance of the Stat Database, as it relates to the specifics of your DBMS, are not within the scope of this manual. Refer to your DBMS vendor documentation for information.

Application Environments

Stat provides version control and change management support for PeopleSoft, Oracle Applications, and other application environments.

PeopleSoft Environments

Stat provides advanced change management support for all PTools-based PeopleSoft applications version 8.54 and higher. System Administrators define and maintain the connections between Stat and individual PeopleSoft environments. This entails specifying in Stat various database login IDs and passwords and other DBMS-specific parameters.

In addition to the native PeopleSoft proprietary object types that Stat supports by default, system administrators can configure Stat to support any type of file object used in PeopleSoft environments.

Oracle Applications Environments

Stat provides a complete change management solution for Oracle Applications environments. This includes the file objects and data objects native to Oracle Applications as well as application patches. As with PeopleSoft, system administrators define and maintain the connections between Stat and individual Oracle Applications environments.

The Stat Oracle Agents are background daemons that run on each Oracle Applications server. They receive requests from the Stat Central Agent, process the requests, and send resulting information back to the Stat Central Agent.

Generic Application Environments

System administrators can configure Stat to provide change management support for application environments other than PeopleSoft and Oracle Applications. In general terms, this is done by defining in Stat the connection pathways and source directories of the application servers or databases, as well as the types of objects that Stat will support. Once these configuration parameters are in place, users can lock, archive, and migrate objects in generic application environments the same way they do objects in PeopleSoft and Oracle Applications environments.

Stat Administrator Responsibilities

Stat is a client-server application that uses some of the most advanced technologies available today. Stat system administrators are responsible for maintaining the dynamic integration of these technologies and optimizing their performance. Their job is to customize and configure the internal workings of Stat so as to meet the specific needs of end-users.

System administrators use maintenance tables to configure the Stat application environment. Practically every parameter in Stat is defined in a maintenance table, from high-level parameters like service domains and user classes to low-level parameters like printer queues and CSR log topics. Managing and updating maintenance tables are the most critical aspects of Stat system administration.

Most maintenance tables are accessed from the Maintenance menu and are displayed in a standard user interface window. Depending on the type of table displayed, this window features a number of controls and command buttons that let you quickly edit the table as needed.

The primary responsibilities of a Stat administrator are:

- Manage Stat maintenance tables
- Administer security
- Manage the Stat Central Agent
- Provide end-user support
- Upgrade Stat
- Perform database maintenance functions (these functions may also be delegated to a Database Administrator or DBA)

In later chapters, the actual execution of each of these responsibilities is discussed in greater detail, but a brief overview is provided here.

Manage Stat Maintenance Tables

The Stat Central Agent and the Stat Client utilize data stored in maintenance tables. A maintenance table serves as a kind of template that defines certain operational parameters. For example, the options available on drop down lists, business rules, and email message formats are defined in maintenance tables.

Some of the maintenance tables are shared across all service domains while others are service domain-specific.

Administer Security

Administering Stat security is a highly critical responsibility. It primarily involves defining user classes (which determine the level of access that each user has throughout the system), adding new users, inactivating users, and password maintenance.

Manage the Stat Central Agent

When properly configured, the Stat Central Agent requires minimal supervision or maintenance. However, on occasion you may need to re-configure the Stat Central Agent to perform certain jobs as they come up, such as routine database maintenance.

Managing the Stat Central Agent also involves monitoring it for problems. In most cases, whenever the Stat Central Agent encounters a problem, it simply generates an error log and continues. However, you can configure the Stat Central Agent to notify you via email whenever an error is encountered. After evaluating the situation, you may need to take steps to prevent the error from recurring.

Provide End-User Support

Stat is designed with two groups of people in mind: those who use the application (users) and those who are supported by the application (customers). After the initial implementation of Stat, end-user support is a relatively minor issue. Generally this entails making sure new users receive adequate training.

Perform Application Upgrades

While Quest may release several upgraded versions of Stat each year, most are optional. Your support agreement may stipulate that to remain eligible for support you must be running a current or recent release. It is your responsibility to be aware of these requirements. Quest notifies you of new releases as they become available. Some are shipped automatically, while others are shipped on an as-requested basis. Upgrades usually entail running an install program and a SQL script against your database.

Perform Database Maintenance

Database maintenance includes performing routine backups, optimizing performance, and defragmenting tablespaces as needed. You can configure the Stat Central Agent to automate some of these activities.

These activities are DBMS-specific and not within the scope of this manual. However, a well-tuned, recoverable database is critical to a successful Stat implementation.

The Stat SYSTEM User Account

Stat is delivered with a single user account named SYSTEM that is used by system administrators to first log in to Stat and perform initial set up tasks, such as defining service domains, user classes, and user accounts.

Regarding the SYSTEM account, be aware of the following:

- The account is NOT included in the site license count
- The account is necessary for initial login to Stat, and is used during version upgrades
- The account is used to set up service domains, user classes and users
- The account may be inactivated, but needs to be reactivated prior to an upgrade, or the site may be locked out
- The account is delivered without an initial password. When you use the SYSTEM account to first login to Stat, you are prompted to create a password. Because this account will be the only way to login to Stat until other users are defined, it is recommended that you create a password that is easily remembered. After other users have been defined, you can change the password to something more secure.
- The account is delivered without an email address assigned to it in the User Maintenance table. It is recommended that you assign it an email address so that if the password must be reset for any reason, Stat can deliver a temporary password to a specified email address.
- New users in Stat receive an auto-generated email containing a temporary password, allowing them to log in to the application. When processing the outbound email, Stat uses the SMTP settings configured for the default service domain of the administrator that defined the new user. The SYSTEM account is delivered without a default service domain, however, as none yet exist. This means that before you can define additional users in Stat, you must define a service domain and associate it with the SYSTEM user account.
- It is recommended that separate, individual accounts be set up for personnel designated as system administrators.

Standard Maintenance Windows

Wherever possible, Stat displays maintenance tables in a standard maintenance window. To view or edit a maintenance table, open the Maintenance menu and select the category to which the table belongs. Then in the submenu, select the table. The Maintenance menu contains the following submenu commands:

- **General Tables** – General tables usually affect an application across all service domains. For example, Customers and Departments.
- **Domain Specific** – These tables are service domain-specific. For example, CSR Status.
- **Stat Central Agent** – These tables allow you to configure and maintain the Stat Central Agent as well as email
- **Security Settings** – These tables are used to manage security settings such as creating new user accounts and user classes

Standard maintenance windows display tables in an easy-to-read, spreadsheet-like interface.

Buttons and Controls

A standard maintenance window contains a records list and several action buttons and controls which vary depending on the table it displays. Below are the buttons and controls featured with most maintenance tables.

Service Domain Selector

This drop down list lets you select the service domain you want to edit records for. The list defaults to your default service domain. Also, since some tables, such as the Customer Maintenance table, are not domain-specific, this list is not always available.

Sort Button

This button opens the standard Specify Sort Columns dialog box, which lets you sort the records by any available field. For more information on the **Specify Sort Columns** dialog box, see the *Stat User Guide*, Chapter 4, “Stat Consoles.”

Filter Button

This button opens the standard Specify Filter dialog box, which lets you filter the records by any available field. This is useful for filtering out inactive codes. For more information on the Specify Filter dialog box, see the *Stat User Guide*, Chapter 4, “Stat Consoles.”

NOTE: You can configure Stat to save sort orders and filter settings for a maintenance table after changing its default settings. For more information, see Parameters Tab on page 51.

New Button

This button creates a new blank record.

Delete Button

This button deletes the currently selected record. Once a record has been saved, it cannot be deleted. This feature protects the integrity of your Stat Repository. You can inactivate a saved record, but you cannot delete it.

Special Function Buttons

Depending on the type of maintenance table you are viewing, one or more special function buttons may be available. These buttons are used for accessing additional information particular to the selected record in the table. For information on the exact purpose and use of each button, see the section pertaining to its respective table in later chapters of this document.

Record Counter

Displays the number of records listed.

OK Button

Saves any changes you have made and closes the standard maintenance window.

Apply Button

Saves your changes but does not close the standard maintenance window.

Cancel Button

Closes the standard maintenance window without saving any changes.

The Record List

The record list displays all the records defined in the maintenance table. The top row of the list displays column headings.

Field Name Coding Convention

Column headings are coded as follows:

Code	Meaning
Diamond	The values displayed in these columns are key values and are required. Key values must be unique. For tables with one key value, each definition must have a unique key. For tables with multiple key values, the combination of the key values must be unique. **NOTE:** Key values may not be changed once a definition has been saved.
Asterisk	Required column. A value must be entered in this column.

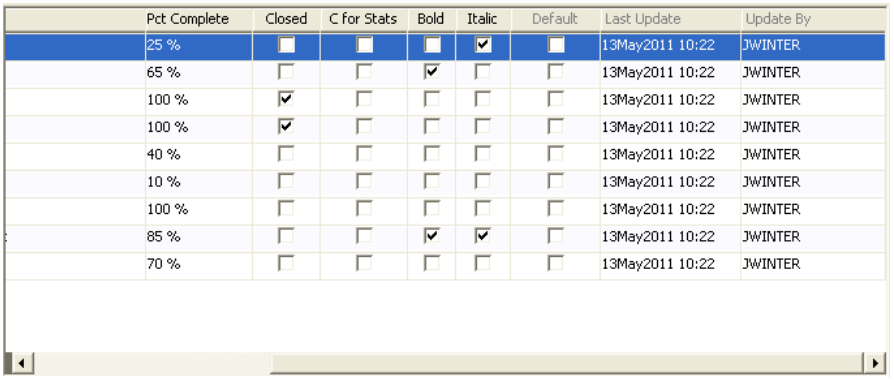
All other columns are either optional (meaning data may be entered in this column or the column may be left blank) or read-only.

Scroll Bar

Along the bottom of the list is a horizontal scroll bar that scrolls the list to the left or right.

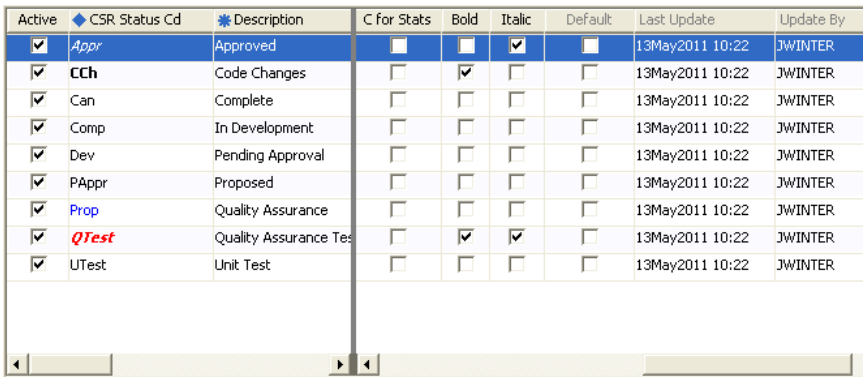
Splitter Bar

The splitter bar is a special tool that lets you keep the columns to the left visible regardless of how far right you scroll. This tool is particularly helpful when working on a table with many columns.



	Pct Complete	Closed	C for Stats	Bold	Italic	Default	Last Update	Update By
	25 %	☐	☐	☐	☑	☐	13May2011 10:22	JWINTER
	65 %	☐	☐	☑	☐	☐	13May2011 10:22	JWINTER
	100 %	☑	☐	☐	☐	☐	13May2011 10:22	JWINTER
	100 %	☑	☐	☐	☐	☐	13May2011 10:22	JWINTER
	40 %	☐	☐	☐	☐	☐	13May2011 10:22	JWINTER
	10 %	☐	☐	☐	☐	☐	13May2011 10:22	JWINTER
	100 %	☐	☐	☐	☐	☐	13May2011 10:22	JWINTER
	85 %	☐	☐	☑	☑	☐	13May2011 10:22	JWINTER
	70 %	☐	☐	☐	☐	☐	13May2011 10:22	JWINTER

When scrolled completely to the right, not all of the data on the left is visible.

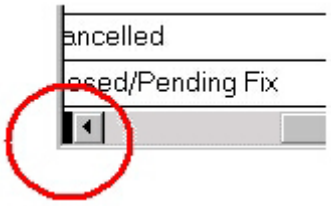


Active	CSR Status Cd	Description	C for Stats	Bold	Italic	Default	Last Update	Update By
☑	*Appr*	Approved	☐	☐	☑	☐	13May2011 10:22	JWINTER
☑	**CCh**	Code Changes	☐	☑	☐	☐	13May2011 10:22	JWINTER
☑	Can	Complete	☐	☐	☐	☐	13May2011 10:22	JWINTER
☑	Comp	In Development	☐	☐	☐	☐	13May2011 10:22	JWINTER
☑	Dev	Pending Approval	☐	☐	☐	☐	13May2011 10:22	JWINTER
☑	PAppr	Proposed	☐	☐	☐	☐	13May2011 10:22	JWINTER
☑	Prop	Quality Assurance	☐	☐	☐	☐	13May2011 10:22	JWINTER
☑	***QTest***	Quality Assurance Tes	☐	☑	☑	☐	13May2011 10:22	JWINTER
☑	UTest	Unit Test	☐	☐	☐	☐	13May2011 10:22	JWINTER

Note that when activating the splitter, a gray vertical line is displayed. A complete display of the list is available on either side of the line. You can move the line to the left or right to resize either list. You can also scroll left or right within each list.

When you scroll up or down, both lists remain synchronized.

To activate the splitter, click and drag the small black line to the left of the horizontal scroll bar.



To deactivate the splitter, simply drag the bar back to its original position.

Field Types

The record list values are displayed in different types of fields.

Check Boxes

Check boxes indicate a yes/no or on/off value. When a check box is deselected, the value is off or no. When selected, the value is on or yes.

Free Text Edit Fields

These fields are used to manually enter text.

Drop Down Lists

These fields are used when the possible values are limited to a specific set. Often times, these lists link back to another table. For example, when specifying a customer value, you must select a department from a list previously defined in the Department Maintenance table.

Spin Controls

Spin controls are used exclusively for numeric values and have small up and down arrow buttons to the right of the control. To increase the value, click the up arrow; to decrease the value, click the down arrow. Spin controls are provided strictly as a convenience. You can also manually enter a value in these fields.

Adding and Deleting Records

Adding a New Record

To add a new record, click **New**. Stat inserts a new blank record at the bottom of the list.

Deleting a Record

To delete a record, select the record. Then click **Delete**. You cannot delete a record once it has been saved.

Inactivating a Record

The first column in most record lists is labeled “Active”. To inactivate the record, deselect the check box and save the change by clicking the **Apply** or **OK** button.

Inactivating a record only makes it unavailable for future use. It does not affect any CSRs or other items that have used the record in the past. Inactive records do not appear on drop down lists.

Activating Record Changes

After another user adds, deletes, or inactivates a record, you may re-cache the codes. This makes those changes immediately available for use. Re-caching codes does not update your security rights. To re-cache codes, select **Tools | Re-cache Codes**.

NOTE: Changes made to your login ID are activated by logging out and logging back in again.

Using the Color Selection Dialog Box

Several of the maintenance tables have a special function button that lets you edit the display color. To edit the display color, select the record you want, then click **Color...**. Stat opens the Color Selection dialog box.

NOTE: Color values selected in the Stat Windows Client do not apply to the Stat Web Client.

Using a Predefined Color

To use a predefined color, click on the color you want in the **Predefined** field.

Using a Custom Color

To create a custom color, slide the red, green and blue scroll bars left or right until the **Sample Text** field displays the color you want.

Importing and Exporting Maintenance Tables

You can import and export data into and from most maintenance tables. This reduces data entry time by moving configuration information between databases or between service domains.

Exporting Data

To export data from one of the standard maintenance windows:

1. Open the standard maintenance window from which you want to export the data.
2. Select **File | Export Data**.

   Stat opens the Save As dialog box, which prompts you to specify a file name, file type, and directory location. The default file type is “Text without headers.” This exports the data into a tab separated text file without header data, which can then be imported into another service domain or database.

Importing Data

You can import into a maintenance table any records that have been exported from a maintenance table of the same type.

To import data into one of the standard maintenance window:

1. Open the maintenance table to which you want to import the data.
2. Select **File | Import Data**.

   Stat displays the Select Import File dialog box, which prompts you to specify the file you want to import. The file must be in a tab-separated format without headers and of the same type as the table into which you want to import the file. When you import the file, Stat adds the imported records to the bottom of the currently opened maintenance window.
3. Once you have imported the rows, you may do the following prior to saving the changes:
   - Edit any of the fields except system-assigned values. Keys are editable up to the time of save.
   - Make sure the imported data values conform to any case requirements in the maintenance table. For example, in the Stat User Maintenance Table, user IDs must be uppercase. If you import a file in which the user IDs that are lowercase, Stat will not convert the values to uppercase and affected Stat users may not be allowed to edit CSRs that are assigned to them.
   - Delete any unwanted rows
4. After editing the records as needed, click **OK**.

Limitations

The following maintenance tables have import/export limitations:

Table	Limitations
Business Rules	Cannot be exported/imported
Templates	Cannot be exported/imported
Work Queues	Queue definitions can be exported/imported but not queue assignments
Stat Central Agent Jobs	Cannot be exported/imported
User Classes	User class rights cannot be imported or exported
Users	Users can be exported/imported but service domain membership and Login information cannot
User Default Directories	Cannot be exported/imported
File Type User Directories	Cannot be exported/imported
File Type Source Locations	Cannot be exported/imported
Migration Paths (all modules)	Paths can be exported/imported but not distributed database lists
Pre/Post Migration Steps	Custom command definitions cannot be exported/imported
Workflows	Templates cannot be exported/imported
Issue Tracking	Cannot be exported/imported

2

Administrative Utilities

- Stat INI Editor
- Encryption Key Update
- Data Replicator
- Table Dump Utility
- PeopleSoft Object Mover Instruction Update Utility
- Configuration Guide for New Installations

Stat INI Editor

The Stat INI Editor is a GUI application designed to create new INI files and edit existing ones. The INI Editor displays all the database profile records contained in the Stat.ini file in an easy-to-read format.

The Stat.ini file contains the information Stat needs to connect to Stat databases. It is located in the Stat version-specific documents folder: *C:\ProgramData\Quest Software\Stat*.

IMPORTANT: If the user does not have access to the folder listed above, the stat.ini file is installed in the Stat version-specific documents folder in the following location: *C:\Users\<user>\AppData\Local\VirtualStore\ProgramData\Quest Software\Stat*.

NOTE: If Stat is installed in a common folder on the network and you would like to share the same stat.ini file for all users, users may copy the stat.ini file to the location where the stat.exe executable is installed.

Access to the Stat INI Editor from within Stat is controlled by the user class right, Launch Ini Editor.

The following is a sample Stat.ini file:

```
----------------------------------------
[Databases]
Dbname1=STAT_ORA
Dbname2=STAT_MSS

[STAT_ORA]
DBMS=O90
OtherDbParm=
DbTrace=No
Unicode=N
ServerName=server.company.com
LoginId=STATLOGIN
LoginPassword=2cac8821a8927cce9b3674bdd177b0dd41f1e9588f67313d4b3f1cd37d7e85cbd7dae
7e7ffc45cd35006d8c07fe80a5e
ConnectTimeOutSecs=10

[STAT_MSS]
DBMS=MSS
Database=DailyBuild570u2014ctp
ServerName=server.company.com
LoginId=STATLOGIN
LoginPassword=117c0c8609f8affe4351e182067229e2c01145e09753e170da6e700ad1c428bac0d27
```

```
d00eb74e7bbad0ebdaefe5f96d4
OtherDbParm=
DbTrace=No
Unicode=Y

[Options]
ClientTimeOffset=0
PSMaxConnections=4
PSCheckObjVersion=Y

[Shared Profile]
SharedProfile=
LocalFailOver=N

----------------------------------------
```

To open the Stat INI Editor, select **Tools | Launch INI Editor**, or select **Ini Editor** from the **Windows Start** menu. The Editor opens with the default Stat.ini file displayed.

To open a different Stat.ini file, select **File | Open**, or click the **Open** toolbar button in the Stat INI Editor toolbar. Then select the file you want. Each INI file opens in a separate record window.

In the INI record window, you can edit all relevant database parameters, including the DBMS, Login ID, and other options.

The record window is comprised of two tabs: Database and Options.

The Database Tab

The Database tab lists the database(s) that Stat can connect to. From here you can edit an existing INI file entry or create a new one. The figure below shows how the INI information appears in the INI Editor. The information is taken directly from the sample INI file on the previous page. The INI Editor helps edit a file by asking for the exact information it needs. For example, if the **DSN** field is not required for a particular database, that field is grayed out.

To create an INI file entry:

1. Select **File | New**.

   The Stat INI Editor opens a blank record sheet.

2. Select **Edit | New Record**.

   The Stat INI Editor prompts you to specify the name of the database.

3. Enter the name of the database. Then click **OK**.

   The Stat INI Editor adds a new database profile to the record sheet.

4. In the **DBMS** field, select a DBMS.

   The default is Microsoft SQL Server. Depending on the DBMS you select, the STAT INI Editor prompts you to define different values.

5. Enter the STATLOGIN password in the **Encrypted Login Password** field, either by entering an encrypted password from another stat.ini file or by clicking **Change Password** and entering the STATLOGIN password.

   For more information, see the section Changing the STATLOGIN Password on page 22.

6. In the remaining fields, specify additional parameters as needed.

7. Select **File | Save as**. Then specify a name for the INI file.

8. Click **Save**.

General Setting Information

The following table contains general database connection settings for the Stat INI Editor. Each record in the Stat INI Editor represents a database in the INI file. For more general information on available DBMS settings, see any of the Environment Connection Maintenance sections in Chapter 4, General Maintenance Tables on page 47.

Value	Description
DBMS	Database interface identifier. This identifier is DBMS and DBMS release specific.
Server Name (MS Sql Server) NET_SERVICE_NAME (Oracle)	The name of the database server that houses the Stat Repository. Formatting for this entry is DBMS-specific.
LoginId	The login ID used for the Stat first-pass login. Not used by all DBMS. This entry should always be STATLOGIN.
Encrypted Login Password	The encrypted password of STATLOGIN. This value can be changed, as described below.
Connect Time Out Secs	Number of seconds to wait for a connection to the database before timing out. Not supported by all RDBMS.
OtherDbParm	Additional database connection parameters, if needed. For Oracle databases that use a comma rather than a period as a decimal separator, enter the value: DecimalSeparator=','.
Unicode	Type Y if you are running Stat on a Unicode database (in order to support PeopleSoft Unicode databases) and the DBMS is SQL Server. Otherwise leave blank.
Enable DB Trace	Configures Stat to write a trace log of all commands. Selecting this option impacts the client application's processing speed and should only be selected if directed to by Support.
Use ODBC	(Applicable for SQL Server) Check this if you want to use ODBC drivers instead of SQL native client
DSN	(Applicable for SQL Server) This field is only visible if Use ODBC is checked. This is the DSN entry of the ODBC data source that you have configured in your windows client installation machine.

Changing the STATLOGIN Password

The initial STATLOGIN password is delivered as part of the installation scripts and is used to define the STATLOGIN user on the database. The system administrator can modify the STATLOGIN password on the database (25 characters maximum) as dictated by internal business processes and update that password in the INI Editor. The password is encrypted and stored in the stat.ini file.

IMPORTANT: Changing the STATLOGIN password should not be confused with changing the Stat database password, which is documented in the section Changing the Database Password on page 30.

There are two options for modifying the password. In either scenario the administrator or DBA needs to first modify the STATLOGIN user password on the database. Then they can either:

1. Distribute the unencrypted password and have each user update their own stat.ini file with the password.

   Or

2. The Administrator changes the password in the INI Editor and then distributes the encrypted password to the users to place into their editini.exe program.

To modify the password using the non-encrypted password:

1. Click **Change Password**.
2. Enter the New Password and the confirmation of the New Password and click **OK**.

The new encrypted password is displayed in the **Encrypted Login Password** field.

3 Click in the field and right click to copy the encrypted password if it needs to be distributed.

4 Click on any other field and click **Test Connection** to test the password.

5 Save your changes.

To modify the encrypted password:

> **NOTE:** This assumes that someone has already followed the procedure above and has sent you an encrypted password.

1 Replace the existing **Encrypted Login Password** value with the new value.

2 Click on any other field and then click **Test Connection t**o test the password.

3 Save your changes.

Testing Connections

After defining a database record, you can make sure that you have entered all the information correctly by selecting the record and clicking **Test Connection**. This makes Stat establish a connection to the database. If successful, Stat immediately disconnects from the database and displays a "Connection Successful" message box. If Stat is unable to connect, it displays a message box stating the cause of the failure, for example, "invalid username/password. logon denied."

Editing Records

To edit a database profile record, select the database whose profile you want to edit and specify different values as needed in the appropriate fields.

Deleting Records

To delete record, select the record. Then select **Edit | Delete Record**.

Duplicating Records

To facilitate INI editing, the Stat INI Editor allows you to duplicate database profile records. You can use the Duplicate function to create a copy within an INI file.

To copy a record:

1 Select the database whose profile record you want to duplicate.

2 Select **Edit | Duplicate**.

The Stat INI Editor creates a new record and assigns it the same name as the duplicated record preceded by the word "Copy" (for example "Copy Development"). You can change this name if you want.

3 Edit the record values as needed.

4 Save your work.

Copying Record Values

The Copy function copies the values of a database record profile which you can then paste into another record in the same or in a different INI file.

To copy a record:

1. Select the database whose profile record values you want to copy.
2. Select **Edit | Copy Values**.
3. Select the database profile record to which you want to copy the record.

   This can be an existing or new record in the same INI file or in a different one.
4. Select **Edit | Paste Values**.
5. Save your work.

Order of Appearance

The list of records created in the INI file becomes the list of databases in the Stat Login window. The databases are displayed in alphabetical order in the drop down list of the Stat Login window.

You can specify a default record to be displayed when the login window opens. To set the default record, select the record and click **Set As Default**. The selected record moves to the top of the list in the INI file.

Printing the Stat INI file

To print a record, select **File | Print**. Or click the **Print** toolbar button in the Stat INI Editor toolbar.

The Options Tab

The Options tab displays information contained in the Options and Shared Profile sections of the Stat INI file. The database parameters displayed on this tab must be set at startup and are workstation specific.

In the Options tab, you can share database profile records if you want to use a file that resides on the network. This field displays the full path and name of the file you want to use in either a “drive:\directory\file” format or a UNC format (\\servername\share\directory\file).

The Local failover options indicate what action the Stat INI Editor takes if the shared profile (.ini file) is not found. Options include:

- **Yes** – The application displays an alert message and then uses the local default INI file instead
- **No** – The application halts and displays an alert message

Encryption Key Update

As a general security precaution, you may want to periodically change the encryption key for all the active passwords contained in the Stat database, including Stat user ID passwords, environment and file server passwords, and email server passwords. When the encryption update utility encounters a password for an inactive record that cannot be decrypted, it substitutes a randomly-generated string for the password and issues a warning. When it encounters a password for an active record that cannot be decrypted, it issues an error message and does not complete the update procedure.

> **!** CAUTION: **Before updating the encryption key, shut down any Stat Central Agents that are running and have all users log out of Stat.**

To change the encryption key:

1. Log in to Stat as the SYSTEM user.
2. Select **Tools | Update Encryption Key**.

Data Replicator

You can use the Data Replicator tool to copy data from one service domain to another, either within the same Stat database or between two Stat databases. This tool allows you to quickly populate new service domains with pre-existing data and to maintain consistency throughout your Stat environment. For example, if you create a new service domain in your Stat production database, you can use the Data Replicator to populate that service domain with data from an existing service domain in your Stat development database.

Access to the Data Replicator should be restricted to system administrators and is controlled by the following user class rights:

- Data Replication - Inbound
- Data Replication - Outbound

Note the following before using Data Replicator to copy either business rules or workflows:

- Both business rules and workflows are keyed on an internal identifier that is unique across the whole Stat environment. It is not service domain unique.
- When either is copied from a Dev Stat environment to a Prod Stat environment for the first time, there should be no issue given that the Prod environment is empty. From that point forward the internal identifier list may never match again. Therefore, both business rules and workflows require that the Description field be unique.
- The Data Replicator can be used to copy business rules between environments, or between service domains in the same environment

  NOTE: To copy business rules to service domains within the same Stat environment, you can also use the copy function in the Business Rule Maintenance table. For more information, see Copying Rules on page 132

- When business rules are copied, it is your responsibility to double-check the Criteria window after the copy and validate that the rules make sense in the new environment or new service domain. The Data Replicator does not validate that all of the criteria fields are exactly the same between environments or service domains.
- The Data Replicator can be used to copy workflows between Stat environments, but do not use the Data Replicator to copy workflows between service domains within the same environment. Instead use the copy function in the Workflow Maintenance table. For more information, see Copying Workflows on page 161.
- For workflows, the Workflow Name, Service Domain, CSR Type, and Migration Path Code must be unique
- When workflows are copied between Stat environments, the assumption is that the CSR fields in the like service domain are exactly the same. The Data Replicator does not do this validation. The user should validate the workflow on the maintenance window after the copy.

To use the Data Replicator:

1. Select **Tools | Data Replicator**.

   Stat opens the Data Replicator tool, which displays a list of all the maintenance tables and CSR information defined in the Stat database. These collections of data are called entities and are grouped into five categories:

   - **General Tables** – General tables usually affect an application across all service domains. For example, Customers and Departments.
   - **Service Domain Specific** – These tables are specific to individual service domains. For example, CSR Status.
   - **Stat Central Agent** – These tables allow you to configure and maintain the Stat Central Agent as well as email
   - **Security Settings** – These tables are used to manage security settings such as creating new user accounts and user classes
   - **CSRs** – These tables contain CSR information, excluding associated objects and archive sets

2 In the **Destination** field, click **Connect**.

   This opens the Connect to Destination Database window, which looks and behaves exactly like the Stat Login window.

3 In the Connect to Destination Database window, log in to the database to which you want to copy data.

   If you want to copy data between service domains within the same Stat database you are currently logged into, select that database in the Connect to Destination Database window.

4 In the **Source** field and select the service domain whose maintenance tables you want to copy.

   If you want to copy maintenance tables regardless of service domain, select **Any Service Domain**.

5 (Optional) If you are want to replicate the data to a service domain that is named differently than the source service domain, select the **Copy to Alternative Service Domain** option and select the service domain you want.

   You do not need to select this option if you are replicating data between databases and the target service domain has the same name as the source service domain.

6 (Optional) Select the **Include Dependencies** option if you want to copy the dependency data of each entity you select.

   Certain entities include information defined in other entities, and you may want replicate all these tables together as a single unit. For example, the Customers maintenance table includes information defined in the Countries and Departments maintenance tables. The **Include Dependencies** option configures Stat to select these tables automatically when you select the Customers maintenance table. You can de-select any dependency table that you do not want to replicate.

   NOTE: Stat does not replicate a record in a maintenance table if that record references dependency data that is not selected for replication and is missing in the target service domain.

7 (Optional) Select the **Copy only active records** option if you only want to replicate only records that are currently active in each entity you select.

8 Select each entity you want to copy.

   To select all the entities, click **Select All**. To deselect all, click **Select None**.

9 Click **Copy Data**.

   Entities that were successfully copied are designated in the Status column by a green check mark. Entities that weren't copied successfully are designated by a red 'X.' If you want to clear the copy status of the maintenance tables and make another attempt at copying data, click **Clear Status...**.

   To view log entries that were generated during processing, select the **Copy Log** tab. Data Replicator saves the log file. You can change the location of the log file on the Copy Log tab.

   You can filter the log entries so that only information, warning, or error messages are displayed.

Table Dump Utility

The Table Dump Utility is a troubleshooting tool that allows you to dump the contents of a table so that it can be emailed to the Quest Support staff. Support then evaluates the contents of the file in order to find the cause of the problem.

You should use this utility only as instructed by the Quest Support staff. If called for, a Support representative may give you a SQL statement to execute or send you a .sql file that you can upload into the utility. You then execute the statement or file and forward the resulting data (as a .psr file) to Support.

Access to this tool should be restricted to system administrators. It is important to note that the tool bypasses service domain security. This means you could dump data from any service domain, regardless of your security restrictions.

To use the Table Dump Utility:

1. Select **Tools | Table Dump Utility**.
2. Do one of the following:
   - Enter the SQL statement manually as instructed.
   - Click Open SQL. Then browse for and select the .sql file you want to load.
3. (Optionally) If you entered a SQL statement manually and want to save the statement as a .sql file for re-use later, click **Save SQL**. Then specify a location and name for the file and click **Save**.
4. Click **Execute**.

   The data appears in the lower box and a counter shows the system's progress.
5. Click **Export**. By default, Stat names the file "tabledmp.psr."
6. Rename the file and save.
7. Attach the file to an email and send it as instructed by the Support staff.
8. Click **Clear**.

   The SQL statement remains in the upper window.

PeopleSoft Object Mover Instruction Update Utility

When you upgrade Stat or when PeopleSoft has a major PeopleTools release, you may need to run the PeopleSoft Object Mover Instruction Update Utility. This utility tells Stat how to migrate and recover different versions of PeopleSoft proprietary object types. The utility works by executing a set of commands contained in a file named psominst.psr located in your Stat directory.

You can also use this utility to fix problems you may experience when migrating archive sets. If Stat displays error messages that read "Load SQL definitions ( ) failed to open cursor" or "Load SQL definitions did not find any definitions for object type:__PeopleSoft version __," this may be because you need to update the Object Mover instructions.

Access to this utility should be restricted to system administrators.

To run the PeopleSoft Object Mover Instruction Update Utility:

1. Select **Maintenance | General | Update PS Object Mover Instructions**.

   You are prompted to shut down the Stat Central Agent for the database you are updating and to verify that you have a new PSOMINST.PSR file in your Stat directory.
2. Click **Update**.

   The utility reads, updates, and executes the new instructions and reports the number of rows that it has updated when complete.
3. Click **OK**.

Configuration Guide for New Installations

The Configuration Guide for New Installations is a list of To Do windows designed to guide Stat Administrators through the task of performing a fresh Stat installation. To use this Guide, in the main menu select **Tools | Configuration Guide**.

Each row in the Configuration Guide represents a maintenance topic in the order necessary to configure Stat. All required categories are indicated by a check mark in the Reqd column. The current status of each topic is represented by a check mark in the Status column.

If you double-click on a specific category, Stat opens the corresponding maintenance window. Status automatically sets when the corresponding maintenance window has at least one row. By using the Configuration Guide, a Stat Administrator may configure General and Domain-Specific data.

Configuration Guide security is controlled by the following user class right:

- Tools - Configuration Guide

3

Stat Security

- Stat Security Layers
- Defining User Classes
- Editing User Class Rights
- Defining Stat Users
- LDAP Connection Maintenance
- Connection Manager

Stat Security Layers

Stat comes equipped with a powerful, two-layered security system. At the first layer, strict login protocols control access to the Stat Repository, and at the second layer, a set of internal security measures controls access to sensitive areas within the application database.

Internal security is based on service domains and user classes. User classes are logical groupings of access rights which are assigned to users according to their functional needs. These rights can include everything from working within different service domains to adding and editing activity codes. User classes effectively maintain security within Stat by limiting users' access to only the data and functions that pertain to them.

Login Security

Whenever a user attempts to login to Stat, two security checks, or "passes," are made against the Stat Repository before the user's login ID and password are validated. In this way, a total of three validations are performed before a user is granted access to the system. This process is as follows:

1. In the Stat Login window, the user selects a database and enters his or her login ID and password.
2. Stat connects to the selected database using the login ID specified in the Stat.ini file (by default, "STATLOGIN") and a special password.
3. The STATLOGIN ID accesses the Stat_Login table. It cannot access any other table. This is the first pass.
4. From the Stat_Login table, the schema owner's login ID and password are selected. The login ID and password are encrypted in the table.
5. The STATLOGIN ID disconnects from the database.
6. Stat re-connects to the database using the schema owner's login ID and password obtained during the first login. This is the second pass.
7. Stat then checks the user table to validate that the user's login ID is in the table. This is the global application validation.

If the ID is valid, the appropriate security is put in place and Stat is loaded with all the internal security measures defined for the user in place. The user never actually logs into the Stat Repository using his or her login ID. First the STATLOGIN ID is used, then the ID from the Stat_Login table. Stat user IDs are used to identify the functions that users can and cannot perform once they are logged in.

Internal Security

Internal Stat security is based on service domains and user classes. User classes are collections of access rights that control a user's ability to view information and perform functions within service domains. To operate within a service domain, a user must be assigned to at least one user class that is associated with that service domain.

For example, the table below illustrates the security rights assigned to a user based on hypothetical service domains and user classes The user has access to the Change Control and Information Systems service domains, but not the Human Resources service domain.

Service Domain	Access	Default	User Class
Change Control	Yes	Yes	Developer
Change Control	Yes	No	Migrator
Information Systems	Yes	No	Staff
Information Systems	Yes	No	Projects
Human Resources	No	No	N/A

In this example, the user is assigned to the Developer and Migrator user classes in the Change Control service domain. The Developer user class lets the user edit and create CSRs, lock objects, and create archive sets, whereas the Migrator user class lets the user migrate archive sets. However, neither user class lets the user edit maintenance tables or add new users. In the Information Systems service domain, the user also has the combined rights of two user classes: Staff and Project. The Staff user class only lets users create new CSRs and view existing CSRs, whereas the Project user class lets the user create and edit projects. Lastly, in the Human Resources service domain, the user is not assigned to a user class and has no access whatsoever.

The indication of default in the Change Control domain means that when Stat prompts the user to select a service domain — for example, when opening a new CSR — the default choice is Change Control.

Changing the Database Password

Upon installation, the second pass Login ID and password are set for you. The Login ID is set to “STAT.” Do not change it.

If your DBA requires that the Stat database password be changed, the password itself must be changed in three locations: the Stat Windows Client, the Stat Central Agent, and at the database level.

Changing the Stat database password for the Stat Windows Client is controlled by the user class right, Master Database Login ID - Change.

> **CAUTION: This is a very critical operation and must be performed carefully. Contact Quest Support if you need assistance.**

To change the Stat database password:

1. Make sure all Stat users have logged out except the one user who will change the password in the Stat Windows Client.

   This user must remain logged in for the password change to take effect.

2. Once the password has been changed at the database level by the DBA, select **Maintenance | Security Settings | Database Login Info**.

3. In the Change Database Password dialog box, enter the password exactly as it is defined at the database level.

4. Confirm the password. Then click **OK**.

5. Without logging out of Stat, start a second session of Stat, logging in with the new password.

   This will confirm that you have entered the password correctly. If you receive a second pass login error, you may have typed the new password incorrectly.

After changing the password at the database level and then in the Stat Windows Client, you need to change the password for the Stat Central Agent. You can use the Configuration Assistant to make this change. For more information on the Configuration Assistant, see the document, *Stat Install Notes*.

6 Open your Internet browser and go to http://<stat_server_host_machine>:8080/stat-config.

This opens the Configuration Assistant.

7 In the **Password** field, enter the password to match the password for the Stat Windows Client and at the database level. When finished, click **Save**.

Stat verifies that the Stat database parameters you entered are correct.

8 Stop and then re-start the Stat Central Agent.

Defining User Classes

One of the first tasks in a Stat implementation is to define user classes. User classes are logical groupings of security rights based on the functional roles of users. For example, Stat system administrators would typically belong to a user class that allows them to define and edit service domains, whereas most other Stat users would not belong to that class.

NOTE: Stat is delivered with a special user account called SYSTEM that system administrators use to log into Stat and perform initial set up tasks, such as defining service domains, user classes, and user accounts. For more information, see The Stat SYSTEM User Account on page 13.

Stat gives you the flexibility to define as many user classes as you need. As a general rule, it is a good idea to start off with a few user classes and add more as necessary.

User classes correspond to business or functional roles within an enterprise, such as Administrators and Developers. Users that fulfill multiple roles can be granted membership in multiple user classes, each corresponding to a different function. A user's rights are the summation of the rights in all the user classes to which that user belongs.

User class security is controlled by the following user class rights:

- User Classes - Add
- User Classes - Edit

The User Class table is displayed in a standard maintenance window. To open this window, select **Maintenance | Security Settings | User Classes**.

Values	Description
Active	If selected, activates the value in Stat
User Class Code (Key Value)	A 1-10 alpha character code which uniquely identifies the user class
Description (Required Value)	A 1-35 character description of the user class
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

To add a new user class:

1 In the User Class Maintenance window, click **New**.

A blank row appears at the bottom of the user class table.

2 In the **User Class Code** field, type a 1-10 character code which uniquely identifies the user class.

3 In the **Description** field to activate the text box. Then type a 1-35 character description of the user class.

4 Click **Apply**.

   Stat automatically displays the current date and time in the **Last Update** field and your user ID in the **Update By** field.

5 Click **Edit Rights...**. Then in the Select Edit Rights window, select the rights you want to assign the user class.

   See the next section for more information on managing user class rights.

6 Click **OK**.

NOTE: You cannot delete a user class once it has been saved in the database. If you want to deactivate it, deselect Active.

Editing User Class Rights

You can edit the security rights of a selected user class by clicking **Edit Rights...** in the User Class Maintenance window. Stat displays the User Class Rights window.

The User Class Rights window displays two tree list views of rights, which are grouped into categories corresponding to functional areas within in Stat. The right side shows all the rights currently assigned to the class, while the left side shows all the unassigned rights. Each group displays the number of rights it contains in relation to its corresponding group. For example, if 15 of the total 33 CSR Edit rights are assigned to a class, the CSR Edits group in the unassigned list will display the number 18 (no number indicates that all the rights are contained in the corresponding group). The total number of rights assigned and unassigned to a class is shown above each list. Double-click a group to expand it, or use the Expand All button.

Be aware of the following when editing user class rights:

- Some user class rights are specific to service domains. Users that belong to a user class with service domain-specific rights (for example, the right to migrate archive sets) can invoke these rights only within the service domains that the user class is associated with. Rights that are not service domain-specific, however, can be used in any service domain that the user is allowed to work in. For example, the user class right, Undocumented Patch Wizard - Run, is not service domain-specific. This means users that have this right in one service domain can run the wizard in all the service domains they can access, including those in which the right is not given.
- Certain object management functions in Stat, such as running wizards, require the user possess two rights, one to perform the function itself, and a second right to access the appropriate change management module. For example, to run the Archive Purge Wizard in the PeopleSoft change management module, the user needs the right, Obj Archive Purge Wizard - Run, and the right to access the PeopleSoft module, Change Management Module Access - PS. The remaining module access rights include Change Management Module Access - Generic Apps and Change Management Module Access - Oracle Apps.

To assign or unassign a right, select it and use the arrow buttons to move it between the two lists. Then click **OK**.

NOTE: In general, if a user class has an Add right, this overrides the absence of an Edit right. For example, if a user class has the right, Activity Codes - Add, the user class also has the right to edit existing records, even if the class has not been granted the right, Activity Codes - Edit.

For a complete description of each user class right, see Appendix: User Class Rights on page 209.

Defining Stat Users

Before users can work in Stat, they must be defined in the User Maintenance table. This table contains all the information about the user that Stat requires.

User account security is controlled by the following user class rights:

- Stat Users - Add

- Stat Users - Edit

NOTE: You can grant users the right to reset the passwords of other Stat users by giving one of the user classes to which they belong the user class right, Stat Users - Reset Password. It is not necessary that you also grant them adding or editing rights. In this case, users can reset passwords by selecting **User Options | Passwords | Administer Passwords**.

The User Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Security Settings | User Maintenance**, or select **User Options | User Maintenance**.

Included in this section are descriptions of the user password settings defined in the System table. The System table is described in the section, System Maintenance on page 47, but due to their relevance to Stat security, the user password settings are also addressed here.

Values	Description
Active	Indicates if this user is allowed to log in. **NOTE:** The number of active users cannot exceed the number stipulated in your license agreement.
User ID (Key Value)	A 1 to 10 character value that uniquely identifies this user. This is the login ID.
Last Name (Required Value)	The user's last name **NOTE:** Each user must have a unique Last Name/First Name combination of values.
First Name (Required Value)	The user's first name
Title (Required Value)	The user's title
License Type (Required Value)	Determines whether the user is licensed as a Technical user with full access to Stat or as a Functional user, which has limited access and is not allowed to perform object management tasks. For more information, see Users Tab on page 49.
Rpt Access (Required Value)	The user's report access level. This value must be greater than or equal to the security level of the report for the user to view it.
Phone Nbr	The user's telephone number
Phone Ext	The user's telephone extension
E-mail Address (Required Value)	The user's e-mail address. **NOTE:** This value is required so that new users and users whose passwords have been reset can receive an auto-generated email from Stat containing a temporary password. The one exception to this is the default SYSTEM account, which does not have an email address assigned to it when Stat is first installed. It is recommended that you assign it an address so that Stat can deliver an email with a temporary password to that address if the original password must be reset for any reason.
Log Destination Directory	The directory where Stat writes migration logs. The default is *C:\Temp*
Related Objects	If selected, Stat prompts the user to insert related objects into the CSR
Default Module	The default value displayed in **Module** fields on CSRs. Options include PeopleSoft, Oracle Applications, and Generic.
Default PS Version	The default value displayed in **PS Version** fields on CSRs.

Values	Description
Enable LDAP	If selected, allows the user to login to Stat using his or her LDAP password. This value is set in LDAP Connection Maintenance table. The passwords for LDAP users cannot be reset from within Stat. For more information, see LDAP Connection Maintenance on page 42.
User DN	The directory of the LDAP user account. This field is pre-populated with the value of the base DN appended to the template DN specified in the LDAP Connection Maintenance table. You can modify this default value as needed. For connections using the SAM-Account-Name attribute, if you leave this field blank, the user's Stat User Id will be passed in for samAccountName when logging into Stat. If you enter a User Id in this field, you will overwrite the Stat User Id being passed for samAccountName. For more information, see LDAP Connection Maintenance on page 42.
Reset Password	Indicates that user password has been reset
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

To add a new Stat user:

NOTE: New users receive an auto-generated password from Stat containing a temporary password. When processing the outbound email, Stat uses the SMTP settings configured in the default service domain of the administrator that defined the new user. If the administrator has not yet been assigned a default service domain, they are prompted to select one when they attempt to save the new user definition.

1. In the User Maintenance window, click **New**.

   A blank row appears at the bottom of the user table.

2. In the **User ID** field, type a 1-10 character code which uniquely identifies the user.
3. Specify the required values for the user as described in the preceding table.
4. Specify any optional values for the user as described in the preceding table.
5. Click **Apply**.

   Stat automatically displays the current date and time in the **Last Update** field and your user ID in the **Update By** field.

6. Click **Access Information...**. Then in the User Access Information window, specify the access rights you want to assign to the user.

   See The User Access Information Window on page 35 for more information.

7. Click **OK**.

   Stat automatically sends an email to the new user with a temporary password to use the first time they log into Stat. The exact message in the email can be modified on the Reset Password tab of the Electronic Mail Interface - Setup window. See Resetting Password Message on page 178 for more information.

Copying User Definitions

If you need to define a Stat user whose information closely resembles that of an existing user, you can save time by copying the definition of the existing user and editing the copy as needed. When you copy a user definition, all the information gets copied over, including working directories, access levels, and user class assignments.

To copy a user definition:

1. In the User Maintenance window, select the user definition you want to copy. Then click **Copy**.

   Stat prompts you to specify a user ID and a first and last name for the new user.
2. Specify the user ID, first and last names of the new user. Then click **OK**.
3. Edit the new user definition as needed.

Resetting Passwords

For non-LDAP enabled users, the **Reset Password** button resets their password. The user then receives an automatically generated email from Stat containing a temporary password and instructions to change their password at the next login or from the User Options window.

NOTE: When processing the email job, Stat uses the SMTP settings configured in the default service domain of the user resetting the password.

The User Access Information Window

The **Access Information...** button opens the User Access Information window. The window features tabs in which you can do the following:

Tab	Description
Service Domain Access Tab	Grant users access to a service domain by assigning them to user classes for that particular service domain.
PS Options Tab (PeopleSoft only)	Define the PeopleSoft Operator IDs and passwords that the selected user will need to physically lock PeopleSoft proprietary objects.
User File Directories Tab	Define the selected user's working file directory for each file type as well as the user's default working directory.
Queue Assignment Tab	Add and remove the selected user from work queues.
Application Access Tab	Restrict a user's access to only specified applications while working within certain service domains.
Object Type Access Tab	Restrict a user's access to only specified object types while operating within a certain change management module and service domain.
Environment Access Tab	Restrict a user's ability to migrate objects to only specified environments while operating within a certain change management module and service domain.
Pre/Post Migration User Parameters Tab	Define public user-based parameters that can be included in the definition of post migration command steps.

TIP: After defining the access settings of one user, you can use that user as the source for the synchronizing the access settings of multiple users. For more information, see Synchronizing User Access Information on page 41.

Except for the **PS Options** and **User File Directories** tabs, each tab in the User Access Information window displays two lists of access rights. The right side shows all the access rights currently assigned to the user, while the left side shows a tree view of all the unassigned rights organized by service domain (except in the case of the **File Server** tab). Each group of unassigned rights displays the number of rights it contains. A bold number indicates that all the rights in the group are currently unassigned to the user, while no number indicates that all the rights are currently assigned to the user. The total number of access rights assigned and unassigned to a user is

shown above each respective list. Double-click a group of unassigned rights to expand it, or use the **Expand All** button.

Service Domain Access Tab

You grant users access to a service domain by assigning them to user classes for that particular service domain. New users start out with no access rights to any service domain. In this case, the first step is to assign them a default service domain, which is the service domain that the user will work with most often and will be the default choice whenever the user is prompted to select a service domain, such as when creating a new CSR.

To set up service domain access:

1 For new users, do the following:

   a In the **Default Service Domain** field, select the user's default service domain.

   b Double-click the default service domain in the unassigned list to view the user classes for that service domain.

   TIP: Use the Expand All and Collapse All buttons to open and close the unassigned tree list view.

   c Select each user class you want the user to belong to for the selected service domain and click the right-pointing arrow button.

   The user classes appear in the list of assigned rights in the left side of the window. After a user is assigned to a user class, you can remove the user by selecting the class in the assigned list and clicking the left-pointing arrow button. The user class then returns to the unassigned list.

   NOTE: If you select a service domain and click the right pointing arrow, the user is assigned to all the active user classes for that service domain.

2 Expand the list of user classes for each additional service domain that you want to grant the user access to.

3 For each service domain, select the user classes you want the user to belong to and click the right-pointing arrow button.

4 Save your changes by clicking either **Apply** or **OK**.

5 (Optional) if you want to edit the user class rights of a user class the user currently belongs to, select the class in the assigned list and click **Class Rights**.

   This opens User Class Rights window where you can edit the rights of the user class. For more information, see Editing User Class Rights on page 32.

6 (Optional) To view all the user class rights currently assigned to the user, click **User Rights**.

   This opens a Stat Report in PDF format showing all the user class rights currently assigned to the user by service domain.

CAUTION: When modifying a user's service domain and environment access, be aware that this may affect migrations and patch applications to environments that require the user's approval. If a user's approval is required for a migration or patch application to an environment that they no longer have access to (which can be restricted either at the service domain or the environment level), the migration or patch application to that environment cannot be approved.

PS Options Tab (PeopleSoft only)

The PS Options tab displays a list of all the PeopleSoft environments defined in Stat. From here you can define the PeopleSoft Operator IDs and passwords that the selected user will need to physically lock PeopleSoft proprietary objects. You do not have to define a password the same time you define a PS Operator ID.

In this tab, you can also configure Stat to do the following:

- Open PeopleSoft and automatically log the user in to the environment in which he or she has staged objects during a PeopleSoft migration. This way, the user can verify the staging of objects without having to manually open the project in PeopleSoft.

- Automatically migrate the objects in the user's project from the staging database to the target environment during a PeopleSoft migration
- Automatically migrate the objects out to all the environments included in the distribution list when the user migrates objects to the distribution environment

If you want to configure Stat to perform any of above mentioned tasks, you must specify both the user's PS Operator ID and password for the selected environment. For auto-migration, you must also define the staging database in a migration path as well as the distribution environment, if any.

In addition to the CLI functionality described above, defining a user's operator ID and password allows that user to physically lock PeopleSoft proprietary objects in the selected environment:

Staging databases are defined in the PeopleSoft Environment Connection Maintenance table, as explained in the section, PeopleSoft Environment Connection Maintenance on page 80. Distribution environments are defined in the PeopleSoft Migration Path Maintenance table, as described in the section, PeopleSoft Migration Path Maintenance on page 140.

NOTE: Users can define their own IDs and passwords in the PeopleSoft Options window, which they open by selecting **User Options | PeopleSoft Options**. In addition, users can share the same PS Operator ID and password for staging purposes if that is how your PeopleSoft environment is configured. For example, you can assign users the ID "PS" or "VP1."

To set up a PeopleSoft Operator ID and password:

1. In the PS Database column, select the PeopleSoft environment in which you want to specify an operator ID and password for the user.

   This automatically activates the text box in the corresponding PS Oprid column.

2. Enter a PS Operator ID in the PS Oprid column.

   This ID is case-sensitive, must correspond to the PeopleSoft Operator ID for the Stat Repository, and must be no more than 30 characters in length.

3. Click the corresponding **Enter Password** button in the PS Password column.

   Stat displays the Change Password dialog box.

4. In the Change Password dialog box, enter the password in the **Password** and **Confirm Password** fields.

   This password is case-sensitive, must correspond to your PeopleSoft Operator ID's password for the given database, and must be no more than 32 characters in length.

5. (Optional) Select **CLI Open** for any designated staging database.

   Selecting this option configures Stat to log automatically into the database and open projects that users staged. Users can then verify the staging of objects and manually push the project to the target database.

   NOTE: If a PeopleSoft configuration file exists for a PeopleSoft environment, you can configure Stat to import it whenever it executes CLI functionality in that environment. This automatically updates the user's %PS_HOME% variable used during CLI functions. For more information, see PeopleSoft Environment Connection Maintenance on page 80.

6. (Optional) Select **CLI Auto-Migration** for any environment designated in a migration path as the target environment for a migration.

   If the target environment is a distribution environment, select the check box for each environment that qualifies for auto-migration within the distribution environment list.

7. If you selected either **CLI Open** or **CLI Auto-Migration**, specify the directory location of the user's PS Tools executable in the **PS Tools Directory** field.

   This information must be specified if the user plans to use CLI functionality in any PeopleSoft environment. You can specify a directory location in one of three ways, either manually or by clicking the folder icon and selecting the location in the Browse for Folder dialog box:

   - If the executable is in the same location as when PeopleSoft was first installed, keep the default value, "PS_HOME\bin\client\winx86," where PS_HOME is the user's PS_HOME variable as defined in the PeopleSoft configuration

- If the executable has been moved to a different location within the %PS_HOME% directory, specify the new subdirectory, for example, “PS_HOME\setup”
- If the executable has been moved to a location outside the %PS_HOME% directory, specify the entire location including the drive, for example, “G:\software\psft\ps815.”

8 After specifying the PS Tools directory location, you can make sure that you have entered all the information correctly for a particular environment by selecting that environment and then clicking **Test Connection**.

Stat attempts to connect to that environment, first by going to the PS Tools directory you specified and launching PeopleSoft, and then by logging on to the selected environment using the oprid and password you defined for the user and additional parameters defined in the PeopleSoft Environment Connection Maintenance table. If Stat is unable to connect, it displays a PeopleSoft generated error message, for example, “Unsuccessful CLI connection to PS Database.”

NOTE: Users can specify the PS Tools directories themselves in the PeopleSoft Options window. For more information, see the *Stat User Guide*, Chapter 11, “Change Management for PeopleSoft.”

9 Save your changes by clicking either **Apply** or **OK**.

User File Directories Tab

The User File Directories tab displays a list of the active file types defined in Stat for PeopleSoft, Oracle Applications, and generic application environments. From here you can define the selected user’s working file directory for each file type as well as the user’s default working directory. Defining a working directory for a file type is optional. If a file type working directory is not defined, Stat places copies of the migrated file objects in the user’s default working directory.

NOTE: For Oracle Applications proprietary file object types, you must define working file directories in the File Type User Directories tab of the File Locations window. After they have been defined there, you can modify their assigned user directories in the Other User Information window. For more information, see File Type User Directories on page 97.

NOTE: Users can define their own working directories in the Stat User Options window. For more information, see the “Object Management” sections in the change management chapters of the *Stat User Guide*.

To set up a user's default working directory:

1 In the **Module** field, select the change management module you are using.

2 In the **Default Working File Server** field, select the server for the default working directory.

3 In the **Default Working File Path** field, enter the path of the default working file location starting after the file server’s root or home path.

4 Click **Apply** or **OK**.

NOTE: You can also define a user’s default working directory in the User Default Directories Maintenance table. For more information, see Object Type Maintenance on page 60.

To set up a file type working directory:

1 In the File Type column, select the file type that the user wants to have a working directory for.

This automatically activates the text box in the corresponding Working File Server column.

2 In the Working File Server column, select the server that the working directory is on.

3 In the Working File Path column, enter the path of the working file location starting after the file server’s root or home path.

NOTE: Make sure you use the proper syntax when specifying working directories. For more information, see File Path Syntax on page 73.

4 Click either **Apply** or **OK**.

Queue Assignment Tab

In the Queue Assignment tab, you can add and remove the selected user from work queues. Queues are specific groups of Stat users with similar skill sets or responsibilities and are defined by system administrators. For more information, see Queue Maintenance on page 152.

NOTE: You can add and remove users to queues in the Queue Maintenance table as well as in the User Access Information window. For more information, see Editing Queue Membership on page 152.

Queues are service-domain specific. For this reason, the unassigned list of queues is organized by service domain. Only the service domains the user has access to are listed (for more information, see Service Domain Access Tab on page 36). Double-click a service domain to open the list of associated queues the user is currently not assigned to.

To assign a user to a queue:

1. In the unassigned list, double-click each service domain that the queues you want to assign to the user are associated with.

   TIP: Use the Expand All and Collapse All buttons to open and close the unassigned tree list view.

2. Select each queue that you want to assign the user to or select the parent service domain to grant the user access to multiple queues at once.
3. Click the right-pointing arrow button.
4. To remove the user from a queue, select the queue you want to remove the user from in the list of currently assigned queues and click the left-pointing arrow button.

   NOTE: If the user is the owner of the queue, that user cannot be removed.

5. Save your changes by clicking either **Apply** or **OK**.

Application Access Tab

The Application Access tab is where you can restrict a user's access to only specified applications while working within certain service domains. For example, if a user only has access to the Benefits application while in the HR service domain, then that user can only open CSRs that display the value **Benefits** in their **Application** field. In addition, when the user creates a new CSR, **Benefits** will be the only option in the **Application** field of the CSR window. Leaving this tab blank for a service domain gives the user access to every application in that service domain.

Application access also filters the list of users that belong to a queue. When a queue is added to or modified on a CSR, the list of developers is filtered based on the combined queue membership and application access settings. Only members of the queue who have access to the application are displayed. For more information, see Editing Queue Membership on page 152.

Applications are service-domain specific. For this reason, the unassigned access list is organized by service domain, with only the service domains the user has access to included (for more information, see Service Domain Access Tab on page 36). Double-click a service domain to open the list of associated applications the user currently does not have access to.

To set up application access:

1. In the unassigned list, double-click each service domain to open the list of the associated applications the user currently does not have access to.

   TIP: Use the Expand All and Collapse All buttons to open and close the unassigned tree list view.

2. Select each application that you want the user to access or select the parent service domain to grant the user access to multiple applications at once.
3. Click the right-pointing arrow button.

4 To remove access to an application, select the application in the assigned list and click the left-pointing arrow button.

5 Save your changes by clicking either **Apply** or **OK**.

Object Type Access Tab

The Object Type Access tab is where you can restrict a user's access to only specified object types while operating within a certain change management module and service domain.

The tree view of the unassigned list is organized by each service domain that the user has access to (for more information, see Service Domain Access Tab on page 36), then by each change management module (PeopleSoft, Oracle Applications, and Generic Applications). Each module contains each associated class of objects, while each object class in turn includes each associated object type. This means you can grant users access to all the object types within a service domain at once, or you can restrict access to only individual object types.

To set up object type access:

1 In the unassigned list, double-click each service domain to open the list of change management modules.

Modules include **PeopleSoft**, **Oracle Applications**, and **Generic Applications**.

TIP: Use the Expand All and Collapse All buttons to open and close the unassigned tree list view.

2 Double-click a module to open the list of associated object classes.

3 Double-click an object class to open the list of associated object types.

4 Select each object type you want to grant the user access to, or select the parent object class, module, or service domain to grant the user access to multiple object types at once.

5 Click the right-pointing arrow button.

6 To remove access to an object type, select the object type in the assigned list and click the left-pointing arrow button.

7 Save your changes by clicking either **Apply** or **OK**.

Environment Access Tab

The Environment Access tab is where you can restrict a user's ability to migrate objects to only specified environments while operating within a certain change management module and service domain. This also restricts a user's ability to approve migrations only to environments they have access to. For example, if a user only has access to the Development environment while in the HR service domain, then that user can migrate archive sets only to that environment and can only approve migrations to that environment.

Environment Access also restricts users from viewing and editing PeopleSoft Options.

The tree view of the unassigned list is organized by each service domain the user has access to and which is associated with active environments (for more information, see Service Domain Access Tab on page 36). Each service domain opens a list of one or more change management modules (PeopleSoft, Oracle Applications, and Generic Applications), and each module it turn opens a list of associated active environments.

CAUTION: When modifying a user's service domain and environment access, be aware that this may affect migrations and patch applications to environments that require the user's approval. If a user's approval is required for a migration or patch application to an environment that they no longer have access to (which can be restricted either at the service domain or the environment level), the migration or patch application to that environment cannot be approved.

To set up environment access:

1 In the unassigned list, double-click each service domain to open the list of change management modules.

Modules include PeopleSoft, Oracle Applications, and Generic Applications. Environments are associated with modules through service-domain specific migration paths, which means certain service domains may be associated with one module but not another.

> **TIP:** Use the Expand All and Collapse All buttons to open and close the unassigned tree list view.

2 Double-click a module to open the list of associated environments.

3 Select each environment you want to grant the user access to, or select the parent module or service domain to grant the user access to multiple environments at once.

4 Click the right-pointing arrow button.

5 To remove access to an environment, select the object type in the assigned list and click the left-pointing arrow button.

> **TIP:** Remember that when you specify one environment, you are configuring Stat to deny the user access to all the other environments in the service domain, unless you explicitly grant the user access to them as well.

6 Save your changes by clicking either **Apply** or **OK**.

Pre/Post Migration User Parameters Tab

Define public user-based parameters that can be included in the definition of post migration command steps. See the *Stat User Guide*, *Appendix C: User-Specific Parameters*.

Synchronizing User Access Information

After defining the access settings of one user, you can use that user as the source for synchronizing the access settings of multiple users. This way, if several users share many of the same access settings, you can update their settings simultaneously rather than one at a time.

To synchronize user access information:

1 In the User Maintenance window, select the user whose access settings you want to use as the source for synchronizing the settings of other users. Then click **Sync**.

This opens the Synchronize User Access Information window, which displays all the currently defined users in Stat as well as fields corresponding to each access tab in the User Access Information window (except the PS Options and User File Directories tabs, which contain user-specific information).

2 While holding down the <Shift> or <Ctrl> key, select each user you want to synchronize with the user you selected in step 1.

3 In each access field, select one of the following three options:

- **Copy/Replace**: Replace the users' access settings with the settings of the sync user
- **Copy/Add:** Add the sync user's access settings to the users' existing settings. This way, whenever a new application, queue, object type, etc. is added, you can update the access settings of the sync user and then use this option to update multiple users at once.
- **No Action:** Do not modify the selected users' access settings

4 Click **Sync**.

User Password Security Settings

In the Other Options tab of the System table, you can define password parameters for all Stat users.

For more information, see System Maintenance on page 47. To open the System table, select **Maintenance | General | System Table**. Then select the Other Options tab.

Values	Description
Password Lifetime (Required Value)	The number of days that a user's password is valid before they are required to change it. This setting has no effect if the **Password Expire** field is not checked. Valid values are 0 to 999. **NOTE:** If you set the **Password Lifetime** value to 0, then the existing password is valid for 24 hours from the time you click **OK** or **Apply**.
Pswd Hist. Lifetime (Required Value)	The number of days Stat retains users' password history. This value is used with the Limit Lifetime setting to prevent users from re-using the same password within the number of days indicated in this field. A setting of 0 means that no history is maintained. This setting has no effect if the **Limit Lifetime** field is not checked.
Minimum Length	The minimum number of characters required in a user account password
Max Failed Login	The maximum number of failed login attempts before the user account is locked out of Stat
Expire	Indicates whether users' passwords expire after the number of days defined in the **Password Lifetime** field. If selected, users are prompted to change their passwords at login once they have expired. If blank, passwords never expire.
Limit Lifetime	Indicates whether users can use the same password indefinitely
Set Mandatory Characters	Enables the mandatory character fields for passwords. If this check box is selected, the settings for **Upper Number**, **Lower**, and **Spec. Char.** fields are active.
Upper	Indicates if users must have at least one upper-case character in their password. This setting has no effect if **Stat Mandatory Characters** is not selected.
Lower	Indicates if users are required to have at least one lower-case character in their password. This setting has no effect if **Stat Mandatory Characters** is not selected.
Number	Indicates if users must have at least one number in their password. This setting has no effect if **Stat Mandatory Characters** is deselected.
Spec. Char.	Determines if users must have at least one special character in their password. This setting has no effect if **Stat Mandatory Characters** is deselected. Special characters include the following: } | { ' _ ^ }] \[@ ? > = < ; : / . - , + *) (' & % $ # ! "

LDAP Connection Maintenance

For customer sites that maintain LDAP user directories, Stat supports authenticating login credentials based on a user's LDAP password rather than the default password defined directly in Stat. This allows sites that maintain a large number of user accounts to avoid maintaining an additional set of Stat-specific passwords. LDAP-enabled users can login to both the Stat Windows Client and the Stat Web Client and have their accounts authenticated with their LDAP passwords.

You configure LDAP connections in Stat by specifying the LDAP server parameters, including location and port numbers. You can configure an LDAP connection to use the User DN or SAM-Account-Name attribute.

- User DN - Specify the base DN path used to search for user account directories. After specifying the base DN, you then specify a template DN which will be used to pre-populate the DN for individual users in the User Maintenance table. You can also use the Test Connect DN to test the connection between Stat and the LDAP server.
- SAM-Account-Name attribute - Specify the LDAP Domain. You can enter a specific user in Test Connect DN to test the connection or you can leave the Test Connect DN blank, in which case the currently logged-in User Id will be used to test the connection.

After configuring LDAP connections in Stat and assigning them to users, you “turn on” LDAP by selecting the **Enable LDAP** option in the System Maintenance table, Other Options tab, as described in the section Other Options Tab on page 49.

Stat supports encrypting communication between Stat and the LDAP server by enabling SSL.

LDAP connection security is controlled by the following user class rights:

- LDAP Connection - Add
- LDAP Connection - Edit

The LDAP Connection Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Security Settings | LDAP Connect**.

Defining LDAP Connections

To define an LDAP connection (using User DN):

1. Click **New** to create a new LDAP connection.
2. In the **LDAP Cd** field, enter a code that uniquely identifies the LDAP connection.
3. In the **Description** field, enter a short description of the LDAP connection.
4. In the **Host** field, enter the network name that identifies the host machine on which the LDAP server is installed.
5. In the **Ports** field, enter the port number of the LDAP server.

   The port number is typically 389.
6. In the **Base DN** field, enter the DN path used to search for users.

   Although the format for the base DN may vary depending on your LDAP implementation, a typical base DN is derived from the name of your company and its DNS domain, for example, “DC=Quest,DC=com.”

   After specifying the base DN, you can specify a template DN that will be used as the default value for individual user DN values in the User Maintenance table. However, before you do that, you have the option of entering a valid user DN and password to test the connection between Stat and the LDAP server.
7. (Optional) If you want to test the connection between Stat and the LDAP server, do the following:
   a. In the **Test Connect DN** field, enter the DN of a valid LDAP account.

      For test purposes, this can be the DN of any LDAP account that you know is valid. The DN format may vary, but a typical user DN consists of the user name and organizational unit, for example: “CN=John_Smith,OU=Employees”
   b. Select **Append Base DN** to append the base DN with the test connect DN.

      This allows Stat to read the full LDAP address of the test account, for example: “CN=John_Smith,OU=Employees,DC=Quest,DC=com.”
   c. Click **Test Connect**.

      Stat prompts you to enter the LDAP password of the user account.

d Enter the password and click **OK**.

Stat attempts to connect to the test connect DN on the LDAP server and displays a message that tells you if it was able to connect successfully or not.

8 Do the following to specify a default user DN for individual user accounts in the User Maintenance table:

a In the **Template DN** field, specify the default user DN value.

Stat allows you to use variables for **First Name** and **Last Name** fields so that the default value is dynamically applied to each user account, for example: "CN=%first_name%_%last_name%,OU=Employees"

NOTE: You do not need to specify a password. The Password field is for test connections purposes only.

b Select **Append Base DN** to append the base DN with the template DN.

To define an LDAP connection (using the SAM-Account-Name attribute):

1 Click **New** to create a new LDAP connection.

2 In the **LDAP Cd** field, enter a code that uniquely identifies the LDAP connection.

3 In the **Description** field, enter a short description of the LDAP connection.

4 In the **Host** field, enter the network name that identifies the host machine on which the LDAP server is installed.

5 In the **Ports** field, enter the port number of the LDAP server. The port number is typically 389.

6 In the **LDAP Domain** field, enter the domain name for the connection.

To enable SSL:

1 If your site is equipped to use SSL and you want to use it to encrypt communication between Stat and the LDAP server, select **SSL**. Then specify the location of the SSL keystore for the Stat Windows Client or the Stat Web Client:

- For the Stat Windows Client, enter the location of the SSL keystore in the **Keystore Location** field.
- For the Stat Web Client, enter the location of the SSL keystore In the **Agent Keystore** field.

As an alternative, you can rely on your $JAVA_HOME/jre/lib/security/jssecacerts keystore to provide the certificate for your LDAP server. In this case, you can leave the **Keystore Location** field blank provided that jssecacerts exists in the Windows client jre/lib/security directory and that jssecacerts contains the LDAP certificate. For the Stat Central Agent, you can leave the **Agent Keystore** field blank provided that jssecacerts exists in the Central Agent's jre/lib/security directory and that jssecacerts contains the LDAP certificate.

Note that if both your Stat Central Agent and your LDAP server are running in secure mode, you have to rely on $JAVA_HOME/jre/lib/security/jssecacerts to contain both the LDAP certificate and the Stat Central certificate. This is true for the Windows Client JAVA_HOME and for Stat Central Agent's JAVA_HOME. In this case, both **Keystore Location** and **Agent Keystore** fields should be left blank.

2 Click **OK** or **Apply** to save your work.

After defining an LDAP connection, you can assign it to users. You can also copy LDAP connections and use the copy as the basis for a new LDAP connection. To copy an LDAP connection, select it and click **Copy**.

Assigning LDAP Connections to Users

To assign a LDAP connection to users:

1 Select the LDAP connection you want to assign to users and click **Assign Users**.

The Assign Users window displays all the active users in Stat. You can filter the list to show users currently assigned to particular LDAP connections as well as users that are not currently assigned to a connection.

2 Select the user(s) you want to assign to the connection.

3 Click **Update User DN**.

This updates the user's DN by appending the selected LDAP domain's Base DN to the Template DN. For connections using the SAM-Account-Name attribute, User DN is left blank and the Stat User ID is passed in for samAccountName when the user attempts to log in to Stat. You may also overwrite the Stat User ID by entering a samAccountName value in the User DN field.

4 Click **OK** or **Apply** to save your changes.

Connection Manager

The maximum number of active users (meaning users who can connect to Stat as specified in the User Maintenance table) equals the number of licensed seats. Once the number of active users equals the number stipulated in the license agreement, new user connections are denied.

The Connection Manager window displays a list of all the users currently connected to Stat as well as a record of denied and terminated connections. From this window you can manually disconnect users from the Stat Repository, thereby opening seats and allowing other users to connect.

Connection Manager security is controlled by the user class right, Database Connections - Manage.

To open the Connection Manager window, select **Maintenance | Security Settings | Connections**.

The Current Tab

This tab displays the list of users currently connected to Stat. The number of licensed seats and the number in use are displayed at the bottom of the list. Once the number of licensed seats is met, Stat denies any more connection requests.

NOTE: A Connection Manager window appears on users' workstations whenever their connection to the Stat database is severed, either by a system administrator through the Current tab or due to a network problem.

The Current tab contains the following fields (columns):

Flag

When a connection has been terminated, this column is marked with a red X. Terminating a connection forces the connected user to disconnect. When this happens, a notification appears on the disconnected user's screen.

ID

The unique identifier assigned by the System

User

The name of the user connected to Stat

Connect Dt/Tm

Date and time the user connected to Stat

Last Update Dt/Tm

Approximately every 60 seconds, Stat updates this table to indicate that it still has an active connection. This column indicates the last time this update took place.

Refresh

Click this button to refresh the window

Print

Click this button to print the window contents

Export

Click this button to export the window contents

Disconnect

To disconnect a user, select the user and click this button

Auto-refresh

If selected, Stat automatically refreshes the list at specific time intervals

The History Tab

This tab displays a record of connection denials and terminations.

The History tab contains the following fields (columns):

Date

The date of the termination or denial event

Event

The type of disconnection. There are two events: “Terminated” which means that the disconnection was manually triggered and “No Licenses” which means that the System denied connection to the user(s) because the number of licensed seats has been met.

User

The name of the user for whom the connection was denied or terminated

Caused By

The name of the person who caused the event. In the instance of a No Licenses event, it defaults to “Account, System.”

4

General Maintenance Tables

- System Maintenance
- Service Domain Maintenance
- Department Maintenance
- Issue Tracking Maintenance
- Country Maintenance
- Customer Maintenance
- Object Type Maintenance
- PeopleSoft Environment Connection Maintenance
- Pre/Post Migration Steps Parameters
- Oracle Applications Configuration
- Oracle Applications Connection Maintenance
- Generic Application Connection Maintenance
- Schema Object Parameters Maintenance
- Data Object Maintenance
- PeopleSoft Search Configurations
- Stat Report Definition Maintenance
- Version Control Management Connection Maintenance

System Maintenance

The System Maintenance table defines global operating parameters for your copy of Stat. System Maintenance table security is controlled by the user class right, System Table - Edit. There is no add right.

To open the System Maintenance window, select **Maintenance | General | System Maintenance**.

General Tab

The General tab of the System Maintenance window displays addresses and contact information.

When specifying your company's address, select the country where your company resides in the **Country** field. Depending on the country you select, the labels of certain fields may change in keeping with the address conventions of that country. Stat comes installed with predefined country labels for USA, Canada, Australia, and the United Kingdom. You can define additional countries in the country maintenance table, as described in the section, Country Maintenance on page 57.

The following table describes the value types in the General tab (USA default):

Value	Description
Name (Required Value)	The name of the organization this copy of Stat is licensed to
Country (Required Value)	The country of the address
Unit	A definition of the business unit that Stat is licensed to
Address1 (Required Value)	The street address
Address2	The name of the building, if applicable
Address3	The route number, if applicable
Address4	The post office box number, if applicable
City (Required Value)	The city of the address
State (Required Value)	The state of the address
Zip (Required Value)	The zip code of the address
Phone (Required Value)	A primary telephone number for the organization

License Tab

The License tab displays license information about your currently installed versions of Stat.

The following table describes the information displayed in the License tab:

Value	Description
License Key	The Quest-provided Stat license key number that is unique to your organization. This field is strictly alpha-numeric and is case-sensitive. **NOTE:** This field is critical to Stat system function. Entering an invalid license code may render your system inoperative. Never change this code unless you have purchased a new/additional license or you are advised to do so by Stat Support Staff. If a Stat license is not entered, or if the license is expired or invalid, then only the SYSTEM user or users with Technical-class licensed user with the “System Table - Edit” right can log in to the Stat Windows Client, in which case the System Maintenance table will be the only accessible window. **NOTE:** The Stat Web Client does not have ability to validate the license. As a result, all active users will be able to log in to the Web Client regardless of Stat license validity.

Value	Description
Site Message	The Quest-provided registration key used to verify that the license key you entered is valid. After entering the registration key, click **Verify**. If the key value is verified, further license information is displayed in the Properties field and you can continue using Stat. If the key value is not verified, you will receive an error message and cannot continue until you provide a verified key value.
Properties	Includes the following: • **License Type** - The type of license. Options include Commercial (permanent), Trial (temporary) and Term (a temporary enhancement of licensing rights for commercial users). • **Technical Licenses** - The number of licensed technical users. Technical users have complete access to Stat as defined by their user class rights. • **Functional Licenses** - The number of licensed functional users. Functional users have limited access to Stat and are not allowed to perform object management tasks. • **Oracle Apps** - Indicates whether the license includes access to the change management module for Oracle Applications • **PeopleSoft** - Indicates whether the license includes access to the change management module for PeopleSoft **NOTE:** Access to the change management module for generic applications is included in all Stat licenses.

Users Tab

The Users tab lists all the users that have been defined in Stat along with their currently assigned license status.

Your Stat license determines the number of active technical and functional users that can operate in Stat at any one time. The total number of active licensed users is displayed at the bottom of the tab. Inactive users are not counted against the total number of licensed users.

Technical users have access to all Stat functionality and are only limited by their assigned user class rights.

Functional users are limited and do not have access to the following areas in Stat:

- Maintenance
- Migration Management (except Migration Approvals)
- Object Management
- User Options | PeopleSoft Options
- User Options | Pre/Post Migration user parameters
- The Object Management window

Both types of users have full access to the Stat Web Client.

Other Options Tab

The Other Options tab defines CSR operating parameters and user password settings.

The following table describes all the value types in the Other Options tab, except for the User Password Options section which is described in the section, Defining Stat Users on page 32.

Value	Description
Last Job Number (Required Value)	This is the last Stat Central Agent Job number used by Stat. At setup, you may set this value to any number which defines the next Job number. For example, a setting of 0 causes the first Job number to be 1. **NOTE:** Never set this number backward once Jobs have been entered. An initial setting of 0 is recommended.
Last Rule Number (Required Value)	This is the last business or personal rule number used by Stat. At setup, you may set this value to any number which defines the next Rule number. For example, a setting of 0 will cause the first Rule number to be 1. **NOTE:** Never set this number backward once Rules have been entered. An initial setting of 0 is recommended.
Last Cust. Number (Required Value)	This is the last Customer number used by Stat. At setup, you may set this value to any number which defines the next Customer number. For example, a setting of 0 causes the first Customer number to be 1. **NOTE:** Never set this number backward once Customers have been entered. You will not be able to add new customers. An initial setting of 0 is recommended.
Last PSobj Number (Key Value)	Stat uses a unique numbering system to identify PeopleSoft proprietary objects. When a reference to a new PeopleSoft proprietary object is added in Stat, Stat generates an ID number and displays it in this field. For example, a setting of 0 causes the first PeopleSoft proprietary object ID to be 1. **NOTE:** Never set this number backward once objects have been entered since this will overwrite CSR object history. An initial setting of 0 is recommended.
Last Migr. Number (Required Value)	Stat uses a unique numbering system to identify each migration. When a new migration completes successfully, Stat generates an ID number and displays it in this field. **NOTE:** Never set this number backward once migrations have taken place. An initial setting of 0 is recommended.
Last Object Type (Key Value)	A unique number assigned by Stat to identify the object type. Due to its sensitive nature, the **Last Object Type** field does not appear in the System Maintenance window. However, the values assigned by Stat are contained behind-the-scenes in the table itself. To edit an object type value, you must edit the table using an environment management tool, which is not recommended.
Last Workfl. number (Required Value)	Stat uses a numbering system to identify each workflow defined in the system. **NOTE:** Never set this number backward once workflows have been defined. An initial setting of 0 is recommended.
Min List Refresh (Required Value)	Determines the minimum allowed automatic refresh rate, in minutes, for users' Support Consoles
Max List Refresh (Required Value)	Determines the maximum allowed automatic refresh rate, in minutes, for users' Support Consoles

Value	Description
Default Country (Required Value)	The default country of new customers that are defined in Stat. The list of available countries is determined in the Country Maintenance table.
Enable LDAP	If selected, users are permitted to login into Stat using their LDAP login credentials.

Parameters Tab

The Parameters tab defines miscellaneous configuration settings in Stat, such as the maximum file size of CSR attachments, the minimum number of characters in user IDs, the sort and filter settings on maintenance tables, the option to archive 3rd party objects, and the timeout period for Web Service connections. For Oracle Applications, you can define the patch backout default value, the timeout multiplier factor for Oracle Agents, and the communication protocol.

The miscellaneous settings you can configure in the Parameters tab include:

Parameter	Description
Archive 3rd party objects	If you are integrating Stat with a 3rd party version control management (VCM) tool, you can specify whether you want the objects selected from the VCM repository archived in Stat or just a pointer to those objects. Selecting the option **No** means that Stat only archives the pointer to an object, not the object itself.
CSR date range lower/upper limit	The lower and upper limit of the date range available on CSRs. These values are expressed in a DDMMMYYYY format. The default lower range is 01 January 2016 and the default upper range is 01 January 2025.
CSR default owner rule	Defines the rule on which CSR default owner is calculated by Stat. This is used when creating a new CSR, changing a CSR Queue, or performing a CSR Workflow status transfer. Use the following values: 1 for Current owner, 2 for logged-in user, 3 for Queue owner, and 4 for CSR creator.
Disable Patch Backout Default Value (Ora Apps Only)	When scheduling a patch application request, this option determines whether or not Stat executes a patch impact analysis, which means the patch cannot be backed out later. Because applying patches can take time, this option is available for users who do not want to commit the system resources necessary to enable the backout option for a particular patch. Enter “Yes” if you want the **Disable Patch Backout** option selected by default, or “No” if you want the option de-selected by default.
Mass Migration order by Archive Set	When set to **Yes**, Stat migrates objects in the order that the user specifies in each archive set followed by object type order. When set to **No**, all objects are migrated together in the order of object type.
Max file size for CSR attachment	The default 50MB size of CSR attachments is the recommended maximum. Attachments larger than 50MB can adversely affect performance. For more information on CSR attachments, see the *Stat User Guide*, Chapter 3, “Change/Service Requests.”

Parameter	Description
Maximum number of characters in user id	The default number of characters that must be used in a Stat user ID is a minimum of 2. Enter the value you want to change the minimum number of characters
Number of days on Migration Console	The number of days information regarding an object migration is displayed in the Migration Console. The information itself is retained in the database, and earlier migrations can be displayed by setting this number higher.
OA Agent Wait Multiplier (Ora Apps Only)	For objects that are particularly large, the Stat Central Agent may time out while waiting for an Oracle Agent to finish archiving and migrating the objects. The default time is 30 seconds. However, you can increase or decrease this time by specifying a multiplier. To increase the time, enter a factor greater than 1. The value 2, for example, doubles the time amount to 60 seconds. To decrease the time, use decimals. The value .5, for example, decreases the time by half, or 15 seconds.
OA Migration Default Edition	Sets the default value for Edition in Migration Wizard. Run, Patch, or Both. Defaults to Run.
Prompt to save filter/sort order if it is changed	You can configure Stat to save automatically any changes users make to the sort order or filter settings on a particular maintenance table. The default value for both parameters is **No**, meaning Stat saves changes automatically and not display the message prompt. However, if you want Stat to display a message prompt that gives users the option of not saving any changes to the sort or filter settings, enter the value **Yes** for either parameter.
Protocol for REST HTTPS	Defines secure protocol for REST calls. Used when Stat Windows Client connects to the Central Agent. Use the following values: 0 for auto, 2 for TLS 1.1, 4 for TLS 1.0, and 5 for TLS1.2. Defaults to Zero.
Report maximum number of records allowed	Limits the maximum number of records for a generated report. When the generated report reaches the limit, a warning message displays. The default value is 30,000. **NOTE:** Running extremely large reports may adversely affect the Central Agent.
Require users to enter override comments	Selecting the option **Yes** means that whenever a user overrides the approval requirements for a CSR status transfer, object migration, or patch application, they are prompted to document the reason they are overriding the requirement.
REST calls timeout in seconds	Defaults to 60 seconds. Amount of time that client REST calls wait for the server to process the call.
Restricted CSR attachment file extensions	If there are certain types of files you do not want users opening directly from the Attachments tab (such as executables and .bat files), list the extensions here.
Retention days for MERC_WAKE table	Number of days to save data once it is marked as inactive. This affects the display on the Tools | Stat Central Agent Status window and Stat Oracle Agent Windows.

Parameter	Description
Stop migration on error	If selected, the Stat Central Agent stops migrating objects once an error is encountered. With proper security rights, users can override this option when setting up a migration.
Timeout period for idle Web Service Connections	Stat supports timing out idle Web Service connections. The default value is 3000 seconds. Increase or decrease the default setting by entering the number of seconds.
Use IP address when looking up SCA	Selecting the option **No** means the addressHost name is used to resolve Stat Central Agent's IP address (preferred). Selecting the option **Yes** means the IP address is used to find the Stat Central Agent. Sites with Natted firewalls should always start with the Host name.
The number of rows which will be fetched in a single DB call from PeopleTool tables	This parameter is useful if you are using the Browse Object feature from the Web Client to fetch PeopleSoft propriety objects. This parameter will decide the number of object's whose information will be fetched in one DB trip from the chosen PeopleSoft environment. The higher the number, the lesser the amount of time it will take to fetch values against the options chosen in the Browse Objects popup. However, the higher the number, the higher will be the amount of memory consumed by the Stat Central Agent. The default number will be 10,000.
Maximum amount of concurrent PS migrations than can happen (SCA restart needed)	This is the number of simultaneous PS migrations that SCA can do. This number is only relevant for PS proprietary object's migrations. If this number is equal to five and five migrations are already happening concurrently, then the rest of the migrations will be added in an internal queue in SCA. When the one of older migration finishes, then only a new migration will be picked up from this queue. By default, this number is 10.
Expiry in minutes for the link which is generated to reset user's password	When you use the forgot password feature from the web client, the password reset validity is set using this parameter. By default, it is set to 30 minutes.

DB Scripts Tab

The DB Scripts tab displays in read-only format a history of all the installation and upgrade scripts that have been run against the Stat database. This information can be exported as a plain text or Excel file which can then be sent to Quest Support for troubleshooting purposes.

For each script, the tab shows the version of Stat it was run for, the time it was run, and the user that ran the script and the name of the machine it was run on.

CSR History Tab

The CSR History tab displays a list of all the CSR and object management activities that are tracked in Stat's change history records. By default, all activities are tracked, but because this amount of information can grow to an unmanageable size, Stat gives system administrators the ability to select the types of information they want included in the change history records.

CSR activity is tracked by recording changes to the detail fields of the CSR window. Object management activity is tracked when an object is added, locked, unlocked, reassigned, or removed.

To stop recording the change history of any particular CSR activity or object management activity, deselect its corresponding value in the CSR History tab and select **Apply**.

NOTE: For the changes specified in the CSR History tab to take effect in other currently open Stat Client sessions, each user has to re-cache codes or restart the clients. For Stat Web Clients, each user has to login again to apply the changes.

Approvals Tab

Options in this tab include:

Parameter	Description
Delay Workflow Approvals	If selected, delays the notification of status transfer approval requests in a workflow until all other transfer rules have been marked complete.

Service Domain Maintenance

The Service Domain table defines all the service domains in the Stat Repository. When first installed, there are no service domains in Stat. You must log into Stat initially with the “System” user ID. Then you can open the maintenance table and define your service domains.

Service domain security is controlled by the following user class rights:

- Service Domains - Add
- Service Domains - Edit

The Service Domain table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Service Domains**.

Value	Description
Active	If selected, indicates that the service domain is currently active
SD Cd (Key Value)	A unique 1-3 character code which identifies the service domain. Codes can be alpha and/or numeric. This code prefaces all CSR numbers for the domain. For example: PR-1001 where PR is the SD Cd.
Description (Required Value)	A brief textual description of the service domain
Unit (Required Value)	A definition of the business unit that uses this service domain
Address Line 1 (Required Value)	The first line of the address
Address Line 2	The second line of the address
Address Line 3	The third line of the address
City (Required Value)	The city of the address
State (Required Value)	The state of the address
Zip (Required Value)	The zip or postal code of the address

Value	Description
Country	The country of the address
Telephone (Required Value)	A primary telephone number for the business unit
Last CSR # (Required Value)	The last CSR number used by Stat for this service domain. When creating a service domain, you may set this value to any number that will define the next CSR number. For example, a setting of 999 will cause the first CSR number to be 1000. The maximum allowed CSR ID is 2147483647. **NOTE:** Never set this number backward once CSRs have been entered for the service domain. Serious data integrity problems may result.
CSR PS Tab	Determines if the PeopleSoft tab is displayed on the CSR window
CSR Oracle Tab	Determines if the Oracle Applications tab is displayed on the CSR window
CSR Generic Tab	Determines if a generic application tab is displayed on the CSR window
Generic Application Label	The label of the generic application tab displayed on the CSR window, for example, “Siebel”
PS Locking	Specifies whether or not physical locking is used for PeopleSoft proprietary objects
CSR Task Tab	Determines if the Task/Time tab is displayed on the CSR window
CSR Issue Tab	Determines if the Issues tab is displayed on the CSR window
Daily Time Entry	Determines if the Daily Time Entry feature appears in the Task window for this service domain
Use Appl Env	Determines if the **Application Environment** field is displayed on the CSR window
Use Cust Prio	Determines if the **Cust Prio** field is activated on the CSR window
Chk Cust Open	Determines if Stat checks for other open CSRs in the service domain when a customer is selected on the CSR. If set to 'on', Stat will notify the user if the customer has other open CSRs in the service domain.
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user who last updated this record

Each service domain must be configured to process outbound email via SMTP. After defining a service domain, click **Email Settings**. This opens the Electronic Mail Interface Setup window where you configure the Stat Central Agent to manage outbound and inbound email for the selected service domain. For more information, see Configuring the Stat Central Agent for Email on page 174.

Department Maintenance

The Department table defines all the departments in the Stat Repository. Departments can represent either divisions within your business enterprise, such as Accounting, or outside organizations, such as client companies.

Departments are primarily used for reporting purposes. However, before you can define individual customers, you must define the companies (departments) they work for or represent.

Department security is controlled by the following user class rights:

- Departments - Add
- Departments - Edit

The Department table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Departments**.

If you want to add or update information in the Department Maintenance table, click **Search** and use the Search PeopleSoft Country/Department Engine to retrieve department information from PeopleSoft environments. You can also add countries defined in PeopleSoft to the Country Maintenance table. For more information, see the section, Updating PeopleSoft Country and Department Definitions on page 58.

Value	Description
Active	If selected, indicates that department is currently active
Dept Cd (Key Value)	A 1-10 character code which uniquely identifies the department
Description	A brief description of the department
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Issue Tracking Maintenance

The Issue Tracking table defines the two custom label fields on the Issue tabs of the CSR window and Project window. From this table you also define issue statuses.

Issue tracking security is controlled by the following user class rights:

- Issue Labels - Add
- Issue Labels - Edit

The Issue Tracking table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Issue Tracking**.

Custom Label Fields

Stat provides two fields that you can customize to display and capture specific types of information. These fields can be used to capture either free-form text or a set of predefined values.

To define a custom field:

1. In the **Custom1 Label** field or **Custom2 Label** field, type the name of the label as you want it to appear in the Issue tab and the Edit Issue window.
2. In the **Field Type** field, select either **Free Form** or **Pre-Defined,** depending on the type of values that you want the field to capture.
3. If you select **Pre-Defined**, the next step is to define the values that can be displayed in this field. To define a value, do the following:
    a. Click **New**.
    b. In the **Custom Type** field, select the Custom Field for which you want to define a value.
    c. In the **Value** field, enter the value name.
    d. Click **OK**.

e Repeat these steps for each value you want the field to display.

Issue Statuses

Like CSR statuses, issue statuses are either open type or closed type. Issue statuses represent the states in an issue's life cycle.

To define an issue status:

1 In the Issue Tracking Maintenance window, click **Status**. Stat opens the Issue Tracking Status window.

2 Click **New**.

3 In the **Status Cd** field, enter a code (from 1 to 5 characters) that uniquely identifies the issue status.

4 In the **Description** field, enter a short description on the issue status, such as "on Hold."

5 If the issue status is a closed-type status, select **Closed**.

6 Click **OK** to save your work.

Country Maintenance

The Country table defines all the countries in the Stat Repository. For each country that you define in the Country table, you can specify a unique set of address field labels in keeping with that country's postal conventions. This way, when a user needs to enter customer or department information (for example, when defining a new customer in the Customer Maintenance table), Stat can change the field labels based on the country the user selected.

Countries are primarily used for reporting purposes. However, before you can define individual customers, you must define the countries in which they or the companies they represent reside. Stat comes installed with default settings for USA, UK, Australia, and Canada.

Country security is controlled by the following user class rights:

- Countries - Add
- Countries - Edit

The Country table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Countries**.

If you want to add or update information in the **Country Maintenance** table, click **Search** and use the Search PeopleSoft Country/Department Engine to retrieve country information from PeopleSoft environments. You can also update the Department Maintenance table by retrieving department information from PeopleSoft. For more information, see the section, Updating PeopleSoft Country and Department Definitions on page 58.

This updates or transfers information to the Stat database and returns you to the previous window.

You can enter any set of values you want when defining a country's postal conventions. The column headings in the Country Maintenance table are suggestive only.

Value	Description
Active	If selected, indicates that country is currently active
Country Cd (Key Value)	A 1-3 character code which uniquely identifies the department
Description (Required Value)	The name of the country
Short Description (Required Value)	A 1-15 character country description
Address Line 1 Label (Required Value)	Address field label

Value	Description
Address Line 2 Label (Required Value)	Address field label
Address Line 3 Label (Required Value)	Address field label
Address Line 4 Label (Required Value)	Address field label
City Label (Required Value)	Address field label
State Label (Required Value)	Address field label
Country Label (Required Value)	Address field label
Postal Label (Required Value)	Address field label
Custom1 Label (Required Value)	Custom field label
Custom2 Label (Required Value)	Custom field label
Comment Label (Required Value)	Comment field label
Phone Mask (Required Value)	The country's telephone number scheme. Use the number character (#) and other special characters when defining the scheme. For example, the number scheme for USA is (###)###-####.
Phone Ext Label (Required Value)	Telephone extension label
SIN Label (Required Value)	The personal identification number used by the country. For example, the SIN label for USA is SSN.
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Updating PeopleSoft Country and Department Definitions

If you want to add or update department or country information in Stat, you can use the Search PeopleSoft Country/Department Engine. This feature allows you to retrieve department and/or country codes from a PeopleSoft environment based on search criteria that you specify. This information can then be added to the Stat database automatically.

Stat's Department and Country Search functionality returns data as specified by views defined in selected PeopleSoft environments. These views are listed in the PeopleSoft Search Configurations table. For more information, see PeopleSoft Search Configurations on page 111.

Click **Search** to open the Search PeopleSoft Country/Department Engine.

To use the Search PeopleSoft Country/Department Engine:

1. In the **Database** field, select the PeopleSoft database to search.
2. Depending on the **Search By** option you selected, enter a proper value in either the **Department** or the **Country** field. Then press the <F6> key.

Stat searches the selected database and displays matching departments or countries in the lower half of the window.

3 If you want to add or update a department or country to the Stat database, double-click on the department or country, or select it and click **Add/Update**.

Customer Maintenance

The customer table defines all of the customers in the Stat Repository. Customers report the problems or initiate the requests that result in the opening of CSRs. They can be members of client companies or internal employees.

Customer security is controlled by the following user class rights:

- Customers - Add
- Customers - Edit
- Customers - Edit/View EID. This right allows users to view and edit employees IDs if they have the rights to edit or add customers.

TIP: You can also define customers in the Stat Web Client.

The Customer table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Customers**.

If you want to add or update customer information, click **PS Employee** and use the Search PeopleSoft Customer Engine to retrieve customer information from PeopleSoft environments. This feature is described in detail in the *Stat User Guide*, Chapter 7, “Search Engines.”

NOTE: You can store a maximum of 32767 customer definitions in the Stat Repository.

Value	Description
Active	If selected, indicates that the customer is currently active
Last Name (Required Value)	The customer's last name
First Name (Required Value)	The customer's first name
Department (Required Value)	The department that the customer is associated with. This is a lookup on the Department table.
Employee ID	This number, used primarily with the Stat Employee Service Center module, uniquely identifies the customer in the Human Resources System. This is the EmplId in PeopleSoft. You can use this field when searching for customers.
Telephone	The customer's telephone number
Ext.	The customer's telephone extension
Address Line 1	The first line of the address
Address Lines 2,3,4	The second, third, and fourth lines of the address
City	The city of the address
State	The state of the address
Zip	The zip code of the address
Country (Required Value)	The country of the address
Email Address (Primary)	The customer's primary email address. Stat uses this address for outbound mail to a customer.

Value	Description
Email Address (Additional)	This secondary email address is used by Stat to identify inbound mail. A match is first attempted on the primary address. If none is found, Stat attempts to find a match on the secondary address. This field is helpful if the customer wants to send emails from two different addresses. Stat never sends outbound mail to this address.
Comments	Any comments regarding the customer
Custom 1 and 2	Customized fields
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

Object Type Maintenance

In the Object Type Maintenance table, you configure Stat to support change management and version control for all the objects used in PeopleSoft, Oracle Applications, and generic application environments. For most of the object classes supported in Stat, this involves activating or deactivating object types. However, for file object classes, this involves specifying, setting up, and updating the following:

- File Types – The types of file objects which Stat supports, including PeopleSoft, Oracle Applications, and generic application file types. You can configure Stat to support any type of file (with an extension) based on an ASCII, EBCDIC, or Image format.
- File Servers – The servers where the source file objects are located as well as users' working directories
- User Default Directories – The working directories where Stat copies the file objects assigned to users. For each user, you can specify a default working directory, and you can also specify a different directory for each file type.
- Oracle Apps Base Directories– For Oracle Applications, the file locations for generic Oracle Apps file types. The locations of the proprietary file types (forms, reports, etc.) are managed by Stat automatically.

Object type security is controlled by the following user class rights, all of which are contained in the Maintenance - File Objects user class rights group:

- File Servers – Edit
- File Servers – Add
- File Types – Edit
- File Types – Add
- File Locations – Add
- File Locations – Edit
- File Templates – Add
- File Templates – Edit
- File Templates – Delete
- User Directories – Edit

To open the Object Type Maintenance window, select **Maintenance | General | Object Types**.

In the Object Types tab, you can activate or deactivate any object type currently defined in Stat. Deactivated object types cannot be archived or migrated and do not appear on drop down lists.

To activate or deactivate an object type:

1. In the **Object Class** field, select the class of objects that the object type belongs to.
2. To activate an object type, select **Active,** or deselect the check box to deactivate the object type.

   Object types are active by default.
3. Click **OK** or **Apply**.

File Types

Stat provides change management support for file types in PeopleSoft, Oracle Applications, and generic application environments. To avoid confusion, file types for the three change management modules are defined and maintained separately in the Object Type Maintenance window. Generally, the maintenance procedures are the same, except that additional parameters are required for Oracle Applications.

NOTE: By default, Stat supports the following predefined file types for PeopleSoft: SQR, SQC, COBOL, and COBOL Copy.

Value	Description
Active	Indicates if this file type is activated in Stat
File Type (Key Value)	The name of the type of file, for example, COBOL and SQL
File Extension (Required Value)	The suffix following a filename that identifies the file type, for example, .cbl and .sql **NOTE:** For Oracle Applications only, generic and custom file types can be associated with multiple file extensions, separated by commas.
File Format (Required Value)	The file type format. Options include ASCII, EBCDIC, and Image. **NOTE:** FTP inserts carriage returns into ASCII-type file objects when they are migrated from a Windows environment to a Unix environment. For this reason it is recommended you base file objects on the Image format if you plan on migrating them from Windows to Unix environments.
Database Script (Required Value)	Indicates if the file type is a database script. Objects marked as database scripts may be parsed by the Impact Analysis Wizard.
Files to all Paths (Required Value)	If selected, indicates that when a file of this type is migrated to an environment, Stat copies the file to all the predefined source file locations for the environment. If not selected, Stat copies the file only to those defined locations where it already exists. If the file exists in none of the defined locations, Stat copies it to the default location.
File Permission	For Unix-style file types, the file permission mask in octal for files of this type. **NOTE:** Selecting **Unix File Permission** in the File Server tab overrides any value you specify in this field.

Value	Description
Migr. Order	(Oracle Applications only) For schema object, file object, and setup object types. Indicates the order in which objects of this type are migrated relative to other file object, schema object, and setup (AOL) object types in an archive set. The values specified here override the default values displayed in the **Default Order** field. Object types assigned a lower number are migrated before object types assigned higher numbers. The highest number you can assign an object type is 999 and two object types can be assigned the same migration order number.
Default Order	(Oracle Applications only) For schema object, file object, and setup object types. The default order in which objects of this type are migrated relative to other file object, schema object, and setup (AOL) object types in an archive set. These values are read-only and can be overridden by values in **Migr. Order** field.
Create Path on Migr.	(Oracle Applications only) For custom and generic file object types. If selected, creates the file path of the object on the target environment prior to migrating the object.
Last Update (Read Only)	The date and time this record was last updated
Updated By (Read Only)	The user who last updated this record

In addition to the file type maintenance values common to all modules, generic and custom file types defined for Oracle Applications include the following maintenance values:

Value	Description
Custom Type (Required Value)	Indicates the file type. Options include **Predefined**, **Generic**, **Custom with Language**, and **Custom w/o Language**.
For Web (Required Value)	Indicates that the file type is managed within the Web partition of the Oracle file server
For Form (Required Value)	Indicates that the file type is managed within the Form partition of the Oracle file server
For Db (Required Value)	Indicates that the file type is managed within the Database partition of the Oracle file server
For Concurrent Mgr (Required Value)	Indicates that the file type is managed within the Concurrent Manager partition of the Oracle file server

File Types for Oracle Applications

Stat supports different types of file objects for Oracle Applications. These include:

- **Predefined** file types are proprietary, such as forms and reports, and cannot be modified
- **Generic** file types are user-defined file types that exist outside the Oracle Applications file structure but which can still be archived and migrated.

  NOTE: Generic file types are supported for backward compatibility. For new objects that exist outside the Oracle Applications file system, it is recommended that you use custom file types instead of generic file types.

- **Custom** file types are user-defined file types that exist within or outside of the Oracle Applications file system. There are three types of Custom file types:
  - **Custom with Prod** file types that exist within the Oracle Applications file system and are associated with Products.
  - **Custom with Prod/Lang** file types that exist within the Oracle Applications file system and are associated with a Products and Language.
  - **Custom** file types that exist outside the Oracle Applications file system.

NOTE: Be aware of the following regarding generic and custom file types:

- All generic and custom file types must be associated with at least one of the services (form, web, concurrent managers or database). The Stat Oracle Agent defined for the selected service(s) processes the archiving and migrating requests for the generic file type.
- After you define a generic or custom file type or edit the definition of an existing one, shut down and re-start the Stat Oracle Agent for the environment in which the object type is defined. This allows the agent to register the new or modified object type.

Custom File Types

As with predefined file types, when a user adds a Custom with Prod/Lang file type object to a CSR, they are prompted to specify the object's product and language. With Custom with Prod file type objects, users are only prompted to specify the product.

When defining a custom file type, you can specify a set of commands that you want the Stat Oracle Agent to execute after migrating objects of that type to a selected environment.

To define a custom file type:

1. In the **Custom Type** field, do one of the following:
   - Select **Custom with Prod** to create a custom file type that is associated with a product.
   - Select **Custom with Prod/Lang** to create a custom file type that is associated with a product and language.
   - Select **Custom** to create a custom file type that is outside the Oracle Applications file structure.
2. Specify the file type properties you want, including file extensions, format, services, source file locations, and migration order.

   Separate multiple file extensions with a comma.

   NOTE: After you have defined a custom file type, you need to specify where files of this type are located. See the section Source File Locations on page 65 for more information. Be aware that the value in the **Custom Type** field cannot be modified after source file locations have been set or after an object of that custom file type has been added to a CSR (e.g., a Custom with Prod file type cannot be changed to a Custom with Prod/Lang file type).

3. (Optionally) If you want to associate the file type with a file template, or if you want the Stat Oracle Agent to execute commands after migrating file objects of the selected type, click **Templates/Generate**.

   This opens the File Template Maintenance window for the selected file type.

   Associating a file type with a file template helps standardize development by defining the basic characteristics and structure of new file objects in a reusable format. See the section File Templates on page 67 for more information.

   In the Define Generate Command tab, you can specify commands that you want the Stat Oracle Agent to execute after migrating objects of the file type to a selected environment. After selecting the environment, define the command in the **Command** field. You can use any of the predefined parameters in the following table used to login into an environment during a migration.

   NOTE: For R12.2, certain parameters are “Edition Aware,” meaning that when migrating to Run Edition, these parameters refer to corresponding values from the Run Edition and when migrating to Patch Edition, they refer to corresponding values from the Patch Edition.

Parameter	Description
DB_CONNECTION	Refers to the AD_APPS_JDBC_URL variable for the environment. Edition Aware for R12.2.
LANGUAGE	Language associated with the file name being migrated
PRODUCT	Product associated with the file name being migrated
TARGET_APPLSYS_PASSWORD	APPLSYS password
TARGET_APPLSYS_USERNAME	APPLSYS user name
TARGET_APPS_PASSWORD	APPS password
TARGET_APPS_USERNAME	APPS user name
TARGET_DB_LISTENER_PORT	Port defined in the Environment Connection Maintenance
TARGET_DB_NAME	Database Name defined in the Environment Connection Maintenance
TARGET_ENV_CD	Environment Code defined in the Environment Connection Maintenance
TARGET_HOSTNAME	Host Name defined in the Environment Connection Maintenance
TARGET_OBJECT_NAME	The file name being migrated
TARGET_OBJECT_NAME_FULL_PATH	The full path of file name being migrated. Edition Aware for R12.2.
TARGET_OBJECT_NAME_FULL_PATH_NE	The full path of file name without extension. Edition Aware for R12.2.
TARGET_OBJECT_NAME_NE	The file name without extension
TARGET_SERVICE_NAME	Service Name defined in the Environment Connection Maintenance
TARGET_SYSTEM_PASSWORD	SYSTEM password
TWO_TASK	Refers to the TWO_TASK variable for the environment. Edition Aware for R12.2.

NOTE: As an example note how TARGET_OBJECT_NAME_FULL_PATH_NE parameter could be used to create a soft link to a file name being migrated:
`ln -s %%FND_TOP%%/bin/fndcpesr %%TARGET_OBJECT_NAME_FULL_PATH_NE%%`

In addition to predefined parameters, you can also specify your own parameters, the values of which Stat retrieves from the *stat.conf* file. For example, if you use `%%param1%%`, you need to define the value for param1 in **stat.conf** as follows: <env>.env.PARAM1: <value for param1>. After defining a command, click **Interpret** to see how the command is interpreted by the client server.

4 Click **Ok** or **Apply**.

Generic File Types

You can define generic file types that you want to associate with a CSR, but which do not exist in an Oracle Applications environment. For example, you may want to manage on a CSR design and training documents, but these documents do not exist in any environment.

NOTE: If setting up new file objects that exist outside the Oracle Application file system, it is recommend that you use Custom file types instead of Generic.

The following example illustrates how to create generic file types:

1 Create base directory “DOC_TOP” in the OraApps Base Directories tab.

See Case Sensitivity and File Name Conversion on page 74 for more information.

2 Define the base directory in the configuration for each Stat Oracle Agent:

- DEV.env.DOC_TOP=/mnt/oracle/documents
- TEST.env.DOC_TOP=/mnt/oracle/documents
- PROD.env.DOC_TOP=/mnt/oracle/documents

You can define a different directory for each agent, such as:

- DEV.env.DOC_TOP=/mnt/oracle/documents/dev
- TEST.env.DOC_TOP=/mnt/oracle/documents/test
- PROD.env.DOC_TOP=/mnt/oracle/documents/prod

See the document, *Stat Install Notes* for more information on configuring the Stat Oracle Agent.

3 Create “Design Documents” and “Training Documents” generic file types and associate both file types with the “Web” service.

NOTE: When creating a generic file type, do not to use the same name as one of the Oracle proprietary file types supported by Stat.

4 Define source file locations using the DOC_TOP base directory and “design” and “training” relative directories, respectively.

See the next section for information on defining source file locations.

5 Make sure each Stat Oracle Agent running on the web server has read/write access to the /mnt/oracle/documents file system.

Source File Locations

After you have defined a file type, you need to specify where files of this type are located by selecting the file type and clicking **File Location**. This opens the File Locations window. Here you specify per environment the server and pathway where files of the selected type are stored. In this window you can also specify a different working directory for each user.

For Oracle Applications, you need to specify the source locations only for generic and custom file types. Remember that proprietary file types are managed by Stat automatically. The procedure for defining source locations is similar to that of PeopleSoft or generic applications, except instead of servers, you specify base directories.

The Source File Locations tab shows a list of all the active environments connected to Stat (as defined in the environment connection maintenance tables corresponding to the change management modules supported by Stat). For each environment, you can specify an unlimited number of source file locations. Source files can be located on different servers (base directories in Oracle Applications), or they can be located on the same server but in different file pathways.

NOTE: In the case of PeopleSoft, the list of environments does not include those that have been designated as staging databases.

When creating an archive set that includes a file object, Stat searches for the file in the first location you specified for the environment (for example, Path ID = 1). If the file is not there, Stat searches in the second location, and so on.

TIP: You can also specify source file locations by environment. For more information, see the environment connection sections in this chapter for PeopleSoft, Oracle Applications, and generic applications.

To define a source file location:

1 Click **New**. Stat activates a new row in the Source File Locations tab.

2 In the **Environment** field, select the environment in which you want to define a source file location.

In the **Path ID** field, Stat displays a unique ID number that it assigns to each source file location you define per environment. Path IDs determine the order in which file locations are searched during the file archive process. The path with the ID 1 is searched first, and so on.

3 Do one of the following:

- For PeopleSoft and generic application file types, select the server where the source file resides in the **File Server** field
- For Oracle Applications generic file types, select the base directory where the source files reside in the **OA Base Directory** field
- For Oracle Applications custom file types, specify the directory where the source files reside in the **Directory** field

4 (Optional) Do one of the following:

- For PeopleSoft and generic application file types, type the file pathway where the files are located in the **File Path** field
- For Oracle Applications generic file types, type the directory path where the source files are located in the **Directory** field

Make sure you use the proper syntax when specifying source file locations. For more information, see File Path Syntax on page 73.

5 (Optional) Select **Default Path** if you want this to be the file type's default source file location.

This is where Stat will copy file objects of the selected type during a migration. Each file type must have one of its source file locations designated as the default.

6 Click **Test Connection**.

See the section, Testing File Locations, Servers, and Default Directory Locations on page 79.

7 Click **OK** or **Apply** to save your changes.

File Type User Directories

In the File Type User Directories tab, you can specify for each active Stat user a separate working directory for the selected file type. This way, whenever an archive set containing a file object of a certain type is migrated to the working directories of the Development environment, Stat migrates the file object in the archive set to the assigned user's working directory defined for that type. From there it can then be modified as needed.

If you don't define a separate file type working directory for a user, whenever a file object of that type is assigned to the user and migrated to the "working directory," Stat places the file object in the user's default working directory. See the following section for more information on user default directories.

When defining file type user directories, keep in mind the following considerations:

- User can define their own working directories in the Stat User Options window. For more information, see the "Object Management" sections in the change management chapters of the *Stat User Guide*.
- You can also define working directories by user in the User File Directories tab of the Other User Information window. For more information, see Defining Stat Users on page 32.
- Make sure you use the proper syntax when specifying directories. For more information, see File Path Syntax on page 73.

Value	Description
Stat User (Key Value)	The Stat user's ID
Working File Server	Server where the working folder is located
Working File Path	File server path where the working folder is located
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

VCM Locations

In the VCM Locations tab, you can specify subdirectories for specific object types for any defined VCM connection.

Value	Description
Active	Indicates if this subdirectory is activated in Stat
VCM Connection	VCM Connection
Path	Subdirectory off of main VCM Connection Project Path for specific object type
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

File Templates

File templates help standardize development by defining the basic characteristics and structure of new file objects in a reusable format. In Stat, you can define and manage file templates associated with selected file types. This way, when developers need to create a new file object of a particular type, they can use the associated template as a starting point. This helps enforce adherence to development standards and saves time.

For more information on using file templates, see the “Object Management” sections in the change management chapters of the *Stat User Guide*.

To open the File Template Maintenance window, select the file type you want to create a template for and click the **File Templates** button (or the **Templates/Generate** button in the case of Oracle Applications custom file types).

To create a file template:

1. Click **New**.
2. In the **Template Name** field, type a name for the template.
3. In the **Template** field, browse and locate the file out on your network that you want to use as the basis for the template. Click **Open**.

   Stat displays the location of the file in the **Origin** field.
4. Click **OK** or **Apply** to save your work.

   The actual file is copied to the Stat database.

To modify a file template:

1. Click **New**.
2. In the **Template Name** field, type a name for the template and add a version number.
3. In the **Template** field, browse and locate the file on your network that you want to use as the basis for the template. Click **Open**.

   Stat displays the location of the file in the **Origin** field.
4. Click **OK** or **Apply** to save your work.
5. Inactivate the original template.
6. Click **OK** to save your work.

Setup Object Types for Oracle Applications

The Stat-supported Oracle Apps Setup object types allow for archiving and migrating data stored in Oracle Applications tables and views. The Stat Oracle Agent utilizes the FNDLOAD utility provided by Oracle to download or upload rows of data from one Oracle instance to another. FNDLOAD in turn uses a set of instructions available in an Oracle-provided .lct file, which defines the fields that are extracted, as well as the actual Sql statement for downloading and uploading the data item.

A unique object type can be defined in Stat for any Setup object, if:

- Oracle has provided an .lct file for that object type.
- The .lct file is defined in such way that allows for download and upload of a unique record for that object type.

Stat's Implementation

A typical installation of Stat comes with a number of Setup objects. These objects are referred to as AOL objects. These objects support archiving and migration of data from the FND (Application Object Library) product top.

In addition, Stat provides a resource kit, which gives customers the option of adding support for object types from 10 other product tops, including ALR, AP, AR, BOM, FA, FF, GL, INV, and ONT.

New Setup Objects Interface

Stat facilitates the creation of new Setup object types. In the following section, the interface is used to configure Stat support for the Setup object type, Advanced Benefits Startup Action Types. The R12 version of the .lct file is located under *BEN_TOP/patch/115/admin/benstact.lct*.

A quick examination of the .lct file shows that it is a good candidate for Stat:

```
DEFINE ACTION
  KEY    TYPE_CD                 VARCHAR2(30)
  CTX    OWNER                    VARCHAR2(7)
  TRANS NAME                     VARCHAR2(240)
  TRANS DESCRIPTION      VARCHAR2(240)
END ACTION


#
# Download Section
#
DOWNLOAD ACTION  <----- Entity Name
  "select v.TYPE_CD,<----- Entity Column Name
          decode(v.LAST_UPDATED_BY, 1, 'SEED', 'CUSTOM') OWNER,
          v.NAME,
          v.DESCRIPTION <----- Additional parameter to identify the row
   from   BEN_STARTUP_ACTN_TYP_VL v
          where ((:TYPE_CD is null) or
                 ((:TYPE_CD is not null) and
                  (v.TYPE_CD like :TYPE_CD)))" <----- Parameter which uniquely
identifies the row
```

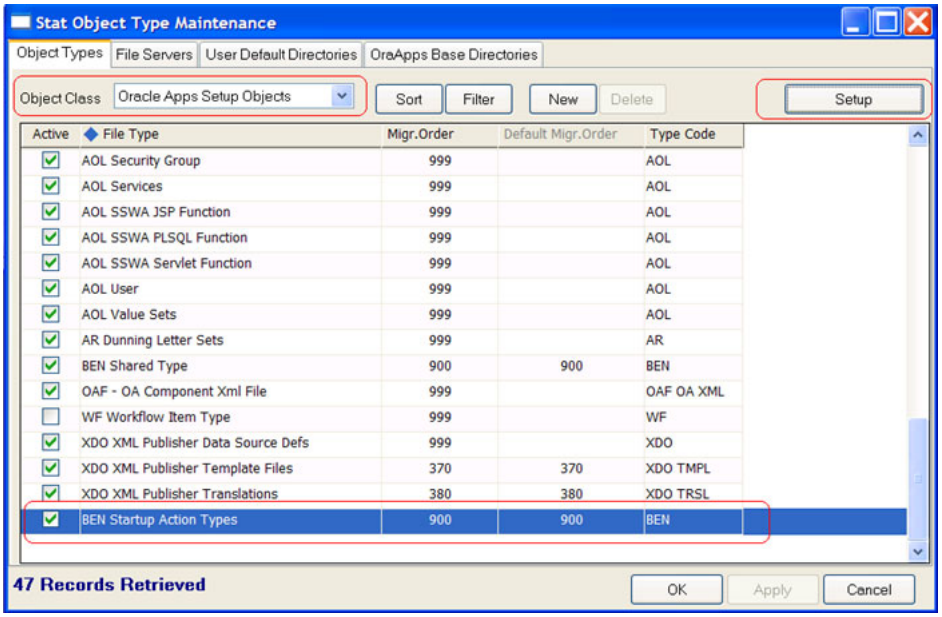
The view BEN_STARTUP_ACTN_TYP_VL is the source for data, and each row is uniquely identified by TYPE_CD column.

To configure support for new object types:

1 In the **Object Class** field, select **Oracle Apps Setup Objects**.

2 Click **New**.

3 Create an entry for BEN Startup Action Types, as illustrated below.



The Migration Order has a default value that can be changed. Type Code should have the value for the product.

4 Click **Apply**.

5 Click **Setup**.

This opens the Object Details window.

6 Select the version of Oracle Applications you are using.

Next, you need to map the contents of the .lct file into Stat.

7 In the **Lct Filename** field, enter **benstact.lct**.

8 In the **Entity Name** field, enter **ACTION**.

9 Next, you can optionally pass any appropriate parameters to the FNDLOAD utility in the **Parameters** field.

For new records, it defaults to the value, “CUSTOM_MODE=FORCE.”

10 In the **Lov Partial Sql** field, enter
FROM BEN_STARTUP_ACTN_TYP_VL v.

This is the sql statement that retrieves the list of objects.

Next, you need to define the parameters that identify a unique row. In our example, the parameter name is **TYPE_CD**, column name is **v.TYPE_CD**, and the display name is **Type**.

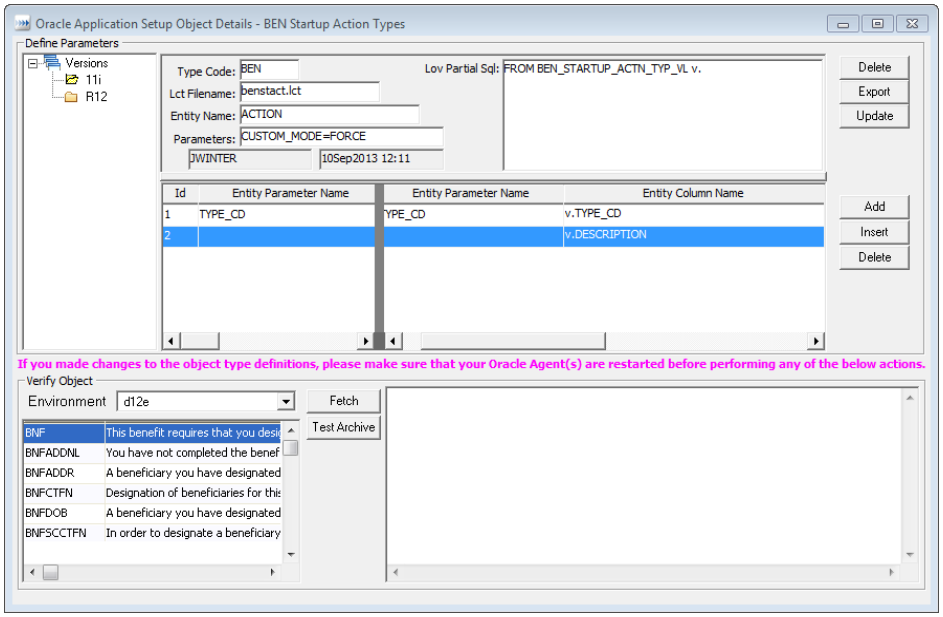
> **NOTE:** Optionally, you can specify additional parameters to identify each row. This parameter does not participate in the where clause of the sql statement. In the illustration above, the parameter name is left blank, column name is **v.DESCRIPTION**, and the display name is **description**.

11 Click **Update** to save your changes.

> **TIP:** If you need to modify an existing row, click **Update** again. Click **Export** to export the sql script for the new created object type. Click **Delete** to delete the object type definition.

12 Restart the Stat Oracle Agent to test our new configuration.

Once the agent is restarted, you can perform a Fetch Object list to verify the new object type.

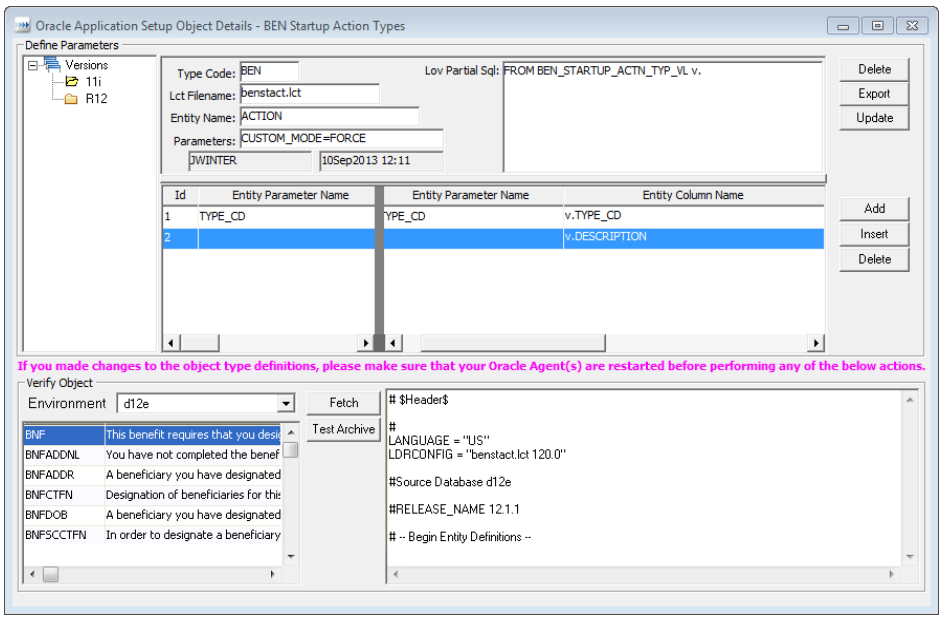


13 In the **Environment** field, select an environment.

14 Click **Fetch**.

If the object is defined correctly, a list of objects will be retrieved. In our example, the list has 2 columns corresponding to each parameter that you defined.

Now you can test the archive for any particular row from the retrieved list.



15 Select a row from the list and click **Test Archive**.

16 Once agent is done, examine the content of the archive to make sure a unique row was retrieved.

17 If content of the archive textbox does not identify a unique record or it is empty, you will likely get an error on the Oracle Agent log. In this case, you may need to run your Oracle Agent in Debug mode to identify any problems.

File Servers

The File Servers tab defines the servers that Stat accesses when archiving file objects for a specified environment or a user's working directory. For Oracle Applications, the file servers defined here are used only for working directories. Servers for Oracle Applications environments require a different configuration and are defined in the Oracle Application Environment Connection Maintenance table, as described in the section, Oracle Applications Connection Maintenance on page 92.

NOTE: In addition to the file servers that run on NT or Unix platforms, Stat also supports mainframe file servers. For more information, see Mainframe Servers on page 73.

You can check the connection between Stat and a file server by selecting the server and clicking **Test Connection**. This works the same way as testing connections to change management environments. For more information, see Testing File Locations, Servers, and Default Directory Locations on page 79.

NOTE: The connection between Stat and a file server is always established through the Stat Central Agent. For this reason, you need to make sure that the Stat Central Agent is up and running before clicking **Test Connection**.

The following table defines the value types on the File Server tab of the Object Type Maintenance window. Some of the value types, although not required, are necessary for archiving by Stat.

Value	Description
Active	Indicates if this server is activated in Stat
Server Name (Key Value)	A user defined character code which uniquely identifies the server in Stat
Description	A description of the server. 35 character maximum.
Host (Required Value)	The actual FTP host name or IP address (as opposed to the value in the **Server Name** field, which is user defined)
OS (Required Value)	The operating system the server runs on. Options include Unix, NT, and MVS.
Directory	The FTP server directory where Stat accesses file objects. Make sure you use the proper syntax when specifying server directories. For more information, see File Path Syntax on page 73.
User (Required Value)	The ID Stat uses to connect to the file server. 50 character maximum.
AuthType	The type of user ID authentication you want for Stat on this server. options include Password and (for SFTP servers only) Public Key. You can also select None if you do not want to use authentication. **NOTE:** For SFTP servers, Stat supports either Password or Public Key authentication routines only. If the Password authentication fails, Public Key exchange will be attempted.

Value	Description
Authentication	If you selected the value “Password” in the **Auth Type** field, this field displays the **Enter Password** button, which opens the Change Password dialog box. Enter the password in the **Password** and **Confirm Password** fields. Then click **OK**. 50 character maximum. If for an SFTP server you selected the value **Public Key** in the **Auth Type** field, this field displays the **Public Key Config** button, which opens the **Public key Maintenance** window. Here you can import/export key files and generate keys.
Port	The port number that the FTP server is running on. Default is 21. **NOTE:** For mainframe servers, the default number 21 should be kept. If for whatever reason 21 does not work, the specific port number should be entered in this field instead.
Passive	FTP setting used with firewalls. The default value for ftp in Stat is passive. Uncheck this option for active mode.
Post login cmmd	Any commands you want Stat to run after connecting to the FTP server. Must begin with the prefix “cd.”
File Case Sensitive	If selected, Stat handles file names on a case sensitive basis when migrating files to this server
Protocol (Required Value)	The security protocol used by the server when archiving or migrating objects. Options include FTP and SFTP. Default is FTP.
Unix File Permission	For Unix File Servers Only. If selected, Stat automatically executes the Unix command, chmod 666, after users migrate file objects to their working directories. This command gives all users that have access to the specified working directory read-write access to the migrated file objects. **NOTE:** You can specify file permission settings for individual file types in the Object Types tab. Selecting **Unix File Permission**, however, overrides any file type-specific setting.
Cobol Compiler Location: Drive and Root Directory	Location of the Cobol Compiler used to compile PS cobol programs that reside on this server
JCL File Location	The file name and location (local or network) of the jcl file that users can invoke to run the Compile Cobol post migration command on mainframe servers only.
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

NOTE: For customers who use AIX as their Stat file server and experience slow FTP services, consult your network administrator to examine your network settings. In the meantime, it is recommended that you add an entry for the file server to the hosts file on the Stat Central Agent host machine (/etc/hosts for Unix/AIX and c:\winnt\system32\drivers\etc\hosts for Windows) or using the IP address of the file server as your host name.

File Path Syntax

In Stat, there are syntactical rules for specifying file paths. These rules vary somewhat depending on whether you are defining paths on Unix and NT servers or on mainframe servers.

NOTE: For Oracle E-Business Suite customers, there are a separate set of rules for defining Oracle Apps Base Directories. For more information, see Oracle Apps Base Directories on page 79.

Unix and NT Servers

The full path of a source file location or working directory on a Unix or NT server can be composed of up to three separate elements, the topmost being the Stat home directory defined on the server, followed by the directory of the server that hosts the source file location or working directory (as specified in the **Directory** field of the **File Servers** tab), and lastly the source file location or working directory itself.

NOTE: When a file archive or migration request is made in Stat, Stat opens a FTP/SFTP connection to the server, logging in with the username specified in the **User** field of the File Server tab, for example, “StatFTP.” This means whenever particular Stat users archive or migrate files, they log into the server using Stat’s login credentials rather than their own. Like all users, however, Stat has a default home directory assigned to it on the file server as part of its account setup. This Stat home directory in turn serves as the topmost element in any file path defined in Stat.

File paths starting with “/” or “\” are assumed to be absolute paths, and are not concatenated with or relative to the element that directly precedes them, which can be either the server directory or the Stat home directory.

File paths that do not start with “/” or “\” are assumed to be relative, and are concatenated with the element that directly precedes them. See the table below for examples.

Note that Stat ignores slashes at the end of file paths.

Also, if you do not define either a source file location or a working directory, Stat assumes the path at the server directory level. Likewise, if no server directory is defined, the path is assumed at the level of the Stat home directory.

The table below illustrates the how Stat processes the syntactical combinations of the three path elements.

Stat Home Directory	Server Directory	Source File Location/ Working Directory	Resulting Path
/usr/local/statftp	/p701dp01	/SQR	/SQR
/usr/local/statftp	p701dp01	/SQR	/SQR
/usr/local/statftp	/p701dp01	SQR	/p701dp01/SQR
/usr/local/statftp	p701dp01	SQR	/usr/local/statftp/p701dp01/SQR
/usr/local/statftp	Blank	/SQR	/SQR
/usr/local/statftp	Blank	SQR	/usr/local/statftp/SQR
/usr/local/statftp	p701dp01	Blank	/usr/local/statftp/p701dp01
/usr/local/statftp	/p701dp01	Blank	/p701dp01
/usr/local/statftp	Blank	Blank	/usr/local/statftp

NOTE: File paths in Unix servers are case sensitive, but not on NT servers. Also, the direction of the slashes (“/” or “\”) in the pathways and root directories doesn’t matter.

Mainframe Servers

Mainframe file servers are defined much the same way as NT or Unix-based servers, except source file locations for mainframe servers are defined as datasets.

Access to a dataset is granted through its owner. You only need to specify the dataset in the File Path field if the login user (as specified in the File Servers tab) is the dataset owner. However, if the dataset owner is not the login

user, you must fully qualify the dataset by appending the owner name and enclosing it in single quotes (‘owner.dataset’).

For example, in the table below, STATTAB is the login user specified in the File Servers tab and the owner of the first dataset. The second dataset, however, is owned by STATSYS, which means the file path must be fully qualified with the owner name and enclosed in single quotes.

Login User	File Path	Resulting Dataset
STATTAB	QA.STATSOFF.PARMLIB	STATTAB.QA.STATSOFF.PARMLIB
STATTAB	‘STATSYS.QA.STATSON.PARMLIB’	STATSYS.QA.STATSON.PARMLIB

Case Sensitivity and File Name Conversion

You can configure Stat to conform to the case sensitivity requirements of your file servers. For example, certain file servers may be case insensitive when handling the names of file objects, but because Stat is case sensitive by default, this can result in Stat not recognizing file objects that exist on a file server as being the same objects that exist in the Stat Repository. You can resolve this issue on a per server basis by deactivating case sensitivity in Stat. Also, if a file server requires that the names of files of a specific type be all uppercase or lowercase, you can configure Stat to convert the case of file names when migrating to that server.

Deactivating Case Sensitivity

You can deactivate case sensitivity in Stat for file servers that are case insensitive. This way, when archiving or migrating file objects, Stat can locate objects in the file server’s source locations, even if the names of the files are in a different case.

To deactivate case sensitivity:

1. In the File Servers tab, deselect **File Case Sensitive** for the file server you want.
2. Click **OK**.

Setting Up File Name Case Conversion

A file server may require that the names or the extensions of certain types of objects be all in uppercase or lowercase. You can configure Stat to convert the names or extensions of these types of file objects into the required case when they are migrated to that server.

To set up file name case conversion:

1. In the File Servers tab, select the file server you want. Then click **Other Options**.

   Stat opens the Other Options dialog box. The first tab displays a list of all the file object types that have been defined for the selected server, sorted by change management module.
2. For each file type you want to configure, select the option you want in the **File Name Conversion** field.

   These include options for the conversion of both the name of the file and the extension. For example, if you select the option **Lower File Name - Upper Extension**, Stat converts the name of the file into lower case and the extension into uppercase. To deactivate file name conversion for a file type, select **None** in the field.
3. Click **OK**.

Server-Specific Pre/Post Migration Step Parameters

In the Pre/Post Migration Step Parameters Maintenance table, system administrators define public server-based parameters that can be included in the definition of pre and post migration command steps executed on any file server configured in Stat. However, because these parameters specify a set of default values that may not be

applicable to all servers, such as home directories or version numbers, you can define server-specific parameters in the Server Parameters tab of the Other Options window. Here you can define entirely new parameters, or you can specify server-specific values that override the default values of public parameters.

See the section, Pre/Post Migration Steps Parameters on page 88 for more information.

To define server-specific parameters:

1. In the File Servers tab, select the file server you want.
2. Click **Other Options**.

   Stat opens the Other Options dialog box.
3. Select the Server Parameters tab.

   When first opened, the tab displays all the public server parameters that have been defined in the Pre/Post Migration Parameters Maintenance table. Here you can create a new parameter that is specific to the selected server, or you can define a value specific to the selected server that overrides the public value of a public parameter.
4. To define a new parameter, do the following:
   a. Click **New**.
   b. Enter the parameter name.
   c. Enter the parameter value in the **Value** field.

      NOTE: If you do not enter a parameter value, the value defaults to null.

   d. (Optional) Select the encrypted option if you do not want the parameter value to be visible to users executing the pre or post migration custom command step.
5. To define a server-specific value for a public parameter, do the following:
   a. Enter the value you want in the **Value** field.

      When used in the definition of a custom command pre or post migration step executed on the server, this value will be used instead of the public value.

   b. (Optional) Select the encrypted option if you do not want the parameter value to be visible to users executing the pre or post migration custom command step.
6. Click **OK**.

SFTP Public Key-Based Authentication

Whenever Stat accesses file objects on a file server, Stat “logs in” using the username configured in Stat for that server. The file server then authenticates the user ID, typically with a password. For customers wanting a more secure method of authenticating user accounts on their SFTP file servers, Stat supports public key-based authentication.

With public key-based authentication, each user ID has a set of public keys which are authenticated by a set of corresponding, mathematically related private keys. Data encrypted with public keys can only be decrypted by their associated private keys and vice versa. When the user (in this case Stat) attempts to log into a SFTP server, the user ID is sent to the server with an associated public key. The server then checks the list of public keys associated with the user ID. If the public key is identified, the server then requires that the user authenticate their ownership of the public key by sending data encrypted with the associated private key. If the server is able to decrypt the data using the public key, the user is authenticated and granted access to the server.

Stat supports public key-based authentication using either the RSA or DSA algorithms. DSA is recommended as the more secure choice and is used by default. RSA is supported for SFTP servers already configured to use RSA.

To configure public key authentication, you must first assign Stat a user ID on each SFTP server. Then you must define in the Stat Repository a set of public and private keys associated with that ID. Remember that the public keys associated with the user ID must be defined on the server as well.

There are two ways you can acquire the key sets you need:

- Stat can generate both the public and private keys. You can then export the public keys from Stat to the SFTP server. In this case, the private key is automatically stored in Stat repository.
- The key set can be generated by some third party. You can then import the private keys into Stat and the public keys into the SFTP server.

NOTE: Configuring your servers to use public key authentication is platform-specific and lies outside the scope of this document. However, some SFTP servers have key generation capabilities, which typically write key pairs to a file stored in their home directories, such as ~/.SSE/authorized_keys for SSH1 and ~/.ssh/authorized_keys2 for SSH2.

To setup SFTP public key authentication in Stat:

1. In the Object Type Maintenance window, select the File Servers tab.
2. In the **FTP Protocol** field, select **SFTP**.
3. In the **Auth Type** field, select **Public Key**.

   NOTE: Select **Password** if you want to use standard user ID/password authentication. When you select this option, the **Authentication** field displays an **Enter Password** button. To create a password, click **Enter Password**, and in the Change Password dialog box, enter the password in the **Password** and **Confirm Password** fields (50 characters maximum). Then click **OK**.

4. In the **Authentication** field, click **Public Key Config**.

   This opens the Public Key Maintenance window where you can generate a key pair and export the generated public key to add to the list of public keys on your file server. If you already have a key pair, you can use this window to import the private key into Stat.

To import a private key:

1. Enter the fully qualified path to the file in the **Import/export file** field and then click **Import Private**.

   You must have a key that is stored in a text file in the appropriate format.

   If the import is successful, the contents of this key are reflected in the Status section of the window.

   If the operation fails, Stat displays a pop-up message. Likely causes are (a) the specified file is not accessible, (b) the contents of the importation file are not in a format that is understood by Stat's SFTP component, or (c) the file contains a public key (you must import a private key).

CAUTION: Imported or generated RSA keys are limited to 1024 bits and DSA keys are limited to 2048 bits. Longer keys are not supported and may cause database corruption.

To export a public key:

1. Enter the fully qualified path to the file in the text box and then click **Export Public**.

   The Status section of the window must indicate the presence of a key. The key can come from the database, be freshly generated, or recently imported.

   If the export is successful, the public key is written to the specified file.

   If the operation fails, Stat displays a pop-up message. The most likely cause of failure is that the specified file location is not accessible.

To generate a key:

1. Select the key type, either DSA or RSA. DSA is recommended.

   RSA is only provided for backwards compatibility with older SFTP servers.

2. In the **Size** field, select the desired key size.

   Options include **768**, **1024**, and **2048**. Longer keys are more secure but take more time to generate. The default is **1024**.

CAUTION: Currently, imported or generated RSA keys are limited to 1024 bits, and DSA keys are limited to 2048 bits. Keys longer than these limits are not supported and may cause database corruption.

3 Click **Generate**.

If the generation is successful, the contents of this key are reflected in the Status section of the window. Note that once the key pair is generated, the private key is automatically stored in Stat repository.

PT Servers

These servers are SSH enabled remote machines where PeopleTools related utilities like Application Designer and Data Mover are installed. This configuration is only relevant for users who want to migrate PeopleSoft objects using the Web Client. See Enabling Web Client to perform PeopleSoft migrations.

NOTE: The connection between Stat and a PT server is always established through the Stat Central Agent. For this reason, you need to make sure that the Stat Central Agent is up and running before clicking Test Connection.

The following table defines the value types on the PT Server tab of the Object Type Maintenance window. Some of the value types, although not required, are necessary for migration by Stat.

Value	Description
Active	Indicates if this server is activated in Stat
Server Name (Key Value)	A user defined character code which uniquely identifies the server in Stat
Host (Required Value)	The actual FTP host name or IP address (as opposed to the value in the **Server Name** field, which is user defined)
OS (Required Value)	The operating system the server runs on. Options include Unix, NT, and MVS.
User (Required Value)	The ID Stat uses to connect to the file server. 50 character maximum.
AuthType	The type of user ID authentication you want for Stat on this server. options include Password and (for SFTP servers only) Public Key. You can also select None if you do not want to use authentication. **NOTE:** For SFTP servers, Stat supports either Password or Public Key authentication routines only. If the Password authentication fails, Public Key exchange will be attempted.
Authentication	If you selected the value “Password” in the **Auth Type** field, this field displays the **Enter Password** button, which opens the Change Password dialog box. Enter the password in the **Password** and **Confirm Password** fields. Then click **OK**. 50 character maximum. If for an SFTP server you selected the value **Public Key** in the **Auth Type** field, this field displays the **Public Key Config** button, which opens the **Public key Maintenance** window. Here you can import/export key files and generate keys.
Port	The port number that the FTP server is running on. Default is 21. **NOTE:** For mainframe servers, the default number 21 should be kept. If for whatever reason 21 does not work, the specific port number should be entered in this field instead.

Value	Description
Passive	FTP setting used with firewalls. The default value for ftp in Stat is passive. Uncheck this option for active mode.
Post login cmmd	Any commands you want Stat to run after connecting to the FTP server. Must begin with the prefix “cd.”
Protocol (Required Value)	The security protocol used by the server when archiving or migrating objects. Options include FTP and SFTP. Default is FTP.
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record
Time out	The PS migrations initiated by the Stat Web Client is done by running shell commands in the PT server via SSH. These commands have to have some kind of a timeout. The Stat Admin can add timeout (in seconds). If a shell command is taking more than this specified timeout value, then the shell command will throw a timeout exception.

User Default Directories

The User Default Directories Maintenance table defines the default working directories for each Stat user. Whenever an archive set containing a file object is migrated to the working directory, Stat checks to see if a separate working directory for that type of file object has been defined for the assigned user (as described earlier in the Source File Locations section). If not, Stat places the file object in the user’s default directory.

NOTE: You can also define a user’s default working directory in the User File Directories tab of the Other User Information window. For more information, see Defining Stat Users on page 32. User can also define their own working directories in the Stat User Options window. For more information, see the “Object Management” sections in the change management chapters of the *Stat User Guide*.

Value	Description
Stat User (Key Value)	The user’s Stat user ID
User Name (Read Only)	The user’s name
Working File Server	Server where the working folder is located
Working File Path	File server path where the working folder is found. Make sure you use the proper syntax when specifying working directories. For more information, see File Path Syntax on page 73.
Last Update (Read Only)	The date and time this record was last updated
Update Userid (Read Only)	The user who last updated this record

After defining a default directory in the maintenance table, you can make sure that you have entered all the information correctly by clicking **Test Connection**. See the section, Testing File Locations, Servers, and Default Directory Locations on page 79 for more information.

Oracle Apps Base Directories

For Oracle Applications, you need to specify file locations only for custom file types (Custom, Custom with Product or Custom with Product and Language). The locations of the proprietary file types (forms, reports, etc.) are managed by Stat automatically. The base directories are defined on the OraApps Base Directory tab, while the file “pathways” are defined on the file type window.

The agent must be able to resolve the server environment variable into a known file location. For all non-R12.2 environments, this is done via the stat.conf file. For example, if in the Object Type Maintenance table you defined a base directory code COMMON_TOP, you must add the following parameter to all the Oracle agents that will process the custom objects using this base directory code:

```
Dev.env.COMMON_TOP=/apps/dev/common
```

The syntax for the parameter is <EnvCode>.env.<BaseDirectory>=<value>. The value should be an absolute (i.e., fully qualified) directory with read/write privileges for the Oracle agent. The parameter in this example is added to the Oracle agent for the “Dev” environment. The parameter can be set to a different directory for each agent.

For R12.2 environments, if these base directories are under the Edition-based File System, then the value for each Base Directory must come from the context file. An example of these types of Base Directories would be OA_HTML. This parameter is defined in the context file with a value for both the fs1 and fs2 file system. To retrieve values from the context file, you always need an XPath expression. The **Context Pattern** field in Stat stores the XPath expression for retrieving the value from the context file. (You may need to consult with your DBA and refer to documentation for EXTRACTVALUE command). For example the expression for retrieving OA_HTML from the context file is: //OA_HTML[@oa_var="s_oahtml"].

Note that if these Base Directories are not under the Edition-based File System, then the value for the Base Directory is defined in stat.conf.

Also Note that in general if a value is defined for any parameter in stat.conf, it always overrides the value read from the context file.

NOTE: Be aware of the following:

- Custom objects in Stat are specially affected by R12.2 file system. For Custom and Generic custom objects, OA Base Directory values should exist in the Environment's Context File, or it should come from a location outside the AppsTier File System. In the latter case, the values are defined in the stat.conf file as before.
- Context patterns may be used be all releases of R12, in which case you don’t need to define the base directory as a parameter in the stat.conf file.

To define an Oracle Applications base directory:

1. In the OraApps Base Directories tab, click **New**.
2. In the **Base Directory Cd** field, type a name that uniquely identifies the directory.
3. In the **Server Environment Variable** field, enter the base description as defined in the stat.conf file.
4. For R12.2 environments, if the base directories is under the Edition-based File System, enter the XPath expression for retrieving the value from the context file in the **Context Pattern** field.
5. Click **OK** or **Apply** to save your changes.

Testing File Locations, Servers, and Default Directory Locations

You can test the connection between Stat and any file location, server, directory or change management environment by selecting the row and clicking **Test Connection**. This directs Stat to test its connectivity to the selected file location, file server, directory or environment. If successful, Stat displays a “Connection Successful” message box. If Stat is unable to connect, it displays a message box stating the cause of the failure, for example, “User ID or Password is not defined.” The connection between Stat and the file server is always established by the

Stat Central Agent. For this reason, ensure that the Stat Central Agent is up and running before testing any connections.

PeopleSoft Environment Connection Maintenance

The PeopleSoft Environment Connections Maintenance table defines the PeopleSoft environments to which Stat can connect. These are the environments available for selection on CSRs and the various PeopleSoft wizards. Within the definition for each environment is the information Stat needs to connect to it.

PeopleSoft environment connection security is controlled by the following user class rights:

- PeopleSoft Connection - Add
- PeopleSoft Connection - Edit

The PeopleSoft Environment Connection Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | PeopleSoft Connect**.

Stat provides change management support for PeopleSoft running on a several different platforms, including Oracle, and SQL Server. Although most of the values that you specify in the PeopleSoft Environment Connection Maintenance table are the same regardless of which platform you are running on, some values are DBMS-specific. For this reason, the following sections describe each value in the maintenance table for each platform supported by Stat, along with any special considerations you should bear in mind when defining connections between Stat and your PeopleSoft environments.

Oracle

Value	Description
Active	If selected, indicates that this environment definition is active in Stat
Environment Cd (Key Value)	A 1-10 character code which uniquely identifies the environment
Staging DB	Indicates if the environment is used as a staging database
PS Version (Required Value)	The tools release of the environment
Data Obj Version	The version number of the PeopleSoft application, as defined in the Data Objects Maintenance table. Select a value in this field only if you plan on using Stat to manage data objects within this environment.
Description (Required Value)	A 1-35 character description of the environment
Physical Locking	Specifies whether or not physical locking is used for PeopleSoft proprietary objects in this environment
Req. Migr. Approval	If selected, indicates that archive sets cannot be migrated into the environment without migration approval
DBMS (Required Value)	Oracle
Syntax Override	N/A
ODBC DSN	This is the DSN of your PeopleSoft connection. This field is compulsory if you have checked the Use ODBC checkbox.

Value	Description
Database Name	The name of the environment (TNS Alias). Used by the Stat Client for auto-migration to the staging database and to the target.
DB User ID	N/A
DB Password	N/A
Database Server	The name of the environment (TNS Alias). The same as the Database Name above. Neither should be preceded by a “@” sign.
Srv Login ID	The Oracle user ID for the PeopleSoft schema owner. The PeopleSoft default is “sysadm.”
Server Pwd	The Oracle password for the Srv Logon ID
Host Name	Name of the machine hosting the database. Required value for the Stat Central Agent connection. However, N/A if the **Use Tns** option is selected.
Service Name	The listener service of the database. Used by the Stat Central Agent and the Stat Oracle Agent to establish JDBC connections to the Oracle database. Required value for the Stat Central Agent connection. However, N/A if the **Use Tns** option is selected.
DB Listener Port	Port number for the database listener (Oracle default value is 1521). Required value for the Stat Central Agent connection. However, N/A if the **Use Tns** option is selected.
Use Tns	For RAC Oracle databases, configures Stat to invoke TNS
Tns Entry	The full description as it appears in the tnsnames.ora file with no line breaks or carriage returns
Other Database Parameters	Additional DBMS-specific parameters, if needed
PS Config File	The path and name of the PeopleSoft configuration file, if any, that Stat imports when executing CLI functionality for this environment. You can either enter the location manually, or you can click the folder icon and select the location in the Browse for Folder dialog box. **CAUTION: Specifying an incorrect value in this field can result in the deletion of a user’s configuration data during a migration in which CLI functionality is invoked.**
Base Language	For PeopleSoft 8.54 or higher, the base language of the environment. The default is **ENG**. **CAUTION: When migrating archive sets, the base language of the staging database must be the same as the base language of the environment that the archive set came from (i.e., the source).**
Stat PS OprId (Required Value)	Required for PeopleSoft Object Locking in Stat. 30 characters in length maximum. Default is **STAT**.
Last Update (Read Only)	The date and time this record was last updated

Value	Description
Update By (Read Only)	The user who last updated this record
Use ODBC	Check this if you want to use ODBC drivers instead of SQL native client. If this field is checked, then ODBC DSN field become compulsory

Microsoft SQL Server

Value	Description
Active	If selected, indicates that this environment definition is active in Stat
Environment Cd (Key Value)	A 1-10 character code which uniquely identifies the environment
Staging DB	Indicates if the environment is used as a staging environment
PS Version (Required Value)	The tools release of the environment
Data Obj Version	N/A
Description (Required Value)	A 1-35 character description of the environment
Use Physical Locking	Specifies whether or not physical locking is used for PeopleSoft proprietary objects in this environment
Req. Migr. Approval	If selected, indicates that archive sets cannot be migrated into the environment without migration approval
DBMS (Required Value)	Microsoft SQL Server
Syntax Override	N/A
ODBC DSN	This is the DSN of your PeopleSoft connection. This field is compulsory if you have checked the Use ODBC checkbox
Database Name	The name of the environment (database instance). Used by the Stat Client for auto-migration to the staging database and to the target.
DB User ID	The name of the account used to login to the database
DB Password	The password for the account used to login to the database
Database Server	The name of the machine hosting the SQL Server database. **NOTE:** If the database is running on a SQL Server instance, the format must be “host name\instance name”
Srv Login ID	The login ID (commonly “sa”) that connects you to the SQL Server itself without connecting to a DB. Can be “sa,” but if that is a security concern, it can be another user with similar privileges, or it can be the DB user id for the database being configured.
Server Pwd	The password for the Srv Logon ID above
Host Name	Name of the machine hosting the database. Required value for the Stat Central Agent connection.
Service Name	N/A
DB Listener Port	Port number for the database listener (SQL Server default value is 1433). Required value for the Stat Central Agent connection.
Use Tns	N/A

Value	Description
Tns Entry	N/A
Other Database Parameters	Additional DBMS-specific parameters, if needed. **NOTE:** If the database is running on an SQL Server instance, you must define the name of the instance using the following format: `"instance=instance name"` **NOTE:** If you enabled ssl on a Stat Database server running SQL Server, you must add `ssl=require` to the list of properties.
PS Config File	The path and name of the PeopleSoft configuration file, if any, that Stat imports when executing CLI functionality for this environment. You can either enter the location manually, or you can click the folder icon and select the location in the Browse for Folder dialog box. **CAUTION: Specifying an incorrect value in this field can result in the deletion of a user's configuration data during a migration in which CLI functionality is invoked.**
Base Language	For PeopleSoft 8.54 or higher, the base language of the environment. The default is **ENG**. **CAUTION: When migrating archive sets, the base language of the staging database must be the same as the base language of the environment that the archive set came from (i.e., the source).**
Stat PS OprId (Required Value)	Required for PeopleSoft Object Locking in Stat. 30 characters in length maximum. Default is "STAT."
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record
Use ODBC	Check this if you want to use ODBC drivers instead of SQL native client. If this field is checked, then ODBC DSN field become compulsory

Testing Environment Connections

After defining an environment in the maintenance table, you can make sure that you have entered all the information correctly by clicking **Test Connection**. This makes Stat establish a connection to the newly defined environment. If successful, Stat immediately disconnects from the environment and displays a "Connection Successful" message. If Stat is unable to connect, it displays an error message.

You can also test connections to multiple databases simultaneously. To test multiple connections, hold the <Ctrl> or <Shift> keys and select the databases you want to test. Then click **Test Selected**. Stat attempts to establish a connection to each database and reports its results in the Database Test Connect window

Note that when you test a single environment, Stat does not validate the values specified in the fields **Host Name, Service Name**, or **DB Listener Port**. If any of these fields are not configured properly, the Stat Central Agent will log an error when the user attempts to migrate an object to or from the environment. When you test multiple connections, however, Stat does test both client and agent connections, including **Host Name**, **Service Name**, **DB Listener Port** or (in the case of Oracle-based environments) **TNS Entry**.

NOTE: When testing environment connections in the Stat Web Client, Stat Web attempts to connect using the **Host Name**, **DB Listener Port**, **Service Name**, or the **TNS Entry** values specified in the Stat maintenance tables for each particular environment. If there is no TNS Entry value specified for an environment, it uses the Host/Port/Service Name values. If a TNS Entry value is specified, it uses that value and disregards the others.

Inactivating PeopleSoft Environments

To inactivate an environment, de-select **Active**. Stat displays a warning message if the environment is currently part of a migration path.

CAUTION: Be careful inactivating environments that are part of migration paths. Objects in inactive environments cannot be archived or migrated.

Managing File Locations by Environment

For each PeopleSoft environment connected to Stat, you can define an unlimited number of source file locations for each type of file object in that environment. When Stat creates an archive set for a file object from a PeopleSoft environment, it searches for the file in the first location you specified (Path ID = 1). If the file is not there, Stat searches in the second location, and so on. If you plan to archive file objects from, or migrate to, a particular PeopleSoft environment, you must define at least one source file location for each file type.

To define source file locations by environment, select the environment in the PeopleSoft environment Connection Maintenance window and click **File Locations**. This opens the Stat File Locations window, which displays a list of all the active PeopleSoft file types defined in Stat. For each file type, you can specify as many source file locations as you want. Source files can be located on different servers, or they can be located on the same server but in different directories.

NOTE: You can also specify source file locations by file type. For more information, see Object Type Maintenance on page 60.

To set source file locations for an environment:

1. Click **New**.
2. In the **File Type** field, select the file type for which you want to define a location.

   Stat assigns a unique ID number to each file location you define per file type and displays the number in the **Path ID** field. This number determines the order that file locations are searched during the file archive process. The path with the ID 1 is searched first, and so on.
3. In the **File Server** field, select the server that the file directory is on.
4. In the **File Path** field enter the path of the file location starting after the predefined server's root or home path.
5. (Optional) Select **Default Path** if you want this to be the file type's default source file location.

   This is where Stat will copy file objects of the selected type during a migration. Each file type must have one of its source file locations designated as the default.
6. Click **Test Connection**.

   See the section, Testing File Locations, Servers, and Default Directory Locations on page 79 for more information.
7. Define additional file locations as needed.
8. Save your changes by clicking either **Apply** or **OK**.

PeopleSoft Options

To physically lock objects in a PeopleSoft environment, a user requires an operator ID and password by which to connect to that environment. You can define these operator IDs and passwords by user, as discussed in the section, Defining User Classes on page 31, or you can define them by environment. This is done in the PS Options window. In this window, you can also exclude certain object types from object locking within a selected environment and create migration approval lists.

Setting Up User Connections

The PS Options by Environment tab resembles the PS Options tab of the Other User Information window. The difference is that unlike the PS Options tab, which displays a list of all the environments that a specific user can connect to, the PS Options by Environment tab displays a list of all the users that can connect to a specific environment. From here you can assign to each user a separate operator ID and password. You can also configure CLI functionality. For more information, see Defining Stat Users on page 32.

NOTE: Users can define their own IDs and passwords by selecting **User Options | PeopleSoft Options** and entering the information in the PeopleSoft Options window. In addition, users can share the same PS Operator ID and password for staging purposes if that is how your PeopleSoft environment is configured. For example, you could assign all users the operator ID “PS” or “VP1.”

To set up user environment connections:

1. In the maintenance table, select the environment you want and click **PS Options...**.

   Stat opens the PS Options window for that environment.
2. Select the user that you want to set up the database connection for.
3. Complete the remaining steps for defining the user’s PS operator ID and pass-word and, optionally, enabling CLI functionality.

   These steps are identical to those described earlier in the section, Defining User Classes on page 31.

Setting Up Physical Object Lock Exclusions

The second tab of the PS Options window, Object Lock Exclusions, displays a list of all the PeopleSoft proprietary object types that can be physically locked in the selected non-staging environment. You can exclude any of these file types from physical object locking, which lets you control which types of objects users can physically lock while operating in a certain environment. The list of object types varies depending on the version number of the PeopleSoft environment.

To set up object lock exclusions:

1. In the PeopleSoft Environment Connection Maintenance table, select the non-staging environment you want and click **PS Options...**.

   Stat opens the PS Options window for selected environment.
2. Select the Object Lock Exclusions tab.

   This tab is available only for non-staging environments.
3. Click the check box next to each object type you want to exclude from physical object locking. To select all the objects, click **Select All**. To deselect multiple objects, click **Select None**.
4. Click **OK** or **Apply**.

For more information on physical object locking, see PeopleSoft Proprietary Object Security on page 189 and the “Object Management” sections in the change management chapters of the *Stat User Guide*.

Setting Up Migration Approval Lists

If an environment requires the approval of certain users before an archive set can be migrated into it, you can specify who these users are in the Migration Approval List tab. Stat activates this tab only if **Req. Migr. Approval** has been selected for the environment in the PeopleSoft Environment Connection Maintenance table.

When setting up a migration approval list, you can include different approver groups, including individual users and entire user classes or a combination of the two. The approval of any user or user class that you add to a list can be either required or optional.

Approval requirements that involve multiple approver groups or that can be satisfied in more than one way are defined using AND and OR operators. As you add approver groups using AND and OR operators, Stat displays the list as a tree structure and in the form of a SQL statement at the bottom of the window.

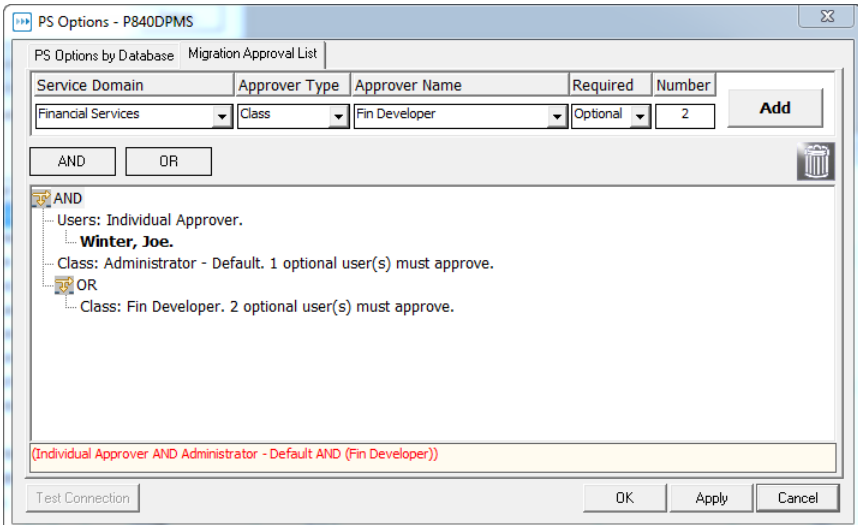
For example, let's say a migration to a particular environment in the Financial Services service domain can be approved in one of two ways:

- By a certain user AND one user in the Administrator user class

  OR

- By two users in the Fin Developer user class

In this case, your approval list would look like this:



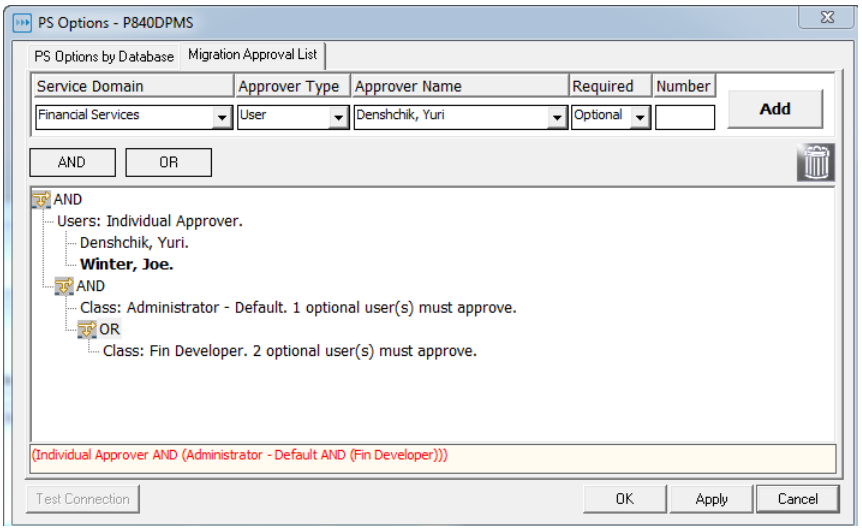
To further illustrate, let's say that the migration must be approved by:

- Two users

  AND

- One user in the Administrator user class OR two users in the Fin Developer user class.

In this case, the approval list would look like this:



NOTE: Migration approval lists closely resemble status transfer approval lists and the procedures for defining them are much the same. For more information on transfer approval lists, see Setting Up Transfer Approval Lists on page 156.

It is recommended that before setting up a migration approval list, you have a basic idea of what approver groups (users and user classes) you want involved in the approval process as well as the relationships between these groups, which you define using AND and OR operators. For example, if the approval of one or more approver groups are required, you would begin the approval list with the AND operator. If, however, the approval of only one of two or more approver groups are required, you would begin the list with the OR operator.

To set up a migration approval list:

1 Do one of the following:

- Click **AND** if the approval of one or more approver groups are required
- Click **OR** if the approval of one of two or more approver groups are required

The operator icon is added to the approval list diagram.

2 Click on the AND or OR operator icon you just added.

> **TIP:** The icon background appears blue when selected and changes to gray when other fields or action buttons are activated. As long as the background of the operator icon is blue or gray, then approver groups and other operators can be attached to the operator.

3 In the **Service Domain** field, select the service domain that you plan to associate the environment with in the PeopleSoft Migration Path Maintenance table.

4 In the **Approver Type** field, select the approver group you want to add to the list.

Options include **User** and **User Class**.

When adding approvers, be aware of the following:

- Although you can add any user or class to an approval list, be aware that only users that have access to an environment and the selected service domain (as defined in the User Maintenance table) will be able to approve a migration into that environment or receive email notifications regarding their pending approval. If an approver does not have access to the environment, the migration cannot be approved until either the user is granted access to the environment or the migration's approval requirements are overridden by another user with proper security rights. For this reason, it is recommended that you first verify users have access to a particular environment and service domain before adding them to an approval list.
- Adding individual users to approval lists could create problems if those same users are later inactivated or have their service domain and environment access restricted. For this reason, it is recommended that you add user classes to approval lists rather than individual users whenever possible.
- Users assigned to a migration approval list must have the user class rights to operate in the same change management module in which the migration takes place. Also, you can assign user class rights that enable users to migrate objects regardless of approval status and also to approve migrations on the behalf of other users.

5 In the **Approver Name** field, select the name of the user or user class you want to add.

6 In the **Required** field, select **Required** if the approval is required or **Optional** if it is not required.

The **Required** option means that the individual user and every member of the user class must approve the migration. **Optional** means that the individual user's approval is not required, whereas for user classes, it means that the approval of only a specified minimum number of users within that class is required.

7 If you selected **User Class** in the **Approver Type** field and **Optional** in the **Required** field, specify the minimum number of users in that class who must approve the migration in the **Number** field.

8 Click **Add**.

The approver is added to the tree structure under its approver group label and the initial AND or OR operator. Required approvers are displayed in bold.

At this point, how you proceed depends on the different approver groups you want to add to the list and how you want to define the relationships between these groups using AND and OR operators.

9 (Optional) Do the following to add additional AND or OR operators to your approval list:

a Depending on the relationship between approver groups in your list, select the operator icon to which you want to attach additional operators.

b Click **AND** or **OR**.

c Repeat as necessary to add more operator icons to the approval diagram.

10 (Optional) To add additional user classes, select the appropriate operator icon in the approval diagram and repeat steps 4 through 8.

When you the first add an individual user to an approval list, Stat automatically creates the ad hoc group “users” in the approval diagram and attaches it to the appropriate operator icon. All subsequent users you add to the list must belong to this group.

TIP: In a scenario in which you want to create approval relationships between multiple user approver groups, you may consider adding users to new user classes or queues created expressly for this purpose.

11 (Optional) To add additional users, select the “users” group and repeat steps 4 through 8.

12 (Optional) Do any of the following to edit the diagram as needed:

- To change an operator from AND to OR or from OR to AND, right-click on the icon.
- To change the Required status of an approver, right click on it in the diagram. This changes required user classes to optional with 1 minimum user approval.
- To change the minimum number of user approvals in an optional user class, double-click on the group label and specify the minimum number of user approvals you want.
- To move approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to a different operator icon in the diagram.
- To delete approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to the Trash Can icon.

13 Click **OK** or **Apply**.

Copying PeopleSoft Environments

If you need to define a PeopleSoft environment that closely resembles an existing environment, you can save time by copying the definition of the existing environment and editing the copy as needed. When you copy a PeopleSoft environment, all the information gets copied over, including file locations and selected PS options.

To copy a PeopleSoft environment definition:

1 In the PeopleSoft environment Connection Maintenance window, select the environment definition you want to copy.

2 Click **Copy**.

Stat prompts you to specify a database code and short description.

3 Specify the database code and short description. Then click **OK**.

4 Edit the new environment definition as needed.

Pre/Post Migration Steps Parameters

In the Pre/Post Migration Steps Parameters Maintenance table, you can define user and server-based parameters that can be included in the definition of pre and post migration custom command steps. This provides a convenient way to insert variables such as server names and passwords in custom commands. And because parameter values can be encrypted, sensitive information that you do not want visible to the users executing the commands can be secured.

The table also includes a number of predefined parameters, which specify commonly invoked values used to login into an environment during a migration or to invoke Stat web services.

A user must have one of the following rights to open the Pre/Post Migration Step Parameters Maintenance table:

- Pre/Post Migration Server Parm - Add
- Pre/Post Migration Server Parm - Edit
- Pre/Post Migration User Parm - Add
- Pre/Post Migration User Parm - Edit

For more information on pre and post migration steps, see the sections, Pre Migration Steps on page 152.

The parameters defined in this table are public, meaning that they specify a set default parameter values that can be included in the definition of any custom command pre and post migration step. It is possible, however, to define parameters and parameter values that are specific to individual users or servers. User and server-specific parameters can be used in conjunction with public parameters, while parameter values specific to users and servers can be used to override the default values of public parameters:

- User-specific parameters (such as user names and passwords) apply to particular Stat users, who define them themselves. For more information on user-specific parameters, see the *Stat User Guide*, “Appendix: User-Specific Parameters.”
- Server-specific parameters (such as home directories and version numbers) apply to particular file servers. You can define server-specific parameters here, or you can define them on the File Servers tab of the Object Type Maintenance window. For more information, see the section, Server-Specific Pre/Post Migration Step Parameters on page 74.
- Predefined parameters are commonly used parameters included as a convenience. These parameters, which specify values used to login to an environment during a migration or to invoke Stat web services, are read-only and cannot be modified or removed. Certain predefined parameters are specific to particular change management modules, as noted in the table below:

Predefined Parameter	Description	Module
CSR_ID	CSR ID	All
SD_CD	Service domain code	All
PS_PROJECT	PeopleSoft Project	PS and Generic only
SOURCE_DB_NAME	Source database name	All
SOURCE_DB_PASSWORD	Migration source database user password	All
SOURCE_DB_USERNAME	Migration source database user name	All
SOURCE_ENV_CD	Source environment code	All
TARGET_APPLSYS_PASSWORD	Target application system password	Oracle Apps only
TARGET_APPLSYS_USERNAME	Target application system user name	Oracle Apps only
TARGET_APPS_PASSWORD	Target apps password	Oracle Apps only
TARGET_APPS_USERNAME	Target apps user name	Oracle Apps only
TARGET_DB_LISTENER_PORT	Target database listener port	All
TARGET_DB_NAME	Migration target database name	All
TARGET_DB_PASSWORD	Migration target database user password	All
TARGET_DB_USERNAME	Migration target database user name	All
TARGET_ENV_CD	Target environment code	All
TARGET_HOSTNAME	Target host name	All
TARGET_OBJECT_NAME	Target object name	All
TARGET_OBJECT_PATH	Target object path	PS and Generic only
TARGET_SERVICE_NAME	Target service name	All
TARGET_SYSTEM_PASSWORD	Target system password	Oracle Apps only
TARGET_TNS_ENTRY	Target TNS entry	

NOTE: The parameters used to login into source and target environments include the database (identified by name or environment code) as well as user names and passwords. These values are encrypted.

To define a pre/post migration step parameter:

1. Depending on the type of parameter you want to define, select either the User Parameters or Server Parameters tab.
2. Click **New**.
3. Enter the parameter name.
4. Enter the parameter value.

   This is the parameter's public default value, which can be overridden by a user or server-specific value that is defined for the public parameter.

   NOTE: If you do not enter a parameter value, the value defaults to null.
5. Select the encrypted option if you do not want the parameter value to be visible to users executing the pre/post migration custom command step.
6. (Optional) Enter a description of the parameter.
7. Click **OK**.

Oracle Applications Configuration

The Oracle Applications Configuration table defines operating parameters for uploading Oracle Applications patches into the Stat Repository and providing change management support for Oracle Applications objects. These parameters include patch types, products and product families, and the languages supported by your Oracle environments.

For more information on Oracle Patches, see the *Stat User Guide*, Chapter 12, "Change Management for Oracle Applications."

The Oracle Application Configuration table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Oracle Application Configuration**.

Patch Types

In the Patch Types tab, you specify which Oracle Applications patch types you want Stat to support. Patch types are used in the Patch Console to categorize uploaded patches. When first installed, Stat is pre-configured to support the most common Oracle Applications patch types. You can edit the names of these patch types as needed, or you can define new patch types.

To define a patch type:

1. Click **New**. Then in the **Patch type** field, enter the name of the patch type, for example, Family Pack.
2. Click **OK** or **Apply**.

Product Families

Stat comes pre-configured with all Oracle product families. In the Product Families tab, you can define new Oracle Applications product family groups or de-activate existing ones. The product family values specified here are used in the Oracle Apps Patch Console to categorize Oracle patches that are uploaded to the Stat Repository and then applied to your Oracle Applications environments.

The individual products that make up a product family are defined on a per environment basis in the Products tab.

Platforms

When users upload a patch to the Stat Repository, they are prompted to specify the target platform. The list of available platforms is defined in the Platform tab.

Stat uses the value displayed in the **Description** field to identify the platform that an uploaded patch targets by matching the text to the patch file name.

Stat comes pre-configured to support AIX, SunOS, Windows, Linux, and generic platforms. You cannot define new platforms, but you can deactivate existing ones to reduce the number of options in other fields. Deselect **Active** to deactivate a platform.

Updating Products

Each of your Oracle Applications environments may feature a different set of Oracle Applications products. In order to utilize Stat's change management support for the proprietary file objects in your Oracle Applications environments, as well as apply product-specific Oracle patches to the appropriate environments, you need to specify the products that each environment contains. For Oracle Apps Setup objects, each environment may have a different list of active products. To retrieve the proper list of Setup Objects in Stat, it is imperative that the list of products are updated. This is done in the Products tab.

Except for the **Active** check box, the Products tab is read-only. It displays a list of all the products contained in the selected environment along with their release level. When you first define an environment, install new Oracle Applications products to a particular environment, create a custom product, or apply a maintenance pack, you should update the environment's product list. To do this, select the environment you want to retrieve the product list for and click **Update Products**. This sends a request to the Stat Oracle Agent, which updates the list with any fully installed, shared, or custom products it finds for the selected environment. To deactivate a product, deselect **Active**.

NOTE: You can also update the products list of an environment in the Products tab of the Application Options window, which you open from the Oracle Application Environment Connection Maintenance table.

When updating products, be aware of the following considerations:

- For Stat to recognize a custom product, the product must have a record created in the FND_PRODUCT_INSTALATIONS table. To create this record, select **System | Installations** in the Oracle Alert Manager responsibility and use the form to define the custom product. It will be necessary to re-start the Stat Oracle Agent after this record is created. Also, custom products may need to be defined in the stat.conf file before they can be updated in Stat. For Release 12.2, Stat reads the values for custom product locations from the Context File of the environment. If these parameters are present in stat.conf, they override the values in the Context File.
- Oracle stores all form FMB files in the same directory ($AU_TOP/forms/<lang>). When getting a list of forms for a user to assign to a CSR, Stat uses two sources to determine the FMBs associated with the product selected by the user: All FMBs registered for the product are considered and all FMBS with a corresponding FMX file in the product top are considered. If a form is not registered or does not have an FMX file, Stat will not include it when displaying a list of forms. This limitation does not affect forms for custom applications since Stat also considered FMBs in the product top for custom applications.

Languages

In the Languages tab you configure Stat to support change management for language-specific, proprietary Oracle Applications file objects as well as translation patches. The Language tab is read-only. It displays a list of all the languages enabled for all environments. The default language is American English. You can update the list for any Oracle Application environment first by selecting an environment in the dropdown list and then clicking **Update Languages**.

To deactivate a language, deselect **Active**.

If you need to migrate AOL objects in multiple language versions, do the following to configure language support AOL object in Stat.

1. Select the Oracle Application environment containing the AOL objects you want to migrate in the drop-down list and click **Update Languages**.
2. Verify that the languages you want supported are installed.
3. Add the AOL objects you want to migrate to a CSR.

   When you select the AOL object in a multi-lingual environment, you are prompted to select a language.

   > **NOTE:** The following objects are exceptions: XDO Templates, XDO Translations, OAF Component XML, and XDF Editioning View (R12.2). Also, no prompt is displayed if only American English is installed.

   After adding the objects to the CSR, each object's description will have the language appended to the end. Also, after an archive set has been created successfully, you can view and verify the content of the archive set.
4. Open the archive set in the Objects tab, select an object, and click **View**.

   A View Archive window is displayed showing specifics about the object, including the language.

Patch Prerequisites

In the Patch Prerequisites tab you specify the default environment against which Stat will process patch prerequisite requests whenever users upload and save a patch. Specifying a default environment is optional.

Oracle Applications Connection Maintenance

The Oracle Applications Connections Maintenance table defines the Oracle Applications environments and servers that Stat can connect to. These are the environments available for selection on CSRs and the various object wizards. Within the definition for each environment is the information Stat needs to connect to it.

Oracle Applications connection security is controlled by the following user class rights:

- Oracle Connection - Add
- Oracle Connection - Edit

The Oracle Application Connection Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Oracle Applications Connect**.

Value	Description
Active	If selected, indicates that this environment is active in Stat
Environment Cd (Key Value)	A 1-10 character code which uniquely identifies the environment. This is the code that must be used in the Stat Oracle Agent configuration file.
Description (Required Value)	A 1-35 character description of the environment
OraApps Version (Required Value)	The version number of the Oracle Applications environment. Options include 11i and R12.
Data Obj Version	The Oracle Applications version number, as defined in the Data Objects Maintenance table. Select a value in this field only if you plan on using Stat to manage data objects within this environment.

Value	Description
Req. Mgr. Approval	If selected, indicates that archive sets cannot be migrated to the environment without approval
Req. Patch Approval	If selected, indicates that patches cannot be applied to the environment without approval
DBMS (Required Value)	The Oracle database management system that the environment is running on
Database Name	TNSNAMES.ORA entry on all Stat users' workstations. Used by Stat Client for Oracle Net connections to the Oracle Applications database.
APPS User	Name of the APPS database account holder
APPLSYS User	Name of the APPLSYS database account holder
SYSTEM Pwd	SYSTEM database account password
APPS Pwd	APPS database account password
Host Name	Name of the machine hosting the database. Used by the Stat Central Agent and the Stat Oracle Agent for JDBC connections to the Oracle Applications database. Required value for the Stat Central Agent.
Service Name	For Oracle, the listener service of the database. Used by the Stat Central Agent and the Stat Oracle Agent to establish JDBC connections to the Oracle database. **IMPORTANT:** Required value for the Stat Central Agent, even when Tns values are specified.
DB Listener Port	Port number for the database listener. Used by the Stat Central Agent and the Stat Oracle Agent for JDBC connections to the Oracle Applications database. Required value for the Stat Central Agent.
Use Tns	For RAC Oracle databases, configures Stat to invoke TNS
Tns Entry	The full description as it appears in the tnsnames.ora file with no line breaks or carriage returns
Other Database Parameters	Additional environment-specific parameters, if needed
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record
System user	The schema name which the EBS is using for database Administrator. **IMPORTANT:** Until now this value was hard coded as SYSTEM and it's still SYSTEM by default, however this value is configurable now. After the EBS_SYSTEM schema migration completion patch is applied on the user's EBS instance, this value should be updated EBS_SYSTEM manually by the user. This column is introduced in 6.2 HF-o.

Testing Environment Connections

After defining an environment in the maintenance table, you can make sure that you have entered all the information correctly by clicking **Test Connection**. This makes Stat establish a connection to the newly defined environment. If successful, Stat immediately disconnects from the environment and displays a "Connection

Successful" message. If Stat is unable to connect, it displays an error message. Test Connect verifies that APPS and SYSTEM passwords.

You can also test connections to multiple databases simultaneously. To test multiple connections, hold the <Ctrl> or <Shift> keys and select the databases you want to test. Then click **Test Selected**. Stat attempts to establish a connection to each database and reports its results in the Database Test Connect window

Note that when you test a single environment, Stat does not validate the values specified in the fields **Host Name, Service Name**, or **DB Listener Port**. If any of these fields are not configured properly, the Stat Central Agent will log an error when the user attempts to migrate an object to or from the environment. When you test multiple connections, however, Stat does test both client and agent connections, including **Host Name**, **Service Name**, **DB Listener Port** or (in the case of Oracle-based environments) **TNS Entry**.

NOTE: When testing environment connections in the Stat Web Client, Stat Web attempts to connect using the Host, Port, Service Name, and TNS Entry values specified in the Stat maintenance tables for each particular environment. If there is no TNS Entry value specified for an environment, it uses the Host/Port/Service Name values. If a TNS Entry value is specified, it uses that value and disregards the others.

Defining Oracle Applications Servers

In the Oracle Apps Environment Servers table, you define one or more servers that host the four service partitions required for each Oracle Applications environment. These service partitions include Web Service, Forms Service, Concurrent Manager Service, and Admin Service. To open the table, select the environment you want and click **Servers**.

Value	Description
Active	If selected, indicates that the server is active
Server Name (Required Value)	A user defined character code which uniquely identifies the server in Stat
Server Host (Required Value)	The physical hostname (as opposed to the value in the **Server Name** field, which is user defined). This must be the server's exact name (i.e., the value returned by hostname).
Platform (Required Value)	The server's operating system
Working Directory (Required Value)	The location where the Stat Oracle Agent temporarily unzips patch files. A patch file is only stored in the directory while Stat is applying the patch with AutoPatch. After the patch has been applied, the patch file is removed.
Autobatch Size	Batch size parameter for AutoPatch
Autoparallel Workers	The number of parallel workers used by autopatch
Web Srv	Indicates if the server hosts a Web Service
Forms Srv	Indicates if the server hosts a Forms Service
Concurrent Srv	Indicates if the server hosts a Concurrent Manager Service
Admin Srv	Indicates if the server hosts the Database Service, also known as the "Administration Server" in Oracle documentation
Start Concurrent Cmd	Command run by the Stat Oracle Agent to start Concurrent Manager Service
Stop Concurrent Cmd	Command run by the Stat Oracle Agent to stop Concurrent Manager Service
Start Forms Cmd	Command run by the Stat Oracle Agent to start Forms Service
Stop Forms Cmd	Command run by the Stat Oracle Agent to stop Forms Service

Value	Description
Start Web Cmd	Command run by the Stat Oracle Agent to start Web Service
Stop Web Cmd	Command line run by the Stat Oracle Agent to stop Web Service
Ping Multiplier	The rate in 30 second increments at which the Oracle Agent updates the MEC_WAKE table and reports its status in Oracle Agent Status window (opened from the Tools menu). The default value is 1, meaning every 30 seconds. To increase the time amount, enter a higher value, e.g., meaning 120 seconds (4x30=120 seconds). The default value is 1. If the value is set to 0, the agent does not report its status and will always be shown as 'Not Responding'. **NOTE:** You must stop and re-start the Oracle Agent if the value of the ping multiplier is modified.
Server Code	If you want to start/stop the Oracle Agent associated with this server from the Window's Client, you must first define a Server entry for this agent in the **Maintenance | General | Object Types | File Servers** window. This entry must be defined with an SFTP protocol, and SSH must be running on the server running the Oracle Agent. Generally, the applmgr user should be used for the Username and Password or Key exchange authentication for logging into the Oracle Agent server. Once the Server entry is created, you may associate the Server Code with this Oracle Agent entry. **NOTE:** In order to source the environment when SSH logs in, you might be required to add the "./.ssh/rc" command to **Post login cmd** on the File Servers tab of the Object Type Maintenance window. In this case make sure that the rc file sources your Oracle E-business environment and sets your STAT_JAVA_HOME.
OA Stat Home	This is the STAT_HOME location defined for this Oracle Agent on the Oracle E-Business server.
OA Config File	If you override the default location for the OA config file with a "-s" switch, you must enter it here.
OA Stat Java Home	If you override the default STAT_JAVA_HOME of the Oracle Agent with a "-j" switch, you must enter it here.
Update Date (Read Only)	The date and time this record was last updated
Updated By (Read Only)	The user who last updated this record

When defining servers for an Oracle Applications environment, be aware of the following:

- When specifying commands that start and stop any of the Oracle Apps services, you can use the `appsusername` and `appspwd` parameters to pass the user name and password values specified in the Apps User and Apps Pwd columns in the Oracle Applications Environment Connection Maintenance table. For example, to start a Concurrent Manager in R12, you would specify:
  `$INST_TOP/admin/scripts %%appsusername%%/%%appspwd%%`
- Each of the four service partitions must be hosted on at least one active server. For a shared APPL_TOP, all four service partitions can be configured on one server.
- For each active server, at least one of the service partition check boxes must be checked.
- Only one active server can host the Database Service partition.

Start/Stop Oracle Applications Agents

After you install the Oracle Application Agent on each defined server, you may start/stop the agent, edit the stat.conf file, retrieve OA Agent logs, or change OA Agent log mode from the server list.

- **Oracle Agent Configuration** - You may use this button to retrieve your stat.conf file from the OA Agent conf directory. At this point, you may view or edit the content of the file before saving it back to the server.
- **Start/Stop Oracle Agent** - You may use this button to start/stop the OA Agent for the selected server. Once the OA agent is started, the Status column for the server will display Started along with a green check mark. Once the OA agent is stopped, the Status column for the server will display Stopped along with a red X.
- **Oracle Agent Logs** - You may use this button to retrieve a list of logs from the OA Agent log directory. Once the list is retrieved, you may view the content of the log or export it.
- **Oracle Agent Log Mode** - The current log mode defined for the Oracle Agent is displayed in the drop-down and can be changed while the agent is running. Select the desired mode from the drop-down and click the button beside it.
- **Refresh Oracle Agent Status** - Once you attempt to start or stop the Oracle Agent, you may use this button to refresh the current status of the OA agent.
- **Show SSH logs** - SSH protocol is used to run the Start/Stop commands on the Oracle Agent server. For troubleshooting purposes, you may need to view the SSH logs generated by the commands that are run on the server. Make sure to select this check box before executing the Start or Stop command.

Inactivating Oracle Applications Environments

To inactivate an environment, de-select **Active**. Stat displays a warning message if the environment is currently part of a migration path.

! **CAUTION: Be careful inactivating environments that are part of migration paths. Objects in inactive environments cannot be archived or migrated.**

Setting Up Migration and Patch Approval Lists

If an environment requires the approval of certain users before an archive set can be migrated into it or a patch can be applied, you can specify who these users are in the Migration Approval List and Patch Approval List tabs of the Application Options window. To open this window, select the environment you want and click **App Options** in the Oracle Application Environment Connection Maintenance table.

When setting up a migration or patch approval list, you can include different approver groups, including individual users and entire user classes or a combination of the two. The approval of any user or user class that you add to a list can be either required or optional.

Approval requirements that involve multiple approver groups or that can be satisfied in more than one way are defined using AND and OR operators. As you add approver groups using AND and OR operators, Stat displays the list as a tree structure and in the form of a SQL statement at the bottom of the window.

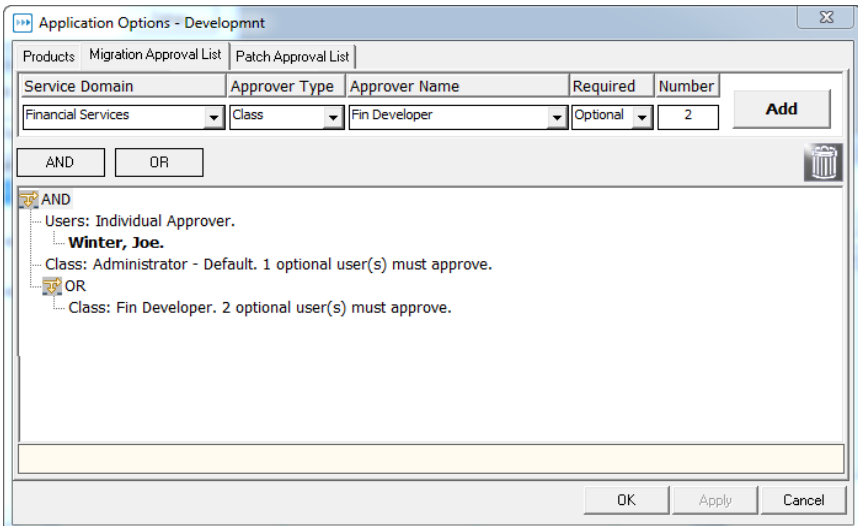
For example, let's say a migration to a particular environment in the Financial Services service domain can be approved in one of two ways:

- By a certain user AND at least one user in the Administrator user class

  OR

- By at least two users in the Fin Developer user class

In this case, your approval list would look like this:



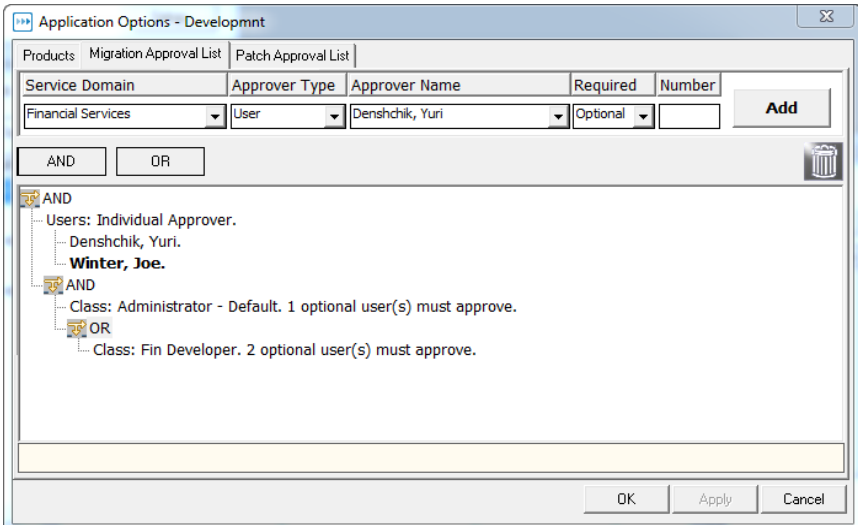
To further illustrate, let's say that the migration must be approved by:

- Two users, one of whom is required

  AND

- At least one user in the Administrator user class OR at least two users in the Fin Developer user class.

In this case, the approval list would look like this:



NOTE: Migration and patch approval lists closely resemble status transfer approval lists and the procedures for defining them are much the same. For more information on migration approval lists, see Setting Up Transfer Approval Lists on page 156.

It is recommended that before setting up a migration or patch approval list, you have a basic idea of what approver groups (users and user classes) you want involved in the approval process as well as the relationships between these groups, which you define using AND and OR operators. For example, if the approval of one or more approver groups are required, you would begin the approval list with the AND operator. If, however, the approval of only one of two or more approver groups is required, you would begin the list with the OR operator.

To set up a migration or patch approval list:

1 Do one of the following:

- Click **AND** if the approval of one or more approver groups are required
- Click **OR** if the approval of one of two or more approver groups are required

The operator icon is added to the approval list diagram.

2 Click on the AND or OR operator icon you just added.

> **TIP:** The icon background appears blue when selected and changes to gray when other fields or action buttons are activated. As long as the background of the operator icon is blue or gray, then approver groups and other operators can be attached to the operator.

3 In the **Service Domain** field, select the service domain that you plan to associate the environment with in the Oracle Applications Migration Path Maintenance table.

4 In the **Approver Type** field, select the approver group you want to add to the list.

Options include **User** and **User Class**.

When adding approvers, be aware of the following:

- Although you can add any user or class to an approval list, be aware that only users that have access to an environment and the selected service domain (as defined in the User Maintenance table) will be able to approve a patch application or migration into that environment or receive email notifications regarding their pending approval. If an approver does not have access to the environment, the patch or migration cannot be approved until either the user is granted access to the environment or the approval requirements are overridden by another user with proper security rights. For this reason, it is recommended that you first verify users have access to a particular environment and service domain before adding them to an approval list.
- Adding individual users to approval lists could create problems if those same users are later inactivated or have their service domain and environment access restricted. For this reason, it is recommended that you add user classes to approval lists rather than individual users whenever possible.
- Users assigned to a migration or patch approval list must have the user class rights to operate in the same change management module in which the migration takes place. Also, you can assign user class rights that enable users to migrate objects or apply patches regardless of approval status and also to approve migrations and patches on the behalf of other users.

5 In the **Approver Name** field, select the name of the user or user class you want to add.

6 In the **Required** field, select **Required** if the approval is required or **Optional** if it is not required.

The **Required** option means that the individual user and every member of the user class must approve the migration or patch. **Optional** means that the individual user's approval is not required, whereas for user classes, it means that the approval of only a specified minimum number of users within that class is required.

7 If you selected **User Class** in the **Approver Type** field and **Optional** in the **Required** field, specify the minimum number of users in that class who must approve the migration or patch in the **Number** field.

8 Click **Add**.

The approver is added to the tree structure under its approver group label and the initial AND or OR operator. Required approvers are displayed in bold.

At this point, how you proceed depends on the different approver groups you want to add to the list and how you want to define the relationships between these groups using AND and OR operators.

9 (Optional) Do the following to add additional AND or OR operators to your approval list:

a Depending on the relationship between approver groups in your list, select the operator icon to which you want to attach additional operators.

b Click **AND** or **OR**.

c Repeat as necessary to add more operator icons to the approval diagram.

10 (Optional) To add additional user classes, select the appropriate operator icon in the approval diagram and repeat steps 4 through 8.

When you the first add an individual user to an approval list, Stat automatically creates the ad hoc group “users” in the approval diagram and attaches it to the appropriate operator icon. All subsequent users you add to the list must belong to this group.

> **TIP:** In a scenario in which you want to create approval relationships between multiple user approver groups, you may consider adding users to new user classes or queues created expressly for this purpose.

11 (Optional) To add additional users, select the “users” group and repeat steps 4 through 8.

12 (Optional) Do any of the following to edit the diagram as needed:

- To change an operator from AND to OR or from OR to AND, right-click on the icon.
- To change the Required status of an approver, right click on it in the diagram. This changes required user classes to optional with 1 minimum user approval.
- To change the minimum number of user approvals in an optional user class, double-click on the group label and specify the minimum number of user approvals you want.
- To move approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to a different operator icon in the diagram.
- To delete approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to the Trash Can icon.

13 Click **OK** or **Apply**.

If an environment requires the approval of certain users before an archive set can be migrated into it or a patch can be applied, you can specify who these users are in the Migration Approval List and Patch Approval List tabs of the Application Options window. To open this window, select the environment you want and click **App Options** in the Oracle Application Environment Connection Maintenance table.

When setting up an approval list, you can include individual users, entire user classes, or a combination of the two. Also, the approval of any user or user class that you add to a list can be either required or optional.

To add users to an approval list:

1 Depending on the type of approval list you want, select either the Migration Approval List tab or the Patch Approval List tab.

2 Click **New**.

3 In the **Approver Type** field, select **User**.

4 In the **Approver Name** field, select the name of the user you want to add.

5 Select **Required** if the user’s approval is required.

If you do not select the check box, the user’s approval is optional.

6 Repeat steps 1 through 4 to add as many users to the list as needed.

7 If you added more than one optional user, enter the minimum number of optional users whose approval is required in the **Min Approver (s) for Optional Users** field.

This number must be equal to or less than the number of optional users.

To add user classes to an approval list:

1 Select the service domain for this environment.

2 Click **New**.

3 In the **Approver Type** field, select **Class**.

4 In the **Approver Name** field, select the user class you want to add.

5 Select **Required** if the approval of every user in the class is required.

Do not select the check box if the approval of only a certain number of users in the class is required.

6 If you did not **Required**, enter the number of users belonging to the class whose approval is required in the **Min Approver (s) for Optional Classes** field.

Updating Products per Environment

Each Oracle Applications environment you define may feature a different set of Oracle Applications products. In order to utilize Stat's change management support for proprietary Oracle Applications file objects, as well as apply product-specific Oracle patches to the appropriate environments, you need to specify the products that each environment contains. For Oracle Apps Setup objects, each environment may have a different list of active products. To retrieve the proper list of Setup Objects in Stat, it is imperative that the list of products are updated. This is done in the Products tab of the Application Options window.

IMPORTANT: Many new features in Stat supporting R12.2 rely on the Release Level of the AD record in the list of products for each environment. After successfully starting the Oracle agent, the next step is to update the product list for each R12.2 environment.

Except for the **Active** check box, the Products tab is read-only. It displays a list of all the products contained in the selected environment. When you first define an environment, or when you install new Oracle Applications products to a particular environment, you should update the environment's product list. To do this, click **Update Products**. This sends a request to the Stat Oracle Agent, which updates the list with any fully installed, shared, or custom products it finds.

NOTE: You can also update the products list of an environment in the Products tab of the Oracle Application Configuration window. For more information, see Updating Products on page 91.

Copying Oracle Applications Environments

If you need to define an Oracle Applications environment that closely resembles an existing Oracle Applications environment, you can save time by copying the definition of the existing environment and editing the copy as needed. When you copy an Oracle Applications environment, all the information gets copied over, including server definitions and approval lists.

To copy an Oracle Application environment definition:

1 In the Oracle Application Environment Connection Maintenance window, select the environment definition you want to copy. Then click **Copy**.

Stat prompts you to specify an environment code and short description.

2 Specify the environment code and short description. Then click **OK**.

3 Edit the new Oracle Application environment definition as needed.

Generic Application Connection Maintenance

The GenApps Environment Connection Maintenance table defines the generic (non-PeopleSoft and non-Oracle Applications) application environments connected to Stat. The table closely resembles the connection maintenance tables for PeopleSoft and Oracle Applications, and many of the maintenance procedures are the same. Within the definition for each environment is the information Stat needs to connect to it.

Connection security for generic applications is controlled by the following user class rights:

- Generic App. Connection - Add
- Generic App. Connection - Edit

The GenApps Environment Connection Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Generic Application Connect.**

Value	Description
Active	If selected, indicates that this environment is available for selection
Environment Cd (Key Value)	A 1-10 character code which uniquely identifies the environment
Description (Required Value)	A 1-35 character description of the environment.
Data Obj Version	The version number of the generic application, as defined in the Data Objects Maintenance table. Select a value in this field only if you plan on using Stat to manage data objects within this environment.
Req. Migr. Approval	If selected, indicates that Archive sets cannot be migrated into the environment without migration approval
DBMS	Name of the APPS database account holder
Database Name	The name of the environment (database instance). Options include Oracle, Microsoft SQL Server, and N/A.
DB User ID (SQL Server Only)	The SQL Server user ID for the schema owner. The default is “sysadm.”
DB Password (SQL Server Only)	The password for the DB User ID
Database Server	The name of the database server housing the generic application repository. Format for this entry is DBMS-specific. **NOTE:** If the database is running on a SQL Server instance, the format must be “host name\instance name”
Srv Login ID	The login ID used for Stat login to the environment. Not used by ODBC.
Server Password	The password associated with the Srv Logon ID
Host Name	Name of the machine hosting the database **NOTE:** Required value for the Stat Central Agent.
Service Name	For generic applications running on Oracle, the listener service of the database. Used by the Stat Central Agent to establish JDBC connections to the Oracle database. **NOTE:** Required value for the Stat Central Agent.
DB Listener Port	Port number for the database listener. **NOTE:** Required value for the Stat Central Agent.
Use Tns	For RAC Oracle databases, configures Stat to invoke TNS
Tns Entry	The full description as it appears in the tnsnames.ora file with no line breaks or carriage returns
Other Database Parameters	Additional environment-specific parameters, if needed
Unicode DB	If selected, indicates the database is Unicode
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

Testing Environment Connections

After defining an environment in the maintenance table, you can make sure that you have entered all the information correctly by clicking **Test Connection**. This makes Stat establish a connection to the newly defined environment. If successful, Stat immediately disconnects from the environment and displays a “Connection Successful” message. If Stat is unable to connect, it displays an error message.

You can also test connections to multiple databases simultaneously. To test multiple connections, hold the <Ctrl> or <Shift> keys and select the databases you want to test. Then click **Test Selected**. Stat attempts to establish a connection to each database and reports its results in the Database Test Connect window

Note that when you test a single environment, Stat does not validate the values specified in the fields **Host Name, Service Name**, or **DB Listener Port**. If any of these fields are not configured properly, the Stat Central Agent will log an error when the user attempts to migrate an object to or from the environment. When you test multiple connections, however, Stat does test both client and agent connections, including **Host Name**, **Service Name**, **DB Listener Port** or (in the case of Oracle-based environments) **TNS Entry**.

NOTE: When testing environment connections in the Stat Web Client, Stat Web attempts to connect using the Host, Port, Service Name, and TNS Entry values specified in the Stat maintenance tables for each particular environment. If there is no TNS Entry value specified for an environment, it uses the Host/Port/Service Name values. If a TNS Entry value is specified, it uses that value and disregards the others.

Inactivating Generic Application Environments

To inactivate an environment, de-select **Active**. Stat displays a warning message if the environment is currently part of a migration path.

CAUTION: Be careful inactivating environments that are part of migration paths. Objects in inactive environments cannot be archived or migrated.

Managing Source File Locations by Environment

After defining an environment, the next step is to specify the source file locations for the file types defined for that environment. For each file type, you can specify an unlimited number of source file locations. When Stat creates an archive set that includes a file object from that environment, it searches for the file in the first location you specified (Path ID = 1). If the file is not there, Stat searches in the second location, and so on. For each type of file that you plan to archive from or migrate to a particular environment, you must define at least one source file location.

To define source file locations by environment, select the environment in the Generic Application Environment Connection Maintenance window and click **File Locations**. This opens the Stat File Locations window, which displays a list of all the active generic application file types defined in Stat. For each file type, you can specify as many source file locations as you want. Source files can be located on different servers, or they can be on the same server but in different directories.

NOTE: You can also specify source file locations by file type. For more information, see Object Type Maintenance on page 60.

To define source file locations for an environment:

1. Click **New**.
2. In the **File Type** field, select the file type for which you want to define a location.

   Stat assigns a unique ID number to each file location you define per file type and displays the number in the **Path ID** field. This number determines the order that the file location is searched during the file archive process. The path with the ID 1 is searched first, and so on.

3 In the **File Server** field, select the server that the file directory is on.

4 In the **File Path** field enter the path of the file location starting after the predefined server's root or home path.

5 (Optional) Select **Default Path** if you want this to be the file type's default source file location.

This is where Stat will copy file objects of the selected type during a migration. Each file type must have one of its source file locations designated as the default.

6 Click **Test Connections**.

See the section, Testing File Locations, Servers, and Default Directory Locations on page 79 for more information.

7 Define additional file locations as needed. Then save your changes by clicking either **Apply** or **OK**.

Setting Up Migration Approval Lists

If an environment requires the approval of certain users before an archive set can be migrated into it, you can specify who these users are in the Migration Approval List tab. To open this window, select the environment and click **App Options** in the Generic Application Connection Maintenance table. Stat activates this tab only if the **Req. Migr. Approval** option has been selected for the environment.

When setting up a migration approval list, you can include different approver groups, including individual users and entire user classes or a combination of the two. The approval of any user or user class that you add to a list can be either required or optional.

Approval requirements that involve multiple approver groups or that can be satisfied in more than one way are defined using AND and OR operators. As you add approver groups using AND and OR operators, Stat displays the list as a tree structure and in the form of a SQL statement at the bottom of the window.

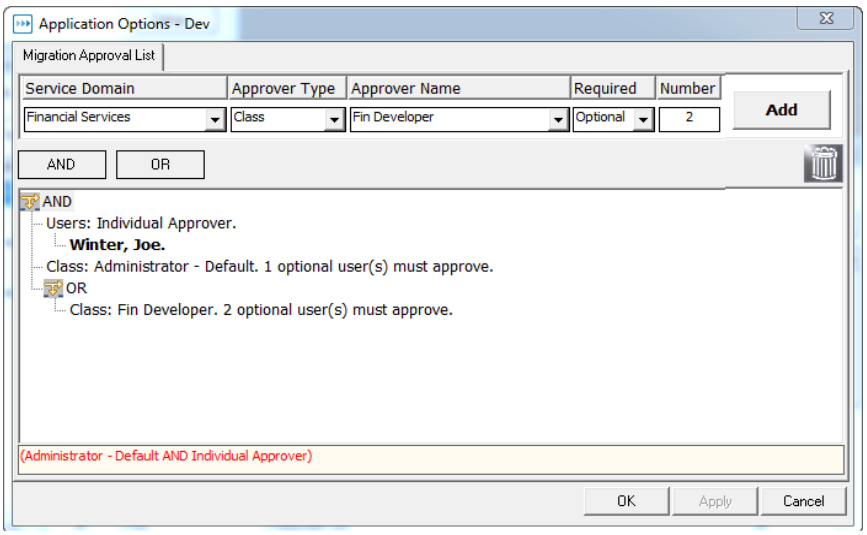
For example, let's say a migration to a particular environment in the Financial Services service domain can be approved in one of two ways:

- By a certain user AND at least one user in the Administrator user class

  OR

- By at least two users in the Fin Developer user class

In this case, your approval list would look like this:



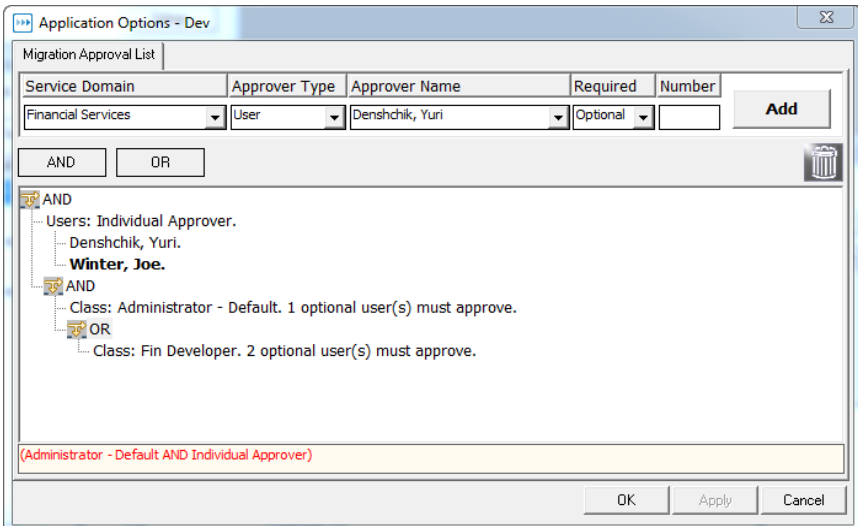
To further illustrate, let's say that the migration must be approved by:

- Two users, one of whom is required

  AND

- At least one user in the Administrator user class OR at least two users in the Fin Developer user class.

In this case, the approval list would look like this:



NOTE: Migration approval lists closely resemble status transfer approval lists and the procedures for defining them are much the same. For more information on migration approval lists, see Setting Up Transfer Approval Lists on page 156.

It is recommended that before setting up a migration approval list, you have a basic idea of what approver groups (users and user classes) you want involved in the approval process as well as the relationships between these groups, which you define using AND and OR operators. For example, if the approval of one or more approver groups are required, you would begin the approval list with the AND operator. If, however, the approval of only one of two or more approver groups are required, you would begin the list with the OR operator.

To set up a migration approval list:

1 Do one of the following:

- Click **AND** if the approval of one or more approver groups are required
- Click **OR** if the approval of one of two or more approver groups are required

The operator icon is added to the approval list diagram.

2 Click on the AND or OR operator icon you just added.

TIP: The icon background appears blue when selected and changes to gray when other fields or action buttons are activated. As long as the background of the operator icon is blue or gray, then approver groups and other operators can be attached to the operator.

3 In the **Service Domain** field, select the service domain that you plan to associate the environment with in the Generic Application Migration Path Maintenance table.

4 In the **Approver Type** field, select the approver group you want to add to the list.

Options include **User** and **User Class**.

When adding approvers, be aware of the following:

- Although you can add any user or class to an approval list, be aware that only users that have access to an environment and the selected service domain (as defined in the User Maintenance table) will be able to approve a migration into that environment or receive email notifications regarding their pending approval. If an approver does not have access to the environment, the migration cannot be approved until either the user is granted access to the environment or the migration's approval requirements are overridden by another user with proper security rights. For this reason, it is recommended that you first verify users have access to a particular environment and service domain before adding them to an approval list.

- Adding individual users to approval lists could create problems if those same users are later inactivated or have their service domain and environment access restricted. For this reason, it is recommended that you add user classes to approval lists rather than individual users whenever possible.
- Users assigned to a migration approval list must have the user class rights to operate in the same change management module in which the migration takes place. Also, you can assign user class rights that enable users to migrate objects regardless of approval status and also to approve migrations on the behalf of other users.

5 In the **Approver Name** field, select the name of the user or user class you want to add.

6 In the **Required** field, select **Required** if the approval is required or **Optional** if it is not required.

The **Required** option means that the individual user and every member of the user class must approve the migration. **Optional** means that the individual user's approval is not required, whereas for user classes, it means that the approval of only a specified minimum number of users within that class is required.

7 If you selected **User Class** in the **Approver Type** field and **Optional** in the **Required** field, specify the minimum number of users in that class who must approve the migration in the **Number** field.

8 Click **Add**.

The approver is added to the tree structure under its approver group label and the initial AND or OR operator. Required approvers are displayed in bold.

At this point, how you proceed depends on the different approver groups you want to add to the list and how you want to define the relationships between these groups using AND and OR operators.

9 (Optional) Do the following to add additional AND or OR operators to your approval list:

a Depending on the relationship between approver groups in your list, select the operator icon to which you want to attach additional operators.

b Click **AND** or **OR**.

c Repeat as necessary to add more operator icons to the approval diagram.

10 (Optional) To add additional user classes, select the appropriate operator icon in the approval diagram and repeat steps 4 through 8.

When you the first add an individual user to an approval list, Stat automatically creates the ad hoc group "users" in the approval diagram and attaches it to the appropriate operator icon. All subsequent users you add to the list must belong to this group.

TIP: In a scenario in which you want to create approval relationships between multiple user approver groups, you may consider adding users to new user classes or queues created expressly for this purpose.

11 (Optional) To add additional users, select the "users" group and repeat steps 4 through 8.

12 (Optional) Do any of the following to edit the diagram as needed:

- To change an operator from AND to OR or from OR to AND, right-click on the icon.
- To change the Required status of an approver, right click on it in the diagram. This changes required user classes to optional with 1 minimum user approval.
- To change the minimum number of user approvals in an optional user class, double-click on the group label and specify the minimum number of user approvals you want.
- To move approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to a different operator icon in the diagram.
- To delete approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to the Trash Can icon.

13 Click **OK** or **Apply**.

Copying Generic Application Environments

If you need to define a generic application environment that closely resembles an existing generic application environment, you can save time by copying the definition of the existing environment and editing the copy as needed. When you copy a generic application environment, all the information gets copied over, including file locations and migration approval lists.

To copy a generic application environment definition:

1. In the Generic Application Environment Connection Maintenance window, select the environment definition you want to copy. Then click **Copy**.

   Stat prompts you to specify an environment code and short description.
2. Specify the environment code and short description. Then click **OK**.
3. Edit the new generic application environment definition as needed.

Schema Object Parameters Maintenance

Oracle and SQL Server database schema objects include a set of predefined true/false parameters that are executed before the definition of the object is captured in Stat. You can change the true/false values of these parameters in the Schema Object Parameters Maintenance table.

The ability to change default schema object parameter values is controlled by the following user class right:

- Schema Object Parameters - Edit

The Schema Object Parameters Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Schema Object Parameters**.

The Schema Object Parameters Maintenance table lists each parameter by DDL type and name. The Default Value column indicates whether a particular parameter is true or false by default. To change the value of a parameter, select its corresponding check box in the Param Value column to make it true, or de-select it to make it false. Then click **OK** or **Apply**.

Data Object Maintenance

Data objects are user-defined or third party data sets developed for specific application environments. You can configure Stat to support data objects by defining in the Data Object Maintenance table the tables and table keys that make up the definition of these objects within their native environment. Data objects can be locked, archived, and migrated just like the proprietary objects already supported by Stat.

Data objects are specific to the change management module that they are defined for. This means that data object types supported in one change management module are not supported in the other modules. To avoid confusion, data object types for PeopleSoft, Oracle Applications, and generic applications are defined and maintained in separate tabs on the Data Objects Maintenance window. The maintenance procedures for all three are the same.

NOTE: Data objects are currently supported only in environments running on Oracle.

The Data Object Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Data Objects**.

Defining Application Version Numbers

Because data objects are directly associated with a change management module, the first step in defining a data object type is to associate it with its module, and if that module does not already have one, to assign it a version number. This allows Stat to maintain an archive of the object definition in the event you upgrade your application environments and modify your data object definitions at some point in the future. For example, let's say you upgrade from PeopleSoft 8.14 to 8.17 and need to add a table to the definition of one of your data objects. By archiving object definitions according to application version number, you can maintain different versions of the same object and roll back to previous versions as necessary.

To define an application version number:

1. In the Data Object Version Number tab, click **New**.
2. In the **Module** field, select the object type's change management module.

   Options include **PeopleSoft**, **Oracle Applications**, and **Generic Applications**.
3. In the **Appl Number** field type a number or code that uniquely identifies the version of the application.
4. (Optional) In the **Description** field type a brief description of the application version.
5. Click **OK** or **Apply**.

Defining Data Objects

After defining any necessary application version numbers, you can define the data object type. The Data Object Maintenance window features three tabs that correspond to the change management modules featured in Stat.

Naming Data Objects

To begin defining a data object type, the name of the object type must be saved in the Stat Repository.

To name a data object type:

1. Select the tab for the change management module tab that the data object is associated with.

   Each tab displays the names of the data object types that have been defined for that change management module.
2. Click **New**.
3. In the **Object Name** field type the name of the object.
4. Click **OK** or **Apply**.

   This saves the object type definition in the Stat Repository and activates the **Edit** button. At this point, you can complete the definition of the object type by specifying its application version number, identifiers, and data tables.

The Edit Data Objects Window

You complete the definition of a new data object, or edit the definition of an existing one, in the Edit Data Objects window. This window is divided into three sections:

- The Version section displays all the module-specific application version numbers defined on the first tab of the maintenance window. For each application version number, you can define a different definition for the data object type.
- The Identifiers section displays the name and type of each table field that uniquely identifies a data object type

- The Tables Definition section displays each data table that defines the object type, including the SQL Where Clause

If more than one application version number has been defined, select the version number you want in the Versions section to view the object definition associated with that version.

You can edit any active object definition associated with an application version number. When defining a new data object type or a new version of an existing one, the first step is to select the application version number you want to associate with the object type.

Defining Object Identifiers

You need to specify the table fields that uniquely identify each object of this object type. This is done in the Identifiers section of the Edit Data Objects window. The identifying table fields are used when specifying the SQL Where Clause in the table definitions. Each field defined as an identifier must be in the table that is defined with sequence 1. It must be also part of that table's Where Clause.

To define data object identifiers:

1. In the Versions section, select the application version number you want to associate with the data object type.
2. In the Identifiers section, type the name of the table field that uniquely identifies the object in the **Identifier** Field of row A.
3. In the **Type** field, select the field type.

   Options include **Number**, **Character**, and **String**.
4. Repeat steps 2 and 3 for each table field that uniquely identifies the object.

   You can specify up to 7 identifier fields.
5. Click **OK** or **Apply**.

Defining Tables

You must define at least one table for Stat to save the definition of the data object type. The first table you define is considered the parent table which holds each unique object of this object type. Its Where Clause must use each Identifier. When users add data objects to their CSRs, Stat obtains the list of objects for the selected object type from this table.

To define a table:

1. Click **New**.

   Stat activates a new row in the Table definitions section. By default, the Where Clause displayed in the **SQL Where Clause** field uses each identifier specified in the Identifiers section. You can modify this Clause as needed, but the first table must contain each identifier. Subsequent tables must contain at least one identifier.
2. Type the name of the table in the **Table Name** field.

   The name of the table should begin with the schema, if applicable.

> **CAUTION: For Oracle Applications users, make sure the name of the table is preceded by the name of its schema, such as GL, AP, AR. For example, the table RA_CUSTOMERS belongs to the AR schema, which means in the Table Name field you would enter "AR.RA_CUSTOMERS."**

3. (Optional) Modify the Where Clause in the **SQL Where Clause** field as needed.
4. (Optional) In the **Table Keys** field specify the fields that uniquely identify the table.

   This information is used when performing an object comparison between two versions of the same data object.

   At this point, the names of table columns and blobs (if any) need to be entered in the **List of Columns** and **Blob** fields, respectively. You can do this manually of you plan on running the SQL script outside of Stat, or

you can have this information entered automatically by running the SQL script in the Create Archive Table window.

5 Do one of the following:

- Enter the names of the table columns and blobs in the **List of Columns** and **Blob** fields, respectively. When finished, click **Apply**.

  Do this if you plan on running the SQL Script outside of Stat.

- Click **Create Tables**.

  This opens the Create Stat Archive Table window. Here you specify the tablespace in the Stat Repository where you want to maintain an archive of the table definition and the application environment that contains the original SQL script. If you want to write the table definition to the Stat Repository, you can do so by running the SQL script.

To create a table:

1 (Optional) Specify a different tablespace in the **Tablespace** field.

By default, an archive of the table definition is written to the STSWAT tablespace in the Stat Repository.

2 In the **Environment** field, select the environment that contains the SQL Script for the table.

When you select the environment, the SQL Script is displayed in the SQL section of the window.

3 If you want to write the table definition to the Stat Repository, click **Run SQL**.

The Status section displays the results of the SQL script. The values specified in the SQL Script are automatically entered in the **List of Columns** and **Blob** fields of the Edit Object window. Any previous values are overwritten.

4 (Optional) Click **Export** if you want to save the SQL Script to a directory outside of Stat.

5 When finished, click **Close**. Then in the Edit Data Objects window, click **Apply**.

Copying Data Object Definitions

You can save time by copying the definition of a data object to other application versions. You can also use the copy function to overwrite data objects defined for a particular application version, so long as the data objects of that version are not already associated with a CSR. To maintain referential integrity, Stat does not permit data objects already associated with CSRs to be modified.

To copy a data object definition:

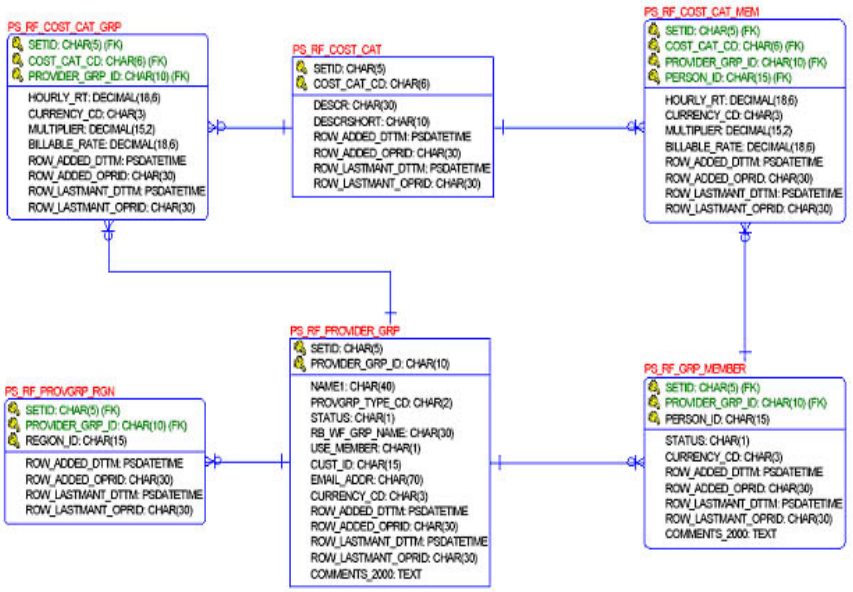
1 In the Edit window, click **Copy**.

This opens the Versions window, which displays a list of application versions to which you can copy the data object definition.

2 In the Versions window, select the application version you want to copy the definition to. Then click **OK**.

Data Object Example

The following example is taken from PeopleSoft and is meant to illustrate the process of defining data object types in Stat. In this example, the goal is to configure Stat to support Provider Group data objects, which can then be archived and migrated from the CRM Field Service module to a PeopleSoft CRM environment. We will use the PeopleSoft-delivered Data Model to define our Provider Group data object type. The Provider Group tables and identifiers are detailed in the diagram below.



Provider Groups are associated with PeopleSoft version 8.40. Before defining the Provider Group data object type, the first step is to associate it with the appropriate application version number. To lock, archive, and migrate Provider Group data objects, make sure all the PeopleSoft environments in the CSR's migration path are defined in the PeopleSoft Environment Connection Maintenance table with the Data Object Version '8.40'.

The parent table for Provider Groups is PS_RF_PROVIDER_GRP. Each unique combination of values for the fields SETID and PROVIDER_GRP_ID represents a Provider Group.

Identifiers

- Identifiers are the fields whose combined values make each object of this type unique. In our example, these fields are SETID and PROVIDER_GRP_ID.
- Each Identifier field must be in the parent table. This is because when adding an object of this type to a CSR, Stat retrieves the object list by selecting from this table all distinct rows for the identifier fields.
- The Identifier fields do not have to be in any of the other tables in the Data Object definition.

Tables

- The first table you define is the Parent table (Seq value =1). This does not need to be a true "parent" table in the sense of its database definition. Stat obtains from this table the list of objects that the user picks from when adding objects to a CSR. It is usually the parent table but it does not need to be.
- All the tables listed in the Data Model contain data that must be included in the definition of the Provider Group data object type. This data needs to be archived/migrated when archiving/migrating an object of this type.
- If the tables do have a parent-child relationship, the parent table must be listed before the child tables to ensure that its rows are processed before the rows of the child tables.
- When archiving/migrating, Stat pulls the data from each table using the where clause that you define in the **SQL Where Clause** fields.
- The tables do not have to be related but you do need to be able to pull data from the table using the where clause constraints listed below.

Where Clauses

- The where clause can have hard coded values (e.g., WHERE STATUS = 'A' AND EFFDT > 01-01-2000. The date format must match your RDBMS required format).
- The where clause can have variables that are filled in during archiving/migrating using any of the identifier fields (e.g., WHERE SETID = %A%, or WHERE GRP_ID = %B%. In this case %B% is replace by the object's value for the PROVIDER_GRP_ID field since 'B' is its identifier ID even though the constraint is on the GRP_ID field).
- If the where clause contains identifier variables (e.g., %A%, %B%), Stat replaces the variables with the object's field values during archiving/migrating (e.g., if you add to your CSR the Provider Group that has SETID = 'CRM01' and PROVIDER_GRP_ID = 'APLW,' when you archive this object the where clauses will replace %A% with 'CRM01' and %B% with 'APLW').
- The where clause can have embedded select statements (e.g., WHERE GRP_ID IN (SELECT PROVIDER_GRP_ID FROM PS_RF_PROVIDER_GRP WHERE SETID = %A%)).
- The tables do not have to be related but you do need to be able to pull data from the table using the where clause constraints listed above.
- If the tables do have a parent-child relationship, the parent table must be listed before the child tables to ensure that its rows are processed before the rows of the child tables.

The Provider Croup tables, along with their Where Clauses, include:

Table	Where Clause
PS_RF_PROVIDER_GRP (Parent Table)	SETID = %A% AND PROVIDER_GRP_ID = %B%
PS_RF_GRP_MEMBER	SETID = %A% AND PROVIDER_GRP_ID = %B%
PS_RF_PROVGRP_RGN	SETID = %A% AND PROVIDER_GRP_ID = %B%
PS_RF_COST_CAT_GRP	SETID = %A% AND PROVIDER_GRP_ID = %B%
PS_RF_COST_CAT	SETID = %A% AND COST_CAT_CD = (SELECT COST_CAT_CD FROM PS_RF_COST_CAT_GRP WHERE SETID = %A% AND PROVIDER_GRP_ID = %B%)
PS_RF_COST_CAT_MEM	SETID = %A% AND PROVIDER_GRP_ID = %B%

All the tables, where clauses, table keys, columns, and blobs in the Data Model must be entered in the Tables Definition section of the Edit Data Objects window.

The PS_RF_PROVIDER_GRP and PS_RF_GRP_MEMBER tables contain Blob fields. This information need to be defined in the **Blob Column** fields.

The next step is to create the Stat Archive table, which contains the object archives.

At this point, Provider Group data objects are fully defined in Stat and now can be added to a CSR, archived, and migrated.

PeopleSoft Search Configurations

The PeopleSoft Search Configuration table specifies the PeopleSoft environments from which customer, department or country information can be retrieved and inserted into the Stat Repository. Information can be retrieved from PeopleSoft employee, department or country views.

PeopleSoft security is controlled by the following user class rights:

- PeopleSoft Search Cfg - Add
- PeopleSoft Search Cfg - Change

The PeopleSoft Search Configurations table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | PeopleSoft Srch Configs**.

Value	Description
Active	Indicates if this record is available for selection
PeopleSoft Database (Required Value)	The PeopleSoft environment that contains the customer information
Description (Required Value)	Description of the configuration or environment
Search View Name (Required Value)	An 18-character field that contains the name of a table or view in PeopleSoft against which the search is conducted. See the next section, Creating Tables and Views on page 112.
Type (Required Value)	Indicates the type of PeopleSoft view that is the basis for the search. Options included **Employee**, **Department** or **Country**.
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

Creating Tables and Views

A table or view must be created in each PeopleSoft environment in which you want to conduct searches. For example, in the case of an employee-based search, the view must contain the following fields:

EMPLID	COUNTRY
NAME	SSN
ADDRESS 1	COMMENTS
ADDRESS 2	COMPANY
ADDRESS 3	PAYGROUP
ADDRESS 4	DEPTID
CITY	DEPTNAME
STATE	WORK_PHONE
ZIP	WORK_PHONE_EXT
EMAIL_ADDR	EMAIL_ADDRESS2
CUSTOM1	CUSTOM2
SIN	

For employee-based searches, Stat parses the NAME column based on the original PeopleSoft format of Employee table Name column: LastName, FirstName.

In addition, for any column, you may insert a space instead of a value, or indicate a default value. You may wish to populate the comment, custom1 or custom2 fields from other employee related fields.

NOTE: Newer versions of the PeopleTools employee table (8.48 and higher) store the Name field as FirstName LastName, but also have a separate FirstName and LastName column. For those versions of PeopleTools the view must concatenate FirstName and LastName as a.LAST_NAME || ',' ||a.FIRST_NAME.

The following are examples of views. The first example below displays an employee view formatted for PeopleTools versions prior to 8.48, while the second example displays the format for PeopleTools versions 8.48 and higher. In both examples the phone extension, SSN, SIN and second email address values are not being

populated from PeopleSoft. The employee's job title is being placed into the comment field. This is configurable based on your site needs.

Employee View Example (Pre PeopleTools Version 8.48)

```
CREATE OR REPLACE FORCE VIEW sysprod.ps_stat_cust_vw
(emplid,
NAME,
deptid,
deptname,
ssn,
SIN,
work_phone,
work_phone_ext,
address1,
address2,
address3,
address4,
city,
state,
zip,
country,
email_addr,
email_address2,
comments,
custom1,
custom2,
company,
paygroup
)
AS
SELECT a.emplid, a.NAME,, a.deptid, a.deptname, a.ssn, a.SIN,
       a.work_phone,' ', a.address1, a.address2, a.address3, a.address4, a.city,
       a.state, a.postal, a.country, b.email_addr, ' ', a.jobtitle, ' ', ' ',
       a.company, a.paygroup
FROM ps_employees a, ps_email_addresses b
WHERE a.emplid = b.emplid
```

Employee View Example (PeopleTools Version 8.48 and Higher)

```
CREATE OR REPLACE FORCE VIEW sysprod.ps_stat_cust_vw
(emplid,
NAME,
deptid,
deptname,
ssn,
SIN,
work_phone,
work_phone_ext,
address1,
address2,
address3,
address4,
city,
state,
zip,
country,
```

```
email_addr,
email_address2,
comments,
custom1,
custom2,
company,
paygroup
)
AS
SELECT a.emplid, a.LAST_NAME || ',' ||a.FIRST_NAME, a.deptid, a.deptname, a.ssn,
a.SIN,
       a.work_phone,' ', a.address1, a.address2, a.address3, a.address4, a.city,
       a.state, a.postal, a.country, b.email_addr, ' ', a.jobtitle, ' ', ' ',
       a.company, a.paygroup
FROM ps_employees a, ps_email_addresses b
WHERE a.emplid = b.emplid
```

Country View Example

```
create or replace force view ps_stat_country_vw
(COUNTRY,
DESCR,
DESCRSHORT,
ADDR1_LBL,
ADDR2_LBL,
ADDR3_LBL,
ADDR4_LBL,
CITY_LBL,
STATE_LBL,
POSTAL_LBL,
CUSTOM1_LBL,
CUSTOM2_LBL,
COMMENT_LBL  )

as
select a.country,
a.descr,
a.descrshort,
a.addr1_lbl,
a.addr2_lbl,
a.addr3_lbl,
a.addr4_lbl,
a.city_lbl,
a.state_lbl,
a.postal_lbl,
a.country_2char,
' ',
' '

from ps_country_tbl a
```

Department View Example

```
CREATE OR REPLACE FORCE VIEW ps_stat_dept_vw (deptid, descr)
AS
   SELECT a.deptid, a.descr
     FROM ps_dept_tbl a
    WHERE a.setid = 'CDN';
```

Exclusions

You can exclude certain companies, departments, or pay groups from the search results.

To define an employee search exclusion:

1. In the PeopleSoft Employee Search Configurations window, select the environment you want and click **Exclusions**.

   Stat opens the Employee Search Exclusions window.

2. Click **New**.
3. In the **Exclusion Type** field, select the type of entity you want to exclude.

   Options include **Company**, **Dept ID**, and **Pay Group**.

4. In the **Value** field, enter a 1-10 character code which identifies a valid department, company, or pay group in the PeopleSoft environment.
5. Click **OK** to save your work.

Stat Report Definition Maintenance

The Stat Report Definition Maintenance table defines the security levels of all the reports available in the Stat Report Library. It also defines how they are presented and described in the Stat Report Wizard.

The Stat Report Library includes all predefined reports, and any custom reports defined by users. With a predefined report type, you can change the security level and its description in the Stat Report Library, but you cannot directly modify the report format itself.

Stat report security is controlled by the user class right, Stat Report Definition - Edit. There is no add right.

The Stat Report Definition Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | Stat Reports**.

Value	Description
Available	Indicates if this report type is available in Stat
Custom	Indicates if the report type is user-defined
Description (Required Value)	A brief description of the report. This description is displayed in the report list of the Report Library.
Long Description (Required Value)	A longer description of the report. This is displayed just below the layout preview in the Report Library when a report is selected from the list.
Category (Required Value)	The order in which the Report is grouped on the report list in the Stat Report Library window.
Presentation (Required Value)	Presentation style of the report; Option include: Bar Graph Cross Tab Excel List Pie Chart Standard **NOTE:** This value only affects how the presentation style of the report is described in the Stat Report Library window. It does not affect the actual presentation style of the report.

Value	Description
Security Level (Required Value)	The security level of the report. In order for a user to open a report, their report security level (defined on the Stat users table) must be greater than or equal to this value. Valid values are 0 - 99, with 0 equaling minimum security and 99 equaling maximum security.
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

Editing Reports

If at any time you want to modify the definition of a report or upload an updated .jrxml file, select it in the maintenance window and click **Edit**. This opens the Edit Report window where you can modify the report as needed. Only the fields that can be modified are enabled. For predefined reports, you can edit the short and long description and security level.

If desired, you can also select the **Inactive** option if you do not wish the report to display on the Report Wizard list.

Adding Custom Reports

All Stat reports are defined by corresponding .jrxml files. Custom reports are created by formatting a .jrxml file using the 3rd party reporting tool Jaspersoft Studio. You can create a report file from scratch, or you use a copy of an existing file as a starting point. For more information on creating report files, see Appendix: Custom Report Files on page 319.

After you have defined the .jrxml file that is the basis for your custom report, you can add it to the Stat Report Library.

To add a custom report:

1. Click **New**.

   This opens the Define New Custom Report window.

2. Click **Load** and select the custom report .jrxml file you want use as the basis for the report.

   The file name is displayed in the **Report** field without the extension. This file name must be unique. This is the name that the agent searched for to compile the report.

3. Enter a short description of up to 40 characters.

   This description is displayed in the Stat Report Library.

4. Enter a long description of up to 250 characters.

   This description appears in the Presentation Preview and can give the user an idea of what data will appear on the report or when to use this report.

5. Select a report category or enter a new category.

   You can add a custom report to a predefined category, or you can add it to a new category that you create.

6. Select a report format type.

   The format is a graphical representation of what the report will look like displayed in the Presentation Previews.

7. Set the security level for the report (1-99 with 1 being the least secure).

8. Click **OK**.

Stat adds the report file information to the Stat Repository and loads the report to <stat_home>report\custom\format on the Stat Central Agent file structure.

Turning off the Emailing of Blank Reports

Stat reports are configured to bring up a blank page with a report title if there is no data. This is intended to demonstrate to the user that the report actually ran. Some sites however may not want Stat to email blank reports.

Stat report files (.jrxml files) are stored on the Stat Central agent under Stat_home/report/%category%/format. The subfolder they are stored under is named the same as the Report Category drop down listing on the Stat Report Wizard. Under each category subfolder the .jrxml files are located in the /format folder.

Each report has a file name that starts with dw_ and has a .jrxml extension. The linkage between the file name and the report name is in the STAT_REPORT_DEFN table.

Select DESCR, DW_NAME, CATEGORY from STAT_REPORT_DEFN where DESCR like '%Report name from Stat Report Wizard%' will give you the file name that needs to be modified.

As with customized reports, if you modify the .jrxml file in situ it may be overridden the next time you upgrade Stat. If this is a concern, then follow the procedure for creating a custom report which places a copy of the .jrxml file in the stat_home/report/custom directory/format folder and add the custom report to the Stat repository.

To turn off the emailing of blank reports:

1. Open the .jrxml file with Jaspersoft Studio.
2. Right click on the report name under Outline view and choose **Show Properties**.
3. In Report Properties View, open the Advanced tab, scroll down to the option **When No Data** and change the value from **All Sections, No Detail** to **No Pages**.
4. Close the Properties Window and save the report.
5. If there is a corresponding file name with a .jasper extension in the folder you save the file in, delete the .jasper file.

   This is a compiled report file. The Central agent will recreated the .jasper file with the new properties the next time the report is run.
6. Run the scheduled report in Stat.

   If there is no data on the report the Central agent will log a message:

   “Job ID:xxx generated empty report. Email has been skipped.”

Version Control Management Connection Maintenance

You can integrate Stat with your 3rd party version control management (VCM) system. This allows you to save your file objects from a VCM repository directly into Stat to control the process and the migration of the objects. Currently Stat supports the following VCM platforms: SVN, PVCS, Perforce, and CVS.

VCM Maintenance security is controlled by the following user class rights:

- 3rd Party VCM Connection - Add

- 3rd Party VCM Connection - Change

IMPORTANT: Before connecting to a VCM system, be aware of the following:

- All Stat VCM functionality is performed by the Stat Central Agent. Except for P4 and TFS, this means that for the connection to be established the machine hosting the Stat Central Agent must have a client copy of the VCM software installed and that the Stat Central Agent must be running.
- For Stat to archive file objects from a VCM repository, the subdirectories where the object types reside in the repository must match the subdirectories in the source environments. For example, if *sql files reside in a .../*admin/sql* subdirectory in the source environment, the sql files in the VCM repository must also reside in a .../*admin/sql* directory.

The 3rd Party Version Control Connection maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | General | VCM Connect**.

To connect to a VCM repository:

1. In the 3rd Party Version Control Connection maintenance table, click **New**.
2. Specify unique code which identifies the VCM repository.
3. Enter a description of the VCM repository.
4. Select the type of VCM platform you are connecting to.

   Options include **CVS**, **PVCS**, **SVN**, **P4**, **GIT**, and **TFS**.

   After defining the VCM repository, you must define the required connection parameter values that allows Stat to connect to the VCM repository.

   Click **Apply** to save your work.
5. Click **Setup**.

   This displays the VCM Connection Setup window where you specify the connection parameter values. The list of parameters varies depending on the type of VCM platform you are connecting to.
6. Enter the parameter values required to establish a connection to the VCM repository.

   See the following tables for a description of each parameter. Which parameter values are required will depend on the configuration details of your VCM repository.

CVS Parameters

Parameter	Description
CVS_CONNECTION_TYPE	CVS connection type
CVS_HOST	CVS host machine
CVS_MODULE	CVS module
CVS_PASSWORD	CVS password
CVS_PORT	CVS host port
CVS_REPOSITORY_PATH	CVS root directory
CVS_RSH	CVS protocol used when connection type is ext
CVS_TAG_BRANCH	CVS tag or branch
CVS_TAG_BRANCH_FILE	CVS entity filename (full path) to use for retrieving list of tag/branch labels
CVS_USERNAME	CVS username

PVCS Parameters

Parameter	Description
PVCS_LABEL	PVCS revision label
PVCS_LABEL_FILE	PVCS entity filename (full path) to use for retrieving list of revision labels
PVCS_PASSWORD	PVCS password
PVCS_PROJECT_DATABASE	PVCS project database
PVCS_PROJECT_PATH	PVCS current project
PVCS_PROMO_GROUP	PVCS use label for promotional group
PVCS_REPOSITORY_PATH	PVCS entity folder
PVCS_USERNAME	PVCS username

P4 Parameters

Parameter	Description
P4_CLIENT	Perforce client/workstation
P4_DEPOT	Perforce depot path (ex. //depot)
P4_PASSWORD	Perforce password
P4_PORT	Perforce host port
P4_PROJECT_PATH	Perforce project path relative to depot (ex. //depot/project1)
P4_REVISION	Perforce revision (if left blank, latest revision is used)
P4_REVISION_USING	Perforce revision can be retrieved using revision, label, or changelist
P4_SERVER	Perforce server hostname
P4_TICKET_PATH	Perforce ticket path (ex. c:\\p4tickets.txt)
P4_USERNAME	Perforce username

SVN Parameters

Parameter	Description
SVN_ALT_CONFIG_DIR	SVN configuration directory
SVN_CONNECTION_TYPE	SVN connection type
SVN_HOST	SVN host machine
SVN_PASSWORD	SVN password
SVN_PORT	SVN host port
SVN_REPOSITORY_PATH	SVN repository directory
SVN_REVISION	SVN revision
SVN_USERNAME	SVN username

Git Parameters

Parameter	Description
GIT_CONNECTION_TYPE	GIT repository connection type (ssh://, http://, https://)
GIT_HOST	Hostname of the repository
GIT_PORT	Port number (Optional)
GIT_REPOSITORY_PATH	Path to the remote repository
IT_PROJECT_PATH	An optional path to a directory under the main repository (Optional)
GGIT_TAG_BRANCH	Specific branch or tag. If left blank, objects are pulled from master branch. (Optional)
GIT_USERNAME	Username to connect to the repository
GIT_PASSWORD	Password

TFS Parameters

Parameter	Description
TFS_CONNECTION_TYPE	TFS connection types (http or https)
TFS_HOST	Hostname of the machine housing the repository
TFS_PORT	Port number
TFS_COLLECTION	The TFS project collection including the virtual directory, like /tfs/DefaultCollection
TFS_SERVER_PATH	The mapping server folder including $/ and project, like $/Project/folder.
TFS_USERNAME	Usually the network username that has access to the repository
TFS_PASSWORD	Network user password
TFS_HTTP_PROXY_URL	The url to the proxy server including the port, like http://server:9191
TFS_HTTP_PROXY_USERNAME	The proxy server username
TFS_HTTP_PROXY_PASSWORD	The proxy server password

Parameter	Description
TFS_VERSION_USING	Has 3 values: **Label**, **Changeset**, or **LatestVersion**. • By default files are retrieved from the repository by **LatestVersion** (T). • If **Label** is used, files are retrieved from a specific Label in the repository. • If **Changeset** is used, files are retrieved from a specific Change Set (C11 for example)
TFS_VERSION	Used to retrieve from a specific Label or Changeset. • If **TFS_VERSION_USING** is set to **Label**, set **TFS_VERSION** to a specific Label from which files are retrieved. • If **TFS_VERSION_USING** is set to **Changeset**, set **TFS_VERSION** to a specific Change set from which files are retrieved.

IMPORTANT: When users add file objects from a VCM repository to an archive set, a VCM-specific field is displayed in the Archive Set window (**Revision** for SVN and P4, **Tag/Branch** for CVS and Git, **Label** for PVCS, and **Version** for TFS). In this field users can override the default value specified by system administrators by specifying the particular version of the objects they want to add from the VCM repository. If left blank, Stat adds the most recent version of the objects in the repository.

7 Click **Apply**.

8 Click **Test Connect** to make sure that you have entered all the information correctly.

This makes Stat establish a connection to the VCM repository. If successful, Stat immediately disconnects from the repository and displays a “Connection Successful” message. If Stat is unable to connect, it displays an error message.

9 Click **OK**.

5

Service Domain-Specific Maintenance

- Working With Service Domains
- Activity Code Maintenance
- Application Maintenance
- Application Environment Maintenance
- Auto Task Maintenance
- Business Rule Maintenance
- CSR Log Topics Maintenance
- CSR Priority Maintenance
- CSR Type and Status Maintenance
- Customer Priority Maintenance
- Generic Application Migration Path Maintenance
- PeopleSoft Migration Path Maintenance
- Oracle Application Migration Path Maintenance
- Pre and Post Migration Steps
- Release Management Maintenance
- Template Maintenance
- Queue Maintenance
- Workflow Maintenance

Working With Service Domains

Service domain-specific maintenance tables are displayed in standard maintenance windows, which by default display information regarding your default service domain. You can switch to a different service domain by selecting it in the **Domain** field located at the top of each window.

Any value you specify in a service domain maintenance table pertains only to the service domain displayed in the **Domain** field. For example, users working in the Human Resources service domain are not affected by any changes you make to a table pertaining to the Change Control service domain. You can, however, specify the same value for two or more service domains. This is because Stat invisibly prefixes service domain codes to each value, thereby uniquely identifying them in the system. For example, let's say you define a CSR status named "URG" (for urgent) in both the Change Control and the Human Resources service domains; even though they appear the same to users working in both service domains, internally Stat distinguishes them by the code prefixes of their respective service domains, "CHG-URG" and "HR-URG."

User class rights control access to each service domain-specific maintenance table. Since you can have a different user class for each service domain, you may have access to a table for one service domain but not for another. It is recommended that system administrators have user class rights to all tables.

Activity Code Maintenance

The Activity Code Maintenance table defines categories of tasks and auto tasks. Each task must be associated with an activity code.

The use of tasks and activity codes is optional in a Stat implementation.

If you choose not to define activity codes for a service domain, you should not display the Tasks tab on CSRs created within that service domain.

Activity code security is controlled by the following user class rights:

- Activity codes - Add
- Activity codes - Edit

The Activity Code Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Activity Codes**.

Value	Description
Active	Indicates whether the record is activated in Stat
Activity Cd (Key Value)	A 1-10 character code which uniquely identifies the activity
Description (Required Value)	A 1-35 character description of the activity
Comment Req'd	If selected, the user will be required to enter a free text comment at the time the task is marked as completed
Allow Descr Edit	If selected, the user is allowed to change the task description. This is commonly used for a miscellaneous task which allows the user to enter a more appropriate description for the task.
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Application Maintenance

The Application Maintenance table defines the products or facets of your enterprise that can be represented in CSRs. Application codes define available items on the CSR Application drop down list.

Application security is controlled by the following user class rights:

- Applications - Add
- Applications - Edit

The **Application Maintenance** table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Applications**.

Value	Description
Active	If selected, activates the value in stat
Applic Cd (Key Value)	A 5-character code which uniquely identifies the application
Description (Required Value)	A 1-35 character description of the application
Application Tab (Required Value)	The change management tab displayed on the CSR when the application is selected. Options include PeopleSoft, Oracle Applications, Generic Applications, and None.
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Application Environment Maintenance

The Application Environment Maintenance table defines subsystems of an application. Application environment codes are used to further define or describe applications.

Not all applications have environments. Defining application environments is optional; you can define environments for all, some, or none of the applications in a service domain.

Application environment security is controlled by the following user class rights:

- Application Environments - Add
- Application Environments - Edit

The Application Environment Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Application Environments**.

NOTE: For any service domain in which you want to use application environments, be sure to select **Use Appl Env** in the **Service Domain** maintenance table. Otherwise, the **Application Environment** field will be grayed out on CSRs opened in that service domain. For more information, see Service Domain Maintenance on page 54.

Value	Description
Active	If selected, activates the value in stat
Application (Key Value)	Select an application from the list
Env Cd (Key Value)	A 1 to 5-character code that uniquely identifies the environment for this application. For example, you may have a TEST environment code for several different applications but you can only have one TEST environment code for a single application.
Description (Required Value)	A 1-35 character description of the application environment
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

Auto Task Maintenance

Auto Task Maintenance tables define tasks that Stat automatically creates based on certain application, type, and status values selected on a CSR. As soon as the user makes a selection in one of these fields, Stat determines if there are auto tasks defined for that particular code. If so, Stat adds them to the task list.

Stat features a separate maintenance table for each of the three values on which you can define auto tasks. All three tables are displayed in a standard maintenance window and include the same set of fields or columns.

Auto task security is controlled by the following user class rights:

- Auto Tasks - Add
- Auto Tasks - Edit

To open the Auto Tasks by Application table, select **Maintenance | Domain-Specific | Auto Tasks | Application Tasks**.

To open the Auto Tasks by CSR Type table, select **Maintenance | Domain-Specific | Auto Tasks | CSR Type Tasks**.

To open the Auto Tasks by CSR Status table, select **Maintenance | Domain-Specific | Auto Tasks | CSR Status Tasks**.

Value	Description
Active	Indicates if this task will be automatically generated or not
Source Application, Source CSR Type, Source CSR Status (Key Value)	Depending upon the type of auto task you are maintaining, one of these fields will be displayed. Select a value from the drop down list that, when selected on a CSR, will generate the task
Activity Code (Key Value)	Select an activity code from the list
Assignment (Required Value)	Select one of the following: • A particular user who has access to this service domain • {Prompt for User} requires the user to select a name from the list prior to saving the CSR. **NOTE:** In the Stat Web Console, the {Prompt for User} setting defaults to the user assigned to the CSR • {Assigned User} assigns the task to the person assigned to the CSR • {Current User} assigns the task to the person currently editing the CSR • {Open User} assigns the task to the person listed in the **Open By** field on the CSR
Due Date (Required Value)	Select an option that defines how Stat calculates the due date for the task. Due dates are based upon either the CSR Open Date, Due Date or the Current Date. The '+' and '-' options calculate the date plus or minus the number of days specified.
Hrs Est (Required Value)	Enter a default value for the estimated number of hours it will take to complete this task
Description Override	Enter a description in this field to override the description associated with the task
Comment	If you want to have Stat automatically enter a comment with the task, enter it here

Value	Description
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Business Rule Maintenance

The Business Rule Maintenance table defines sets of instructions which, based on a combination of trigger events and specified criteria, direct Stat to send out email notifications to a list of users and customers and/or execute user defined commands.

The Business Rule Maintenance table also displays personal rules defined by other users within the same service domain. Business rules are identical to personal rules with two exceptions:

- You must define a distribution list to which the email is sent.
- The owner of a business rule is always the special 'SYSTEM' account.

Business rule security is controlled by the following user class rights:

- Business Rules - Add
- Business Rules - Edit

With proper security, you can also edit personal rules from the Business Rule Maintenance table, including those belonging to other users. For more information on personal rules, see the *Stat User Guide*, Chapter 9, "Personal Rules."

The Business Rule Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Business Rules**.

Value	Description
Enabled	If selected, activates the value in stat
Rule ID (Key Value)	A 1-10 character code that uniquely identifies this business rule
Owner	By default, the owner of a business rule is "System." For personal rules, this field displays the owner's user ID.
Description (Required Value)	A brief description of the rule
Event	The event that triggers the rule
Last Update (Read Only)	The date and time that this rule was last updated
Update By (Read Only)	The user who last updated this rule

In Stat, outbound email is processed by the Stat Central Agent. You configure the Stat Central Agent that you want to process email in the Electronic Mail Interface - Setup window. For more information, see Configuring the Stat Central Agent for Email on page 174. In addition, for the Stat Central Agent to process outbound email, you must assign to it the **Send Queued Outbound Mail** job. How this job is scheduled is up to you, but it is recommended you have it run frequently in order to promote real-time processing. For more information, see Defining Agent Jobs on page 164.

Defining Business Rules

To define a business rule, click **New**. Stat opens the Rule Editor window. In the **Rule Definition** tab, you select a trigger event and specify rule criteria the same way you do for personal rules.

The System ID is automatically displayed in the **Owner ID** field. The **Rule ID** field displays (New) until you save the rule. When you save, Stat assigns it a unique number.

Selecting a Trigger Event

Every business rule is triggered by a specific, predefined event.

To select a trigger event:

1. In the **Description** field, enter a brief description of your rule, such as “New PeopleSoft CSRs.” The Subject in an outgoing Business Rule email will include the Business Rule description.
2. In the **Event** field, select an event.

   Available events include:

   - **Any** – When any of the events mentioned below occurs. This is the default event for business rules.
   - **Command Error Notification** – Sends an email when a triggered business rule has a defined command that completes with an error.
   - **CSR Close** – When a CSR changes from an open status to a closed status
   - **CSR Open** – When a new CSR is entered into the system by either a Stat user or the Stat Central Agent
   - **CSR Open-Entry** – When a new CSR is entered into the system by a Stat user
   - **CSR Open-Mail** – When a new CSR is created by the Stat Central Agent in response to an email from a customer or another application. Customers can email their requests to a predefined Stat Central Agent email address. Upon receiving the email, the Stat Central Agent automatically opens a new CSR for that request.
   - **CSR Re-Open** – When a CSR changes from a closed status to an open status
   - **CSR Update** – When a change is made to a CSR.
   - **Migration Notification** - When a migration occurs or is scheduled involving specific migration statuses, migrators, modules or target environments.
   - **OraApps Patch Application Complete** – When the Stat Central Agent for Oracle Apps is done processing the Patch Application request
   - **OraApps Patch Application Scheduled** – When a Patch Application is scheduled via a CSR or Patch Mgmt Console
   - **OraApps Patch Rollback Complete** – When the Stat Central Agent for Oracle Apps is done processing the Patch Rollback request
   - **Past Due CSR Escalation** – When a CSR is past due for a specified amount of time
   - **Past Due Migration Approval Escalation** – When a migration has not been approved or rejected after a specified amount of time
   - **Past Due OraApps Patch Approval Escalation** – When a patch application has not been approved or rejected after a specified amount of time
   - **Past Due Post Migration Step** – When a post migration step has not been completed after a specified amount of time
   - **Past Due Project Escalation** – When a project is past due for a specified amount of time
   - **Past Due Status Approval Escalation** – When a status transfer that has not been approved or rejected after a specified amount of time

- **Past Due Status Transfer Escalation** – When a status transfer that has been marked as Ready has not been transferred after a specified amount of time
- **Past Due Task Escalation** – When a task is past due for a specified amount of time
- **Unopen CSR Escalation** – When a CSR has remained unread by the assigned user for a specified amount of time

NOTE: The fields **Type** and **Value** appear whenever you select a past due escalation-type event. Here you specify the amount of time that the item must be past due to trigger the rule.

3 If you selected a past due escalation-type event, select the type of time interval you want to use in the **Type** field.

Options include **Business Days**, **Days**, and **Hours**. Then in the **Value** field, enter a numerical value for the time interval. For example, if you select **Hour** and enter a value of 6, the business rule is triggered when the item is six hours past due.

4 (Optional) Select **Fire only once per CSR**.

This configures the Stat Central Agent to fire the rule the first time the rule criteria are met for a CSR and no time thereafter. In the case of past due escalation events, this option applies to the specified approval, task, project, and so on. To illustrate, consider a business rule based on an Update trigger event and a CSR status of In Process. If you do not select **Fire only once per CSR**, everyone on the mail distribution list will receive an email each time a user saves a CSR with a status of In Process. By selecting **Fire only once per CSR**, users will receive an email only the first time a CSR is saved with an In Process status. The same is true when a Business Rule has a defined command. Later changes made to the CSR will not trigger the rule.

NOTE: Selecting **Fire only once per CSR** adds the **History** tab to the **Rule Editor** window. This tab displays a list of CSRs that have triggered the business rule. Deselecting **Fire only once per CSR** removes the **History** tab from the window. For more information, see Viewing Rule History on page 133.

Defining Rule Criteria

After selecting the trigger event, you can specify additional criteria that qualify the trigger event under your rule definition. Stat needs to know what values the CSR must display for the rule to take effect.

You specify the criteria by selecting criteria types (CSR fields) and the matching values. You may concatenate multiple CSR values.

NOTE: Be sure to create a Stat Central Agent job for each type of “past due” event triggered by either a business or personal rule. Also, when scheduling the job, be aware of the timing of the rule. For example, if you want CSRs that are more than 1 hour past due to trigger an email, scheduling the job to run every 2 hours could result in an email being sent 3 hours after the trigger event.

Field

Fields correspond to certain types of information contained in a CSR. The Field list displays the following options:

• Application Environment	• Application
• Assigned Queue	• Assigned User
• CSR Opened by User	• CSR Priority
• CSR Status	• CSR Type
• Customer	• Customer Department
• Equipment ID	• Logged in User
• Vendor	• Workflow

NOTE: Depending on the trigger event, the Field list may include different options:

- For business rules triggered by past due escalation events, the list above also includes options specific to that event. For example, for the event Past Due Task Escalation, the list includes the option **Assigned User of Task**.
- For migration events, the list includes the **Migration Status**, **Migrator**, **Module**, and **Target Environment**.
- For the Oracle Apps business rules, OraApps Patch Application Complete and OraApps Patch Rollback Complete, the list of fields includes the option **Process Status**, which corresponds to the field in the Oracle Applications Patch Management Console.

Operator

After you select a CSR field type, you need to establish its relationship to a value or set of values you specify. Options include:

- **Is** – Select if the CSR field must equal the specified value, meaning a match must occur
- **Not** – Select if the CSR field cannot equal the specified value. This tells Stat to initiate the rule whenever a trigger event occurs in a CSR with a value different than the one you specify.
- **Change From** – Select if upon saving the CSR, the field has changed from one specified value to another
- **Not Change From** – Select if upon saving the CSR, the field has not changed from one specified value to another. In this case, the rule takes effect when a trigger event occurs on a CSR with a field value that has not changed exactly as specified.

Value

The list of value options depends on the CSR field you select. If you select the **Is** operator, the corresponding value found in the CSR must match your selection for the business rule to take effect. Likewise, if you select **Not**, the corresponding value cannot equal your selection.

The table below shows some examples of rule criteria. You can define several criteria for one business rule.

Value	Operator	Value	Explanation
CSR Status	Not	Cancelled OR Denied	Rule takes effect when trigger events occur on CSRs with a status that is neither Cancelled nor Denied
Assigned Queue	Is	Dev	Rule takes effect when trigger events occurs on CSR assigned to the queue Development (Dev)
Application	Changed From	Self Service to HR, Benefits to Pay Roll, or HR to Benefits	Rule takes effect when trigger event occurs on CSRs where the Application has changed from Self Service to HR, or Benefits to Pay Role, or HR to Benefits

NOTE: For the operators **Change From** and **Not Change From**, **Any** is a permitted value for the **From** field, and **Any** and **Any except original value** are permitted values for the **To** field. However, using the **Any** value in both the **From** and **To** fields will not trigger the rule. Instead, use the **Any** value in the **From** field and the **Any except original** value in the **To** field.

If you define more than one set of criteria for a business rule, each set must be met for the rule to take effect. The exception to this is when you define more than one value on a CSR field. In this case, the rule takes effect if the CSR field matches one of the possible values.

For example, let's say you add a business rule based on an Open trigger event that uses each set of criteria shown in the preceding table. This means that everyone on the email distribution list will receive an automatic email notification whenever a Stat user or the Stat Central Agent opens a CSR with a status that is anything but

Cancelled or Denied, is assigned to the Development queue, and an application value that has changed from one specified value to another.

NOTE: For past due rules you may want to exclude closed CSRs from the rule. Otherwise closed CSRs will continue to be evaluated.

To add criteria to a rule:

1. In the **Field** field, select the CSR field you want.
2. In the **Operator** field, select an operator.
3. In the **Value** field, select a value for the field.
4. Click **Add**.

   Your new criteria appear in the window with an indicator that it has been added to your rule.
5. Repeat for each additional criteria.

To remove criteria:

Select the row and click **Remove**.

NOTE: To edit a rule, select the rule in the **Business Maintenance** table and then click **Rule Details.** Stat opens the **Rule Editor** window where you can edit the rule as needed.

Defining Message Content

After selecting the trigger event and optionally specifying rule criteria, the next step is to open the email Message tab and define the content of the email message that is to be sent out when the rule is triggered.

To define email message content:

1. In the Rule Editor window, click the email Message tab.
2. Select the check box corresponding to each type of CSR information you want included in the email message.

   NOTE: If you select the **Most Recent Log** option and the most recent log entered on the CSR is flagged as confidential, the log is not included in the email message. Also, if you select the **Attachments** option, any attachments on the original CSR will be forwarded with the email message.
3. (Optional) Enter any header and footer information you want inserted in the email.

   It is a good idea to put information in the message header about the rule itself. The Stat Central Agent includes the rule ID number in the message subject, but does not include any information about the event or rule criteria.

Defining a Distribution List

After specifying the content of the email message, the next step is to specify a distribution list of mail recipients.

To define a distribution list:

1. Click the Send To tab.

   This is where you define the distribution for the email. You must define at least one recipient.
2. In the **Send To** field, select a value. Send to options are based on a selected rule event and could be different for each rule.

   Options include:

   - Approver, Migrations – The user assigned to approve migrations
   - Approver, OraApps – The user assigned to approve Oracle patch applications

- Approver, Status Transfer – The user assigned to approve status transfers

  NOTE: Emails sent out for Approval Escalation events (OraApps Patch Application, Migration, and Status Transfer) include links that allow the recipient to approve or reject the request.

- Customer – The customer on the CSR
- Customer, CSR – The customer specified on the CSR
- Customer, Specified – A specific customer

  NOTE: The Stat Central Agent does not send an email to inactive customers.

- Email Addr, Specified – A manually entered email address
- Migrator - The user listed as the default developer of a migration
- Queue, All Members – All members of the queue specified on the CSR
- Queue, Owner – The owner of the queue on the CSR
- User, All Historic Owners – All the users that at one time owned the CSR
- User, Assigned – The user assigned to the CSR
- User, Logged In – The user logged in to Stat when the trigger event occurs
- User, Opened By – The user the opened the CSR
- User, Specified – A specific Stat user
- User, Task Assigned – The user assigned to a task specified on the CSR

  NOTE: Stat sends emails only to active users and customers and recipients that have been individually specified.

3 In the **Field** field, select how you want the message addressed to the recipient.

  Options include **To**, **CC**, and **Blind CC**.

4 If you selected **User, Specified** in the **Send To** field, select the Stat user you want in the **Other Address** field.

5 If you selected **Other Address** in the **Send To** field, enter the email address in the **Other Address** field.

6 Click **Add**.

To remove a recipient:

1 In the list of recipients, click on the recipient you want to remove.

  The Hand icon moves to that row indicating that the row is selected.

2 Click **Remove**.

Defining a Command to Run

When a Business Rule is triggered, Stat can execute a user-defined command. The command is executed by Stat Central Agent. The command can be used for any purpose, for example, to notify a third party system about a Stat event. To define a custom command, navigate to the **Define Command** tab.

Command Parameters

Stat offers many predefined and custom parameters that can be used to build a command. Predefined parameters can be used when a Business Rule triggers CSR-specific events, for example, a CSR Update. A drop-down list displays the CSR fields available in the Stat Database view CSR_BUS_RULE_PARAMS_VW1. The parameters drop-down list displays the User Parameters defined for the Pre/Post Migration steps.

To add a parameter to a command, select the desired parameter from the drop-down list of predefined parameters and click the **Add** button. The selected parameter is inserted at the cursor position in the command field and uses the following format: %%PARAMETER%%.

The following is an example of a command:

```
curl

--user %%JIRA_USERID%%213:%%JIRA_PWD%%

-k -X POST

--data "{

     \"body\": \"CSR: %%SD_CD%%-%%CSR_ID%%:%%TITLE%% - has been updated by
%%UPDATED_USER_ID%% on %%UPDATE_DATE%% :)

   \"}"

-H "Content-type: application/json"

https://yourcompany.com/rest/api/2/issue/%%TRACKING_NUMBER%%/comment
```

This command will add a comment to Jira for a case defined in the CSR Tracking number. Notice that JIRA_USERID and JIRA_PWD are defined in the User predefined parameters.

You can also specify a command time-out and specify conditions for the executed command to trigger a “Command Error Notification” business rule.

- **Trigger “Command Error Notification” when return code...** – Select this option to trigger the Command Error Notification business rule if the command errors. Then refine the trigger by selecting specific trigger conditions applicable to your custom command.

Resetting a Rule

Occasionally, you may want to reset a rule that fires only once so that it can be triggered again. To do this, open the History tab for the rule. Select the CSR or past due item that you want to reset. Click **Delete**. Then click **Apply** or **OK**.

Saving Rules

Click **OK** to save your rule. Stat checks your rule for errors. If an error is found, Stat informs you what you need to correct. When Stat saves your rule, it assigns it a unique number.

Disabling Rules

To prevent a rule from triggering, open the rule in the Rule Editor window and deselect **Rule Enabled**. The Stat Central Agent does not process disabled rules. This change goes into effect the next time the Stat Central Agent checks for new rules.

Copying Rules

If you need to define a business rule that closely resembles an existing rule, you can save time by copying the previously defined rule and editing the copy as needed. You can copy the business rule to the same service domain or a different service domain. When you copy a business rule, the entire rule definition gets copied over, including the rule criteria and distribution list.

NOTE: Business rules can also be copied with the Data Replicator. For more information, see Data Replicator on page 25.

To copy a business rule:

1 In the **Business Rule Maintenance** window, select the rule you want to copy. Then click **Copy**.

Stat prompts you to specify the service domain and name for the copy.

2 Select the service domain you want to copy the business rule to.

If any of the rule criteria (statuses, types, priorities, etc) do not exist in the newly selected SD, then the rule will not save. Stat prompts you to modify the fields.

3 In the **Rule Description** field enter a name for the rule. Then click **OK**.

4 Open the new business rule and edit as needed.

Viewing Rule History

When you select **Fire only once per CSR** in the Rule Definition tab, Stat adds the History tab to the Rule Editor window. This tab displays a list of all the CSRs that have been triggered by the business rule. In the case of past due escalation events, the tab changes to display a record of the past due item specified by the rule. For each record, the tab also shows the date and time that the rule fired.

CSR Log Topics Maintenance

CSR log topics are used to group CSR logs. When a new log is entered, the user must select a topic from the drop down list which is populated by this table.

CSR log topic security is controlled by the following user class rights:

- CSR Log Topic - Add
- CSR Log Topic - Edit

The CSR Log Topic Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | CSR Log Topics**.

Value	Description
Enabled	If selected, activates the value in stat
Log Topic (Key Value)	A 1-15 character code/description of the topic
Last Update (Read Only)	The date and time that this rule was last updated
Update By (Read Only)	The user who last updated this rule

CSR Priority Maintenance

The CSR Priority Maintenance table defines the levels of urgency behind a CSR. Priority codes define what values are displayed on the CSR Priority drop down list on CSRs. They also define how Stat calculates the due date for the CSR.

CSR priority security is controlled by the following user class rights:

- Priority codes - Add
- Priority codes - Edit

The CSR Priorities Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | CSR Priorities**.

You define CSR priorities by specifying the following values in the CSR Priority Maintenance window.

Value	Description
Active	If selected, activates the definition in Stat
Prio Cd (Key Value)	A 4-character code which uniquely identifies the Priority
Description (Required Value)	A 1-35 character description of the priority
Prio Order	A number that determines the sort order for the priority codes on the drop down list on the CSR. Priorities with a lower number are displayed at the top of the list.
TAT (Turn-Around-Time) Value (Required Value)	A number that, used in conjunction with the TAT Type, determines the calculated due date for the CSR. For example, if the TAT Value is 30 and the TAT Type is Days, Stat will set the CSR due date for 30 Days after the open date.
TAT Type (Required Value)	The Turn-Around-Time type which is used in conjunction with the TAT Value. Valid options are: • Days • Hours • Business Days
Bold	If selected, the Priority will display in a bold font on console lists
Italic	If selected, the Priority will display in an italic font on console lists
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

NOTE: You can change the display color of a selected type code by clicking **Color...** and specifying a different color in the Color Selection dialog box. For more information, see Using the Color Selection Dialog Box on page 17.

CSR Type and Status Maintenance

CSR types divide CSRs into categories. They help identify what kind of problem or request the CSR represents. CSR statuses, on the other hand, represent the states a CSR goes through in its life cycle. After you define a CSR type in the CSR Type Maintenance table, you can associate it with a set of CSR statuses that you define in the CSR Status Maintenance table. This way, when a user creates a CSR of a particular type, the drop down list in the **Status** field displays only the statuses defined for that type.

CSR type security is controlled by the following user class rights:

- Type Codes - Add
- Type Codes - Edit

The CSR Type Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | CSR Types and Statuses**.

Value	Description
Active	If selected, activates the value in stat
CSR Type Cd (Key Value)	A 3-character code which uniquely identifies the type

Value	Description
Description (Required Value)	A 1-35 character description of the type
Bold	If this option is set to yes, the type appears bold on console lists. This option does not apply to the Stat Web Client
Italic	If this option is set to yes, the type appears italicized on console lists This option does not apply to the Stat Web Client
Use Default	Indicates if this types use CSR statuses associated with the Default type
CSR Patch Tab	Determines if the Patches tab is displayed on CSRs of this type
Env Refresh Tab	Determines if the Environment refresh tab is displayed on CSRs of this type
Project Required	Determines if the project field on CRSs is required
Last Update (Read Only)	The date and time this record was last updated
Update By (Read Only)	The user who last updated this record

After you define a CSR type in the CSR Type Maintenance table, select it and click **CSR Status**. This opens the CSR Status Maintenance table. From here you can define all the CSR statuses for the selected type.

If you plan on associating certain CSR statuses with multiple CSR types, you can save time by associating them with the predefined CSR type named Default. Statuses that you associate with the Default type can then be used as default statuses for other CSR types. For example, if you want to associate both a Cancelled status and a Released status with all your CSR types, rather than defining these statuses for each CSR type separately, you can define them just once for the Default type. You can then use Cancelled and Released as default statuses for other CSR types by selecting **Use Default** for each type you want in the CSR Type Maintenance table.

The CSR Status Maintenance table is displayed in a standard maintenance window.

When you open the CSR Status Maintenance window for a particular CSR type, any default statuses assigned to that type are displayed in read-only format. To edit default statuses, you must open the CSR Status Maintenance window for the Default type. Any changes you make to the statuses there are reflected in all the CSR types that use default statuses.

To create a CSR type-specific status, click **New**. This activates a new row in the maintenance table. In the **CSR Status Cd** field, type the name of the status and then complete the remaining fields. When finished click **OK** or **Apply**.

Value	Description
Active	If selected, activates the value in stat
CSR Status Cd (Key Value)	A 5-character code which uniquely identifies the status
Description (Required Value)	A 1-35 character description of the status
Pct Complete	The percentage to which CSRs in the selected status are complete.
Closed	If selected, Stat will treat this code as a closed status. CSRs with this status will no longer appear on CSR lists (except all open and closed) and will be given a closed date.

Value	Description
C For Stats (Closed for Statistics)	This field is used strictly for reporting and allows CSRs to be filtered based on this field. It is commonly used when running reports where you want to filter out CSRs that are not the responsibility of the assigned user (for example, waiting on the customer for info).
Bold	If selected, the status will display in a bold font on console lists
Italic	If this option is set to yes, the Status will display in an italic font on console lists
Default	Indicates if the status is derived from the Default CSR type. Default statuses cannot be modified.
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Customer Priority Maintenance

The Customer Priority table defines the level of urgency customers believe should be assigned to their CSRs. Although a customer priority may be different than the priority actually assigned to a CSR in the **Priority** field, this is a way to record how important customers regard the issues addressed in their CSRs.

To open the Customer Priority Maintenance table, select **Maintenance | Domain-Specific | Customer Priorities.**

NOTE: For any service domain in which you want to use customer priorities, be sure to select **Use Cust Prio** in the service domain maintenance table. Otherwise, the **Customer Priority** field will be grayed out on CSRs opened in that service domain. For more information, see Service Domain Maintenance on page 54.

Value	Description
Active	If selected, activates the priority definition in Stat
Prio Cd (Key Value)	1-4 character code that uniquely identifies the priority
Description (Required Value)	1-35 character description of the priority
Prio Order	The position of the priority in the **Customer Priority** field
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Generic Application Migration Path Maintenance

The Generic Application Migration Path Maintenance table defines migration paths used in Stat's generic application change management module. Migration paths define the progression of objects from one environment to another. When a user associates objects with a CSR, they must first select a migration path.

For more detailed information on migration paths, see the book, *Change Management for Generic Applications*, Chapter 1, "Object Management."

When defining migration paths, keep in mind the following considerations:

- Environments cannot be listed on the path more than once
- The environments defined as Base, Development, and Distribution must also appear on the path. It is not required that they appear as environment 1, 2, and 3, but they must appear somewhere.
- Environments connected to a distribution environment (i.e., the distributed environments) should not appear in any other migration path. This is because objects are not locked in the connected environments and overwrites could occur if the same objects exist in other environments.
- Environments cannot exist on migration paths of different service domains. An environment cannot be shared by multiple service domains.
- An environment can exist in multiple migration paths in a service domain
- If you attempt to remove from a migration path an environment that is used in a workflow transfer rule, Stat displays a warning message. If you proceed in removing the environment, Stat automatically deletes the transfer rules from any workflow in which the environment is used.
- Service domains and environments have a one-to-many correlation

Generic application migration path security is controlled by the following user class rights:

- Generic Application Migration Paths - Add
- Generic Application Migration Paths - Edit

The Generic Application Migration Path Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Generic Application Migration Paths.**

The following table defines the fields (columns) in the Generic Application Migration Path Maintenance window.

Value	Description
Active	If selected, activates the value in stat
Migration Cd (Key Value)	A 1-10 character code that uniquely identifies this migration path **NOTE:** Special characters are not allowed, including: ~ ‘ “ * % ( ) ,
Description (Required Value)	A 1-35 character description of the path
Base Object Source (Required Value)	The Base environment from where the base archive set is created
Development Environment (Required Value)	The environment where development takes place
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user who last updated this record

Migration Path Diagram

After you have specified the migration code and description, click **Apply** to save your work. Then select the migration path and click **Template...**. This opens the Migration Path Definition window. The left section of the window displays a list of each environment that can be added to the new migration path (environments previously applied to a migration path in a different service domain will not be displayed). The right section of the window is where you arrange the icons to create a graphical diagram representing the sequence of the migration.

NOTE: It is recommended that you have the basic design of your migration path diagram in place before you build it in the Migration Path Definition window. This avoids the time-consuming process of rebuilding a diagram if mistakes or oversights occur.

To create a migration path:

1. In the left section of the window, click and hold on the first environment of the migration path. Then drag into the right section of the window to where you want to place the graphic and release the mouse button.
2. Following the sequence of the migration path, place the other environments in the migration path in the diagram.

   Environments are labeled according to the order in which they are placed in the diagram. The first environment you place in the diagram is labeled “1”, the second “2” and so on.
3. Right-click on the graphic representing the base environment in the migration path. Then in the pop-up menu, select **Set base environment**.
4. Right-click on the graphic representing the development environment in the migration path. Then in the pop-menu, select **Set dev environment**.
5. (Optional) If you want to designate a distribution database, right-click on the graphic representing the distribution environment in the migration path. Then in the pop-up menu, select **Enable distribution environment**.

   For more information, see Defining Distribution Environments on page 138.
6. (Optional) If you want to modify the migration path, right-click the graphic representing the environment you want to change and do any of the following:
   - To designate the environment as the new base environment in the migration path, select **Set base environment**.
   - To designate the environment as the new development environment in the migration path, select **Set dev environment**.
   - To switch the environment’s place in the migration path with another environment, select **Swap environment number**. Then in the prompt select the number of the environment you want to switch and click **OK**.
   - To remove the environment from the diagram, select **Delete environment**.

   NOTE: After deleting an environment, you may need to adjust the order numbers of the remaining environments in the diagram to make them consecutive. Stat does this for you automatically when you save.

Defining Distribution Environments

Distribution environments allow users to migrate objects to multiple environments distributed over a network at one time. When a user migrates an archive set to a distribution environment, Stat automatically migrates the archive set to a list of connected environments.

You define distribution environments at the migration path level. The first step is to designate certain environments in a migration path as distribution environments. Then you determine which environments you want to connect to them. For example, let’s say you have ten production environments. All of your development work is done centrally, and when ready, changes are migrated out to all the production environments at the same time. Most likely you would define the local or ‘in-house’ production environment as the distribution environment on the migration path and connect it to the nine other production environments.

Although connected to the distribution environment, the other environments are not represented graphically and are not technically part of the migration path. This means that objects cannot be locked in the environments connected to a distribution environment. Likewise, objects can only be migrated to them; you cannot archive objects from these environments.

For more information on distribution environments, see the book, *Change Management for Generic Applications*, Chapter 3, “Object Migrations.”

CAUTION: Because objects are not locked when migrated to the environments connected to a distribution environment, it is recommended that you do not include these environments in any other migration path. This eliminates the possibility of two developers accidently overwriting each other’s work.

To define a distribution environment:

1. Open the migration path diagram containing the environment you want to designate as a distribution environment.
2. Right-click on the graphic representing the distribution environment in the migration path. Then in the pop-up menu, select **Enable distribution environment**.

   An icon is displayed next to the environment graphic signifying its status as a distribution environment.
3. Double-click the distribution icon.

   Stat opens the Distributed database window.
4. In the left section of the Migration Path Definition window, select the environment you want to add to the list of distributed environments.
5. Click **Add**.
6. Repeat steps 4 and 5 for each environment you want to add.
7. If you want to deactivate an environment, deselect **Active**.

   When a user migrates an archive set to a distribution environment, Stat migrates the objects only to the active environments in the distribution list and ignores the rest. However, this setting can be changed on the CSR at the time of migration, in which case deactivated environments are reactivated only for that CSR.
8. Click **OK**.

Updating CSR Migration Paths with Additional Environments

You can add environments to existing migration paths that are already associated with CSRs. You then have the option of updating the migration path on selected CSRs to include the new environments.

IMPORTANT: Be aware of the following:

- Although you can add and remove environments from migration paths, you can only update the migration paths of existing CSRs after adding environments, not after removing them (see 2nd bullet below). Furthermore, you cannot update the migration paths of existing CSRs after replacing environments (i.e., removing one environment and adding another in its place).
- Environments can be removed from the migration path maintenance table. However, removing an environment from a migration path will only be reflected on newly created CSRs. The environment will not be removed from existing or closed CSRs.

To add environments to CSR migration paths:

1. Open the migration path diagram you want to add an environment to.
2. Follow the instructions in the section Migration Path Diagram on page 137 to add environments to the migration path.
3. Click **Add new env. to CSR**.

   Stat displays a list of any open CSRs currently associated with the migration path. You can select the CSRs you want to update. You can also opt to copy the objects from the Base or Development environment to the newly added environments on the migration path.
4. Select the **Update** option for each CSR you want to update.
5. Optionally, select the **Update Object List** option if you want to copy the objects from either the Base or Development environment to the newly added environments. Then select **Base** or **Dev**.
6. Click **OK**.

PeopleSoft Migration Path Maintenance

The PeopleSoft Migration Path Maintenance table defines migration paths used in the PeopleSoft change management module. Migration paths define the progression of objects from one environment to another. When users add objects to a CSR, they must first select a migration path.

For more detailed information on migration paths, see the book, *Change Management for PeopleSoft*, Chapter 1, “Object Management.”

When defining migration paths, keep in mind the following:

- Environments cannot be listed on the path more than once
- The environments defined as Base, Development, and Distribution must also appear on the path. It is not required that they appear as environment 1, 2, and 3, but they must appear somewhere.
- Environments connected to a distribution environment (i.e., the distributed environments) should not appear in any other migration path. This is because objects are not locked in the connected environments and overwrites could occur if the same objects exist in other environments.
- Environments cannot exist on migration paths of different service domains. An environment cannot be shared by multiple service domains.
- If you attempt to remove from a migration path an environment that is used in a workflow transfer rule, Stat displays a warning message. If you proceed in removing the environment, Stat automatically deletes the transfer rules from any workflow in which the environment is used.
- An environment can exist in multiple migration paths in a service domain
- Service domains and environments have a one-to-many correlation

PeopleSoft migration path security is controlled by the following user class rights:

- PeopleSoft Migration Paths - Add
- PeopleSoft Migration Paths - Edit

The PeopleSoft Migration Path Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | PeopleSoft Migration Paths**

The following table defines the fields (columns) in the PeopleSoft Migration Path Maintenance window.

Value	Description
Active	If selected, activates the value in stat
Migration Cd (Key Value)	A 1-10 character code that uniquely identifies this migration path **NOTE:** Special characters are not allowed, including: ~ ‘ “ * % ( ) ,
Description (Required Value)	A 1-35 character description of the path
Base Object Source (Required Value)	The Base environment from which the base archive set is created
Development Environment (Required Value)	The environment where development takes place
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user who last updated this record
Stage Database	The default PeopleSoft staging database.

Migration Path Diagram

After you have specified the migration code and description, click **Apply** to save your work. Then select the migration path and click ***Template...***. This opens the Migration Path Definition window. The left section of the window displays a list of each environment that can be added to the new migration path. The right section of the window is where you arrange the icons to create a graphical diagram representing the sequence of the migration.

NOTE: It is recommended that you have the basic design of your migration path diagram in place before you build it in the Migration Path Definition window. This avoids the time-consuming process of rebuilding a diagram if mistakes or oversights occur.

To create a migration path:

1. In the left section of the window, click and hold on the first environment of the migration path. Then drag into the right section of the window to where you want to place the graphic and release the mouse button.
2. Following the sequence of the migration path, place the other environments in the migration path in the diagram.

   Environments are labeled according to the order in which they are placed in the diagram. The first environment you place in the diagram is labeled “1”, the second “2” and so on.
3. Right-click on the graphic representing the base environment in the migration path. Then in the pop-up menu, select **Set base environment**.
4. Right-click on the graphic representing the development environment in the migration path. Then in the pop-menu, select **Set dev environment**.
5. (Optional) If you want to designate a distribution database, right-click on the graphic representing the distribution environment in the migration path. Then in the pop-up menu, select **Enable distribution environment**.

   For more information, see Defining Distribution Environments on page 141.
6. (Optional) If you want to modify the migration path, right-click the graphic representing the environment you want to change and do any of the following:
   - To designate the environment as the new base environment in the migration path, select **Set base environment**.
   - To designate the environment as the new development environment in the migration path, select **Set dev environment**.
   - To switch the environment’s place in the migration path with another environment, select **Swap environment number**. Then in the prompt select the number of the environment you want to switch and click **OK**.
   - To remove the environment from the diagram, select **Delete environment**.

   NOTE: After deleting an environment, you may need to adjust the order numbers of the remaining environments in the diagram to make them consecutive. Stat does this for you automatically when you save.

Defining Distribution Environments

Distribution environments allow users to migrate objects to multiple environments distributed over a network at one time. When a user migrates an archive set to a distribution environment, Stat automatically migrates the archive set to a list of connected environments.

You define distribution environments at the migration path level. The first step is to designate certain environments in a migration path as distribution environments. Then you determine which environments you want to connect to them. For example, let’s say you have ten production environments. All of your development work is done centrally, and when ready, changes are migrated out to all the production environments at the same time. Most likely you would define the local or ‘in-house’ production environment as the distribution environment on the migration path and connect it to the nine other production environments.

Although connected to the distribution environment, the other environments are not represented graphically and are not technically part of the migration path. This means that objects cannot be locked in the environments connected to a distribution environment. Likewise, objects can only be migrated to them; you cannot archive objects from these environments.

In order for Stat to migrate PeopleSoft proprietary objects automatically to a distribution environment and its associated environments, the CLI Auto-Migration option must be activated for the distribution environment, as well as each connected environment to which you want to migrate PeopleSoft proprietary objects. If the CLI Auto-Migration option is activated for just some of the environments in the distribution list, Stat migrates PeopleSoft proprietary objects to the activated environments and ignores the rest. For more information on activating the CLI Auto-Migration option, see PeopleSoft Environment Connection Maintenance on page 80.

For more information on distribution environments, see the book, *Change Management for PeopleSoft*, Chapter 3, "Object Migrations."

CAUTION: Because objects are not locked when migrated to the environments connected to a distribution environment, it is recommended that you do not include these environments in any other migration path. This eliminates the possibility of two developers accidently overwriting each other's work.

To define a distribution environment:

1. Open the migration path diagram containing the environment you want to designate as a distribution environment.
2. Right-click on the graphic representing the distribution environment in the migration path. Then in the pop-up menu, select **Enable distribution environment**.

   An icon is displayed next to the environment graphic signifying its status as a distribution environment.
3. Double-click the distribution icon.

   Stat opens the Distributed database window.
4. In the left section of the Migration Path Definition window, select the environment you want to add to the list of distributed environments.
5. Click **Add**.
6. Repeat steps 4 and 5 for each environment you want to add.
7. If you want to deactivate an environment, deselect **Active**.

   When a user migrates an archive set to a distribution environment, Stat migrates the objects only to the active environments in the distribution list and ignores the rest. However, this setting can be changed on the CSR at the time of migration, in which case deactivated environments are reactivated only for that CSR.
8. Click **OK**.

Updating CSR Migration Paths with Additional Environments

You can add environments to existing migration paths that are already associated with CSRs. You then have the option of updating the migration path on selected CSRs to include the new environments.

IMPORTANT: Be aware of the following:

- Although you can add and remove environments from migration paths, you can only update the migration paths of existing CSRs after adding environments, not after removing them (see 2nd bullet below). Furthermore, you cannot update the migration paths of existing CSRs after replacing environments (i.e., removing one environment and adding another in its place).
- Environments can be removed from the migration path maintenance table. However, removing an environment from a migration path will only be reflected on newly created CSRs. The environment will not be removed from existing or closed CSRs.

To add environments to CSR migration paths:

1. Open the migration path diagram you want to add an environment to.
2. Follow the instructions in the section Migration Path Diagram on page 141 to add environments to the migration path.
3. Click **Add new env. to CSR**.

   Stat displays a list of any open or closed CSRs currently associated with the migration path. You can select the CSRs you want to update. You can also opt to copy the objects from the Base or Development environment to the newly added environments on the migration path.
4. Select the **Update** option for each CSR you want to update.
5. Optionally, select the **Update Objects List** option if you want to copy the objects from either the Base or Development environment to the newly added environments. Then select **Base** or **Dev**.
6. Click **OK**.

Oracle Application Migration Path Maintenance

The Oracle Applications Migration Path Maintenance table defines migration paths used in the Oracle Applications change management module provided by Stat. Migration paths define the progression of objects from one environment to another. When a user adds objects to a CSR, they must first select a migration path.

For more detailed information on Oracle Applications migration paths, see the *Stat User Guide*, Chapter 12, “Change Management for Oracle Applications.”

When defining migration paths, keep in mind the following:

- Environments cannot be listed on the path more than once
- The environments defined as Base, Development, and Distribution must also appear on the path. It is not required that they appear as environment 1, 2, and 3, but they must appear somewhere.
- Environments connected to a distribution environment (i.e., the distributed environments) should not appear in any other migration path. This is because objects are not locked in the connected environments and overwrites could occur if the same objects exist in other environments.
- Environments cannot exist on migration paths of different service domains. An environment cannot be shared by multiple service domains.
- If you attempt to remove from a migration path an environment that is used in a workflow transfer rule, Stat displays a warning message. If you proceed in removing the environment, Stat automatically deletes the transfer rules from any workflow in which the environment is used.
- an environment can exist in multiple migration paths in a service domain
- Service domains and environments have a one-to-many correlation

Oracle migration path security is controlled by the following user class rights:

- Oracle Migration Paths - Add
- Oracle Migration Paths - Edit

The Oracle Environment Migration Path Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Oracle Migration Paths**.

The following table defines the fields (columns) in the Oracle Applications Migration Path Maintenance window.

Value	Description
Active	If selected, activates the value in stat
Migration Cd (Key Value)	A 1-10 character code that uniquely identifies this migration path **NOTE:** Special characters are not allowed, including: ~ ‘ “ * % ( ) ,
Description (Required Value)	A 1-35 character description of the path
Base Object Source (Required Value)	The Base environment from which the base archive set is created
Development Environment (Required Value)	The environment where development takes place
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user who last updated this record

Migration Path Diagram

After you have specified the migration code and description, click **Apply** to save your work. Then select the migration path and click **Template...**. This opens the Migration Path Definition window. The left section of the window displays a list of each environment that can be added to the new migration path. The right section of the window is where you arrange the icons to create a graphical diagram representing the sequence of the migration.

NOTE: It is recommended that you have the basic design of your migration path diagram in place before you build it in the Migration Path Definition window. This avoids the time-consuming process of rebuilding a diagram if mistakes or oversights occur.

To create a migration path:

1. In the left section of the window, click and hold on the first environment of the migration path. Then drag into the right section of the window to where you want to place the graphic and release the mouse button.
2. Following the sequence of the migration path, place the other environments in the migration path in the diagram.

   Environments are labeled according to the order in which they are placed in the diagram. The first environment you place in the diagram is labeled “1”, the second “2” and so on.
3. Right-click on the graphic representing the base environment in the migration path. Then in the pop-up menu, select **Set base environment**.
4. Right-click on the graphic representing the development environment in the migration path. Then in the pop-menu, select **Set dev environment**.
5. (Optional) If you want to designate a distribution database, right-click on the graphic representing the distribution environment in the migration path. Then in the pop-up menu, select **Enable distribution environment**.

   For more information, see Defining Distribution Environments on page 145.
6. (Optional) If you want to modify the migration path, right-click the graphic representing the environment you want to change and do any of the following:
   - To designate the environment as the new base environment in the migration path, select **Set base environment**.

- To designate the environment as the new development environment in the migration path, select **Set dev environment**.
- To switch the environment's place in the migration path with another environment, select **Swap environment number**. Then in the prompt select the number of the environment you want to switch and click **OK**.
- To remove the environment from the diagram, select **Delete environment**.

NOTE: After deleting an environment, you may need to adjust the order numbers of the remaining environments in the diagram to make them consecutive. Stat does this for you automatically when you save.

Defining Distribution Environments

Distribution environments allow users to migrate objects to multiple environments distributed over a network at one time. When a user migrates an archive set to a distribution environment, Stat automatically migrates the archive set to a list of connected environments.

You define distribution environments at the migration path level. The first step is to designate certain environments in a migration path as distribution environments. Then you determine which environments you want to connect to them. For example, let's say you have ten production environments. All of your development work is done centrally, and when ready, changes are migrated out to all the production environments at the same time. Most likely you would define the local or 'in-house' production environment as the distribution environment on the migration path and connect it to the nine other production environments.

Although connected to the distribution environment, the other environments are not represented graphically and are not technically part of the migration path. This means that objects cannot be locked in the environments connected to a distribution environment. Likewise, objects can only be migrated to them; you cannot archive objects from these environments.

For more information on distribution environments, see the *Stat User Guide*, Chapter 12, "Change Management for Oracle Applications."

CAUTION: Because objects are not locked when migrated to the environments connected to a distribution environment, it is recommended that you do not include these environments in any other migration path. This eliminates the possibility of two developers accidently overwriting each other's work.

To define a distribution environment:

1. Open the migration path diagram containing the environment you want to designate as a distribution environment.
2. Right-click on the graphic representing the distribution environment in the migration path. Then in the pop-up menu, select **Enable distribution environment**.

   An icon is displayed next to the environment graphic signifying its status as a distribution environment.
3. Double-click the distribution icon.

   Stat opens the Distributed database window.
4. In the left section of the Migration Path Definition window, select the environment you want to add to the list of distributed environments.
5. Click **Add**.
6. Repeat steps 4 and 5 for each environment you want to add.
7. If you want to deactivate an environment, deselect **Active**.

   When a user migrates an archive set to a distribution environment, Stat migrates the objects only to the active environments in the distribution list and ignores the rest. However, this setting can be changed on the CSR at the time of migration, in which case deactivated environments are reactivated only for that CSR.

8 Click **OK**.

Updating CSR Migration Paths with Additional Environments

You can add environments to existing migration paths that are already associated with CSRs. You then have the option of updating the migration path on selected CSRs to include the new environments.

IMPORTANT: Be aware of the following:

- Although you can add and remove environments from migration paths, you can only update the migration paths of existing CSRs after adding environments, not after removing them (see 2nd bullet below). Furthermore, you cannot update the migration paths of existing CSRs after replacing environments (i.e., removing one environment and adding another in its place).
- Environments can be removed from the migration path maintenance table. However, removing an environment from a migration path will only be reflected on newly created CSRs. The environment will not be removed from existing or closed CSRs.

To add environments to CSR migration paths:

1 Open the migration path diagram you want to add an environment to.

2 Follow the instructions in the section Migration Path Diagram on page 144 to add environments to the migration path.

3 Click **Add new env. to CSR**.

Stat displays a list of any open or closed CSRs currently associated with the migration path. You can select the CSRs you want to update. You can also opt to copy the objects from the Base or Development environment to the newly added environments on the migration path.

4 Select the **Update** option for each CSR you want to update.

5 Optionally, select the **Update Objects List** option if you want to copy the objects from either the Base or Development environment to the newly added environments. Then select **Base** or **Dev**.

6 Click **OK**.

Pre and Post Migration Steps

The Pre and Post Migration Steps Maintenance table defines the actions to be taken on certain types of objects in an archive set before or after it has been migrated. Pre and Post migration steps are either manual or automatic, i.e., they are triggered either manually by users or automatically during Stat migration.

The Pre and Post Migration Steps Maintenance table defines actions that should be taken before an archive set is migrated.

Pre and post migration steps security is controlled by the following user class rights:

- Migration Steps - Add
- Migration Steps - Edit

The Pre and Post Migration Steps Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Pre and Post Migration Steps**.

Value	Description
Active	If selected, activates the value in Stat
Step Type	Defines whether step is Pre or Post

Value	Description
Migration Step (Required Value)	The type of step. Options include **Custom Command**, **Run DMS**, **Create Project Build Script**, **Compile Cobol**, and **Manual Step**.
Auto	If this check box is selected, the step will be triggered automatically. Only Custom Command steps can be set to run automatically.
Description (Required Value)	The name of the step
Object Class (Key Value)	The class of object for which the step is defined. Options include data objects and file object for all three change management modules supported by Stat, as well as PeopleSoft Proprietary objects.
Object Type (Key Value)	The object type the step is associated with (if any)
Run Order (Required Value)	A number that determines the sort order for the step on the pre and post migration checklist. Steps with a lower number are executed first.
Target Environment	The target environment the step is associated with (if any)
Include Distributed	If this check box is selected, the step is also propagated to each distributed environment.
Run Once Per Env	If this check box is selected, the step will be deselected by default when it was already executed in the past. User would still be able to add such step to the migration
Last Update (Read Only)	The date and time that this record was last updated
Updated By (Read Only)	The user that who updated this record

Step Types

Stat offers the following types of steps:

Custom Command	User can define custom command	
Run DMS	Run PeopleSoft Data Mover script	PeopleSoft only
Manual Step	Step that is run outside of Stat	
Create Project Build Script	Generate/execute PeopleTools Project Build script	PeopleSoft only
Compile Cobol		PeopleSoft only

Custom Command steps can be triggered automatically by Stat or manually. Other steps types are triggered manually.

Predefined Steps

Stat has three predefined PeopleSoft pre and post migration steps: Create Project Build Script, Compile COBOL, and Run DataMover Script. These steps are triggered manually by the migrator.

Create Project Build Script

When this step is triggered, Stat logs into the target PeopleSoft environment of the migration and creates the project build script for the project used during the migration. Stat uses the command line statement to launch PeopleSoft. It uses the PeopleSoft build settings from the Windows registry to generate the SQL script for create or alter.

Compile COBOL

When this step is triggered, Stat launches the PeopleSoft COBOL Compile program, either CBLBLD for NT or pscbl.mak for Unix. When executing this step, Stat uses the following file server variables:

- The definition of the file server operating system (NT, Unix, or Mainframe).
- The location of the COBOL Compiler for each file server that PeopleSoft COBOLs reside on. This location is defined in the File Servers tab of the Object Type Maintenance window.
- The %PS_HOME% location for the COBOLs to be compiled. This value is taken from the Windows registry entry for PS_HOME. All the COBOL source programs residing in %PS_HOME%\src\cbl are compiled.
- For NT servers, The location where the compile is to take place. By default, *C:\temp\compile*.
- For Mainframe servers, the name and location of the JCL file used to upload cobols

Except for the definition of the operating system, all of these settings can be changed at the time of execution.

Run DataMover Script

When this step is triggered, Stat logs in to the PeopleSoft environment (by default, the target environment of the migration) using the user's PS operator ID and password and runs the selected Data Mover script. By default, Stat uses the .dms file in the subdirectory "\script," which is appended to the PeopleSoft Home Directory (PS_HOME) defined in the PeopleSoft Configuration Manager. All of these settings can be changed at the time of execution.

Defining a Custom Command

You can define custom commands for pre and post migration steps. These are operating system commands executed by the Stat Central Agent. Commands can be executed locally where the Central Agent is running or remotely on a migration target server via SSH. All drive mappings and file paths are relative to the server where the Central Agent is running. Commands can be triggered automatically during the migration or manually by the migrator.

To define a custom command:

1. In the Pre and Post Migration Step Maintenance window, click **New** and specify the object class and object type of the step you want to create.
2. Select the type of executed step: Pre or Post.
3. In the Migration Step drop-down list, select **Custom Command**.
4. Select **Auto** if you want the step to trigger automatically.
5. Specify a name for the step in the **Description** field.
6. Select Object Class and Object Type.
7. Select Default Run Order. The step execution order can be changed later during migration initialization.
8. (Optional) Add **Target Environment** to trigger a migration step for a specific environment.
9. Click **Apply** to save your work.
10. Click **Define Command**.

    Stat opens the Pre/Post Migration Step Command Editor window.

Pre and Post migration steps can be run locally on the Stat Central Agent machine. Some steps can also be configured to run remotely via an SSH connection.

- For PeopleSoft and Generic file objects, the step can be run on all defined file locations or on the default file location.
- For Oracle E-Business objects, the step can be run on all target servers. Note, for each Server, the file server entry has to be defined in **Object Type - Server**.

Note that in order to run the step remotely, SSH must be configured for the target server.

When defining a command, you can include predefined parameters as well as user and server-based parameters that have been defined in Stat. This provides a convenient way to specify values commonly invoked by operating system commands, such as server names and download directories. In addition, parameters offer a way to secure sensitive information by encrypting values that you do not want visible to users such as passwords.

Predefined parameters specify values used to login into an environment during a migration (database name, user name and password) or to invoke Stat web services (service domain and CSR ID). User and server-based parameters, on the other hand, generally invoke values associated with the users and file servers defined in Stat. Also, certain parameters may be defined so that their values are different depending on which user or server they are being applied to. For more information, see the section, Pre/Post Migration Steps Parameters on page 88.

NOTE: In the case of Oracle-based environments, predefined parameters also include host name, service name, DB listener port, and TNS entry, and for Oracle Applications environments, APPL_SYS_USERNAME and APPL_SYS_PASSWORD.

11 In the **Command** field, enter the command you want Stat to run.

If you want to include parameters in the definition of the command, click the location in the command line where you want to insert the parameter. Then select parameter type and double-click the parameter you want to insert. When included in a command, the parameter name is enclosed by two percent symbols (%%), for example, “%%GL_PWD%%.”

Certain users and file servers may have parameters that have been defined specifically for them, or the value of a particular parameter may be different depending on which user or server it is being applied to. When the Stat Command Editor is first opened, the parameters are listed as they have been defined for the local client server and the current user. If you want to include parameters defined for a different server, click the **Server defined** option. Click the **User defined** option to insert a user-specific parameter.

12 Stat includes a predefined TARGET_OBJECT_NAME parameter that you can use in custom run commands for objects. When this parameter is present in a command, the step will be executed as many times as the number of migrated objects of that type.

13 To run multiple commands on Unix, separate the commands with a semicolon. To run multiple commands on Windows, separate the commands with “&&”. To run commands on Windows, use “cmd /c” before the command.

14 If the command is still running when the connection times out, no log is attached to Stat. However, you can adjust the 5 second default SSH connection timeout setting. A longer connection timeout setting allows the SSH session to stay connected the entire time the command is being processed, in which case the SSH session log will be attached to Stat.

15 (Optional) In the **SSH time-out in seconds** field, specify a longer connection timeout amount.

16 (Optional) Specify the command return code condition on which migration will be stopped. When a pre-migration step completes with an error, the entire migration will halt with status “Waiting for Pre-Step.” When a post-migration step completes with an error, then migration will halt with status “Waiting for Post-Step.” To continue migration, a migrator can manually trigger that step or change the status of that step to Completed or Canceled.

17 Click **Apply**.

Release Management Maintenance

The Release Management Maintenance table defines major and minor release labels that users can assign to archive sets. This gives users the ability to upgrade their applications or roll back to previous versions by mass migrating archive sets based on application release number. For more information on mass migrating archive sets based on application release labels, see the “Object Migrations” sections in the change management chapters of the *Stat User Guide*.

Application releases are based on a branching concept by which minor releases reference their immediate parent releases. This way, when a user mass migrates archive sets based on a minor release label, for example, 2.1, any archive set assigned its parent release label, 2.0, are migrated as well.

Application release security is controlled by the following user class rights:

- Application Releases - Add
- Application Releases - Edit

The Release Management Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Release Management**.

Application release numbers are specific to service domain and change management module.

Value	Description
Release Level (Key Value)	A tree view displaying major and minor releases
Active	If selected, activates the value in Stat
Release Name	Name assigned to the release number
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user who last updated this record

To define an application release number:

1 In the **Domain** field, select the service domain.

2 In the **Module** field, select the change management module.

3 Do one of the following:

- To define a new major release number, click **New Major**.

Stat adds a folder icon to the Release Level view on the left side on the maintenance table window.

- To define a minor release number, select the major release you want and click **New Minor**.

Stat adds a subfolder icon beneath the release number icon you selected. You can define minor releases of minor releases.

> **NOTE:** When assigning a release label to an archive set, Stat concatenates the name of a minor release with the name of its parent releases, separated by decimal points. For example, if you name a minor release “2”, and its parent major release “1”, Stat displays the value as “1.2” when assigning an archive set a release label. This is also true for minor releases of minor releases.

4 Enter a name for the release.

Typically application releases use a sequence of ordinal numbers, such as 1, 2, and so on. However, you can name the release anything you want.

> **NOTE:** You can use the same name for a major and a minor release, but you cannot use the same name for two releases defined on the same level. This includes names that use leading or trailing spaces.

5 (Optional) If you want to delete the release numbers you just defined, click **Reset**.

6 Click **Apply** or **OK**.

Template Maintenance

Template Maintenance tables define text templates that are placed in the Description and Resolution tabs of a CSR. Templates are triggered by CSR type and application codes. When a user working on a CSR selects a type or application associated with a template, Stat automatically inserts that template into the text field of the tab that it has been defined for. You can define a separate template for each application and CSR type in a service domain. If a template exists for both the selected CSR type and application, Stat displays the type template above the application template.

Although templates are optional, they are strongly recommended to get the most out of your Stat system.

Template security is controlled by the following user class rights:

- Templates - Add
- Templates - Edit

The Application Template Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Templates for Description/Resolution | Application Templates**.

The CSR Type Template Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Templates for Description/Resolution | CSR Type Templates**.

The following table defines the fields (columns) in the both the Application Template Maintenance window and the CSR Type Template Maintenance window.

Value	Description
Active	If selected, activates the value in stat
Application/ CSR Type (Key Value)	The application or CSR type that the template is based on
Type (Key Value)	Determines whether the template is to be used in either the Description or Resolution tab
Description	A 1-35 character description of the template
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

The Edit Template Window

After you have defined a new template record, click **Apply** to save your work. Then click **Template...**. Stat opens the Edit Template window. Here you can specify the information that a user is required or recommended to enter in the Description or Resolution tab of a CSR. The Edit Template window features the same rich text editing capabilities supported in the Description and Resolution tabs, including a Formatting toolbar. For more information on rich text editing, see the *Stat User Guide*, Chapter 3, “Change/Service Requests.”

To create a template, type a short description of each piece of information that the user is required or recommended to enter. For required information, use double angle brackets: <<>>. In the example above, the sample template specifies recommended information, including User ID and Description of the Request.

After defining the template, click **OK** or **Apply** to save your work.

Queue Maintenance

The Queue Maintenance table defines work queues, which are specific groups of Stat users with similar skill sets or responsibilities. A queue determines which users are available to have a CSR assigned to them. After you define a queue, you can then determine its membership by selecting individual users.

Queue security is controlled by the following user class rights:

- Queues - Add
- Queues - Edit

The Queue Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Work Queues | Queue Definition**.

Value	Description
Active	Indicates if the record is activated in Stat
Queue Cd (Key Value)	A 1-10 character code which uniquely identifies the queue
Description (Required Value)	A 1-35 character description of the queue. **NOTE:** All queues in a service domain should have a unique description to allow users to choose the correct queue from drop down lists.
Queue Owner (Required Value)	Open the drop down list and select the Stat user who will have primary responsibility for managing this queue. This value is used primarily for automated emails and past-due escalation. The queue owner is automatically assigned membership to the queue and cannot be removed.
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Editing Queue Membership

After you have defined a queue, the next step is to assign Stat users to work in the queue. This is referred to as queue membership or queue assignment.

To access queue membership, select the queue and click **Membership...**. Stat displays the Queue Membership Maintenance window.

> **NOTE:** You can also access this function directly by selecting **Queue Assignment** from the **Work Queues** submenu. In addition, you can add or remove individual users from queues in the User Access Information window. For more information, see Queue Assignment Tab on page 39.

The Queue Membership Maintenance window displays two lists of users. The list on the right lists the users currently assigned to this queue, including the queue owner, who is automatically assigned membership and cannot be removed. The list on the left shows all users in the service domain that are not members of this queue. To edit the membership of a different queue, select it in the **Queue** field. Each queue includes its associated service domain code in braces.

Adding Members to a Queue

To add members to the queue, simply drag and drop a user from the list on the left to the list on the right.

Removing Members from a Queue

To remove a member from the queue, drag the user from the list on the right to the list on the left. You cannot remove the queue owner. To change the owner of the queue, close this window and specify a different owner in the Queue Maintenance table. You can then remove the previous owner from the list.

Workflow Maintenance

The Workflow Maintenance table defines sets of rules that regulate the sequence and conditions by which CSRs can change from one status to another. For example, a workflow can enforce that all the tasks associated with an activity must be completed or that a migration to a specific environment take place before a CSR can be changed to a closed-type status. Workflows are based on a combination of service domain and CSR type. If you define more than one workflow for a given combination of service domain and CSR type, you can designate one of them as the default workflow.

When defining a workflow, you first specify such basic information as its name and the CSR type that triggers it in the Workflow Maintenance table. Then in a separate window you create a template diagram that defines the sequence of status changes, beginning with an initial, opening status and ending in one or more closed-type statuses. As you build the diagram, you can also define transfer rules and status rules, which further regulate CSR status changes. Transfer rules enforce conditions which must be met before a CSR can change from one status to another, whereas status rules apply restrictions to a CSR while it is in a particular status.

Workflow security is controlled by the following user class rights:

- Workflow Maintenance - Add
- Workflow Maintenance - Edit

The Workflow Maintenance table is displayed in a standard maintenance window. To open this window, select **Maintenance | Domain-Specific | Workflows**.

NOTE: If you select a migration path, only that migration path will be available on the CSR. If you want the availability of multiple migration paths on the CSR, in the **Module** field, select N/A and in the **Migration Path** field, select Any. However, be aware that if you plan on defining transfer rules or status rules that involve environments, you must select a migration path for the workflow.

Value	Description
Active	If selected, activates the value in stat
WorkFlow Name (Required Value)	The name of the workflow
CSR Type (Key Value)	The CSR type that, in combination with the service domain, triggers the workflow. Options include all the CSR types defined for the selected service domain.
Module	If the workflow involves migrations, the change management support module that determines which migration paths are available on the CSR. Options include any module defined for the service domain, such as PeopleSoft, generic application, or N/A (if none).
Migration Path	The migration path, if any, assigned to CSRs controlled by the workflow. If you plan on defining transfer rules or status rules that involve environments, you must select a migration path for the workflow.
Default	Indicates if this is the default workflow for the combination of service domain and CSR type
Obj Control	If selected, allows the user designing the workflow to define status rules that prevent users from adding objects to a CSR while it is in a particular status.

Value	Description
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user who last updated this record

NOTE: Defining a workflow involves referencing several other items in Stat, such as CSR types and statuses, activity codes, migration paths, and queues. For this reason, you should define workflows only after you have defined these other items.

Template Diagrams

After you have defined a new workflow in the maintenance window, click **Apply** to save your work. Then select the workflow and click **Template...**. This opens the Workflow Template window. The left section of the window contains a list of CSR statuses defined for the selected CSR type. The right section of the window is where you arrange the icons to create a graphical diagram representing the sequence of the workflow, beginning with an initial, opening status and ending in one or more closed-type statuses.

To create a workflow diagram:

1. In the left section of the window, click and hold on the status of the workflow. Then drag into the right section of the window to where you want to place the graphic and release the mouse button.
2. Right-click on the graphic you just placed. Then in the pop-up menu, select **Set Start**.

   An “S” flag appears to the left of the graphic indicating that this is the start status in the workflow.

   NOTE: Designating a start status is required. When you designate a start status, that status is automatically the status for new CSRs controlled by the workflow. For this reason, you can designate only one start status in a workflow.
3. Place other icons within the diagram representing the statuses that follow the start status within the workflow sequence.

CAUTION: Positioning status graphics very close together or using the maximum number of character s allowed in status names may cause the workflow diagram to display improperly in Stat Web with transfer arrows and connection lines becoming entangled with status graphics. If you intend to have the workflow diagram viewed in Stat Web, position status graphics with enough horizontal and vertical space between them.

4. Do one of the following to begin connecting the statuses in your diagram:
   - Click and hold on the start status. Then drag to the next status in the workflow and release the mouse button.
   - Double-click on the start status. Then double-click on the next status in the workflow.

   A line appears connecting the two statuses with an arrow indicating the direction of the sequence. If you want the sequence to be bi-directional, meaning that the CSR can go to one status and then back again, use the drag and drop method or double-click the second status and then double-click the first status. A second arrow pointing in the opposite direction appears on the line connecting the two statuses.

   NOTE: When you begin connecting statuses in your template diagram, the lines that connect statuses all display hollow arrows, which in a CSR would mean the transfers are invalid. In this case, however, it only means that while you can define status transfers in the Workflow Template window, you cannot execute them.
5. Repeat steps 3 and 4 until the workflow diagram accurately represents the sequence of CSR statuses that you want.

At least one status in the diagram must be designated as Closed in the CSR Status Maintenance table. An “E” flag appears to the left of the graphic, signifying the end of the CSR’s life cycle and is for informational purposes only.

TIP: You can use duplicate icons to represent the same status more than once in a diagram. This can make your diagram easier to understand if a particular status appears at different points within a workflow sequence.

6 (Optional) Do any of the following:

- Click **Print Preview** to print the diagram if it’s entirely visible in the window.
- Click **Update CSRs** to synchronize workflow changes with the existing CSRs containing this Workflow. This action opens a window where the user can select which CSRs to update.

7 Click **OK** or **Apply** to save your work.

If the workflow diagram does not include both a start status and a closed-type status, Stat displays an error message.

You can move status icons in a workflow diagram either by dragging and dropping, or you can select an icon and use the arrow keys. When you move icons with the arrow keys, any transfer connection line graphics are moved as well.

To remove a status icon or a transfer connection, right-click on the graphic and in the pop-up menu, select **Delete Step** or **Delete Link**, respectively. To remove a status icon connected to another icon, you must first remove the transfer connection.

Workflow Rules

In addition to the status change sequence defined by a workflow diagram, you can further regulate the life cycle of CSRs by defining transfer rules and status rules. Transfer rules stipulate conditions which must be met before a CSR can move from one status to another. Status rules limit the range of certain values available in a CSR while it is in a particular status.

NOTE: Status rules and transfer rules are optional. By default, there are no special conditions imposed on the CSR statuses affected by a workflow.

Transfer Rules

After connecting two statuses in the Workflow Template window, you can define a set of transfer rules that specify conditions that must be met before the status change may occur. Using transfer rules you can stipulate the following:

- The queue the CSR must belong to
- The tasks the must be performed (identified by activity codes)
- The environments that objects must be migrated to
- The user who can perform the actual status change
- Whether or not the transfer requires the approval of other users, and if so, which users are authorized to make the approvals
- For the Oracle Applications module, the environments that a patch must be applied to

NOTE: The user class right, Status Transfer Override, enables users to perform status changes even if the transfer rules are incomplete.

Stat records the time and date when a CSR enters a status and when it exits that status. This means if you define two or more transfer rules in a workflow that requires migrations to the same environment, performing the migration the first time will not satisfy the other rule(s) that require the same migration. For example, let’s say you define two transfer rules: the first rule says a migration must occur to the Production environment before a CSR can transfer from the status A to the status B. The second rule also says a migration to Production must occur

before the CSR can change from the B status to a third status, C. Because Stat records the time and date that a CSR is in a particular status, the first transfer rule can only be satisfied if the migration occurs during the time the CSR is in status A, and the second transfer rule can only be satisfied if the migration occurs during the time the CSR is in status B.

To define a transfer rule:

1. In the Workflow Template window, right-click on the arrow that appears on the line connecting the two statuses, or if the connection is bi-directional, right-click on the arrow indicating the transfer connection you want. Then in the pop-up menu, select **Transfer Rule**.

   Stat opens the Transfer Rules window for the selected transfer. In this window you can define several different transfer rules, all of which are optional.

2. If you want the CSR to belong to a particular queue before it can be transferred, select the queue in the **In Queue** field.

   Default value is **Any**.

3. If you want to enforce that only certain users or user classes to make the transfer, in the **Status Changed By** field do one of the following:

   - Select **User** if you want to authorize individual users to make the status change. Then in the displayed list of users, select each user you want to authorize.
   - Select **Users in Class** if you want to authorize all the users in specific user classes to make the status change. Then in the displayed list of user classes, select each user class you want.

4. To require that activities associated with a CSR are completed before a transfer can occur, select those activity codes in the **Complete Activity** field.

CAUTION: When you select an activity in the Transfer Rules window, all the tasks associated with that activity must be completed before the status change can occur. This includes auto tasks. Also, if you specify an activity but no tasks associated with the activity have been associated with the CSR, the transfer cannot take place.

5. If migrations to a certain environment must occur before a status transfer can occur, select those environments in the **Migration To** field.

   NOTE: The environments displayed in the **Migration To** field, if any, are determined by the migration path specified in the Workflow Maintenance table. In addition, you can assign user class rights that enable users to migrate to any environment in the migration path regardless of transfer rules.

6. If you are defining a transfer rule for a workflow in the Oracle Applications module and you want to stipulate that a patch must be applied to a particular environment before the transfer can occur, select those environments in the **Apply Patch To** field.

   The patch application option is not used for workflows in the PeopleSoft and generic applications modules.

CAUTION: Make sure your status rules and transfer rules are consistent. For example, if you define a status rule that says a CSR must belong to the Mgmt queue, do not then define a transfer rule that does not allow a CSR to belong to the Mgmt queue.

7. If you want certain users to approve the status change before it can take place, select **Require Approval**.

   This activates the Approval List tab. See the next section for information on setting up transfer approval lists.

8. Click **OK** or **Apply** to save your work.

   In the workflow diagram, a red line is displayed at the base of the arrow appearing on the line connecting the two statuses, indicating the presence of a transfer rule.

Setting Up Transfer Approval Lists

If a CSR status transfer requires the approval of certain users, you can specify who these users are in the Approval List tab of the Transfer Rules window.

When setting up a transfer approval list, you can include different approver groups, including individual users, entire user classes or queues, or a combination of the three. The approval of any user, user class, or queue that you add to a list can be either required or optional.

Approval requirements that involve multiple approver groups or that can be satisfied in more than one way are defined using AND and OR operators. As you add approver groups using AND and OR operators, Stat displays the list as a tree structure and in the form of a SQL statement at the bottom of the window.

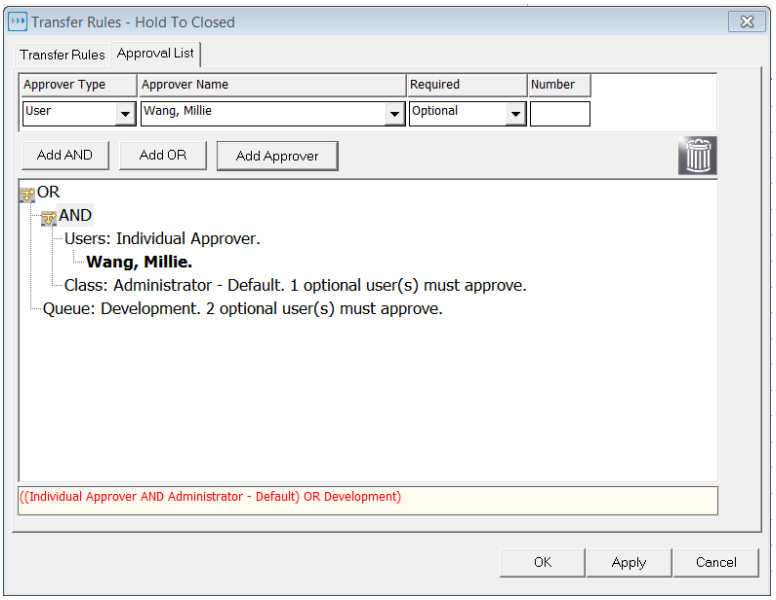
For example, let's say a status transfer can be approved in one of two ways:

- By an individual user AND at least one user in the Administrator - Default user class

  OR

- By at least two users in the Development queue

In this case, your approval list would look like this:



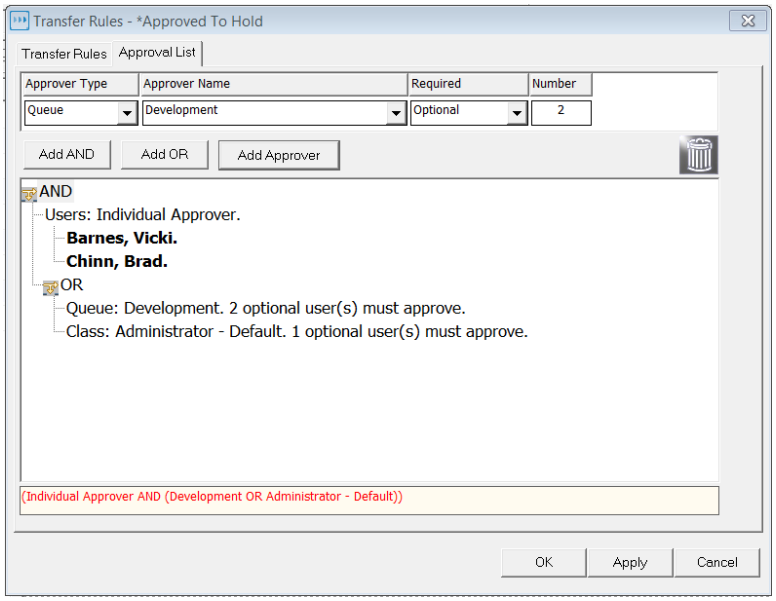
To further illustrate, let's say that the status transfer must be approved by:

- Two individual users

  AND

- At least one user in the Administrator - Default user class OR at least two users in the Development queue.

In this case, the approval list would look like this:



It is recommended that before setting up a transfer approval list, you have a basic idea of what approver groups (users, user classes, and queues) you want involved in the approval process as well as the relationships between these groups, which you define using AND and OR operators. For example, if the approval of one or more approver groups are required, you would begin the approval list with the AND operator. If, however, the approval of only one of two or more approver groups are required, you would begin the list with the OR operator.

After defining a transfer approval list, you can configure Stat to automatically transfer the status once all the required approvals and any other conditions of the transfer rules have been met.

To set up a transfer approval list:

1 Do one of the following:

- Click **AND** if the approval of one or more approver groups are required
- Click **OR** if the approval of one of two or more approver groups are required

The operator icon is added to the approval list diagram.

2 Click on the AND or OR operator icon you just added.

> **TIP:** The icon background appears blue when selected and changes to gray when other fields or action buttons are activated. As long as the background of the operator icon is blue or gray, then approver groups and other operators can be attached to the operator.

3 In the **Approver Type** field, select the approver group you want to add to the list.

Options include **User**, **User Class,** and **Queue**.

When adding approvers, be aware of the following:

- Adding individual users to approval lists could create problems if those same users are later inactivated or have their service domain and environment access restricted. For this reason, it is recommended that you add user classes to approval lists rather than individual users whenever possible.
- Users assigned to a transfer approval list must have the user class rights to operate in the same change management module in which the status transfer takes place. Also, you can assign user class rights that enable users to change CSR statuses regardless of approval status and also to approve status transfers on the behalf of other users.

4 In the **Approver Name** field, select the name of the user, user class, or queue you want to add.

5 In the **Required** field, select **Required** if the approval is required or **Optional** if it is not required.

The **Required** option means that the individual user and every member of the user class or queue must approve the status transfer. **Optional** means that the individual user's approval is not required, whereas for user classes and queues, it means that the approval of only a specified minimum number of users within that class or queue are required.

6 If you selected **User Class** or **Queue** in the **Approver Type** field and **Optional** in the **Required** field, specify the minimum number of users in that class or queue who must approve the transfer in the **Number** field.

7 Click **Add**.

The approver is added to the tree structure under its approver group label and the initial AND or OR operator. Required approvers are displayed in bold.

At this point, how you proceed depends on the different approver groups you want to add to the list and how you want to define the relationships between these groups using AND and OR operators.

8 (Optional) Do the following to add additional AND or OR operators to your approval list:

a Depending on the relationship between approver groups in your list, select the operator icon to which you want to attach additional operators.

b Click **AND** or **OR**.

c Repeat as necessary to add more operator icons to the approval diagram.

9 (Optional) To add additional user class or queue approver groups, select the appropriate operator icon in the approval diagram and repeat steps 3 through 7.

When you the first add an individual user to an approval list, Stat automatically creates the ad hoc group "users" in the approval diagram and attaches it to the appropriate operator icon. All subsequent users you add to the list must belong to this group.

TIP: In a scenario in which you want to create approval relationships between multiple user approver groups, you may consider adding users to new user classes or queues created expressly for this purpose.

10 (Optional) To add additional users, select the "users" group and repeat steps 3 through 7.

11 (Optional) Do any of the following to edit the diagram as needed:

- To change an operator from AND to OR or from OR to AND, right-click on the icon.
- To change the Required status of an approver, right click on it in the diagram. This changes required user classes and queues to optional with 1 required user.
- To change the minimum number of user approvals in an optional user class or queue, double-click on the group label and specify the minimum number of user approvals you want.
- To move approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to a different operator icon in the diagram.
- To delete approver groups or entire operator relationships, click and hold on the group label or operator icon and drag and drop to the Trash Can icon.

12 Click **OK** or **Apply**.

Auto Advance Option

To instruct Stat to automatically transfer rules, select the **Auto Advance** check box. The Auto Advance option is only available on transfer rules that have either Tasks rules, Migration rules, OA Patch Apply rules, or approval lists. All transfer rules must be completed for an auto-advance to take place.

Setting the Auto Advance option on the two transfer rules from the same status (A>B and A>C) could create a conflict where both rules are satisfied at the same time that the CSR is saved. When this is the case, Stat does not automatically transfer the status because it is not clear which transfer has precedence.

Status Rules

Status rules let you apply restrictions to a CSR while it is in a particular status, such as the queue(s) that it can belong to, whether objects can be added or locked on a CSR and what environments objects associated with the CSR can be migrated to. For Oracle Applications, you can also limit the environments that can have patches applied to them.

To define a status rule:

1. In the Workflow Template window, right-click on the graphic representing the status you want. Then in the pop-up menu, select **Status Rule**.

   Stat opens the Status Rules window for the selected status.

2. If you want to limit the queues that a CSR can belong to while in the selected status, select the queues you want in the **Available Queues** field.

   If you do not select a queue, the CSR can belong to any queue in the list.

3. If the workflow involves migrations and you want to limit the environments that objects can be migrated to while the associated CSR is in the selected status, select the environments you want in the **Environments Available for Migration** field.

   If you select ***{None}***, no migrations can take place while the CSR is in the particular status. If you do not select an environment, the objects can be migrated to any of the environments in the list.

4. If you want to limit the environments in which archive sets can be created while the CSR is in the selected status, select the environments you want in the **Environments Available for Archiving** field.

   If you select **{None}**, no archive sets can be created while the CSR is in the particular status. If you do not select an environment, archive sets can be created in any of the environments in the list.

5. If the **Obj Control** option has been selected for the workflow in the Workflow Maintenance table and you want to allow users to add and lock objects on a CSR while it is in selected status, select the option **Allow Object Add/Lock**.

   If you do not select this option, users will not be able to add or lock new objects on a CSR while it is in the selected status. Object reservations that were in place when the CSR was transferred to the selected status, however, are converted into locks when the objects become available, as they would be normally.

6. If you want to require that developers enter a resolution in the Resolution tab of the CSR before transferring the status, select the **Require Resolution** option.

   By default, users are required to enter a resolution whenever a CSR enters into a closed-type status. However, in certain cases it may be desirable that the resolution of the CSR be documented before it is closed. With this option, you can require that the resolution of the CSR is documented before the CSR changes from the selected status to any connected status in the workflow.

7. If you are defining a status rule for a workflow in the Oracle Applications module and you want to limit the environments that can have patches applied to them while the associated CSR is in the selected status, select the environments you want in the **Environments Available for Patch Application** field.

   If you select **{None}**, no patches can be applied while the CSR is in the particular status. If you do not select an environment, a patch can be applied to any of the environments in the list. The patch application option is not used for workflows in the PeopleSoft and generic applications modules.

> **!** **CAUTION: Make sure your status rules and transfer rules are consistent. For example, if you define a status rule that says a CSR must belong to the Mgmt queue, do not define a transfer rule that does not allow a CSR to belong to the Mgmt queue.**

8. Click **OK** or **Apply** to save your work.

   In the workflow diagram, an asterisk is displayed next to the graphic representing the status, indicating the presence of a status rule.

Copying Workflows

If you want to copy a workflow to another service domain, associate a workflow to more than one CSR type, or if you want to create a new workflow that closely resembles an existing workflow, you can make a copy of that workflow and then modify it as needed.

You can associate a copied workflow with a different CSR type. However, you must associate it with a CSR type that is associated with same CSR statuses as the original CSR type. To copy a workflow to another service domain, the target service domain must include a CSR type that is associated with the same set of CSR statuses as the CSR type in the original workflow.

When copying a workflow, you can also select a different module and migration path. However, if you select a different migration path, this may conflict with any workflow rules you copy that require migrations to specific environments. When this is the case, you can either remove the migration requirements from the copied workflow rules, or you can update the copied workflow rules by referencing the new environments.

To copy a workflow:

1 In the Workflow Maintenance window, select the workflow that you want to copy and click **Copy Template**.

Stat opens the Copy Template window.

2 If you are copying the workflow to another service domain, select the service domain in **service domain** field.

The **CSR Type** field lists all the CSR types in the selected service domain that are associated with the same set of CSR statuses as the CSR type in the original workflow. If there are no matching CSR types, the **CSR Type** field is blank and you cannot copy the workflow to the selected service domain.

3 In the **CSR Type** field, select the CSR type you want to base the copied workflow on.

You can assign a different migration path to the copied workflow. You can select any migration path in any change management module you have access to. Be aware, however, that if the transfer and status rules of the original workflow require migrations to specific environments, you must do one of the following to successfully copy the workflow:

- Opt not to copy the transfer and copy rules from the original workflow, or to exclude rules that specify migration environments, in which case the copied workflow will not require migrations to specific environments
- Map the environments in the original workflow to environments in the migration path of the copied workflow. This way, status and transfer rules copied from the original workflow will be automatically updated with the different migration environments.

4 (Optional) If you want to assign to the copied workflow a migration path that is defined for a different change management module, select that module in the **Module** field.

5 (Optional) In the **Migration Path** field, select the migration path you want to assign to the workflow.

6 Type a name for the workflow in the **Workflow Name** field.

> **NOTE:** You may want to use the same name as the original workflow if all you are doing is assigning the copied workflow to a different CSR type in the same service domain.

7 Deselect the **Copy Status Rules** or **Copy Transfer Rules** options if you do not want to copy either the status rules or transfer rules.

8 Deselect the **Exclude Migr. Env** option if you want to copy status and transfer rules that require migrations to specific environments.

At this point, if you are copying rules that require migrations to specific environments but have assigned a different migration path to the copied workflow, Stat displays the Transfer Migration DB window which prompts you to map the environments in the original workflow to the environments in the copied workflow.

9 Map a new environment to each environment in the original workflow

10 Click **OK** when done.

The copied workflow is displayed in the Workflow Maintenance table. If you copied the workflow to a different service domain, select that service domain in the **Domain** field to see the copied workflow. At this point, you can open the workflow in the Workflow Template window and modify the template diagram and workflow rules as needed.

6

Configuring the Stat Central Agent

- Starting and Stopping the Stat Central Agent
- Defining Agent Jobs
- Stat Central Agent Printers
- Monitoring the Stat Central Agent
- Customizing the What's New Tab in Stat Web
- Customizing Field Labels for the Stat Web Client

Starting and Stopping the Stat Central Agent

The Stat Central Agent is responsible for automating necessary but time-consuming work, such as generating and printing reports, sending email messages, archiving objects, and maintaining specific database parameters.

The Stat Central Agent is designed to run behind-the-scenes with minimal supervision on the part of system administrators. However, you can manually start and stop the Stat Central Agent when circumstances demand it.

You can run the Stat Central Agent on either a Windows or a Unix platform. If configured properly, the Stat Central Agent can also be run as a Windows Service. For information, see *Stat Install Notes*.

Starting the Stat Central Agent

To start the Stat Central Agent on either a Windows or a Unix platform., do one of the following:

- For windows: execute <STAT_HOME>*\app\bin\run.bat*
- For unix: execute <STAT_HOME>*/app/bin/run.sh*

The server log displays the lines, "Stat Central Agent Web Component is started" and "Stat Central Agent is started" when the startup process for Stat Web and the Stat Central Agent have completed successfully.

Optionally, you can run the Stat Central Agent as a Windows service using the wrapper that is provided with Stat. This is done using the service.bat shell command located in the *STAT_HOME/bin/service* folder. For information on starting and stopping the Stat Central Agent as a Windows service, see *Stat Install Notes*.

Stopping the Stat Central Agent

To stop the Stat Central Agent on either a Windows or a Unix platform, do one of the following:

- For Windows, go to <STAT_HOME>\app\bin and run shutdown.bat in a command line editor.
- For Unix, go to <STAT_HOME>/app/bin and run shutdown.sh in a command line editor.

You can also create a desktop shortcut which sends the appropriate command-line shut down argument to the Stat Central Agent.

If you have modified your port offset from the default value of zero due to conflicts with other systems, etc., then you must supply the modified port information to the shutdown command so that it can find the server to shut it down.

For example, if you modified the port offset to one, you need to edit **%STAT_HOME%\app\bin\shutdown.bat** and modify it as below:

```
jboss-cli.bat --connect controller=localhost:9991 command=:shutdown
```

For Unix installations, you need to edit **$STAT_HOME/app/bin/shutdown.sh** and modify it as below.

```
./jboss-cli.sh --connect controller=localhost:9991 command=:shutdown
```

Also, if you running more than one Stat Central Agent on the same host machine, you must specify the port offset. In this case, you must also specify the port number when executing the shutdown command. The port numbers for a port offset of one is 9991 and for a port offset of 100 is 9990+100=10090. Again, these numbers may be modified if they conflict with other applications.

Defining Agent Jobs

After you install the Stat Central Agent, there are certain jobs you need to define and schedule. This is done in the Stat Central Agent Job Maintenance table. To open this window, select **Maintenance | Stat Central Agent | Job Maintenance**.

Value	Description
Enabled	Indicates if this job is active or not
Job ID (Key Value)	The unique number assigned to this job by Stat
Owner (Required Value)	The user ID of the creator of this job. It will always be SYSTEM except for scheduled report jobs added by users.
Class (Required Value)	The class of the job to be performed. Job classes are described in detail in the section, “Job Class Parameters,” later in this chapter.
Description (Required Value)	A user defined description of the job. If not changed by the user, the description will default to the job class.
Last Update (Read Only)	The date and time that this record was last updated
Update By (Read Only)	The user that last updated this record

Error Notification

You can configure the Stat Central Agent to send emails to certain Stat users or user classes when errors are encountered. To configure error notification, click **Domain Options**. This opens the Agent Domain Options dialog box.

NOTE: You can also setup error notification for each job assigned to an agent. If an agent encounters an error while processing a job that has a separate error notification setup, Stat sends emails to the list of recipients defined for the job, not the list defined for the agent.

To setup default error notification:

1. Click **New**.
2. In the **Recipient Type** field, select **User** if you want to add an individual user or select **Class** if you want to add a user class.
3. In the **Recipient** field, select either the individual user or user class you want to add.

4 Repeat steps 2 and 3 for each recipient you want to add.

5 Click **OK**.

Job Maintenance

To create a new job, click **New**. This opens the Job Maintenance window.

The fields displayed in the Job Details tab vary depending on the job class. However, the following fields are displayed for all jobs:

Job Enabled

If selected, indicates that the job is activate.

Job Nbr

The unique identification number assigned to the job by Stat.

Owner

The user ID that created this job. It defaults to “SYSTEM” except for scheduled report jobs defined by users.

Job Class

The category of the job to be performed. For more information, see, Job Classes on page 165.

Description

A user-defined description of the job. This field defaults to the job class, unless changed by a user.

Job Classes

Job classes are predefined jobs that you can assign to the Stat Central Agent. Some job classes require you to define additional parameter values. When you select a job class with parameters, the fields on the Job Definition tab change accordingly. Unless otherwise noted, these jobs are service domain-specific.

Check for Past Due Items

This job checks the environment for CSRs, projects, tasks, CSR status transfers, and approvals that are past due as of the job’s scheduled run time and writes event records for the Stat Central Agent. The Agent then processes these records for business rules and email.

Email Reports and Print Reports

These jobs email and print reports, respectively. When you select either one of these jobs, two additional tabs appear on the Job Maintenance window, Report and Destination. The procedures for setting up an Email Reports job and a Print Reports job are documented in the *Stat User Guide*, Chapter 8, “Reports and Graphs.”

Log Off and Wait

This job instructs the Stat Central Agent to log off of the system and stop all processing for a specified amount of time. This can be used during periods of database maintenance when the Agent should not be connected, for example.

NOTE: You only need to define one Log Off and Wait job per time period. You do not need to define separate jobs for each service domain.

Wait (minutes) parameter: Enter the number of minutes you want the Agent to wait before logging back on to the system.

CAUTION: This job may result in other jobs being skipped. For example, if the Agent logs off at 11:30 P.M. for 60 minutes, all jobs scheduled between 11:30 and 12:30 A.M. are not processed.

PS Object Lock Sync

This job makes sure that the PeopleSoft Object Security groups contain the correct objects. They might not contain the correct objects if, for example, someone has modified the group definitions in PeopleSoft. The job has two steps:

- Sync objects locked in Stat by Stat developers with the Object Security Groups for the PeopleSoft developers in PeopleSoft
- Sync all objects in PeopleSoft with the Stat_Read and Stat_Exclud Groups in Object Security

There are two key differences between the physical locking that occurs when users lock objects in a CSR and the PS Object Lock Sync job:

- When a user saves a CSR after locking an object associated with it, Stat Central Agent automatically processes this object lock. It inserts a row in the Assigned Developer's Object Security Group in PeopleSoft for the locked object. This is not done using the PS Object Lock Sync job. Stat Central Agent does it automatically in the background. Once Stat Central Agent finishes this process, the developer can open and modify this object in PeopleSoft.
- You can schedule the PS Object Lock Sync job to run for the selected PeopleSoft environment any time you wish. It is recommend once a day at night.

PS Database parameter: Click the arrow button and select the PeopleSoft environment that this job is run for.

Purge Agent Event Tables

This job purges entries from the Stat Central Agent event tables. It is recommended that you keep at least 7 to 14 days worth of history for troubleshooting purposes.

Retention Days parameter: Enter the number of days for which you want to retain Stat Central Agent event history.

NOTE: For Oracle Applications users, this job also purges all non-patch related entries.

Purge Audit Tables

Purges the STAT_AUDIT table. Unlike other purge jobs, this job only needs to be set up in one service domain as the data on the table is not service domain-specific. This job is best defined as a "Run Once" job that needs to be coordinated with Auditor visits.

Retention Days parameter: Enter the number of days for which you want to retain data regarding audit ables. Can be set from 1 to 999 days.

Purge Deleted Archive Sets

This job purges all data regarding deleted archive sets. It is service domain independent and needs to be set up only once to purge deleted archive set data across all service domains.

Retention Days parameter: Enter the number of days for which you want to retain data regarding deleted archive sets.

Purge Error Log Tables

This job purges entries from the Stat Central Agent error logs. It is recommended that you keep at least 7 to 14 days worth of history for troubleshooting purposes.

Retention Days parameter: Enter the number of days for which you want to retain Stat Central Agent error logs.

Purge Migration Event Tables

This job purges entries from the Stat Central Agent migration logs. It is recommended that you keep at least 7 to 14 days worth of history for troubleshooting purposes.

Retention Days parameter: Enter the number of days for which you want to retain Stat Central Agent migration logs.

Stat Central Agent Purge System-Generated Logs

This job purges CSR logs created by the Stat Central Agent. These logs primarily document outbound email messages. Other messages include locked/unlocked CSRs.

Inbound and outbound email detail logs will not be purged by this job.

Retention Days parameter: Enter the number of days for which you want to retain CSR logs. 7 days is the default.

Run Operating System Command

This job runs an operating system command on the same server or workstation that the Stat Central Agent is running on. The Stat Central Agent only initiates the command and does not wait for the command to complete before moving on to the next job. Also, all drive mappings and file paths are relative to the server or workstation on which the Stat Central Agent is running.

Window State parameters: If the command you want the Agent to initiate opens a window, specify if you want the window minimized, maximized, or normal size.

Command parameter: Enter the command line you want the Agent to run in the **Command** field, or click the Browse button (**...**). This opens the Stat Central Agent Job Command Editor window.

Enter the command in the top portion of the Stat Central Agent Job Command Editor window. Then click **Interpret >>**. The bottom portion displays how the command is interpreted by the server or workstation on which the Stat Central Agent is running.

NOTE: Keep in mind that the command specified in this window gets executed on the system where the Agent is running. For example, a Windows executable will not run if the Agent is running on a Unix system.

You can also enter special symbols representing date and time that are interpreted by the Stat Central Agent command interpreter prior to execution:

Symbol	Interpretation	Example
<<YY>>	The current year, 2-digit format	01
<<YYYY>>	The current year, 4-digit format	2001
<<MM>>	The current month, 2-digit format	01

Symbol	Interpretation	Example
<<DD>>	The current day of month, 2-digit format	31
<<DDD>>	The current day of week	Monday
<<HH>>	The current hour, 2-digit format	13
<<NN>>	The current minutes of the hour, 2-digit format	45
<<SS>>	The current seconds of the minute, 2-digit format	23

For example, if the current date and time is Monday, June 1, 2004 12:31:58, enter the following special symbols:

```
<<YYYY>>-<<MM>>-<<DD>> <<HH>>:<<NN>>:<<SS>>
```

The Stat Central Agent Job Command Editor interprets this as “2004-06-01 12:31:58.”

Click **OK** to close the command interpreter.

After you enter the command in the **Command** field, you can test the command by clicking **Test Command**. Stat executes the command on your workstation and reports if the operating system returned SUCCESS or FAILURE.

Unlock Locked CSRs

If a user is unexpectedly disconnected from Stat (for example, due to a network failure), any CSRs that the user had opened when the session failed will remain locked. This job unlocks any locked CSRs under the following two conditions:

- When the owner of the locked CSR is no longer logged in to Stat
- When the date and time the user lasted connected to Stat, as indicated in the Connection Manager window, is later than the date and time that Stat locked the CSR.

The Schedule Tab

After you specify the details of the job in the Job Definition tab, click the Schedule tab. From here you schedule the day and time you want the Agent to run the job.

NOTE: For each service domain, it is recommended that you schedule the purge jobs to run once a day. These jobs include:

- Purge Agent Event Tables
- Purge Deleted Archive Sets
- Purge Error log Tables
- Purge Migration Event Tables
- Purge System-Generated Logs

The following explains how to define a day schedule and a time schedule:

Day Schedule

In the **Day Schedule** field, select one of the following:

- Select the **Day of Week** option if you want the job to run on certain days of every week. Then select the check box next to the days you want.
- Select the **Day of Month** option if you want the job to run on either the first day of the month, the last day of the month, or both. Then select the options you want.
- Select the **Run Once** option if you want the Stat Central Agent to run the job only once. Then either select **Run Immediate** if you want the Stat Central Agent to run the job immediately (or as soon as possible

depending on agent status and processing time), or click the **Browse** button and in the Calendar window specify the day and time you want the Stat Central Agent to run the job.

Time Schedule

In the **Time Schedule** field, select one of the following:

- Select the **Schedule Hours** option if you want the job to run at certain hours of the day(s) specified in the Day Schedule section. Select the check box next to the hour (in military time) you want. You may also use the spinner controls to specify a value for the minutes after the hour (between 0 and 59). For example, if you want the job to run at 7:30 am, select **07** and enter **30** for the minutes.
- Select the **Minute Intervals** option if you want the job to run at less than one hour intervals. Use the spinner controls to enter a value between 1 and 59.

After specifying the day and time schedule, click **OK** or **Apply** to save your work.

The Error Notification Tab

In the Error Notification tab, you can configure the Agent responsible for the job to send email notifications to certain Stat users or user classes when errors are encountered. The procedure of setting up error notification for a job is exactly the same as setting up error notification for the Agent. If you do not define a separate error notification mailing list for a job, Stat uses the error notification list defined for the Agent. For more information, see Defining Agent Jobs on page 164.

Stat Central Agent Printers

When you schedule a Print Report job for the Stat Central Agent, you must specify the printer that you want the Agent to use. You define the list of available printers in the Stat Central Agent Printer Maintenance window. To open this window, select **Maintenance | Stat Central Agents | Agent Printers**.

NOTE: Any printer you add must be defined on the same server as the Stat Central Agent.

To add a printer:

1. In the **Domain** field, select the service domain in which the print job is defined.
2. Click **New**.
3. In the **Printer Cd** field enter an alphanumeric code of up to 10 characters that uniquely identifies the printer.
4. In the **Description** field enter a short description of the printer
5. In the **Host Printer Name** field enter the port and name of the printer as it is defined on the server. Then click **OK**.

Monitoring the Stat Central Agent

In the Job Monitor page of Stat Web, you can check the performance of the Stat Central Agent and perform basic administrative tasks, such as manually running jobs and configuring the Stat Central Agent to skip scheduled jobs.

To connect to Stat Web, you must have the user class right to access the Stat Web Client (which by default is granted to all user classes but can be removed by system administrators). After you enter both a valid user ID and password, Stat authenticates your logon information and grants you access.

Accessing the Job Monitor

To access the Job Monitor:

1. Open your internet browser and go to the URL address for Stat Web.

   TIP: The URL address for Stat Web is displayed on the About box of the Stat Windows Client. In the Stat Windows Client, select **Help | About Stat**.... to open the About box.

2. Enter your user name in the **User Name** field.
3. Enter your password in the **Password** field.
4. Click **Log in** or press <Enter>.

   NOTE: Connecting as two different users from the same browser (e.g., in separate windows) will cause the second browser window to cancel the first browser's login session. Similarly, if you use a single browser to connect to two different installations of Stat Web, the second login will cancel the first browser's session.

5. In the CSR Console main window, open your user drop-down menu and select **Job Monitor**.

   NOTE: You do not need to have the Job Monitor open in a browser window to process jobs with the Stat Central Agent. Clicking the Close button ('**X**') on your browser window does not shut down the Stat Central Agent.

Schedule Tab

The Schedule tab shows all the jobs scheduled for the current 24 hour period that have yet to be processed. Because jobs can be scheduled to run at particular hour and minute intervals during the day, any jobs that already have been processed are not shown. Also, whenever you refresh the web page, jobs that were scheduled to be processed since the last time you refreshed are removed from view.

The job schedule is defined in the Jobs Maintenance table located in the Stat Windows Client, but from here you can configure the Stat Central Agent to skip selected jobs. If you do not want the Stat Central Agent to process any of the jobs that it is scheduled to perform, select the job(s) and click **Skip Selected**. An icon appears next to the job indicating that it will be skipped.

Jobs Tab

The Jobs tab displays a list of all the jobs that have been defined for the Stat Central Agent. The Agent processes the jobs according to the schedule defined in the Jobs Maintenance table, but from here you can manually run the jobs you want.

To run selected jobs:

1. Select the check box for each job that you want to run.
2. Click **Run Selected**.

   The Stat Central Agent processes the selected jobs and updates the Jobs tab with the latest information.

Logs Tab

Each time a serious or potentially serious error is encountered by the Stat Central Agent, it logs the error to the database. The Logs tab provides you with a list of error logs generated by Stat Central Agent for the current day.

For each error log, the tab displays the date and time it was entered, as well as the job's service domain, ID number, class, description, and status. To view an error log, click on the job description. This opens a message box containing detailed information about the error.

Filtering and Sorting

You can filter the information displayed in the Job Monitor window so that only the jobs or logs you want to view are displayed. Once you have specified filter settings, you can enable and disable the filter as needed.

You can also sort the information by clicking column headings. By default, information is displayed in ascending order. When you click a column heading, the information is sorted in descending order based on the values displayed in that column. Clicking a column heading a second time sorts the information back in ascending order.

Filters can be based on service domain and job class. In the case of the Schedule tab, you can also base a filter on status and the date the jobs are scheduled to be processed.

To specify filter settings:

1. Click on the tab you want and then click **Show Filter Options**.

   The top portion of the window displays the filter options.

2. Do one or more of the following:

   - In the **Service Domain**, **Job Class**, or (in the case of the Schedule tab) the **Status** field, select the values you want to use as the basis for the filter. For example, in the **Job Class** field, select **RptPrint** if you only want to view Print Report jobs.
   - In the case of the Schedule tab, click the calendar icon and in the Calendar window, select the date whose job schedule you want to view. You can only select the current and future dates. Note that when you view jobs scheduled for a future date, the skip jobs functionality is disabled.
   - In the case of the Logs tab, specify a start date, an end date, or both. For example, if you only want to view logs that were generated after April 1, 2004, activate the **From** field and then enter "04/01/2004" or use the Calendar window and select the date. Logs generated before that date will be filtered from view.

3. (Optional) Click **Enable Filter Options** to filter the information in the tab page with the settings you just specified.
4. (Optional) Click **Hide Filter Options** to remove the filter options from view.

Showing Job and Log Details

To view more information about a job or log, click the link in the Job Description column. In the Schedule and Jobs tabs, this opens the Job Details pop-up window, which shows the owner of the job, its priority, and additional parameters. In the Logs tab, this opens the Log Details pop-up window, which shows the individual entries for that log.

To view the details for all the jobs or logs, click **Show Details**. To close a Details window, click the Hide Details link for individual jobs or logs, or click the **Hide Details** button, which closes all open Details windows.

The Job Details window displays different information about a job depending on the tab from which it is opened. When opened from the Jobs tab, the Job Details window displays the same information about a job as it does when opened from the Schedule tab, however, from the Jobs tab the window also shows the job's weekly processing schedule. Job Details windows feature links that let you open the other Details windows for the same job in different tabs.

Customizing the What's New Tab in Stat Web

The Stat Web client is delivered with an include.txt file that specifies default information displayed in the What's New tab in the About window. This file is embedded in the working folders of the Stat Central Agent when it is started up. The delivered file cannot be modified directly. However, it is possible to edit a copy of include.txt and place it in a known location so you can display site-specific information in the What's New tab.

To implement the What's New tab on the web client, you have to set up an html-formatted file that will replace the include.txt file deployed the first time the agent is started.

The general format is:

```
<ul style="display: list-item">
   <li style="list-style: disc">Thank you for using Quest Software's Stat</li>
<li>this is point #2 </li>
<li>this is point #3 </li>
</ul>
```

Stat_home/config/stat.properties contains the pointer to this file. The pointer can be relative (the default), absolute, or a Web http URL.

Open **Stat_home/config/stat.properties** and find the property `whats.new.include`. Four or five lines above it is a description of how this property can be configured. Note when modifying this parameter that there are no spaces between the property name, the equals sign, and the file name. Also, the file paths should not contain spaces.

```
#============================================================

# Client Global Properties

#

# Valid "whats.new.include" parameters: (See
http://www.cs.tut.fi/~jkorpela/fileurl.html)

#   1. relative to distribution (default)       = ../include.txt

#   2. absolute file Windows (i.e. c:\Temp\...) = file:///c|/temp/readme.txt

#   3. web http URL                             = http://www..quest.com

#============================================================

whats.new.include=../include.txt
```

Note when modifying this parameter that there are no spaces between the property name, the equals sign and the file name.Also, the file paths should not contain spaces.

Setting the value to a relative file means you will have to replace the file each time the agent is redeployed. This is not practical and is not recommended. It only works well for the delivered, non-modifed include.txt file.

```
whats.new.include=../include.txt
```

Alternatively, you may create the file in a location outside of the deploy directory and use an absolute path in the what's new parameter. For example:

```
whats.new.include=file://c/directoryname/include.txt
```

Putting it in a directory outside of the agent home directory will allow you to place the file in any secure location where the person responsible for updating it may do so without having to touch the agent or any of its configuration files.

A third option is to use a Web http file. This needs to be a very simplistic web file or the view on the screen may not be intelligible. In this example, the Quest web page is not fully rendered:

```
whats.new.include=http://www.quest.com
```

If you use the second (absolute path) or third (URL) option, you do not need to restart the agent after changing the stat.properties file, and you do not need to restart the agent after modifying the file in order for the What's New description change to take place.

Below is an example of an include.txt file that contains a logo and a message. Images should not exceed 180 pixels in width or they will be truncated.

```
<a target="_blank" href="http://www.Quest.com">
     <img alt="Quest" title="Quest" src="
http://i.Quest.com/images/global/brand/ui/logo-wt-bl.png">
</a>


<ul style="display: list-item">
   <li style="list-style: disc">Thank you for using Quest Stat</li>
    <li>Stay tuned for future announcements </li>
</ul>
```

Customizing Field Labels for the Stat Web Client

The Stat Web Client is delivered with a text file called StatMessageResources.properties which is located under your <STAT_HOME>/config directory. This file contains all the field labels used in the Stat Web Client. If for any reason you need to customize these labels, you may do so by editing this file. You may also use this file if you need to translate these labels into other languages.

7

Email Configuration

- Configuring the Stat Central Agent for Email
- Outbound Mail Configuration
- Inbound Mail Configuration

Configuring the Stat Central Agent for Email

You can configure the Stat Central Agent to manage incoming email and to format and send outbound email. This way, all Stat-related email is handled automatically, requiring no time or effort from users. For example, you can configure the Agent to send an email notification to a mailing list that includes both users and customers whenever a certain event occurs, such as the opening of a new CSR. Email configurations are service domain-specific.

NOTE: The Stat Central Agent also processes email requests sent from the Stat Client whenever a user attempts to email CSR information manually. For more information, see the *Stat User Guide*, Chapter 3, “Change/Service Requests.”

For each service domain in which you want to process email, you select and configure the Agent in the Electronic Mail Interface - Setup window.

To configure the Stat Central Agent for email:

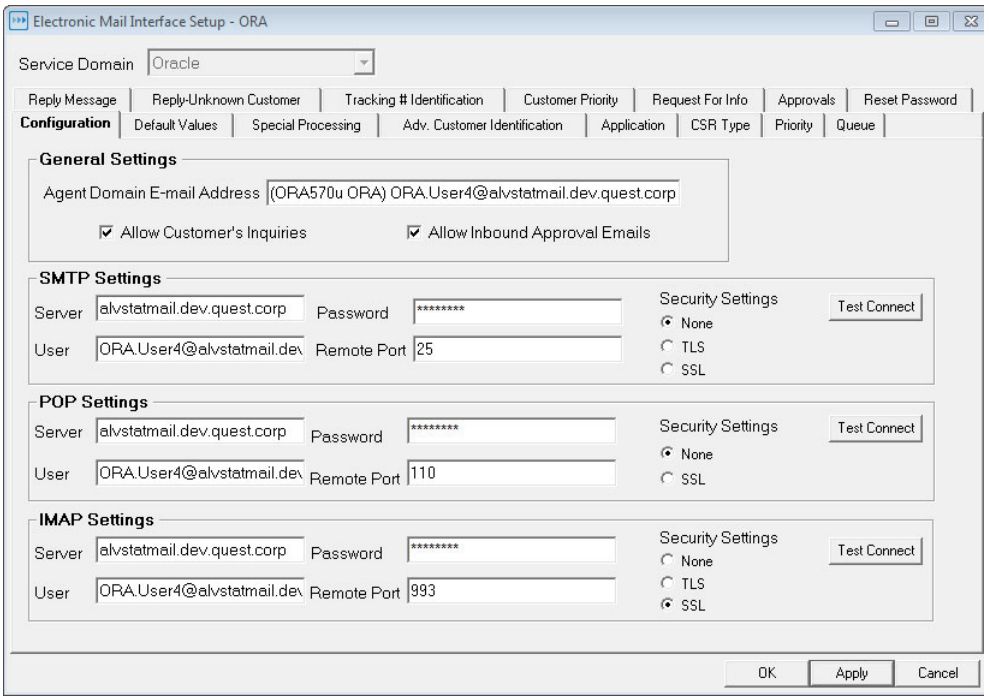
1 Select **Maintenance | Stat Central Agent | Email Settings**.

The Electronic Mail Interface - Setup window opens with the Configuration tab pre-selected.

TIP: You can also access the Electronic Mail Interface - Setup window from the Service Domain Maintenance table. For more information, see Service Domain Maintenance on page 54.

2 In the **Service Domain** field, select the service domain you want.

Each service domain must be configured to process outbound email.



3 In the **Agent Domain Email Address** field, enter the fully qualified email address that will be used solely by the Stat Central Agent for processing email.

The email address must conform to one of the three supported formats described in the table below:

Type	Format	Example
Simple direct address	username@domain.ext	Jdoe@yourdomain.com
Compound name and address with address using brackets	Name <username@domain.ext>	John Doe <Jdoe@yourdomain.com>
Compound comment (name) and address with comment in parenthesis	(comment) username@domain.ext	(John Doe) Jdoe@yourdomain.com

4 (Optional) Select **Allow Customer Inquiries** if you want to let customers make requests via email for automated updates on the status of their CSRs.

5 (Optional) Select **Allow Inbound Approval Emails** if you want to grant approvers the ability to approve or reject a migration, status transfer, or an Oracle Apps patch application by responding to reminder emails sent by the Stat Central Agent.

> **NOTE:** Approval reminders are outbound email messages pre-formatted in the Approval tab, which is described in the section, “Approval Notification” on page 25.

The remaining fields in the Configuration tab involve email server settings. If you have questions regarding these settings or email servers in general, see your email administrator.

6 Specify the settings you want in the SMTP section, which configure the Stat Central Agent to process outbound email. Then, depending on which server you use for inbound email, specify the settings you want in either the POP3 section or the IMAP section.

> **NOTE:** Stat security requires that non-LDAP enabled new users and users whose passwords have been reset receive an auto-generated email containing a temporary password. When processing the email job, Stat uses the SMTP settings configured in the default service domain of the user defining the new user or resetting the password.

The table below describes the appropriate values for each field.

Value	Setting
Server	String. May either be a host name (host.dart.com) or dot address (nnn.nnn.nnn.nnn).
User	Optional String. Specifies the server account. Supported formats include: UserId Domain\UserId Domain\UserId\Mailbox
Password	Optional String. Specifies the Password.
Remote Port	Optional Long. Specifies the port number you wish to connect to. If you do not specify a port number, the following industry standard port numbers are used by default: Port 25 for SMTP Port 110 for POP3 Port 143 for IMAP4
Security	The encryption protocol, if any, used for inbound and outbound communications with the server. Options include **TLS** (for SMTP and IMAP), **SSL**, and **None** (for no encryption). **NOTE:** When you switch from **None** to **SSL** or **TLS**, the port numbers are automatically changed to the corresponding industry standard. These numbers include: • **TLS** - 25 (SMTP) and 143 (IMAP4) • **SSL** - 465 (SMTP), 995 (POP3), and 993 (IMAP4). You can modify these settings as needed.

7 If you use Outlook Exchange as your inbound email server, specify the following settings in the Message Format tab of the Site Default Properties window:

- For POP3, you must select the MIME radio button.
- For both POP3 and IMAP, you must check at least two of the following three check boxes: **Provide message body as plain text**, **Provide message body as HTML**, and **Use Microsoft Exchange rich-text format**.

These settings can be at the exchange server level or at the mailbox level for the user designated to receive Stat emails.

IMPORTANT: Each service domain being configured to accept inbound email needs a separate mailbox. Also, for Development and Test environments, mail should either be turned off or also have separate mailboxes.

8 After specifying server settings, you can make sure that you have entered all the information correctly by clicking **Test Connection**.

This makes Stat establish a connection to the server. If successful, Stat immediately disconnects from the server and displays a “Connection Successful” message box. If Stat is unable to connect, it displays a message box stating the cause of the failure, for example, “User ID or Password is not defined.”

Outbound Mail Configuration

In Stat, there are several events which can trigger outbound mail from the Stat Central Agent. These events include:

- A user attempts to manually email CSR information

- Creating a new CSR, either by a user or the Stat Central Agent
- Closing a CSR
- Re-opening a CSR
- Updating a CSR
- A CSR going unopened for a specified length of time
- Items going past due for a specified length of time
- An object reservation turning into an object lock
- A customer requesting additional information
- An approval notification is sent out by a Stat user for a status transfer, migration, or for Oracle Apps users, a patch application
- Resetting a user's password

The last four events, Object Lock, Request for Info, Approval Notification, and Resetting Passwords trigger email to individual recipients and are set up in their respective tabs on the Electronic Mail Interface - Setup window. However, you configure outbound email triggered by all the other events in terms of business rules. In a business rule, you specify the event that you want to trigger the email, as well as the list of mail recipients and the content of the email message itself. For more information on configuring outbound email as business rules, see Business Rule Maintenance on page 126.

NOTE: Be aware of the following:

- You can change the default presentation of outbound email by opening the file $STAT_HOME\report\business_rule_report.jrxml in Jaspersoft Studio. This tool allows you to customize the email report presentation, including field position, style, header and footer. For Stat to accept the customizations, the compiled version of the file business_rule_report.jasper has to be deleted.
- On the Request for Info and Object Lock tabs, the Explanation tab provides a brief explanation of the event. It is for informational purposes only and cannot be edited.
- The Stat Central Agent formats outbound email using the ISO-8859-1 character set by default. Some Unix based servers may have issue with the character set and accented letters may be dropped from the body of the email. The standalone.conf and standalone.conf.bat are using a parameter that overrides UTF-8 with ISO-8859-1. If it becomes necessary to use UTF-8 for email, scan the standalone.conf/standalone.conf.bat files for the parameter **-Dmail.mime.charset=ISO-8859-1** and set it to **-Dmail.mime.charset=UTF-8**.

Object Lock

When triggered by an Object Lock event, the Stat Central Agent sends an email to CSR owners notifying them that the reservation they placed on an object has been changed to a lock. Because this notification does not require any additional information, the check boxes that correspond to CSR fields are grayed out.

Request for Info

When triggered by the Request for Info event, the Stat Central Agent sends an email to a customer who has requested updated information regarding a CSR. A Request for Info event occurs when someone replies to an email sent to them by Stat. Stat adds CSR-specific information to outbound messages and can check for this information on all inbound emails.

NOTE: If you allow Request for Info emails, it is recommended that you enter instructional text in either the header or footer of the email message. For example, you may include the following header: *You can request an automated update at any time by REPLYING to this message. Stat responds to you with the real-time status of your CSR*. For more information on specifying headers and footers on email, see Business Rule Maintenance on page 126.

Approval Notification

In the Approvals tab, you can define a pre-formatted message that Stat users with the proper security rights can send to approvers reminding them about a migration, status transfer, or Oracle Apps patch application waiting their approval. These messages include links that a recipient can click to send an email immediately back to the Stat Central Agent indicating their approval or rejection of the migration, status transfer, or Oracle Apps patch application. If configured to accept inbound approval email, the Agent then processes the email and changes the approval status from Pending to Approved or Rejected.

The Notify tab allows you to configure a notification email when the approval email is sent. The notification email does not have vote buttons, but it does include approval and approver information

NOTE: To configure the Stat Central Agent to accept inbound approval email, select the **Allow Inbound Approval Emails** option in the Configuration tab. If you have also configured Stat to automatically generate CSRs from inbound email, you may want to specify parameters in the Special Processing tab to keep Stat from generating a CSR whenever a user replies to an approval notification (see Special Processing Tab on page 180 for more information).

Resetting Password Message

In the Reset Password tab, you can modify the pre-formatted message that Stat sends to non-LDAP enabled users whose passwords have been reset (either by a system administrator or another user with the security rights to administer passwords). The Message Header and Message Footer tabs contain information notifying the user that their password has been reset and includes a temporary password and instructions to change their password at the next login or from the User Options window. You can include additional information to the message as needed.

Inbound Mail Configuration

The Stat Central Agent follows a specific protocol when processing inbound mail:

1. The Agent determines if the email should be skipped (ignored), treated as undeliverable mail (mail returned by the email system), or treated as a request for information.
2. If the email does not meet any of the above criteria, the Agent determines if it should create a CSR based on the mail.
3. If configured to do so, the Agent creates a new CSR using default configuration settings.
4. The Agent searches the email for keywords you have defined for each field on the CSR. If any matches are found, the Agent updates the new CSR with the appropriate values.
5. The Agent attempts to locate the customer on the Customer table. A customer match is made by comparing the sender's email address with the two email address columns in the Customer Maintenance table.
6. The Agent saves the CSR and adds the body of the original email message to the CSR Description tab.
7. If the inbound mail has attachments, the Agent adds the attachments to the CSR or forwards them to the designated mailbox.
8. The Agent processes outbound mail rules and determines if any outbound mail needs to be sent in reply to the mail it just received.

Default Values Tab

Whenever the Agent is triggered by an inbound email message to create a new CSR, it uses search strings to populate the fields of the CSR based on information contained in the message. If a matching search string is not

found, the Agent uses default values instead. The first step in configuring the Agent to process inbound email is to specify the default values. You do this in the Default Values tab of the Electronic Mail Interface - Setup window.

To define the inbound mail configuration:

1 In the Electronic Mail Interface Setup window, select the Default Values tab.

When first opened, the Default Values tab displays system-defined values.

2 Select **Accept Inbound CSRs** if you want Stat to create CSRs from email.

Selecting this check box enables the fields on the Default Values tab.

> **NOTE:** Stat does not generate new CSRs from approval emails. See Approval Notification on page 178 for more information.

3 Click the Browse button (...) next to the **Customer** field.

This opens the Search Customer Engine, which you can use to search the Stat Repository for the name of the customer. The name you select serves as the default in the **Customer** field of a CSR if Stat is unable to find a matching customer in the Customer Maintenance table when creating a CSR based on inbound email. You can use an existing customer record or create an Inbound Mail ID specifically for this purpose. The **Department** field is automatically populated based on the customer you select. For more information on using the Search Customer Engine, see the *Stat User Guide*, Chapter 7, “Search Engines.”

4 In the **Application** field, select an application.

You can select any application defined for the service domain. However, it may be useful to create a generic application such as “Other” specifically to handle inbound email.

5 (Optional) In the **Env** field, select an environment.

This field is activated only if the application you selected is associated with any application environments.

6 In the **Cust Priority** field, select a customer priority.

7 In the **Priority** field, select a priority.

8 In the **CSR Type** field, select a type.

You can select any type defined for the service domain. However, it may be useful to create a generic type such as “Other” specifically to handle inbound email.

> **NOTE:** If the CSR Type you select is associated with one or more workflows, the default workflow is automatically displayed in the **Workflow** field. In addition, the **Status** field automatically defaults to the start status of whatever workflow is displayed in the **Workflow** field.

9 (Optional), if the CSR Type you selected is associated with more than one workflow, select a non-default workflow in the **Workflow** field.

10 In the **Status** field, select a status.

> **NOTE:** The Status field automatically displays the start status of whatever workflow is displayed in the **Workflow** field (if any). However, you can select a different status if you want.

11 In the **Queue** field, select a queue that includes the User ID you plan on assigning to the CSR.

12 In the **User ID** field, select an ID.

You can select any User ID belonging to the queue you selected. The ID you select is assigned to the CSR. It may be useful to assign the CSR to a manager who can properly assign ownership.

13 In the **Title** field, enter the text you want to appear in the Title field on the CSR.

The description should be generic, such as “New CSR opened from email.” This value is used in the event that there is no subject defined in the email message.

> **NOTE:** In the Description tab of a new CSR, the Stat Central Agent inserts a notification that the CSR was created automatically from an inbound email and identifies the email sender, number of attachments, and the subject. The Stat Central Agent also copies the body of the inbound email message to the Description tab. Supported formats include both HTML (without JavaScript) and plain text.

14 Do one of the following to configure how Stat manages attachments in the inbound email:

- If you want Stat to store email attachments to the CSR, select **Save attachments in CSR**.

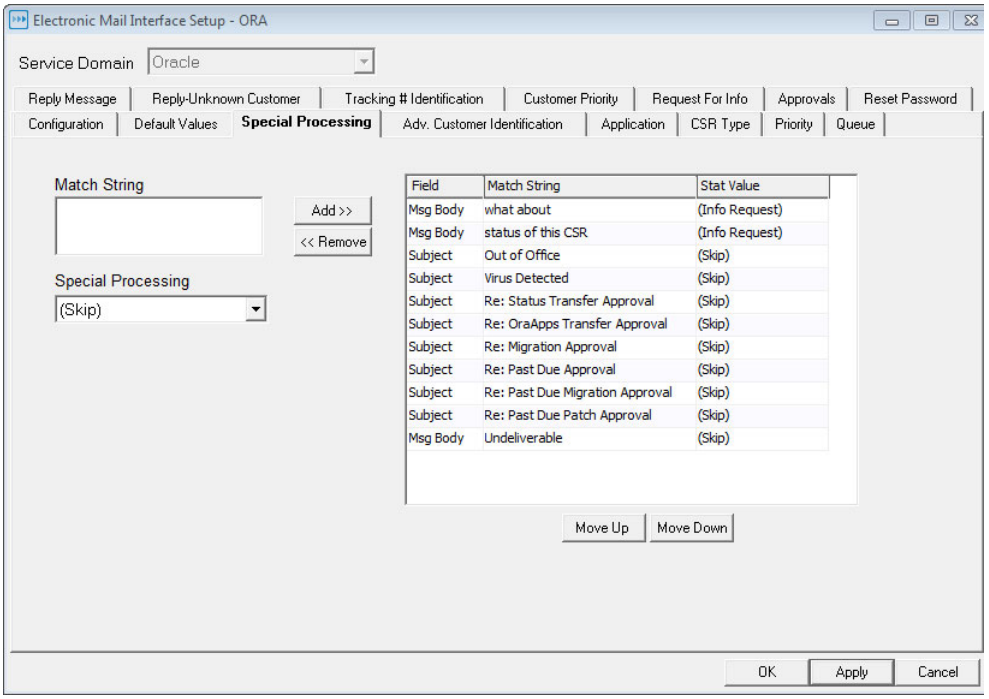
  NOTE: Embedded emails are stored in .eml format in CSR attachments.

- If you want Stat to forward any attachments received to an additional mailbox, select **Forward attachments to:** and then specify that mailbox.

15 If you would like Stat to forward returned (undeliverable) mail, select **Forward Undeliverable Mail to** and specify a mailbox.

Special Processing Tab

The Stat Central Agent is designed to create new CSRs automatically from inbound email. However, there are circumstances when creating a new CSR from an email message is not warranted, such as email that is returned undeliverable. You can configure the Agent to handle these situations by specifying special processing parameters. These parameters tell the Agent if an email is a request for information, returned mail, or something to ignore.



Special Processing, like the configuration parameters defined in the remaining tabs, is driven by keyword searches. Through keyword searches, you instruct the Stat Central Agent to search the inbound email message for certain keywords or phrases and, if found, to take a specified action. In addition to keywords, you must also tell the Agent where in the email message to search. The location options are:

- **Subject** – The message subject field
- **Msg Body** – The message body or text
- **From Name** – The name (not the email address) of the sender
- **Msg+Subj** – Both the subject and message body

NOTE: This tab must be defined for each service domain that uses inbound email. It is recommended that you have match strings such as “Out of office,” “Virus detected,” “Mailbox full,” to avoid email storms. Also, if your company sends broadcast emails (newsletters), you may want to filter for these as well.

There are three different ways the Agent can process an inbound email message if it finds a keyword match. These include Skip processing, Undeliverable processing, and Info Request processing. If the Agent does not find

a keyword match, it processes the email message by creating a new CSR based on the information contained in the message.

Skip Processing

You can configure the Agent to skip an email if it finds a keyword match. Skipped emails are deleted from the inbox. This helps reduce the number of invalid CSRs that are created.

Some examples of keyword variables that prompt the Agent to skip an email are:

- Subject = Out of Office Auto Reply
- From Name = Your email broadcast message sender

TIP: If you have configured Stat to send approval notifications to users, when a user makes an approval or rejection by clicking a link in the notification, Stat does not create a CSR, but if the user simply replies to the notification, it may result in an undesired CSR being created. To avoid this, you may want to specify a Skip Processing parameter.

Undeliverable Processing

You can instruct the Agent to recognize email that is returned undeliverable. If the Agent receives an undeliverable message, it forwards the email to the mailbox defined in the Default Values tab and then deletes the message from the inbox

Most email systems place the word “Undeliverable” in the subject of returned mail. This is often the best way to identify these messages.

Info Request Processing

As discussed in the preceding chapter, you can configure the Agent to send an email message to customers notifying them that a new CSR has been opened. Customers can then send a reply message via email requesting more information about the CSR.

Included at the bottom of the original message is an encrypted special identifier line. This line is specially formatted and contains information on the service domain, CSR number, and sender, as shown below:

<<Stat|CHG|234|SYSTEM>>

For the Agent to recognize the inbound email as an information request, you must specify a match string in the Special Processing tab that includes part of this special identifier line. The match string should not match the special identifier line completely (which is CSR number and sender specific), but should at least include “<<Stat”, and possibly the service domain as well, for example, “<<Stat|CHG”, where “CHG” is the service domain code.

If the special identifier line is not present in the inbound email or has been modified improperly, the request is ignored and the Agent continues processing the email. If it is not picked up by any other filters it is treated as a new CSR request.

IMPORTANT: The identifier line is encrypted in the original email, users must not delete it or modify it in any way in their reply messages. This could result in the wrong CSR information being reported back to them or the request itself being ignored.

If the Agent recognizes a message as an information request, it retrieves the most recent CSR information and sends an email back to the originating mailbox with that information.

Adding a Parameter

To enter a keyword search:

1. In the **Match String** field enter the keyword variables you want the Agent to search for.

   The keyword search is not case-sensitive.

2 In the **Special** field, select the processing parameter you want.

3 Click **Add>>**.

Stat adds the keyword variables and parameter to the processing list.

4 In the Field column click the row you just added. Then select the location in the email message where you want the Agent to search.

5 Click **OK**.

Order of Processing

The Agent processes the values in the order they are displayed. If a match is found, it processes the email appropriately, ignoring any subsequent items.

You can change the processing order by selecting the item you want to move and clicking **Move Up** or **Move Down**.

Removing or Editing a Parameter

To remove or edit a parameter, select the row and click **<< Remove**. The Agent moves the match string and processing parameter from the list back to their respective fields.

If you want, you can then edit the match string and add it back to the list.

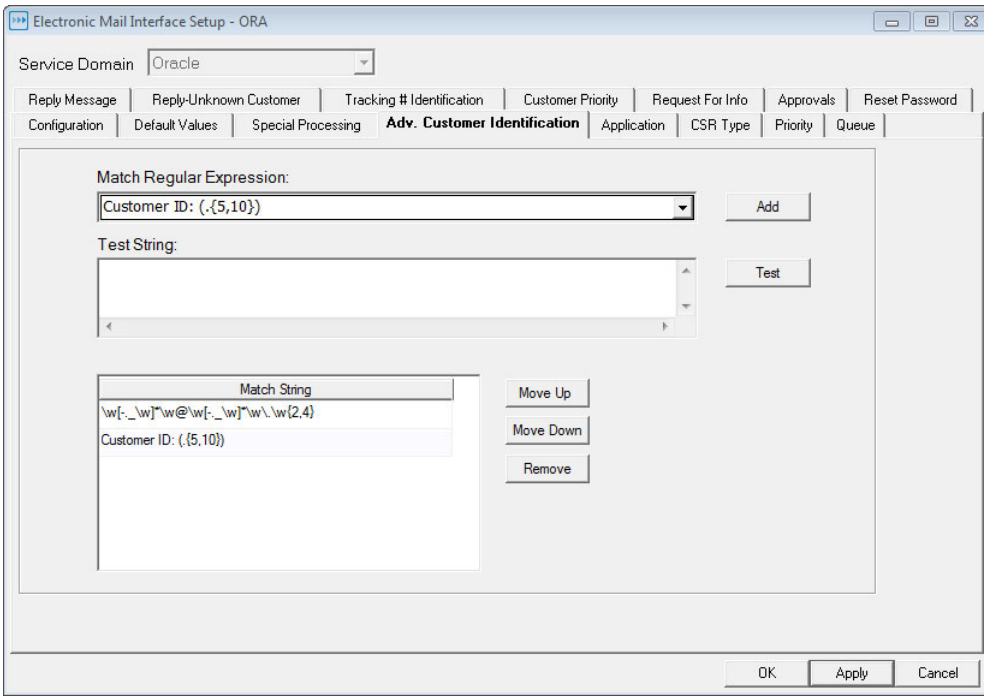
Advanced Customer Identification and Tracking # Tabs

These two tabs function differently from the other email configuration tabs. They both use Regular Expressions to locate the data in the email.

When the Stat Central Agent receives an email it attempts to identify the customer based on the email address. It searches the Customer Maintenance table for a match on the email address located in the From field of the email. If it cannot find a match in either the primary or additional email address columns in the Customer Maintenance table, it performs an advanced customer search. This search is made using parameters specified in the Advanced Customer Identification tab.

During an advanced search, the Agent scans the entire email message looking for an email address based on keyword variables. If an email address is found, the Agent then attempts to match it with an email address in the Customer Maintenance table. If the Agent still cannot find a match, it uses the name you specified in the Default Values tab.

In a similar manner, the Agent scans for a value to insert into the **Tracking Number** field on the CSR if you define this on the Tracking # Identification tab.



The Agent's advanced search functionality is based on regular expressions, which are specially formatted patterns of text variables used to match strings of text. You can use one of the examples provided, modify one of the examples provided, or create your own custom expression.

Regular Expressions

NOTE: This guide is not intended to be a complete manual on regular expressions, but to assist you with expressions that work within the confines of Stat email functionality. Additional information can be obtained on the internet, or possibly from java developers on your staff.

A regular expression, known as regex, allows you to specify advanced search criteria. You can define a search based on a pattern of characters which are unique or which include a wide range of characters.

IMPORTANT: An invalid or incomplete regex could return invalid or incomplete search results. Unless you are proficient in the use of regular expressions, do not write your own regular expressions. Instead, use span parameters to set up the search.

Be aware of the following guidelines when defining regular expressions:

- The expression itself is case sensitive. Example: \d = digit while \D = not digit.
- The search variables are enclosed in parentheses ( ) when used in context with a keyword or label.
- Content can be specified in sets within square brackets [ ].
- The number of characters is specified in curly brackets { }. A single number is an absolute number. That is, the string must be this long. Two numbers separated by a comma designate a minimum and maximum character length.
- The following metacharacters are actual characters without special meaning when they are specified within square brackets: . ^ $? + - (and \ when repeated as \\). Otherwise, they are supported as follows:

  . = any character except a new line
  ^ = start of line
  $ = end of line
  + = one or more
  * = 0 or more
  - = a range

- The . + * ? $ metacharacters can be positioned anywhere within the brackets.

- The ^ - metacharacters must be placed at the beginning or end of the set.
- The backslash \ metacharacter must be repeated as \\ to be treated as a single actual character; for example, [Program Files\system]. If a single \ is specified within brackets, it is an escape metacharacter and identifies a metacharacter after it.
- \w denotes any alphanumeric word
- "\d denotes a number
- "\s* is a useful designator. Place this between a label and the rest of the search string to indicate that you don't care how many spaces if any exist between the two.

Regular Expression Examples

Use these examples as starting points. You can customize them to fit your needs by modifying the label or any part of the expression.

Advanced Customer Identification Examples

Requestor: (.*$)

- This string searches for any string until the end of the line.
- If the string is separated from the label by any spaces, there is not a match.
- You can change the label, or keep the label and change the search string

email: \s*(\w[-._\w]*\w@\w[-._\w]*\w\.\w{2,4})

- This string searches specifically for an email format that occurs after the label.
- The number of spaces after the label is irrelevant.
- You can modify the label from email to something else and add it to your list of match strings

Customer ID: (.{5,10})

- This string is less specific.
- It retrieves any string of 5-10 characters that occurs after the label
- If the string is not separated from the label by one space, there is not a match
- You can modify the number of minimum and maximum characters and add the \s* designator between the label and the left parenthesis.

Tracking Number Examples

NOTE: Not all of these examples are delivered with Stat. However they illustrate ways you can change the match string. Some examples have a space after the label, some do not. What you use depends on how your Tracking Number is formatted, and whether it is auto-formatted in an email, or whether it is manually entered by a user.

Call ID: \s*(\w+)

- Find one word after Call ID: with no space after Call ID:
- If the word has a dash or other punctuation in it, it is considered to be more than one word. Only the data prior to the punctuation will be returned
- There can be zero to many spaces between the label and the expression

Alternate #:(d\+)

- Returns any number following the label
- If there is a space between the label and the number, there will not be a match

Additional Examples

We have arbitrarily used the label 'Call ID:'.

Call ID:(.{5,30})

- Find any characters after Call ID:, minimum 5, maximum 30, no spaces after the label
- If the string is less than 5 characters, there is no match
- If the string is longer than 30 characters, only the first 30 are used
- If there are one or more spaces between the label and the string, there is no match

Call ID: (\w+)

- Find one word after Call ID: and a space
- The word has a dash or other punctuation in it, it is considered more than one word. Only the data prior to the punctuation is returned.
- If there is a not a space between the label and the word, there will not be a match
- If there is more than one space between the label and the word, there is no match

Call ID:(\w+)

- Find one word after Call ID: with no space after Call ID:
- The word has a dash or other punctuation in it, it is considered to be more than one word. Only the data prior to the punctuation is returned
- If there are one or more spaces between the label and the string, there is no match

Call ID: (\d{5,10})

- Find a number with a minimum of 5 digits and a maximum of 10 digits after Call ID: and a space
- If the number is less than 5 digits, there is no match
- If the number is longer than 10 digits, only the first 10 digits is returned
- If there is a punctuation character or a letter in the string only the numerical digits before the punctuation or letter is returned
- If there is no space between the label and the string, there is no match
- If there is more than one space between the label and the string, there is no match

Call ID:\s*(\d{5,10})

- Find a number with a minimum of 5 digits up to a maximum of 10 digits after Call ID, regardless of the number of spaces after the label
- If the number is less than 5 digits there is no match
- If the number is longer than 10 digits only the first 10 digits is returned
- If there is a punctuation character or a letter in the string only the numerical digits before the punctuation or letter is returned
- It does not matter whether or not there are any characters between the label and the number

Adding a Regular Expression

To enter an advanced customer or tracking numbers match string:

1. Click in the **Match String** field and select an example.
2. If necessary, do any of the following to edit the example:
    - Change the label
    - Change the spacing

- Change the character/number designation

3 Alternatively, type in your own string.

4 Type a test string in the Test String box and click **Test**.

This may be done before or after you add the expression.

5 To test an expression that has already been added, highlight it in the Match String List box.

Notice that it is now displayed in the **Match String Expression** field as well.

6 Modify the expression if necessary and retest.

7 Add the expression to the Match String list by clicking **Add**.

8 Check your list of expressions.

There are be no duplicate expressions, but there might be some with subtle typing differences that you no longer want. You may change the search order, or remove any extra expressions that you don't need.

Order of Processing

The Stat Central Agent processes search criteria in the order they are displayed in the criteria list. If a match is found based on the first criteria, the Agent processes the email appropriately, ignoring any subsequent items.

You can change the processing order by selecting the item you want to move and clicking **Move Up** or **Move Down**.

Removing or Editing a Regular Expression

To remove or edit a regular expression, select the row and click **Remove**. The Agent moves the regular expression from the list back to their respective fields.

If you want, you can then edit the match string and span parameters and add them back to the list.

Field-Specific Tabs

Sometimes in an email message, a CSR value may be expressed somewhat differently than in Stat. For example, you may have an application defined in Stat called Human Resources, whereas in an email message this same value may appear as “HR.” This could create a problem when the Agent attempts to generate a CSR from an inbound email message.

In the field-specific tabs, you can define advanced search criteria based on alternative match strings that enable the Agent to handle these differences and populate the fields of a CSR with the appropriate values. For example, in the Application tab, you can configure the Agent to locate the string “HR” and match it with the CSR application value Human Resources. Defining search criteria in the field-specific tabs is optional.

The following field-specific tabs correspond to the fields in a CSR:

- Application (includes Environment value, if applicable)
- CSR Type (includes CSR Status value)
- Customer Priority (includes option to duplicate values for Priority field)
- Priority (if different than Customer Priority values)
- Queue (includes Assigned User value)

To define field-specific search criteria, click on the appropriate tab.

NOTE: The values displayed in the **Tracking #** field of CSRs are user-defined. For this reason, you define match strings in the Tracking # Identification tab with regular expressions, the same way you do in the Advanced Customer Identification tab. See Advanced Customer Identification and Tracking # Tabs on page 182 for more information.

Adding a Parameter

Your keyword searches should be as encompassing as possible. However, because the Agent makes matches on partial entries, it is not necessary to enter the same word in a variety of forms. For example, a search made on the keyword “Enh” would return “enh,” “enhancement,” and “enhance.”

On the Application and Customer Priority tabs, the **Add All Codes** button is provided as a time saver. Clicking this button automatically adds all the defined codes for the service domain to the list. The code description is used as the match string.

Only one value can be entered per row. The Stat Central Agent cannot interpret multiple values inserted in one row. However, you can enter an unlimited number of rows for individual keyword searches.

If the Agent does not find a match on any of the search strings for a particular field, it uses the value you defined on the Default Values tab instead.

To enter a keyword search:

1. In the **Match String** field enter the keyword variables you want the Agent to search for.

   The keyword search is not case-sensitive.
2. In the **Code Value** field, select a parameter.
3. If you are working in the Queue, CSR Type, or Priority tab, do one of the following:
   - In the Queue tab, select a user from the list of users that belong to the selected queue in the **Assigned User Code Value** field
   - In the CSR Type tab, select a CSR status associated with the selected CSR type in the **CSR Status Code Value** field
   - In the Priority tab, select **Priority field uses same values** if the values defined for the **Priority** field on CSRs are the same as those defined for the **Customer Priority** field
4. Click **Add>>**.
5. In the Field column of the row you just added and select where in the email message you want the Agent to search.
6. Click **OK**.

The Agent processes the values in the order they are displayed. If a match is found, it processes the email appropriately, ignoring any subsequent items.

You can change the processing order by selecting the item you want to move and clicking **Move Up** or **Move Down**.

Removing or Editing a Parameter

To remove or edit a parameter, select the row and click **<< Remove**. The Agent moves the match string from the list back to the Match String field. You can then edit the match string and add it back to the list.

Reply Tabs

After the Agent creates a new CSR, it can create and send a reply message to the originator. There are two types of reply messages: identifiable customer and unknown customer. When the Agent cannot locate a customer in the Customer Maintenance table, the reply is sent to the originating mailbox. If the Agent can locate a customer, the reply is sent to the customer’s email address. If the customer has two email addresses, the reply is sent to the primary address.

The Reply Message and Reply-Unknown Customer tabs display the same information as the event-specific tabs in the Electronic Mail Interface - Setup window. For more information, see Outbound Mail Configuration on page 176.

To define reply messages:

1. Click the **Reply Messages** tab.
2. In the Fields to Include in Message section, select the check boxes next to the CSR fields you want to include in the message.
3. (Optional) In the Message Header and Message Footer tabs, enter the header and footer you want included at the top and bottom of the reply message, respectively.
4. In the Send To tab, add any additional recipients you want. By default, the reply message is sent to the customer and a carbon copy is sent to the assigned user.
5. (Optional) Click the Reply-Unknown Customer tab and repeat steps 2 through 4 to define the message that Stat sends to the originating mailbox.
6. Click **OK** to save your work.

8

Object Security

- PeopleSoft Proprietary Object Security
- PeopleSoft Object Security Setup Instructions
- Frequently Asked Questions
- File Object Security

PeopleSoft Proprietary Object Security

You can configure Stat to physically secure PeopleSoft proprietary objects in their native environment the moment they are locked in a CSR. This ensures that the developer assigned to the object is the only one working on it. In addition, you can set up the Stat Central Agent to run synchronization jobs at specified time intervals to ensure that the Stat Repository and your PeopleSoft environments remain synchronized.

A PeopleSoft proprietary object can be assigned to one developer for each environment in which it is locked. If an object is locked in two or more environments, this means that multiple developers may be associated with the object.

Object Security (also known as Definition Security) is assigned to the developer of the object. A different developer may be assigned the object at anytime if necessary, and Stat reassigns the object lock to the new developer when the CSR is saved. Any notifications regarding locking/reservations are sent to the assigned object developer, not the user assigned to the CSR.

PeopleSoft Proprietary Object Security takes effect when the Stat Central Agent processes CSR activity after the CSR is saved. The PeopleSoft proprietary object locks are in place virtually at the same time the lock occurs in Stat, even before the Stat Central Agent starts processing the base archive set. The Stat Central Agent also processes synchronization jobs that can be scheduled to fit the needs of each client. These jobs ensure that Stat recognizes when new objects are added to any environment, as well as ensuring that the security information on Stat remains in sync with PeopleSoft and vice versa.

For special PeopleSoft proprietary object security considerations, see the *Stat User Guide,* Chapter 11, “Change Management for PeopleSoft.”

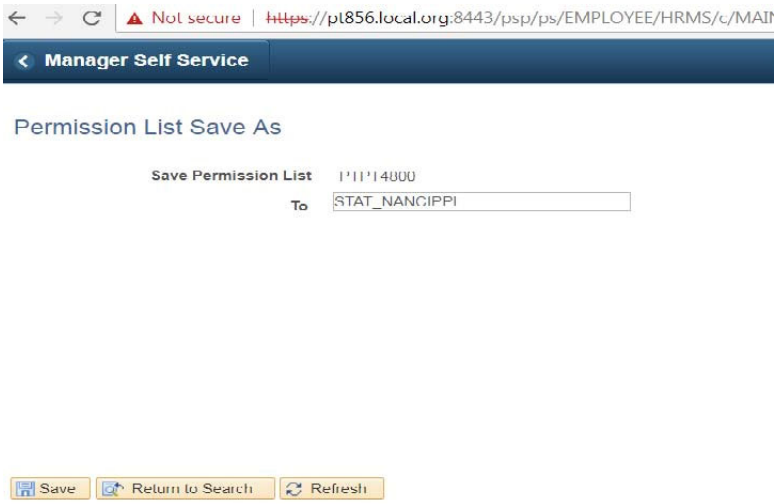
PeopleSoft Object Security Setup Instructions

You can configure Stat to physically secure PeopleSoft proprietary objects in their native environment the moment they are locked in a CSR. This ensures that the developer assigned to the object is the only one working on it. In addition, you can set up the Stat Central Agent to run synchronization jobs at specified time intervals to ensure that the Stat Repository and your PeopleSoft environments remain synchronized. By default, the prefix for POL (Physical Object Locking) will be set to STAT. An alternative group name can be change in **Maintenance | General | Peoplesoft Connect | Stat PSOPRID column**.

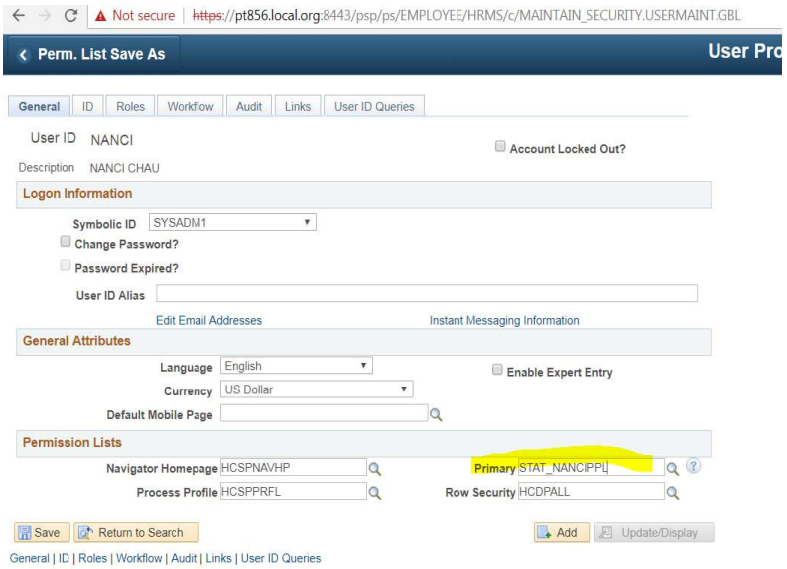
To configure physical object locking

1 Create a unique PSOPRID if you have not already done so by navigating to **PeopleTools | Security | User Profiles**.

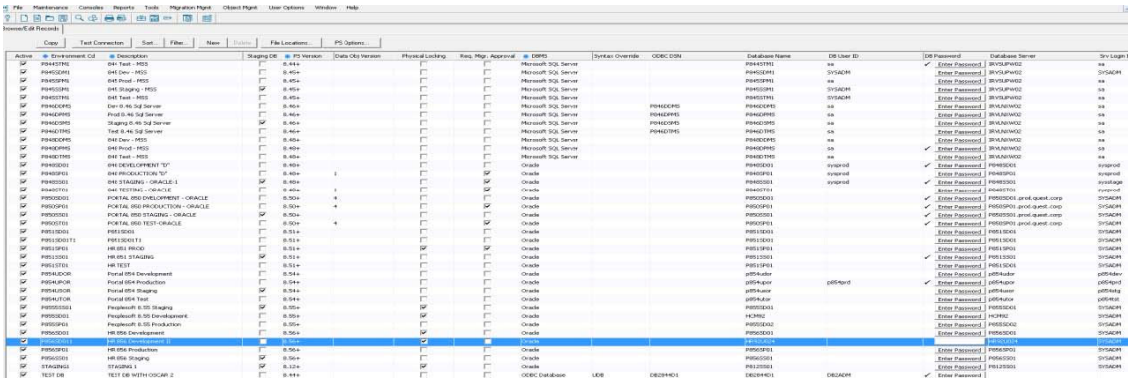
2 Create a unique Primary Permission List for each user. In the following example, the Primary Permission List (PPL) is called STAT_NANCIPPL.



3 Open the user profile. In the General tab, in the **Primary** field under Permissions Lists, specify the unique Primary Permission List for the user.

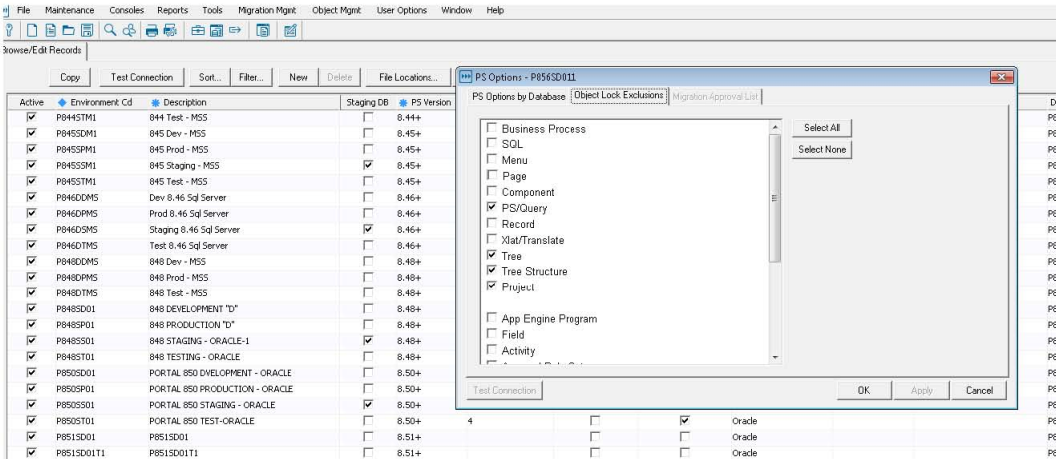


4 Go to **Maintenance | General | PeopleSoft Connect** and select the **Physical Locking** option.

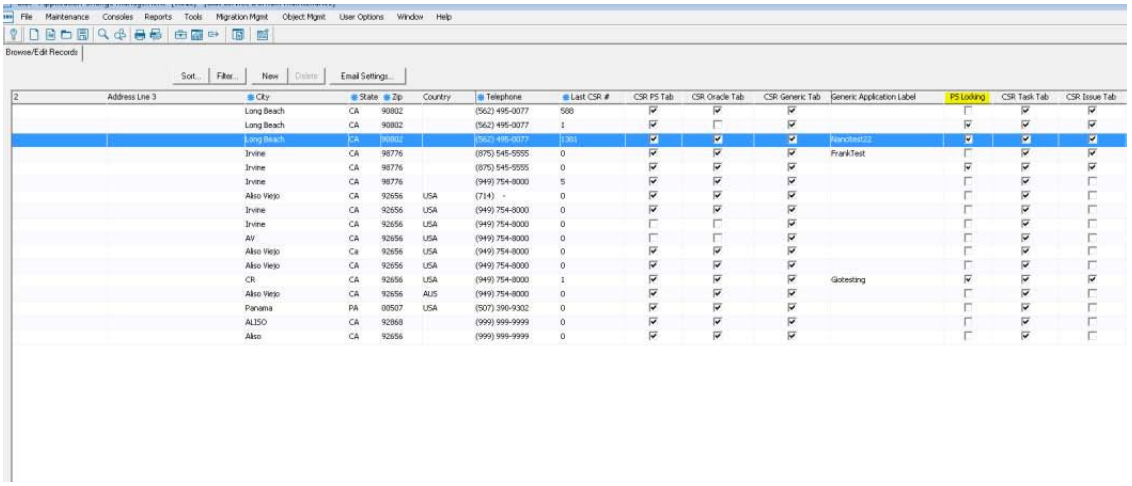


5 (Optional) You can exclude certain object types from Physical Object Locking. This allows a user with a valid PSOPRID/password to open these objects in the Application Designer without locking the objects in Stat.

In the following example, PS/Query, Tree, Tree Structure, and Project will be excluded from Physical Object Locking.



6 Go to **Maintenance | General | Service Domains** and select **PS Locking** for the service domain.



7 Go to **Maintenance | Stat Central Agent | Job Maintenance** and create a new PS Object Lock Sync job. If you could not locate the environment from the drop-down list, verify that the environment is part of the PeopleSoft migration path.

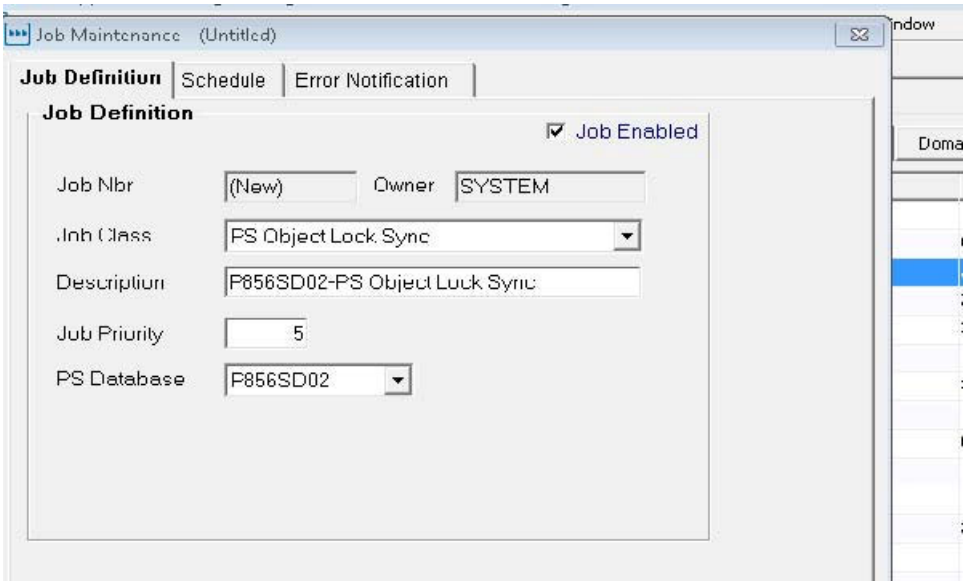
What is PS Object Lock Sync job and why it is necessary to run it?

The PS Object Lock Sync job ensures that the PeopleSoft Object Security groups contain the correct objects. They might not contain the correct objects if, for example, someone has modified the group definitions in PeopleSoft. The job has two steps:

- Sync objects locked in Stat by Stat developers with the Object Security Groups for the PeopleSoft developers in PeopleSoft.
- Sync all objects in PeopleSoft with the Stat_Read and Stat_Exclud Groups in Object Security.

There are two key differences between the physical locking that occurs when users lock objects in a CSR and the PS Object Lock Sync job:

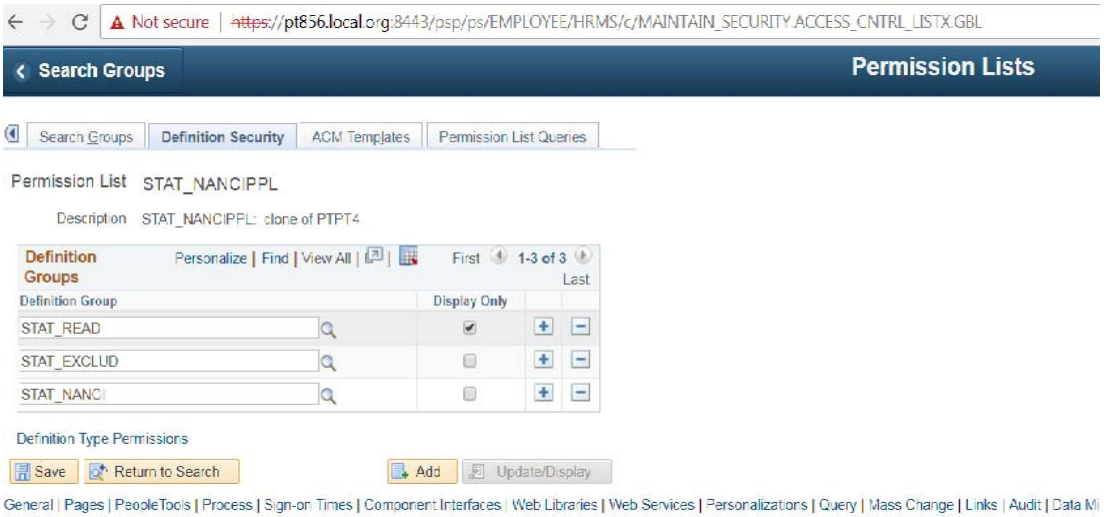
- When a user saves a CSR after locking an object associated with it, Stat Central Agent automatically processes this object lock. It inserts a row in the Assigned Developer's Object Security Group in PeopleSoft for the locked object. This is not done using the PS Object Lock Sync job. Stat Central Agent does it automatically in the background. Once Stat Central Agent finishes this process, the developer can open and modify this object in PeopleSoft.
- You can schedule the PS Object Lock Sync job to run for the selected PeopleSoft environment any time you wish. It is recommended to run it once or twice a day during non-peak hours. However, you might need to run the job more frequently depending on the number of new objects created. If new objects are created often, run the job more frequently or on demand, as necessary.



The first time a PS Object Lock Sync job runs, it creates the STAT_READ, STAT_EXCLUD (if object types are selected for exclusion from Physical Object Locking), and STAT_PSOPRID (if at least one object was added via Stat).

8 Log in to the PeopleSoft portal. Select **PeopleTools | Security | Permission List and Roles**. Locate the user Primary Permission List.

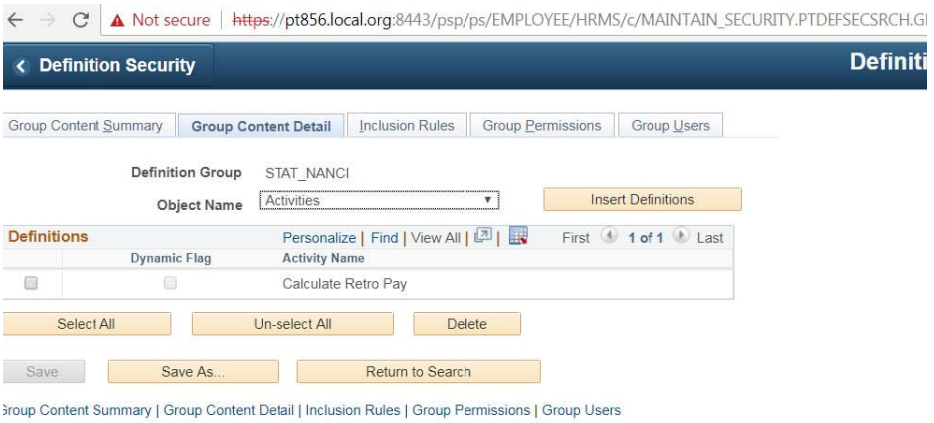
9 Open the Primary Permission List. Select the **Definition Security** tab and add STAT_READ, STAT_EXCLUD (if object types are selected for exclusion from Physical Object Locking), and STAT_PSOPRID. Set STAT_READ to display only.



10 When the PS Object Lock Sync job runs, it will look at all the objects that were added in Stat. In our example, the job would look at the objects added by the user NANCI and put the objects in the STAT_NANCI group. In this way, only the user NANCI, or a user with the PeopleSoft Admin role, can open these objects.

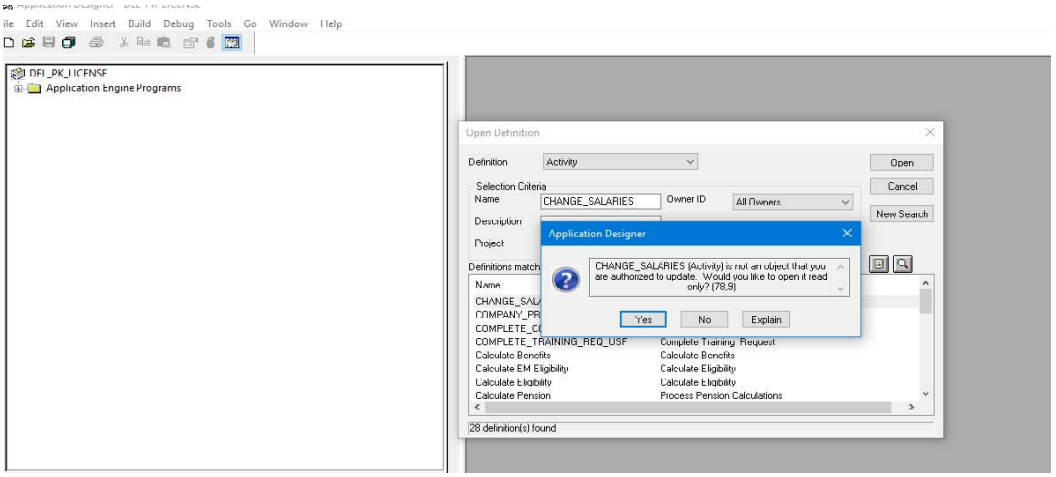
11 To test if Physical Object Locking is working properly, do the following:

1 Add an object to a CSR. In the following example, an activity called Calculate Retro Pay was added. This object will automatically get added to the STAT_NANCI group.



2 Log in as the specified user (e.g., NANCI). If the user can open the objects, POL is working properly.

3 Attempt to open another object that hasn't been locked via Stat. This action should initiate a read-only prompt.



Additional Information. In order to be able to open a Record PeopleCode, Component PeopleCode, or Application Engine PeopleCode object, the user must add the parent object along with it. For example, if you add a Record PeopleCode object named AA_COST_RT_JPN.EMPIL (RowInit) in a CSR, then you must add the record AA_COST_RT_JPN in order to open the Record PeopleCode object.

Frequently Asked Questions

The following provides answers to some of the more frequently asked questions concerning object locking.

Q: What happens if the other classes that the user is assigned to are tied to different Definition Security Groups? Will the rights of these groups override or add to the rights of the three groups tied to the primary class?

A: Object Security only works for the groups that are tied to the operator's Primary Permission List. For example, if you gave the list “ALLPANLS” full object access by tying it to the group, **ALL OBJECTSS**, and added this list to the user's Oprid, the user still would not be granted these full rights since “ALLPANLS” is not his or her primary list.

Q: I have locked a Record PeopleCode object in Stat but when I try to modify the Record PeopleCode in Application Designer, it said that the Record is Read Only and so I can't modify and save my changes to the Record PeopleCode.

A: This indicates that the parent Record object was not locked. Stat's physical locking uses PeopleSoft's Definition (Object) Security to enforce the locks. This means that for those objects that have parent objects, you need to lock their parent object to modify them. For example, to modify Record PeopleCode and Indexes, you must lock the parent Record, to modify Menu PeopleCode, you must lock the parent Menu, etc. When you lock one or more Translate Values in Stat for a field, you have the physical lock on all the Translate Values for that field in PeopleSoft.

Q: I was unable to modify a Menu object in App Designer because it said the object was locked by another user (I didn't lock the menu in Stat). But I was able to modify the object with the PeopleSoft Component Wizard. Should I be allowed to modify locked objects this way?

A: No, this is a bug with PeopleSoft. We have opened a case with PeopleSoft to get this fixed. It is case # 3296742.

Q: I have some users that will not be locking objects but will still need to view all objects. How do I keep some users from being affected by this type of locking?

A: For users that need “Read Only” access to all objects, make sure that the primary class their Oprid is assigned to is also tied to the Object Security Group, **ALL OBJECTS**, in Display Only mode or the group STAT_READ in Display Only mode. Either Group will achieve the same results.

Q: I have users that always need access to modify all objects. How do I keep some users from being affected by this type of locking?

A: If you have users that needs full admin control over all objects at all times, make sure their primary class is tied to the Object Security Group, **ALL OBJECTS** and not other groups.

Q: What if a developer should only have access to some object types, such as records and fields?

A: Stat has the ability to indicate which object types can be assigned to a developer. This is an option in User Maintenance called object type access. You can also control object type access in Object Permissions in PeopleSoft. Each object type can be set to Read Only, No Access, or Full Access.

Q: Object Security appears to be revoked from a developer each time the PS Lock Synch job is run. But if the object is re-locked on the CSR, the developer again has write access.

A: Check the assignment of Oprids in Stat for the environment where the issue occurs. Most likely there are two or more developers with the same Oprid in Stat. The user ID with the last alphabetical Stat sign on probably has objects in his/her Definition group in PeopleSoft while the other has none except the placeholder.

Q: Everything looks to be set up correctly, but a developer still has Read Only privileges to certain or all objects.

A: Check the Object Permissions for this user in PeopleSoft. The access may be set to Read Only.

Q: Some objects appear to be accessible to everyone.

A: Are these new objects? If an object is not any Definition Group then everyone has access to it. Run the Lock Sync job for this environment.

Q: I get the message <object name> is not a definition that you are authorized to access.

A: Does the object exist in Definition Groups specifically assigned to this user? If not, PeopleSoft will generate this message. Run the Lock Sync job for this environment.

Q: I got the message <objectname> is not a definition that you are authorized to update.

A: Check the Security Group associated to this user's Permission List. If Display_only is Yes for all of the groups, this message will occur. Display only should be Yes for STAT_READ and NO for STAT_EXCLUD, STAT_OPRID. There should be no other groups associated with this Permission List.

Q: When are the locks processed in PeopleSoft? Do I have to run the PS Object Lock Sync job in order to process the locks?

A: Once you obtain a lock on an object in a CSR and save the CSR, the Stat Central Agent immediately processes the lock. You do not have to run the Sync job to accomplish this. The Sync job is designed to be a safety measure to ensure that everything stays in sync between the Stat and PeopleSoft environments.

Q: Do I need to do this setup for all my PeopleSoft users?

A: You need to setup object locking only for users that have access to modify the objects that you are trying to manage (i.e. records, panels, trees etc.). Other users are not be affected by this locking and do not need to be setup for it.

File Object Security

Compared to PeopleSoft proprietary object security, file object security in Stat is relatively simple. The locking and reserving of files in Stat is a logical lock that takes place in the Stat Repository. To enable users to physically lock the file objects that are to be archived and migrated in Stat, the file server administrator needs to setup the following security measures:

- Create a User ID for Stat on each file server on which file objects reside. This User ID should have read/write access to any of the file type source locations that have been defined in Stat. Then enter this same User ID in the **User** field on the File Servers tab of the Object Type Maintenance table.
- Change the User ID of developers so that they only have read/write access to their own working directories and no write access to any of the file type source locations.
- If running Stat off a network, make sure that users have at a minimum Change access to the File folder, which is located in the installation directory beneath the Stat executable folder (parent folder). Users should have at a minimum Read access to the Stat executable folder.

The read/write access granted to the Stat User ID allows it to move files in and out of the source locations, and consequently the ability to lock, reserve, archive, and migrate file objects. This physical locking is controlled and managed by the file server administrator and not by Stat.

9

Enabling Web Client to perform PeopleSoft migrations

- Overview
- Present architecture
- Compatibility issues with the current implementation
- How does the test connection of PT servers work?
- How to map PT servers with individual users
- Using same PT server for migration of multiple PT environments

Overview

Currently migration for PeopleSoft happens with the help of the Windows Client. We will have to enable our web client to perform the same migration without having any dependency on the windows client (apart from the administrative configuration).

Present architecture

The Stat central agent changes the status of the current migration to *PS Pending*. At this point windows client will pick the migration and delegate the actual migration to the app designer (or data mover in specific cases).

Compatibility issues with the current implementation

The web client cannot be a substitute the windows client in the current architecture. Through a web application, we cannot control specific applications on the end user's machine.

We can simply install the PS tools utilities on the web server aka Stat central agent's machine. However, there are the following issues with this approach

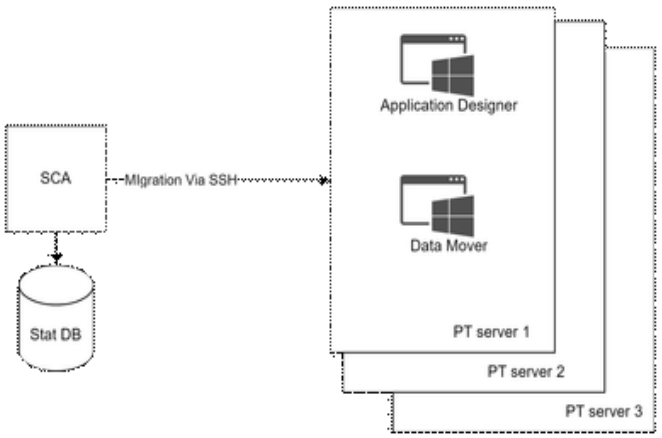
- Application designer can only be installed on Windows. But SCA can be installed on Windows and Linux. Users with Linux based SCA's wont be able to install application designer on their system.
- Couping PeopleTools utilities with SCA would also mean that all migration requests will go to a single PT enabled server. This can become a scaling issue in case of large number of parallel migrations.

It is clear that to mitigate the above problems, we will have to come up with an alternate approach. Users will have to have machines (with SSH enabled) where PT tool utilities are installed.

Goals of an alternate approach

- Users should be able to easily adapt to our new approach.
- Admins should be able to configure multiple servers dedicated for migration. (Will be clearer on the next section). This will help them scale horizontally.
- Admins should have the ability to provide each user with multiple servers for migration. However, users will have only one server for each version of PeopleSoft. With the current Windows Client implementation, users can only migrate for one version at a time, unless they change their PS options configuration.
- Users shouldn't have to re-learn any of the existing feature's workflow.

Alternate Architecture



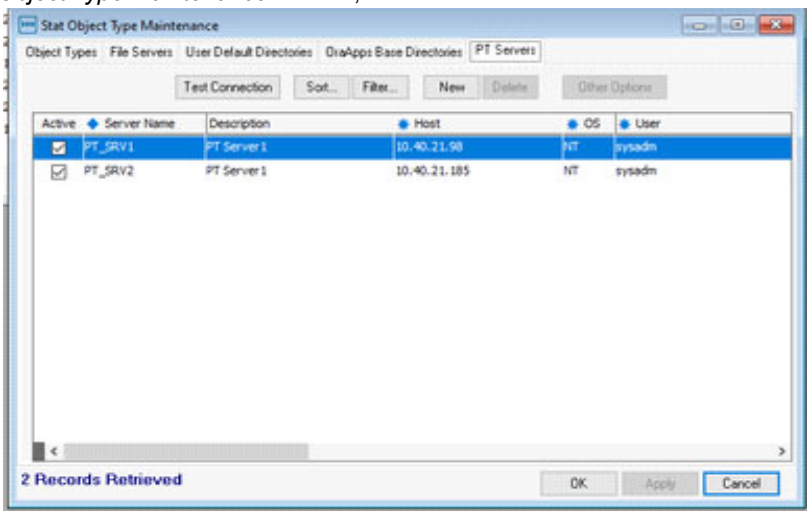
We can inform Stat about servers where application designer and data mover is present. SCA will create an SSH connection to this server and run the same CLI commands which are run by the Windows Client.

When a migration which has PS proprietary objects reaches PS Pending, it will be picked up by Stat Agent Job which runs every 5 seconds for processing. This job has been added in the AGENT_SYSTEM_JOB Stat repository table and will help to conclude this migration.

How to inform Stat about the available PT servers

We will have to configure this from Windows client.

- We have added new user rights to work with PT servers. You should find these two new rights under the PS Migration Mgmt group
  - Right to edit a PT server
  - Right to add a PT server
- In the *Stat Object Type Maintenance* window, we have added another tab called PT Servers.



How does the test connection of PT servers work?

The Stat Central Agent tries to establish a SSH connection the to PT server. If the connection is successful, then Stat tries to establish if there's a PeopleTools installation present in this PT server. This is done by checking the HKEY_CURRENT_USER\SOFTWARE\PeopleSoft\PeopleTools\Release8.40 registry key.

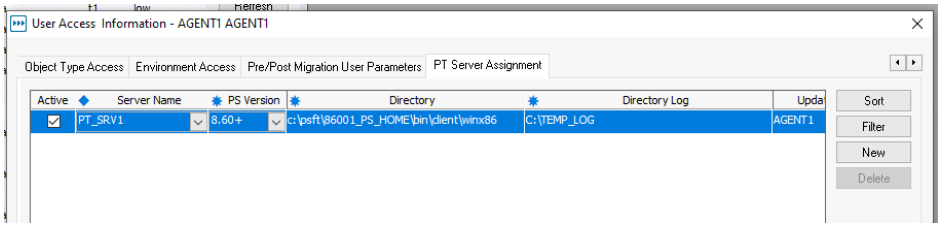
If Stat is able to find this key, then you should see the below message.
`"Successful connection to server PT Server1, with path PT installation server status: Verified"`

The status would have been `UNABLE TO VERIFY` if the registry key was missing.

An untested or unverified PT server can still be used for migration. The testing feature is only available for the Stat Admin to verify the usability of the configured PT server.

How to map PT servers with individual users

1. This information will be configured in User Access Information at Maintenance > Security Settings > User Maintenance > Select user > User Access Information.



2 We have created another tab *PT server assignment*. Here users will have the option to inform Stat about which PT server the user wishes to perform the migration for a particular version.

3 This tab will contain a table with the following columns

Value	Description
Active	Indicates if this server is activated in Stat
Server name	The PT server that you want to add for this user
Directory	The directory in the PT server remote machine where PeopleTool utilities like Application Designer (pside.exe) and Data Mover (psdmt.exe) are present. The admin needs to give the canonical path in this directory. Do not use relative path or environment variables while using providing the path here. Avoid adding any trailing forward or backward slash here.
Directory Log	This is where all the logs related to different PeopleTools CLI operations will be stored. Avoid adding any trailing forward or backward slash here.
PS Config File	This is the.cfg file which will be imported during the migration. This file should reside in the PT server which is mapped to this user.
Updated By	The user who updated this entry
Last Update	Date of the last update operation performed

A single user will not be able to have multiple active PT servers for the same version.

Using same PT server for migration of multiple PT environments

Typically you cannot use PeopleTool utilities belonging to different versions on the same machine as all PeopleTools installations, regardless of their version, store their metadata in the same registry keys. You can find these keys in HKEY_CURRENT_USER\SOFTWARE\PeopleSoft\PeopleTools\Release8.40

Similarly, PeopleTools Configuration Manager also fetches its metadata from a centralized location which is not specific to its version.

Windows Client mitigates this by asking for the version specific .cfg file from the Stat Admin. This cfg file is imported during the migration by the windows client using the pscfg.exe utility of that specific version. Once the migration is over, Windows Client reverts back the PeopleTools configuration to its original configuration.

When a user is migrating using the Web Client, the same workflow is replicated by the Stat Central Agent. The Stat Central Agent also gets the .cfg file which is provided by the user in PT Server Assignment tab. This file is them imported by the Central Agent using the pscfg utility. Once the migration is concluded, the original cfg file is restored.

NOTE: A PT server can be any windows machine that has PeopleTool utilities like Application designer. This machine must have SSH enabled with support for either SSH-1 or SSH-2.

Enable Windows Client to use ODBC for SQL Server

- Overview
- Configuring ODBC DataSource in Windows
- Using editini to create ODBC SQL connections

Overview

We currently use the SQL Native Client (SNC) to establish connections with SQL Servers. This method is utilized for connecting to Stat databases as well as other SQL servers, including PeopleSoft databases.

With Microsoft's deprecation of SNC, it has become important to support other methods of connectivity as well.

In this section we will discuss how to connect to SQL databases using ODBC. We will use an example of connecting to a Stat database.

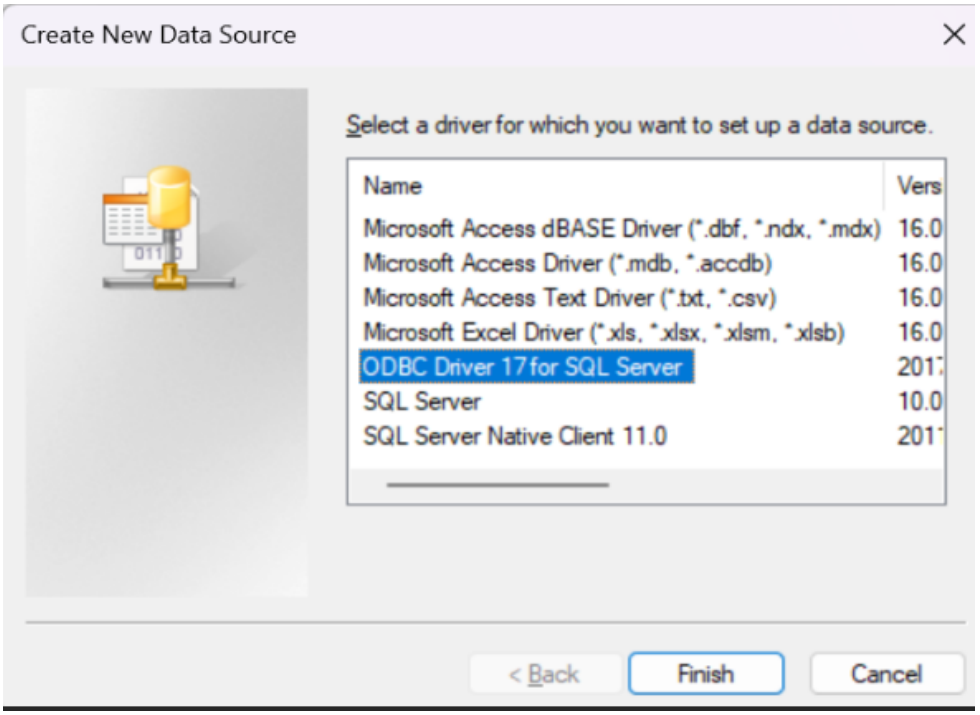
Configuring ODBC DataSource in Windows

1 Open the 64-bit ODBC Data Source Administrator.

   a Press Windows + R, type C:\Windows\System32\odbcad32.exe and press enter.

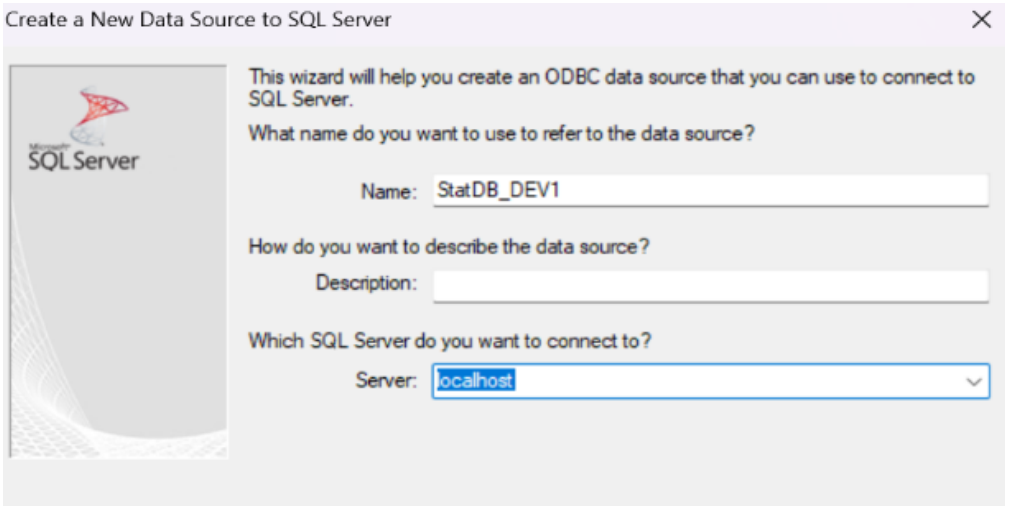
2 Go to the User DSN tab.

3 Click on add and select ODBC Driver 17 for SQL server.

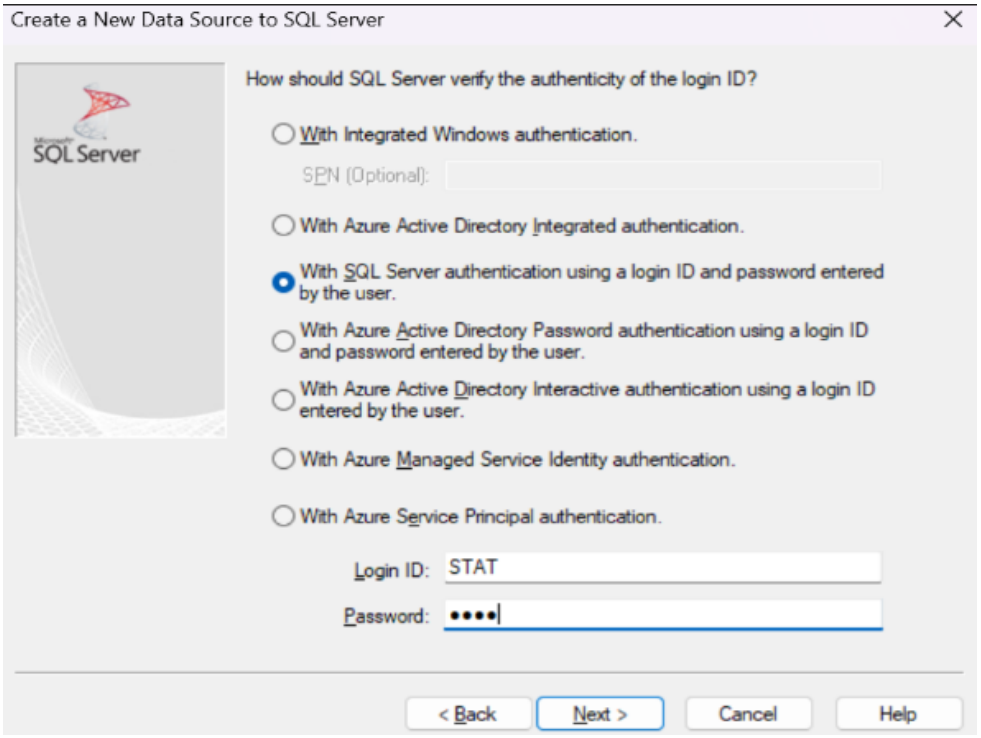


NOTE: We have tested our environments with ODBC Driver 17 for SQL server. Make sure that this ODBC driver is installed on your system; otherwise, this item will not be visible.

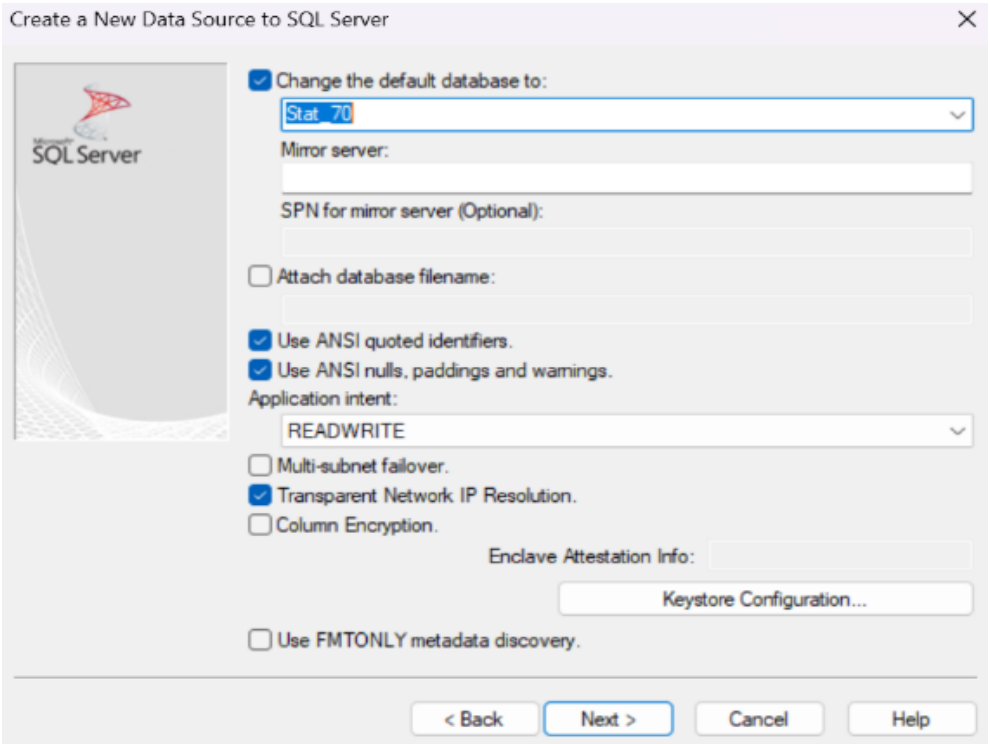
4 Give a user friendly DSN and provide with the server address.



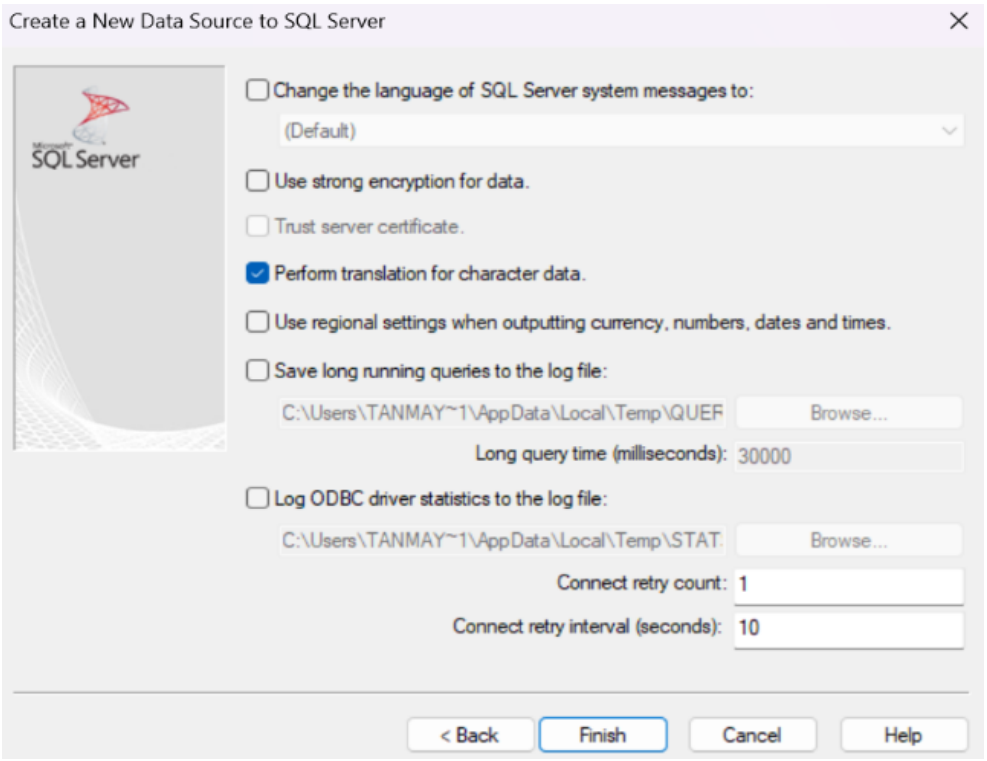
5 Use SQL server authentication using a login ID and password.



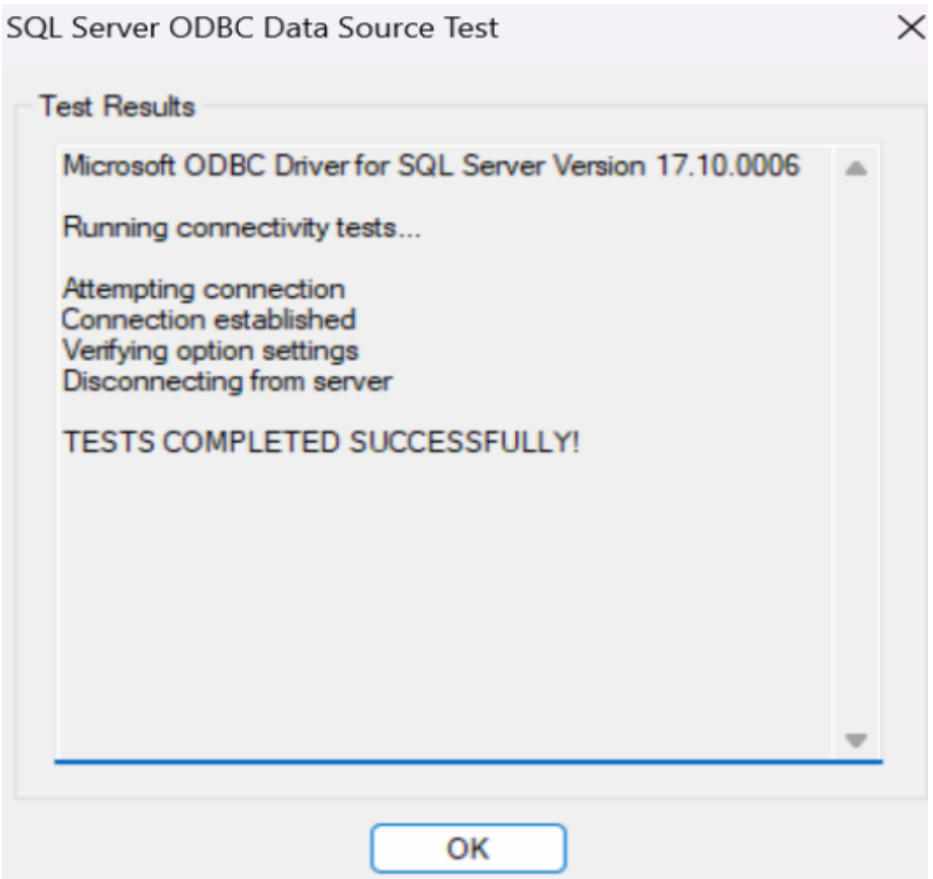
6 Change the default database to the database to which you want to connect.



7 Click **Next** and use the following configurations.



8 Click **Finish** and select **Test Data Source.** Ensure that the test connection is successful.



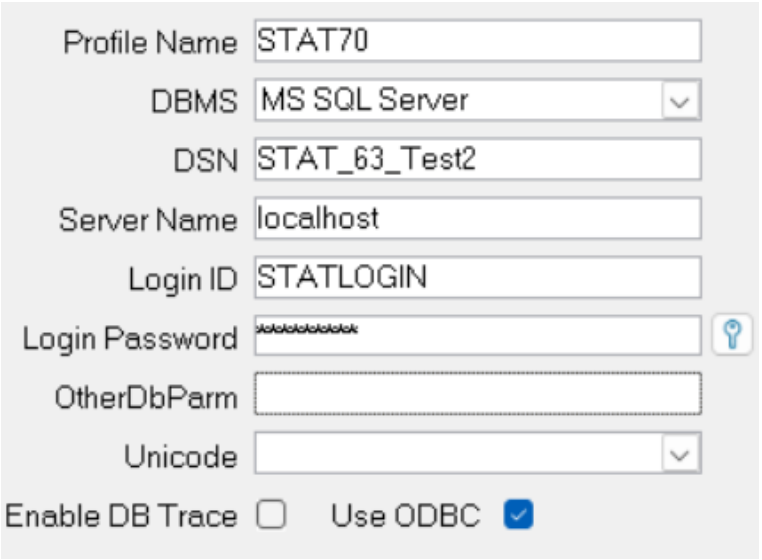
Using editini to create ODBC SQL connections

1 Open the INI editor.

2 Select *MS SQL SERVER* in *DBMS* field.

3 Mark the *Use ODBC* checkbox. This should make the *DSN* field appear.

4 Enter the DSN and then fill their rest of the fields.



A

Appendix: Sample Service Domain Configuration

This appendix shows the configuration of a sample service domain. You can use it to get ideas for setting up service domains for your own organization. All of the values listed here are defined in service domain-specific maintenance tables, which are described in detail in Service Domain-Specific Maintenance on page 122.

Configuration	Values
Applications	**HRMS** Application Environments: Benefits HR Tools **Financials** Application Environments: A/R A/P Purchasing GL Tools
Auto Tasks	**Status - Approved:** Schedule Change Document Pre-Changes Notify Customer User Sign-off Notify Customer Document Post-changes **Status - Released:** Schedule Release **Type -Enhancement:** Document Post-changes Notify Customers **Type - Fix:** Schedule Release
CSR Status (associated with CSR Type, Standard Change)	Approved Cancelled Completed Denied Development Proposed Quality Assurance System Test

Configuration	Values
CSR Type	Standard Change Emergency Change Enhancement Fix
Migration Path	**Emergency:** Production Development Production QA **Standard:** Production Development Testing QA Production Training
Priority	Critical Urgent 7 Days 30 Days 45 Days 90 Days
Queue	Manager Technical System Testing QA
Workflow (associated with the CSR Type, Enhancement)	Upgrade

B

Appendix: User Class Rights

This appendix provides a detailed description of each user class right. These rights are grouped into categories which correspond to functional areas within Stat. These categories include:

- CSR Edit Rights
- CSR Tabs Rights
- CSR Tasks Rights
- Generic Application Migration Management Rights
- Generic Application Object Management Rights
- Maintenance - File Object Rights
- Maintenance - General Rights
- Maintenance - Service Domain Rights
- Oracle Apps Migration Rights
- Oracle Apps Object Management Rights
- Oracle Apps Patch Management Rights
- PeopleSoft Migration Management Rights
- PeopleSoft Object Management Rights
- PeopleSoft Migration Management Rights
- Security Rights
- Stat Central Agent Rights
- Tool Rights
- Wizard Rights

Notes on User Class Rights

Some user class rights are specific to service domains. Users with service domain-specific rights (for example, the right to migrate archive sets) can invoke these rights only within the service domains that their user class is associated with. Rights that are not service domain-specific, however, can be used in any service domain that the user is allowed to work in. For example, the user class right, Undocumented Patch Wizard - Run, is not service domain-specific. This means that users that have this right in one service domain can run the wizard in all the service domains that they can access, including those in which the right is not given. Also, if a user class has an Add right, this generally overrides the absence of an Edit right. For example, if a user class is assigned the Activity Codes - Add right, the user class also has the right to edit existing records, even if the user class has not been assigned the Activity Codes - Edit right.

Another consideration to remember when assigning user class rights is that certain object management functions in Stat, such as running wizards, require that the user possess two rights, one to perform the function itself, and a second right to access the appropriate change management module. For example, to run the Archive Purge Wizard in the PeopleSoft change management module, the user needs the right, Obj Archive Purge Wizard - Run, and the right to access the PeopleSoft module, Change Management Module Access - PS. The remaining module

access rights include Change Management Module Access - Generic Apps and Change Management Module Access - Oracle Apps.

CSR Edit Rights

CSR edit rights are service domain-specific. They control the ability of users to change CSR values.

Table 1. CSR Edit Rights

Right	Description
CSR - Add	Enables the user to create a new CSR
CSR - Edit Closed - Full Rights	Enables the user to edit a CSR with a status of closed
CSR - Edit Closed - Read Only	Enables the user to view a CSR with a status of closed, after the number of CSR Close Lock Days has passed
CSR - Edit Open - Full Rights	Enables the user to edit a CSR with a status of open
CSR - Edit Open - Read Only	Enables the user to view a CSR with a status of open
CSR Application/Env - Change	Enables the user to change the Application Environment on a CSR. Security is applied after the initial save of the CSR.
CSR Assigned User - Change	Enables the user to reassign a CSR from one user to another. If the user does not have CSR Queue - Change rights, a transfer can only be made within the same queue.
CSR Attachments- Add	Enables the user to add attachments to a CSR
CSR Attachments - Delete	Enables the user to delete attachments from a CSR
CSR Closed Date - Change	Enables the user to change the Closed Date on a CSR
CSR Customer - Change	Enables the user to change the Customer on a CSR. Security is applied after the initial save of the CSR.
CSR Customer Priority -Change	Enables the user to change the Customer Priority on a CSR
CSR Due Date - Change	Enables the user to change the Due Date on a CSR. Security is applied after the initial save of the CSR.
CSR Open By - Change	Enables the user to override the default Open By User Name on a CSR
CSR Open Date - Change	Enables the user to change the CSR Open Date
CSR Priority - Change	Enables the user to change the Priority on a CSR. Security is applied after the initial save of the CSR.
CSR Project - Change	Enables the user to change project ID that the CSR is associated to.
CSR Queue - Change	Enables the user to reassign a CSR from one queue to another. A user with this right can reassign from one user to another regardless of CSR Assigned User - Change right.

Table 1. CSR Edit Rights

Right	Description
CSR Title - Edit	Enables the user to edit the Title of a CSR. Security is applied after the initial save of the CSR.
CSR Status - Change	Enables the user to change the status of a CSR. Security is applied after the initial save of the CSR.
CSR Tracking Number - Change	Enables the user to change the Tracking Number on a CSR
CSR Type - Change	Enables the user to change the CSR Type on a CSR. Security is applied after the initial save of the CSR.
CSR Workflow - Change	Enables the user to change the workflow on a CSR after a workflow has been assigned
CSR - Edit Other User - Full Rights	Enables the user to edit CSRs that are not assigned to them
CSR - Edit Other User - Full - Same Queue	Enables the user to edit a CSR that is not assigned to them if the CSR is in a queue that they are a member of
CSR - Edit Other User - Read Only	Enables the user to view CSRs that are not assigned to them
CSR - Override Other User's Lock	Enables the user to override other users' locks on CSRs
CSR - Take Ownership - Same Queue	Enables the user to take ownership of a CSR in a queue that they are a member of
Remove Deleted Objs from Archives	When a user with this right removes an object from the CSR, that object is also removed from all non-base archive sets.
Status Transfer Approval - Email	Enables the user to send approval Emails to the requested approver list for a CSR workflow status transfer
Status Transfer Approval Generate	Enables the user to generate status transfer approvals
Status Transfer Approval Override	Enables the user to approve another user's status transfer approvals
Status Transfer Approval Regenerate	Enables the user to regenerate the status transfer approval list
Status Transfer Override	Enables the user to transfer a CSR status without completing the transfer rules

CSR Tabs Rights

CSR tabs rights are service domain-specific. They control a user's ability to access and work within certain tabs of the CSR window.

Table 2. CSR Tabs Rights

Right	Description
CSR Issues Tab - Add	Enables the user to add issues to a CSR.
CSR Issues Tab - Delete	Enables the user to delete issues from a CSR.
CSR Issues Tab - Edit	Enables the user to edit issues on a CSR.
CSR Patch Tab - Add	Enables the user to add patches to a CSR
CSR Patch Tab - Delete	Enables the user to delete patches from a CSR
CSR Patch Tab - Edit	Enables the user to edit patches and their dependencies on a CSR
Description Tab - Edit	Enables the user to edit the Description tab on a CSR with a status of closed. Security is applied after the initial save of the CSR.
Detail Logs - Edit Any User Log	Enables the user to edit any user detail logs after they have been saved. This does not allow the user to edit System-Generated logs.
Detail Logs - Edit Own Logs	Enables the user to edit their own Detail Logs after a log has been saved
Detail Logs - Manage Confid. Logs	Enables the user to add, view, and print Confidential Logs
Detail Logs - View System Logs	Enables the user to view and print System-Generated Logs on a CSR
Environment Refresh - Modify	Enables the user to add, modify and delete environment refresh records
Patch Tab - Access	Enables the user to access the Patch Tab
Resolution Tab - Edit	Enables the user to edit the Resolution tab on a CSR with a status of closed. Security is applied after the initial save of the CSR.

CSR Tasks Rights

CSR tasks rights are service domain-specific. They control a user's ability to access and work within the Task/Time tab of the CSR window.

Table 3. CSR Tasks Rights

Right	Description
Tasks - Add	Enables the user to add new Tasks to a CSR. This does not affect Auto Task security.
Tasks - Change Estimated Hours	Enables the user to change the estimated time for a task
Tasks - Delete System Added	Enables the user to delete system-added Tasks from a CSR
Tasks - Delete User Added	Enables the user to delete user-added Tasks on a CSR
Tasks - Edit Other User	Enables the user to edit a task that is not assigned to them

Table 3. CSR Tasks Rights

Right	Description
Tasks - Edit Own Tasks	Enables the user to edit a task owned by themselves
Tasks - Edit Task on Closed CSR	Enables the user to edit a task after the CSR it is associated to has been closed
Tasks - Enter Others Time	Enables the user to add, delete, and change Daily Time Entries for other users

Generic Application Migration Management Rights

Generic Application Migration Management rights are not service domain-specific. They control a user's access to object migration functions for generic applications.

Table 4. Generic Application Migration Management Rights

Right	Description
GA Migration status change-Override	Enables the user who is not a migrator to change migration status to Cancel or Complete
GenApp - Allow partial migration	Allows the user to choose which objects in a Generic Application Archive Set will be migrated, effectively creating a partial Archive Set migration
Gen App Archive set - Migrate	Enables the user to migrate an archive set from the Migration Wizard on a CSR
Gen App Archive set - Migrate to Base	Enables the user to migrate an archive set to the Base Database
Gen App Archive set - Ready to Migrate	Enables the user to assign an archive set as ready to migrate
Gen App Base Archive Set - Delete	Enables the user to delete Baseline Archive sets
Gen App Migr. - Workflow Override	Enables the user to migrate to the target database, bypassing workflow status rules.
Gen App Migration Approval -Email	Enables the user to send approval Emails to the requested approver list for a migration
Gen App Migration Approval Override	Enables the user to approve another user's migration approvals
Gen App Migration Override	Enables the user to migrate Archive sets regardless of pending approvals
Gen App Post Migration Steps - Edit	Enables the user to edit Post Migration Steps Complete checklist

Generic Application Object Management Rights

Generic Application Object Management rights are not service domain-specific. They control a user's level of access to generic application object functions in Stat.

Table 5. Generic Application Object Management Rights

Right	Description
Gen App - Archive Release Level	Enables the user to assign a release level to a Generic Application archive set
Gen App - Maintain Other User's obj	Enables the user to maintain an object not assigned to them in a Generic Application CSR.
Gen App Object - Add Archive set	Enables the user to create new Interim or Final Archive sets of Generic Application objects
Gen App Object - Add to CSR	Enables the user to add Generic Application objects to a CSR
Gen App Object - Add without lock	Enables the user to add Generic Application objects to a CSR without locking
Gen App - Assigned Developer	Enables the user to be the assigned developer of an object in a Generic Application CSR.
Gen App Object - Bump Res. Priority	Enables the user to re-prioritize reserved Generic Application objects
Gen App Object - Delete Archive set	Enables the user to delete existing Archive sets of Generic Application objects
Gen App Object - Delete from CSR	Enables the user to remove Generic Application objects from a CSR
Gen App Object - Edit Archive set	Enables the user to edit existing Archive sets of Generic Application objects
Gen App Object - Lock current only	Enables the user to lock Generic Application objects for only the selected environment rather than all the environments on the migration path
Gen App Object - Mark for Del/Copy	Enables the user to mark Generic Application objects for deletion or copy
Gen App Object - Merge Versions	Enables the user to merge two version of a Generic Application object and create a new archive of the resulting merged object
Gen App Object - New from Existing	Enables the user to create a new Generic Application object from an existing object
Gen App Object - New from Template	Enables the user to create a new Generic Application object from template

Maintenance - File Object Rights

File object maintenance rights are not service-domain-specific. They control a user's level of access to file object functions in Stat.

Table 6. File Object Maintenance Rights

Right	Description
File Locations - Edit	Enables the user to edit existing File Locations
File Locations - Add	Enables the user to add new file locations from within Object Type Maintenance
File Servers - Add	Enables the user to add new File Servers from within Object Type Maintenance
File Servers - Edit	Enables the user to edit existing File Servers from within Object Type Maintenance
File Templates - Add	Enables the user to add File Templates
File Templates - Delete	Enables the user to delete existing File Templates
File Templates - Edit	Enables the user to edit existing File Templates
File Types - Add	Enables the user to add new File Types from within Object Type Maintenance
File Types - Edit	Enables the user to edit existing File Types from within Object Type Maintenance
User File Directories - Edit	Enables the user to edit existing User File Directories

Maintenance - General Rights

General maintenance rights are not service domain-specific. They control a user's access to certain miscellaneous functions in Stat.

Table 7. General Maintenance Rights

Right	Description
3rd Party VCM Connection - Add	Enables the user to add new 3rd Party VCM Connection definitions.
3rd Party VCM Connection - Edit	3rd Party VCM Connection - Add
Application Version - Add	Enables the user to add new application versions from within Business Object Maintenance
Application Version - Edit	Enables the user to edit existing application versions from within Business Object Maintenance
Change Mgmt Module Access - GenApp	Enables the user to access the Generic Application Tab
Change Mgmt Module Access - OraApp	Enables the user to access the Oracle Applications Tab
Change Mgmt Module Access - PS	Enables the user to access the PeopleSoft Tab
Countries - Add	Enables the user to add new Countries from within Country Maintenance
Countries - Edit	Enables the user to edit existing Countries from within Country Maintenance
Custom Fields - Administrator	Enables user to add new custom fields or edit existing custom fields

Table 7. General Maintenance Rights

Right	Description
Custom Reports - Add and Edit	Enables the user to add and edit custom reports
Customers - Add	Enables the user to add new customers, either from within Customer Maintenance or by right clicking on the **Customer** field in the CSR window
Customers - Edit	Enables the user to edit existing customers, either from within Customer Maintenance or by right clicking on the Customer field in the CSR window
Customers - Edit/View EID	Enables the user to edit and view customer Employee ID Numbers
Customers - PeopleSoft Search	Enables the user to add and update Customers, Countries, and Departments retrieved from PeopleSoft databases, via the Search PS Employee Search Engine and Country/Dept Search Engine
Data Object Type - Create Tables	Enables the user to create archive tables in Stat for Data Object types from within Data Object Maintenance
Data Object Types - Add	Enables the user to add new Business Object types from within Data Object Maintenance
Data Object Types - Edit	Enables the user to edit new Business Object types from within Data Object Maintenance
Departments - Add	Enables the user to add new Departments from within Department Maintenance
Departments - Edit	Enables the user to edit existing Departments from within Department Maintenance
Gen App Connection - Add	Enables the user to add new Generic Application Environment Connection definitions from within Generic Application Connection Maintenance
Gen App Connection - Edit	Enables the user to edit existing Generic Application Environment Connection definitions from within Generic Application Connection Maintenance
Global Query Administration	Enables the user to add, update, and delete global queries in Stat Web
Issue Labels - Add	Enables the user to add issue tracking labels.
Issue Labels - Edit	Enables the user to edit issue tracking labels.
Migration Approval - Add	Enables the user to add new Migration Approval records
Migration Approval - Edit	Enables the user to edit existing Migration Approval records

Table 7. General Maintenance Rights

Right	Description
OraApp Configuration - Add	Enables the user to add new configuration information for the Oracle Application module
OraApp Configuration - Edit	Enables the user to edit configuration information from within Oracle Application Configuration.
OraApp Configuration-Start/Stop	Enables the user to Start/Stop/Configure Oracle Application Environment Servers
OraApp Connection - Add	Enables the user to add new Oracle Application Environment Connection definitions from within Oracle Application Connection Maintenance.
OraApp Connection - Edit	Enables the user to edit existing Oracle Application Environment Connection definitions from within Oracle Application Connection Maintenance.
PeopleSoft Connection - Add	Enables the user to add new PeopleSoft Database Connection definitions from within PS Connection Maintenance
PeopleSoft Connection - Edit	Enables the user to edit existing PeopleSoft Database Connection definitions from within PS Connection Maintenance
PeopleSoft Search Cfg - Add	Enables the user to add and update PeopleSoft Search Configurations from within PS Search Config Maintenance
PeopleSoft Search Cfg - Change	Enables the user to update PeopleSoft Search Configurations from within PS Search Config Maintenance
Pre/Post Migration Server Parm - Add	Enables the user to add server-based parameters to post migration step definitions
Pre/Post Migration Server Parm - Edit	Enables the user to edit server-based parameters in post migration step definitions
Pre/Post Migration User Parm - Add	Enables the user to add user-based parameters to post migration step definitions
Pre/Post Migration User Parm - Edit	Enables the user to edit user-based parameters in post migration step definitions
Schema Object Parameters	Enables the user to edit existing Schema Object Parameters
Service Domains - Add	Enables the user to add new service domains from within service domain Maintenance
Service Domains - Edit	Enables the user to edit existing service domains from within service domain Maintenance

Table 7. General Maintenance Rights

Right	Description
Stat Report Definition - Edit	Enables the user to edit security and descriptions on Stat Reports from within Stat Report Maintenance
System Table - Edit	Enables the user to edit the System Table from within System Table Maintenance

Maintenance - Service Domain Rights

Service domain maintenance rights are service-domain-specific. They control a user's ability to change service domain parameters in Stat.

Table 8. Service Domain Maintenance Rights

Right	Description
Activity Codes - Add	Enables the user to add new Activities from within Activity Code Maintenance.
Activity Codes - Edit	Enables the user to edit Activities from within Activity Code Maintenance.
Application Environments - Add	Enables the user to add new Application Environments from within Application Environment Maintenance.
Application Environments - Edit	Enables the user to edit existing Application Environments from within Application Environment Maintenance.
Application Releases - Add	Enables the user to add new Application Releases.
Application Releases - Edit	Enables the user to edit existing Application Releases.
Applications - Add	Enables the user to add new Applications from within Application Code Maintenance.
Applications - Edit	Enables the user to edit Applications from within Application Code Maintenance.
Auto Tasks - Add	Enables the user to add new Auto Task definitions from within Auto Task Maintenance.
Auto Tasks - Edit	Enables the user to edit Auto Task definitions from within Auto Task Maintenance.
Business Rules - Add	Enables the user to add new system-level Business Rules from within Business Rules Maintenance.
Business Rules - Edit	Enables the user to edit existing system-level Business Rules from within Business Rules Maintenance.
Business Rules - Edit History	Enables the user to delete Business Rule History from within Business Rules Maintenance.
CSR Log Topics - Add	Enables the user to add new CSR Log topics from within CSR Log Topic Maintenance.
CSR Log Topics - Edit	Enables the user to edit existing CSR Log topics from within CSR Log Topic Maintenance.

Table 8. Service Domain Maintenance Rights

Right	Description
Customer Priority - Add	Enables the user to add new Customer Priority Codes from within Customer Priority Maintenance.
Customer Priority - Edit	Enables the user to edit existing Customer Priority Codes from within Customer Priority Maintenance.
Gen App Migration Paths - Add	Enables the user to add new Generic Application Environment Migration Paths from within Generic Application Migration Path Maintenance.
Gen App Migration Paths - Edit	Enables the user to edit existing Generic Application Environment Migration Paths from within Generic Application Migration Path Maintenance.
Mail Settings - Edit	Enables the user to modify the Mail Configuration.
Migration Steps - Add	Enables the user to add new Pre and Post Migration Steps from within Migration Steps Maintenance.
Migration Steps - Edit	Enables the user to edit existing Pre and Post Migration Steps from within Migration Steps Maintenance.
OraApp Migration Paths - Add	Enables the user to add new Oracle Application Environment Migration Paths from within Oracle Application Migration Path Maintenance.
OraApp Migration Paths - Edit	Enables the user to edit existing Oracle Application Environment Migration Paths from within Oracle Application Migration Path Maintenance.
PeopleSoft Migration Paths - Add	Enables the user to add new PeopleSoft Database Migration Paths from within PeopleSoft Migration Path Maintenance.
PeopleSoft Migration Paths - Edit	Enables the user to edit existing PeopleSoft Database Migration Paths from within PeopleSoft Migration Path Maintenance.
Priority Codes - Add	Enables the user to add new CSR Priorities from within CSR Priority Maintenance.
Priority Codes - Edit	Enables the user to edit existing CSR Priorities from within CSR Priority Maintenance.
Queues - Add	Enables the user to add new Queues from within Queue Maintenance.
Queues - Edit	Enables the user to edit existing Queues and Queue Assignments from within Queue Maintenance.
Templates - Add	Enables the user to add new Template definitions from within Application Template Maintenance and CSR Type Template Maintenance.

Table 8. Service Domain Maintenance Rights

Right	Description
Templates - Edit	Enables the user to edit existing Template definitions from within Application Template Maintenance and CSR Type Template Maintenance.
Type/Status Codes - Add	Enables the user to add new CSR Types and Statuses from within CSR Types and Statuses Maintenance.
Type/Status Codes - Edit	Enables the user to edit existing CSR Types and Statuses from within CSR Types and Statuses Maintenance.
Workflow Maintenance - Add	Enables the user to add new Workflow Records from within Workflow Maintenance.
Workflow Maintenance - Edit	Enables the user to edit existing Workflow Records from within Workflow Maintenance.

Oracle Apps Migration Rights

Oracle Apps Migration rights are service domain-specific. They control a user's access to Oracle Apps object migration functions in Stat.

Table 9. Oracle Apps Migration Rights

Right	Description
OA Migration status change-Override	Enables the user who is not a migrator to change migration status to Cancel or Complete
OraApp - Allow partial migration	Allows the user to choose which objects in a Oracle Application Archive Set will be migrated, effectively creating a partial Archive Set migration
OraApp Archive Set - Migrate	Enables the user to migrate an archive set from the Migration Wizard on a CSR
OraApp Archive Set - Migrate to Base	Enables the user to migrate an archive set to the Base Database
OraApp Archive Set - Ready to Migrate	Enables the user to assign an archive set as ready to migrate
OraApp Base Archive Set - Delete	Enables the user to delete Baseline Archive sets
OraApp Migration - Workflow Override	Enables the user to migrate to the target database, bypassing workflow status rules
OraApp Migration Approval - Email	Enables the user to send approval Emails to the requested approver list for a migration
OraApp Migration Approval Override	Enables the user to approve another user's migration approvals
OraApp Migration Override	Enables the user to migrate Archive sets regardless of pending approvals
OraApp Migration Step Command -Edit	Enables the user to modify CSR migration step custom command.

Table 9. Oracle Apps Migration Rights

Right	Description
OraApp Migration to Run Edition	Enables the user to migrate to Oracle Application Run Edition
OraApp Post Migration Steps - Edit	Enables the user to edit Post Migration Steps Complete checklist

Oracle Apps Object Management Rights

Oracle Apps Object Management rights are service domain-specific. They control a user's level of access to PeopleSoft proprietary object functions in Stat

Table 10. Oracle Apps Object Management Rights

Right	Description
OraApp - Archive Release Level	Enables the user to assign a release level to an Oracle Application Archive Set.
OraApp- Maintain other user's obj	Enables the user to maintain an object not assigned to them in an Oracle Applications CSR.
OraApp Object - Add Archive set	Enables the user to create new Interim or Final Archive sets of OraApp objects
OraApp Object - Add to CSR	Enables the user to add OraApp objects to a CSR
OraApp Object - Add without lock	Enables the user to add OraApp objects to a CSR without locking
OraApp - Assigned Developer	Enables the user to be the assigned developer of an object in an Oracle Application CSR
OraApp Object - Bump Res. Priority	Enables the user to re-prioritize reserved OraApp objects
OraApp Object - Delete Archive Set	Enables the user to delete existing Archive sets of OraApp objects
OraApp Object - Delete from CSR	Enables the user to remove OraApp objects from a CSR
OraApp Object - Edit Archive Set	Enables the user to edit existing Archive sets of OraApp objects
OraApp Object - Lock current only	Enables the user to lock Oracle Application objects for only the selected environment rather than all the environments on the migration path
OraApp Object - Mark for Del/Copy	Enables the user to mark OraApp objects for deletion or copy
OraApp Object - Merge Versions	Enables the user to merge two versions of an OraApp object and create a new archive of the resulting merged object

Table 10. Oracle Apps Object Management Rights

Right	Description
OraApp Object - New from Existing	Enables the user to create a new OraApp File object from an existing object
OraApp Object - New from Template	Enables the user to create a new OraApp File object from template

Oracle Apps Patch Management Rights

Oracle Apps Patch Management rights are service domain-specific. They control a user's level of access to Oracle patch management functions in Stat

Table 11. Oracle Apps Patch Management Rights

Right	Description
OraApp Maintenance Steps - Apply	Enables the user to apply a Maintenance Step
OraApp Maintenance Steps - Edit	Enables the user to edit a Maintenance Step
OraApp Merge Patches	Enables the user to merge patches into a new path from the Oracle Apps Patch Management Console.
OraApp Patch - Apply	Enables the user to request the application of a patch to an OraApp environment
OraApp Patch - Apply Override	Enables the user to apply a patch to an OraApps environment regardless of pending approvals
OraApp Patch - Approval Override	Enables the user to approve another user's patch application approval
OraApp Patch - Impact	Enables the user to request the analysis of a patch in an Oracle Applications environment
OraApp Patch - Rollback	Enables the user to request the rollback of a patch in an Oracle Applications environment
OraApp Patch Approval - Email	Enables the user to send approval Emails to the requested approver list for a Patch Apply
OraApp Patch Download	Enables the user to download an Oracle Application patch from Stat's Patch Inventory in the Oracle Application Patch Management Console
OraApp Patch Upload	Enables the user to upload a patch into the Stat Repository from the OraApps Patch Management Console
OraApp Patch - Completed Status	Enables user to change process status to completed statuses
OraApp Patch - Edit	Enables the user to edit an OraApps patch in the Stat Inventory
Patch Approval - Add	Enables the user to add new Patch Approval records
Patch Approval - Edit	Enables the user to edit new Patch Approval records

PeopleSoft Migration Management Rights

PeopleSoft Migration Management rights are service domain-specific. They control a user's access to PeopleSoft proprietary object migration functions in Stat.

Table 12. PeopleSoft Migration Management Rights

Right	Description
Allow to skip Restage	Enables the migrator to indicate that restaging the PeopleSoft project is not necessary
CSR Distributed Environments - Edit	Enables the user to activate/inactivate Distributed Environments on CSR Migration Path.
PS - Allow partial migration	Allows the user to choose which objects in a PeopleSoft Archive Set will be migrated, effectively creating a partial Archive Set migration
PS Archive Set - Auto Migration	Enables the user to Auto Migrate PeopleSoft proprietary objects to a target database
PS Archive Set - Migrate	Enables the user to migrate an archive set from the Migration Wizard on a CSR
PS Archive Set - Migrate PS Objects	Enables the user to migrate PeopleSoft proprietary objects
PS Archive Set - Migrate to Base	Enables the user to migrate an archive set to the Base Database
PS Archive Set - Ready to Migrate	Enables the user to assign an archive set as ready to migrate
PS Archive Set - Migr Types Separate	Enables the user to migrate just PeopleSoft proprietary objects or file objects when migrating an archive set that contains both types of objects
PS Archive Set - Migrate File Objects	Enables the user to migrate File Objects
PS Audit Flags - Edit	Enables the user to change the PeopleSoft Project audit flags during a migration
PS Base Archive Set - Delete	Enables the user to delete Baseline Archive sets
PS Migration - Workflow Override	Enables the user to migrate to the target database, bypassing workflow status rules
PS Migration Approval - Email	Enables the user to send approval Emails to the requested approver list for a migration
PS Migration Approval - Override	Enables the user to approve another user's migration approvals
PS Migration Override	Enables the user to migrate archive sets regardless of pending approvals
PS Migration status change-Override	Enables the user who is not a migrator to change migration status to Cancel or Complete

Table 12. PeopleSoft Migration Management Rights

Right	Description
PS Migration Step Command - Edit	Enables the user to modify CSR migration step custom command.
PS Recovery Wizard - Rec. Subset	Enables the user to recover subset of objects in an archive set
PS Staging DB Lock - Override	Enables the user to terminate an existing lock in a PeopleSoft staging database
Run Point-To-Point Migration Wizard	Enables the user to run the Point-To-Point Migration Wizard

PeopleSoft Object Management Rights

PeopleSoft Object Management rights are service domain-specific. They control a user's level of access to PeopleSoft proprietary object functions in Stat.

Table 13. PeopleSoft Object Management Rights

Right	Description
PS - Archive Release Level	Enables the user to assign a release level to a PeopleSoft archive set.
PS- Maintain other user's obj	Enables the user to maintain an object not assigned to them in a PeopleSoft application CSR.
PS Object - Add Archive Set	Enables the user to create new interim or final archive sets of PS objects
PS Object - Add to CSR	Enables the user to add PS objects to a CSR
PS Object - Add without lock	Enables the user to add PS objects to a CSR without locking
PS Object - Assigned Developer	Enables the user to be the assigned developer of an object in a PS Application CSR.
PS Object - Bump Res. Priority	Enables the user to re-prioritize reserved PS objects
PS Object - Delete Archive Set	Enables the user to delete existing archive sets of PS objects
PS Object - Delete from CSR	Enables the user to remove PS objects from a CSR
PS Object - Edit Archive Set	Enables the user to edit existing archive sets of PS objects
PS Object - Lock current only	Enables the user to lock PS objects for only the selected environment rather than all the environments on the migration path
PS Object - Mark for Del/Copy	Enables the user to mark PS objects for deletion or copy
PS Object - Mark for No Upgrade	Enables the user to mark a PS object for No Upgrade or for Upgrade
PS Object - Merge Versions	Enables the user to merge two versions of a PS object and create a new archive of the resulting merged object
PS Object - New from Existing	Enables the user to create a new PS file object from an existing object

Table 13. PeopleSoft Object Management Rights

Right	Description
PS Object - New from Template	Enables the user to create a new PS File object from template
PS Object-Refresh Sub-Object List	Enables the user to refresh the Sub-Object list for a PeopleSoft proprietary object in a CSR

Project Rights

Project rights are not service domain-specific. They control a user's ability to change project values in Stat.

Table 14. Project Rights

Right	Description
Projects - Add	Enables the user to create new Projects
Projects - Billing Process	Enables the user to run a Billing Process on Projects.
Projects - Billing Report	Enables the user to run Billing Reports on Projects.
Projects - Edit Others	Enables the user to save changes to Projects that the user does not own
Project Issues - Add	Enables the user to add issues to a project.
Project Issues - Delete	Enables the user to delete issues from a project.
Project Issues -- Edit	Enables the user to edit issues on a project.

Security Rights

Security rights are not service-domain-specific. They control a user's access to security functions in Stat.

Table 15. Security Rights

Right	Description
Access Stat Windows Client	Enables the user to access Stat Windows Client
Access Stat Web Client	Enables the user to access Stat Web Client
Database Connections - Manage	Enables the user to view and terminate User Connections from within the Connection Manager
LDAP Connection - Add	Enables the user to add new LDAP Connection definitions
LDAP Connection - Edit	Enables the user to edit existing LDAP Connection definitions
Master Database Login ID - Change	Enables the user to change the Login User Id and Password for the Stat Repository, within Change Database User ID/Password
Service Domains - Add All	Enables the user to grant other users access to service domains to which the user does not have access
Stat Users - Add	Enables the user to add new Stat Users from within User Maintenance

Table 15. Security Rights

Right	Description
Stat Users - Edit	Enables the user to edit existing Stat Users from within User Maintenance
Stat Users - Reset Password	Enables the user to reset the Password on an existing Stat User account
User Classes - Add	Enables the user to add new User Classes from within User Class Maintenance
User Classes - Edit	Enables the user to edit existing User Classes from within User Class Maintenance

Stat Central Agent Rights

Stat Central Agent rights are not service domain-specific. They control a user's ability to define printers and jobs for the Stat Central Agent.

Table 16. Stat Central Agent Rights

Right	Description
Agent Jobs - Add	Enables the user to add new Stat Central Agent Jobs from within Job Maintenance
Agent Jobs - Edit	Enables the user to edit existing Stat Central Agent Jobs from within Job Maintenance
Agent Printers - Add	Enables the user to add new Stat Central Agent Printer definitions from within Stat Central Agent Printer Maintenance
Agent Printers - Edit	Enables the user to edit existing Stat Central Agent Printer definitions from within Stat Central Agent Printer Maintenance

Tool Rights

Some Tool rights are service domain-specific, while others are not. They control a user's ability to access and work with certain utilities in Stat.

Table 17. Tool Rights

Right	Description
Agent Job Monitor	Gives the user access to the Agent Job Monitor in Stat Web
Agent Test Connect	Gives the user access to the Test Connect Page in Stat Web Client
Archive Sets - Ready to Migrate	Enables the user to access the Archive Sets - Ready to Migrate Window.
Configuration Guide	Enables the user to open the Configuration Guide window and configure maintenance tables.
Create Personal Rules	Enables the user to create Personal Rules
Customer Search Utility	Enables the user to access the Customer Search Utility.

Table 17. Tool Rights

Right	Description
Data Replication - Inbound	Enables the user to replicate data into the current database from a different database
Data Replication - Outbound	Enables the user to replicate data from the current database to a different database
Enterprise Console-Workload Monitor	Enables the user to access the Enterprise Console.
Launch INI File Editor	Enables the user to open the INI File Editor from Stat
Migration Console	Enables the user to access the Migration Console.
Oracle Applications Console	Enables the user to access the Oracle Application Console.
PS Object Mover Instructions - Upd	Enables the user to update the PS Object Mover Instructions
Purge CSRs Without Doing Export	Enables the user to purge a CSR without creating an export file. CSRs purged this way can never be restored.
Run CSR Purge for Open CSRs	Enables the user to run the purge on Open CSRs. This should be rarely used.
Run CSR Purge Wizard	Enables the CSR Purge Wizard to be available on the Tools Menu.
Save System Report Criteria	Enables the user to add and edit system-level Report Criteria from within the Report Library
Schedule Reports	Enables the user to schedule reports to run automatically
Support Console	Enables the user to access the Support Console.
Table Dump Utility - Run	Enables the user to run the Table Dump Utility

Wizard Rights

Some Wizard rights are service domain-specific, while others are not. They control a user's ability to run certain wizards in Stat.

Table 18. Wizard Rights

Right	Description
Archive Set Synchronization Wizard	Enables the user to access the Archive Set Synchronization Wizard.
Archive Set Sync Wizard - Migrate	Enables the user to migrate from the Archive Set Sync Wizard
CSR Search Wizard	Enables the user to access the CSR Search Wizard.
Obj Archive Purge Wizard - Run	Enables the user to run the Archive Purge Wizard
Obj Archive Search Wizard - Run	Enables the user to run the Object Archive Search Wizard

Table 18. Wizard Rights

Right	Description
Obj Mass Migration Wizard - Run	Enables the user to run the Mass Migration Wizard
Obj Migration History Wizard - Run	Enables the user to run the Migration History Wizard
Obj Recovery Wizard - Run	Enables the user to run the Recovery Wizard
Object Compare Wizard	Enables the user to access the Object Compare Wizard.
Object History Wizard	Enables the user to access the Object History Wizard.
Object Impact Wizard	Enables the user to access the Object Impact Wizard.
Release Recovery - Run	Enables the user to run the Release Recovery Wizard
Undocumented Obj Wizard -Run	Enables the user to run the Undocumented Object Wizard
Undocumented Patch Wizard - Run	Enables the user to run the Undocumented Patch Wizard.

C

Appendix: Creating a Staging Database

Staging databases are used when migrating archive sets from your Stat database to a PeopleSoft database. A staging database is essentially a mini-PeopleSoft database with no application data and minimal tools data. Once created it should be maintained and tuned the same as other PeopleSoft databases in your environment.

Depending on the volume of objects moved or number of PeopleSoft tools versions you are supporting, you may decide to have multiple staging databases. This section describes how to create a staging database in Stat.

- **For PS version 8.x and higher** – The staging database can either be a PeopleSoft demo (DEMO) or system (SYS) database. For detailed instructions on creating this database, please see your PeopleSoft Installation and Administration Guide. Financial databases in particular have a large number of tables used for sorting data. These can be dropped from the staging database.

Once you have created your AUD, Demo, or System database, execute the appropriate script

- If running on Oracle, execute **StageORA855.sql**
- If running on SQL Server, execute **StageMSS855.sql**

These scripts complete the creation of a staging database. It is recommended that you create at least 2 staging databases. You may need to alter this script to match your platform.

NOTE: Be aware of the following:

- For each staging database you define in Stat, make sure the Reload Last Project at Startup option is deselected for that database in PeopleSoft App Designer. Stat may have difficulty auto-migrating objects from the staging database if this option is selected.
- When migrating archive sets, the base language of the staging database must be the same as the base language of the environment that the archive set came from (i.e., the source). The base language option is specified in the PeopleSoft Environment Connection Maintenance table. For more information, see PeopleSoft Environment Connection Maintenance on page 80.

PeopleSoft on Oracle

1. Locate the **StageORA855.sql** script.
2. Replace the following variables:
   - **[OWNER/PWD@DATABASENAME]** Replace with the correct values for the PeopleSoft schema owner/password and staging database.
   - **[SPOOLPT]** Replace with the directory for the session log.
   - **[PTAPP]** Replace with the tablespace for the staging table
   - **[PSINDEX]** Replace with the tablespace for the staging table indexes
3. Run the modified script via Sql*Plusor Toad in the PeopleSoft staging database as the PeopleSoft schema owner

PeopleSoft on SQL Server

1. Locate the **StageMSS855.sql** script.
2. Find and replace the variable **[DATABASENAME]** with the name of the database.
3. Using Enterprise Manager, go into SQL Server Analyzer from Tools on the menu bar. Log in as **sa** with SYSTEM-level access and open the modified scripts. After running each script, copy the output of the script results to a file and save the file for review.

D

Appendix: Database Tuning

This appendix provides tuning information for Stat databases running on Oracle and MS SQL Server.

Oracle Database Instance Tuning

Table 19. Init.ora recommended parameters settings

Name	Recommended
session_cached_cursors	150
sort_area_size	1048576
optimizer_index_cost_adj	35
optimizer_index_caching	90
pga_aggregate_target	25165824
workarea_size_policy	AUTO
open_cursors	300

Run the following command on a weekly basis:

```
exec dbms_stats.gather_schema_stats(ownname=>'STAT', CASCADE => TRUE);
```

MSS SQL Server Database Tuning

MSS SQL Server is basically a self tuning system.

Be sure there is adequate space for Transaction logs based on your backup schedule

TempDB should be a minimum 50M for each database on the server, including the master, model, etc). e.g. if there are 6 databases, the tempdb should be, at minimum, 300M in size.

Run the following on a weekly basis:

```
Execute STAT_UPDATESTATS
```

E

Appendix: Oracle Applications File Type Directory

This appendix documents the directories Stat uses for retrieving an object list, archiving an object, and migrating an object for all the proprietary Oracle Applications file object types. Proprietary Oracle Applications file types require that the user select a product and language before Stat retrieves a list of objects. These attributes are used to determine the archive and migration locations.

Notation:

- **$prod** is used to represent the selected product
- **$prodTop** is used to represent the directory for the selected product
- **$lang** is used to represent the selected language.

Oracle follows a precise file structure convention for locating files for specific types. Many sites do not adhere to the convention strictly for their custom object types. Stat provides flexibility where feasible and useful to accommodate common conventions used by many sites for storing custom files. For example, Oracle stores all FMB files in $AU_TOP/forms/<lang>. Many sites do not store custom FMB files in $AU_TOP, nor do they create a sub-directory for each language. Stat allows custom FMBs to be stored in $prodTop/forms directory.

An Oracle Applications environment can be partitioned across several physical servers. Logically, there are four servers: Web Server, Forms Server, Concurrent Manager, and Database. Objects for each object type are stored on one or more of these logical servers. The table also identifies the server type.

Table 20.

Object Type: Exe File (All Servers)	
Object List	Include all files in: - $prodTop/bin/*
Object Archive	$prodTop/bin
Migration Destination	$prodTop/bin

Table 21.

Object Type: Menu File (Forms Server only)	
Object List	Include all files in: $prodTop/resource/$lang/*.mmb
Object Archive	$prodTop/resource/$lang
Migration Destination	$prodTop/resource/$lang **NOTE:** The MMX file is always generated in $prodTop/resource/$lang (not $AU_TOP/resource).

Table 22.

Object Type: Form File (Forms Server only)	
Object List	Consider possible forms in: -Registered Form -FMX files in $prodTop/forms/$lang Include if FMB file exists in $AU_TOP/forms/$lang If $prod is custom Include all FMBs in $prodTop/forms/$lang Include all FMBs in $prodTop/forms EndIf **NOTE:** Stat does not return any objects if selected product is AU*

Object Archive	If $prod is custom
	Consider following directories using first where file is found
	-$prodTop/forms/$lang
	-$propTop/forms
	-$AU_TOP/forms/$lang
	If file not found, throw exception.
	Else
	$prodTop/forms/$lang
	EndIf

Migration Destination	If $prod is custom
	Consider following directories using first where file is found
	-$prodTop/forms/$lang
	-$propTop/forms
	-$AU_TOP/forms/$lang
	If file not found, consider following directories using first that exists
	-$prodTop/forms/$lang
	-$propTop/forms
	If directory not found, throw exception.
	Else
	$prodTop/forms/$lang
	EndIf
	NOTE: The FMX file is always generated in $prodTop/forms/$lang

Table 23.

Object Type: Form Library File (Forms Server only)	
Object List	Include all files in: -$prodTop/resource/*.pll **NOTE:** Since Oracle stores all PLLs in $AU_TOP/resource, no files will typically be returned with standard products except for AU. However, Stat searches the product top to allow custom PLLs to be stored with the custom product top.
Object Archive	$prodTop/resource
Migration Destination	$prodTop/resource **NOTE:** The PLX file is always generated in $prodTop/resource (not $AU_TOP/resource). This requires FORMS60_PATH to include $prodTop/resource if custom PLLs are not stored in $AU_TOP/resource.

Table 24.

Object Type: Oracle Workflow File (Database Server only)	

Object List	If $prod is custom
	Include all files in:
	-$prodTop/admin/import/$lang/*.wft
	-$prodTop/admin/import/*.wft
	-$prodTop/admin/$lang/*.wft
	-$prodTop/admin/*.wft
	Else
	Include all files in:
	-$prodTop/patch/115/import/$lang/*.wft
	-$prodTop/patch/115/import/*.wft
	-$prodTop/admin/import/$lang/*.wft
	-$prodTop/admin/import/*.wft
	EndIf

Object Archive	If $prod is custom
	Consider following directories using first where file is found
	-$prodTop/admin/import/$lang
	-$prodTop/admin/import
	-$prodTop/admin/$lang
	-$prodTop/admin
	If file not found, throw exception.
	Else
	Consider following directories using first where file is found
	-$prodTop/patch/115/import/$lang
	-$prodTop/patch/115/import
	-$prodTop/admin/import/$lang
	-$prodTop/admin/import
	EndIf

Table 24.

Object Type: Oracle Workflow File (Database Server only)	

Migration Destination	If $prod is custom
	Consider following directories using first where file is found
	-$prodTop/admin/import/$lang
	-$prodTop/admin/import
	-$prodTop/admin/$lang
	-$prodTop/admin
	If file not found, consider following directories using first that exists
	-$prodTop/admin/import/$lang
	-$prodTop/admin/import
	-$prodTop/admin/$lang
	-$prodTop/admin
	If directory not found, throw exception.
	Else
	Consider following directories using first where file is found
	-$prodTop/patch/115/import/$lang
	-$prodTop/patch/115/import
	-$prodTop/admin/import/$lang
	-$prodTop/admin/import
	If file not found, consider following directories using first that exists
	-$prodTop/patch/115/import/$lang
	-$prodTop/patch/115/import
	-$prodTop/admin/import/$lang
	-$prodTop/admin/import
	If directory not found, throw exception.
	EndIf
	NOTE: The WFT file is always loaded into the database using WFLOAD
	NOTE: For R12.2 environments, the WFT file is loaded into the Run Edition of the database when migrating to Run or Both Editions and is loaded into Patch Edition of the database when migrating to Patch Edition. Note that you need to have the 'OraApp Migration to Run Edition' right to migrate to Run Edition.

Table 25.

Object Type: PKB (PL/SQL Body) File (Database Server only)	
Object List	Include all files in: -$prodTop/admin/sql/.pkb,.plb $prodTop/patch/115/sql/*.pkb, *.plb
Object Archive	Consider following directories using first where file is found -$prodTop/patch/115/sql -$prodTop/admin/sql

Migration Destination	If $prodTop/patch/115/sql directory exists
	-$prodTop/patch/115/sql
	Else
	-$prodTop/admin/sql
	EndIf
	NOTE: The file is always executed in the database using sqlplus
	NOTE: For R12.2 environments, the file is executed in the Run Edition of the database when migrating to Run or Both Editions and is executed in Patch Edition of the database when migrating to Patch Edition. Note that you need to have the 'OraApp Migration to Run Edition' right to migrate to Run Edition.

Table 26.

Object Type: PKH (PL/SQL Body) File (Database Server only) **NOTE:** This object type looks for files with both .pkh and .pks extensions.	
Object List	Include all files in: -$prodTop/admin/sql/(*.pkh, *.pks) $prodTop/patch/115/sql/(*.pkh, *.pks)
Object Archive	Consider following directories using first where file is found -$prodTop/patch/115/sql -$prodTop/admin/sql

Migration Destination	If $prodTop/patch/115/sql directory exists
	-$prodTop/patch/115/sql
	Else
	-$prodTop/admin/sql
	EndIf
	NOTE: The file is always executed in the database using sqlplus.
	NOTE: For R12.2 environments, the file is executed in the Run Edition of the database when migrating to Run or Both Editions and is executed in Patch Edition of the database when migrating to Patch Edition. Note that you need to have the 'OraApp Migration to Run Edition' right to migrate to Run Edition.

Table 27.

Object Type: PL/SQL File (Database Server only)	
Object List	Include all files in: -$prodTop/admin/sql/*.pls if exists, otherwise $prodTop/sql/*.pls -$prodTop/patch/115/sql/*.pls **NOTE:** All standard products include the $prodTop/admin/sql directory. Stat checks the $prodTop/sql directory to accommodate sites that store their custom PLS files in this directory
Object Archive	Consider following directories using first where file is found -$prodTop/patch/115/sql/ $prodTop/admin/sql if exists, otherwise $prodTop/sql

Migration Destination	If $prodTop/patch/115/sql directory exists
	-$prodTop/patch/115/sql
	Else if $prodTop/admin/sql directory exists
	-$prodTop/admin/sql
	Else
	-$prodTop/sql
	EndIf
	NOTE: The file is always executed in the database using sqlplus
	NOTE: For R12.2 environments, the file is executed in the Run Edition of the database when migrating to Run or Both Editions and is executed in Patch Edition of the database when migrating to Patch Edition

Table 28.

Object Type: Report File (Concurrent Manager Server only)	
Object List	Include all files in: -$prodTop/reports/$lang/*.rdf if exists, otherwise $prodTop/reports/*.rdf **NOTE:** Stat uses the value of $APPLREP instead of “reports” for the subdirectory. This environment variable is always set to “reports
Object Archive	$prodTop/reports/$lang if exists, otherwise $prodTop/reports
Migration Destination	$prodTop/reports/$lang if exists, otherwise $prodTop/reports **NOTE:** The file is always compiled.

Table 29.

Object Type: SQL Report (Concurrent Manager Server only)	
Object List	$prodTop/sql/*.sql
Object Archive	$prodTop/sql
Migration Destination	$prodTop/sql **NOTE:** The file is never executed in the database.

Table 30.

Object Type: SQL Script (Database Server only)	
Object List	Include all files in: -$prodTop/admin/sql/*.sql -$prodTop/patch/115/sql/*.sql
Object Archive	Consider following directories using first where file is found -$prodTop/patch/115/sql -$prodTop/admin/sql

Migration Destination	If $prodTop/patch/115/sql directory exists
	-$prodTop/patch/115/sql
	Else
	-$prodTop/admin/sql
	EndIf
	NOTE: The file is always executed in the database using sqlplus.
	NOTE: For R12.2 environments, the file is executed in the Run Edition of the database when migrating to Run or Both Editions and is executed in Patch Edition of the database when migrating to Patch Edition. Note that you need to have the 'OraApp Migration to Run Edition' right to migrate to Run Edition.

Table 31.

Object Type: OAF - OA Component XML File (Database Server only)	
Object List	Include all .xml files in: MDS Repository for a specific $prodTop
Object Archive	XMLExporter is used to extract the xml file from MDS Repository.
Migration Destination	XMLImporter is used to deploy the xml file to MDS Repository of target **NOTE:** For R12.2 environments, the xml file is loaded into the Run Edition of the database when migrating to Run or Both Editions and is loaded into Patch Edition of the database when migrating to Patch Edition. Note that you need to have the 'OraApp Migration to Run Edition' right to migrate to Run Edition.

Table 32.

Object Type: OAF - OA Component Class File (Web Server only)	
Object List	Include all seeded files in: $JAVA_TOP/oracle/apps/$ProdTop/<component>/webui/*.class And any custom files in: $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/webui/*.class
Object Archive	Consider following directories - $JAVA_TOP/oracle/apps/$ProdTop/<component>/webui - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/webui
Migration Destination	Seeded files are migrated to: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/webui Custom files are migrated to: - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/webui **NOTE:** Custom files could be placed under a directory other than $JAVA_TOP, as long as that directory is on the classpath.

Table 33.

Object Type: OAF - OA Component Java File (Web Server only)	
Object List	Include all seeded files in: $JAVA_TOP/oracle/apps/$ProdTop/<component>/webui/*.java And any custom files in: $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/webui/*.java

Table 33.

Object Type: OAF - OA Component Java File (Web Server only)	
Object Archive	Consider following directories - $JAVA_TOP/oracle/apps/$ProdTop/<component>/webui - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/webui
Migration Destination	Seeded files are migrated to: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/webui Custom files are migrated to: - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/webui **NOTE:** Custom files could be placed under a directory other than $JAVA_TOP, as long as that directory is on the classpath.

Table 34.

Object Type: OAF - BC4J Component XML File (Web Server only)	
Object List	Include all seeded files in: $JAVA_TOP/oracle/apps/$ProdTop/<component>/server/*.xml And any custom files in: $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server/*.xml

Table 34.

Object Type: OAF - BC4J Component XML File (Web Server only)	
Object Archive	Consider following directories: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/server - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server
Migration Destination	Seeded files are migrated to: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/server Custom files are migrated to: - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server **NOTE:** Custom files could be placed under a directory other than $JAVA_TOP, as long as that directory is on the classpath.

Table 35.

Object Type: OAF - BC4J Component Class File (Web Server only)	
Object List	Include all seeded files in: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/server/*.class - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui>/*.class And any custom files in: - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server/*.class - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/<all except webui>/*.class
Object Archive	Consider following directories - $JAVA_TOP/oracle/apps/$ProdTop/<component>/server - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui> - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/<all except webui>
Migration Destination	Seeded files are migrated to: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui> - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui> Custom files are migrated to: - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server **NOTE:** Custom files could be placed under a directory other than $JAVA_TOP, as long as that directory is on the classpath.

Table 36.

Object Type: OAF - BC4J Component Java File (Web Server only)	
Object List	Include all seeded files in: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/server/*.java - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui>/*.java And any custom files in: - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server/*.java - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/<all except webui>/*.java
Object Archive	Consider following directories - $JAVA_TOP/oracle/apps/$ProdTop/<component>/server - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui> - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/<all except webui>
Migration Destination	Seeded files are migrated to: - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui> - $JAVA_TOP/oracle/apps/$ProdTop/<component>/<all except webui> Custom files are migrated to: - $JAVA_TOP/$mycompany/oracle/apps/$ProdTop/<component>/<layer type>/<layer value>/server **NOTE:** Custom files could be placed under a directory other than $JAVA_TOP, as long as that directory is on the classpath.

Table 37.

Object Type: XDO XML Publisher Template Files (Database Server only)	
Object List	Include all templates for a specific $prodTop from XDO_LOB table where LOB_TYPE is one of TEMPLATE, TEMPLATE_SOURCE, XML_SCHEMA, XML_SAMPLE and DATA_TEMPLATE
Object Archive	XDOLoader is used to extract the template from XDO_LOB table
Migration Destination	XDOLoader is used to deploy the template to XDO_LOB table of target **NOTE:** For R12.2 environments, the template file is loaded into the Run Edition of the database when migrating to Run or Both Editions and is loaded into Patch Edition of the database when migrating to Patch Edition. Note that you need to have the 'OraApp Migration to Run Edition' right to migrate to Run Edition.

Table 38.

Object Type: XDO XML Publisher Translations (Database Server only)	
Object List	Include all translations for a specific $prodTop from XDO_LOB table where LOB_TYPE is XDO_TRSL
Object Archive	XLIFFLoader is used to extract the translation from XDO_LOB table
Migration Destination	XLIFFLoader is used to deploy the translation to XDO_LOB table of target environment **NOTE:** For R12.2 environments, the template file is loaded into the Run Edition of the database when migrating to Run or Both Editions and is loaded into Patch Edition of the database when migrating to Patch Edition. Note that you need to have the 'OraApp Migration to Run Edition' right to migrate to Run Edition.

Table 39.

Object Type: XDO XML Publisher DS by Template (Database Server only)	
Object List	Include all active data sources from XDO_DS_DEFINITIONS
Object Archive	FNDLoad is used to extract the data source from XDO_DS_DEFINITIONS table
Migration Destination	FNDLoad is used to deploy the data source to XDO_DS_DEFINITIONS table of target environment

Table 40.

Object Type: XDF Editioning Views (R12.2 and Database Server only)

Object List	Include all Editioning Views from DBA_EDITIONING_VIEWS
Object Archive	xdfgen.pl is used to extract the xdf file from the Run Edition
Migration Destination	-xdf file is copied to If $prodTop/patch/115/xdf directory exists -$prodTop/patch/115/xdf Else if $prodTop/admin directory exists -$prodTop/admin EndIf -xdfcmp.pl is used to deploy the xdf file to the target environment **NOTE:** When migrating xdf files to Run or Both Editions of a target environment: • If there is an active Patch Cycle in effect, Stat deploys the xdf file to the file system and returns with a warning. • If there is no Patch Cycle in effect, Stat deploys the xdf file to the file system and loads it to the Run Edition of the environment. When migrating xdf files to Patch Edition of a target environment: • If there is an active Patch Cycle in effect, Stat deploys the xdf file to the file system and loads it to the Patch Edition of the environment. • If there is no Patch Cycle in effect, Stat deploys the xdf file to the file system and returns with a warning.

Table 41.

Object Type: XDF Editioning View Files (R12.2 and Database Server only)

NOTE: This object type is available to users in case the generated xdf file using the xdfgen.pl needs to be modified before deployment to a target environment.

Object List	Include all files in: -$prodTop/patch/115/xdf/*.xdf
Object Archive	$prodTop/patch/115/xdf
Migration Destination	If $prodTop/patch/115/xdf directory exists -$prodTop/patch/115/xdf and xdfcmp.pl is used to deploy the xdf file to the target environment

F

Appendix: Ports and Firewalls

This appendix provides instructions for resolving port conflicts and firewall issues that may prevent the Stat Central Agent from running. Typical port and firewall conflicts include:

- Other applications are using the same port as the Stat Central Agent
- You are running multiple Stat Central Agents on the same host machine and the installations are trying to access the same ports
- The default timeout setting on a firewall prevents the Stat Central Agent from opening properly

Resolving port and firewall conflicts

If the Stat™ Central Agent will not run when started, the port assigned to it may already in use by a different program or there are firewalls that need to have ports opened for the Stat Central Agent to communicate with the database or with the Stat Client.

Typical port and firewall conflicts include:

- Other applications are using the same port as the Stat Central Agent
- You are running multiple Stat Central Agents on the same host machine and the installations are trying to access the same ports
- The default timeout setting on a firewall prevents the Stat Central Agent from opening properly

If you have port conflicts, the server will display one or more error messages, such as:

```
java.net.BindException: Address already in use: Bind
```

The Stat Central Agent utilizes a set of ports that are already defined.

These values are defined for a default port offset of zero which is set in a variable called `jboss.socket.binding.port-offset` in **standalone.conf.bat** or **standalone.conf** file. If there is a conflict situation or a second or third agent is necessary, you may change the `jboss.socket.binding.port-offset` in **standalone.conf.bat** or **standalone.conf** file. The value for offset is added to all the default values.

For example:

- if offset is zero, ports 8080, 8443, 9990, 9993, 4712, and 4713 are used.
- If offset is one, ports 8081, 8444, 9991, 9994, 4713, and 4714 are used.
- If offset is two, ports 8082, 8445, 9992, 9995, 4714, and 4715 are used.
- If offset is 100, ports 8180, 8543, 10090, 10093, 4812, and 4813 are used.

Table 42. Ports

Description	Ports
HTTP socket binding	8080
HTTPS socket binding (See Note)	8443
Management socket binding	9990

Table 42. Ports

Description	Ports
Management socket binding https (See Note)	9993
Transaction sockets	4712
	4713

NOTE: Be aware of the following:

- Stat invokes the DNS server to resolve the fully qualified server name when communicating between the client and the central agent. When server hostname is not registered on the DNS server, use etc/hosts file to map hostname and its IP address.
- HTTPS connector socket and Management socket — These ports are only necessary if the Stat Central Agent is configured to support HTTPS.

Port configurations

When other applications are using the same port as the Stat Central Agent, you need to change the port offset in your standalone.conf.bat or standalone.conf file.

1. Review the port configurations described above and decide on a proper offset.
2. Open **<STAT_HOME>\app\bin\standalone.conf.bat** with Notepad or other text editor. For Stat Central Agent on Unix, you need to open the **<STAT_HOME>/app/bin/standalone.conf** file.
3. Search for the setting: `-Djboss.socket.binding.port-offset=0`
4. Change the setting to a proper offset. For example, `-Djboss.socket.binding.port-offset=10`

Firewall configuration

The http port is the only port that needs to be opened on existing firewalls.

- Client to Central agent: 8080 (If port-offset has changed, add the value to 8080)
- Central Agent to Oracle agent: 8080 (If port-offset has changed, add the value to 8080)

Other ports used by the Stat Central Agent include the following (the actual port numbers will vary according to your site specifications):

- Stat database (Oracle® default=1521; MSS default = 1433)
- PeopleSoft® databases
- E-Business databases
- FTP/SFTP (default = 21/22)
- Email: SMTP/POP3/IMAP4 (default= 25/995/993)

The Stat Client will need the same ports opened if there is a firewall between the client and any of the above items.

Natted firewall between the Stat Central Agent and Stat Oracle Agents

If there is a natted firewall between the Stat Central Agent and the Stat Oracle Agents, the following options must be configured in the stat.conf file for the Stat Oracle Agents. Older versions of Stat always required the fields to be filled in, but since 5.6.0, the Stat Oracle Agents query the Stat Central Agent for the secure Stat database information. You need only change the stat.db.server: value and indicate the natted ip address. For this scenario, they are not optional.

```
##############################################################################
# Stat Repository
##############################################################################
stat.db.jdbc_driver:oracle.jdbc.driver.OracleDriver
stat.db.server:<stat repository server name/ip> <-- Natted IP Address
```

Appendix: REST Web Services API

Stat provides programmatic access to CSR information via a Web Service API. The Stat Web Services are available when the Stat Central Agent is live. API calls represent specific operations that your client applications can use to retrieve or update data.

The following information is intended for developers and system administrators who want to use Stat Web Services to develop an interface to one or more of their in-house applications.

Authentication

The preferred authentication method for the Stat REST API is HTTP basic authentication (when using SSL).

The Stat Web client uses cookie-based authentication in the browser, so you can call REST from JavaScript on the page and rely on the authentication that the browser has established.

URI Structure

Stat REST APIs provide access to resources (data entities) via URI paths. To use a REST API, your application will make an HTTP request and parse the response. The Stat REST API uses the standard HTTP methods such as GET, PUT, POST and DELETE and uses JSON as its communication format. Refer to each API description below for a list of the HTTP methods available for that resource.

The URI format for Stat REST API resources has the following structure:

http://host:port/stat/api/resource-name

REST API Resources

The Stat REST API provides the following resources.

api/activityCodes 250
api/applications 251
api/assignedUsers 251
api/csrs 251
api/csrAttachments 253
api/csrDescriptions 253
api/csrResolutions 254
api/csrPriorities 254
api/csrTasks 254
api/csrLogs 256
api/csrTemplates 256

api/customers 257
api/customerPriorities 257
api/environments 257
api/projects 258
api/logTopics 258
api/serviceDomains 258
api/statUsers 259
api/csrTypes 259
api/csrQueues 259
api/csrStatuses 260
api/workflows 260
api/workflowTransfers 260
api/migrationApprovals 261
api/patchApprovals 261
api/PSupdatePwd 262
api/transferApprovals 262
api/csrArchiveSets 263
api/csrMigrations 263
api/csrMigrationObjects 263
api/csrMigrationPlannedSubmit 263
api/csrObjects 264
api/csr-object-save 264
api/lock-status-update 265
api/csr-objects/remove 266
api/csr-objects-reassign 267
api/csr-remove-archiveset/remove 268
api/csr-create-archiveset 269
api/archiveset-logs 270
api/csr-ready-to-migr-archiveset 271
api/archiveset-logs-export 272
api/archiveset-logs/remove 272
api/csr-archiveset/setDefMigrOrder 273
api/csr-archiveset/setMigrOrder 274
api/csr-add-objs-archiveset 275
api/archiveset-objs-export 276
api/csr-rearchive-objects 277
api/csr-objs-archiveset/remove 278
api/archiveset-objects-migration-flag 279
api/csr-copy-archiveset 280
api/csr-edit-archiveset 282
api/archiveset-download-objects 283
api/EBSupdateDbPwd 283
api/statRepoUpdatePwd 284

api/activityCodes

Provides access to the Stat Activity Codes.

Request

GET /api/activityCodes?sdCd=

GET /api/activityCodes/<Code ID>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of Activity Codes or a single Activity Code for a Service Domain
400	Invalid Service Domain or no access to the Service Domain
404	Activity Code not found

api/applications

Provides access to the Stat Activity Codes.

Request

GET /api/applications?sdCd=

GET /api/applications /<Code ID>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of Activity Codes or a single Application for a Service Domain
400	Invalid Service Domain or no access to the Service Domain
404	Application not found

api/assignedUsers

Provides access to the Stat Queue Assignments.

Request

GET /api/assignedUsers?sdCd=&queueId=

Responses

Response/Status Code	Description
200	application/json returns list of Queue Assignments for a Queue in a Service Domain
400	Invalid Service Domain or no access to the Service Domain

api/csrs

Provides access to CSRs by using the Service Domain, CSR Id, Tracking Number, or ALT Number.

Request

GET /api/csrs?sdCd=

GET /api/myCsrs?sdCd=

GET /api/csrs?sdCd=&altNumber=

GET /api/csrs?sdCd=&trackingNumber=

GET /api/csrs?sdCd=&csrId=

GET /api/csrs/<csr id>?sdCd=

To create or update a CSR:

POST /api/csrs?sdCd=

Example:

```
{
"applicationCode":"OAP",
"customerId":"102",
"typeCode":"NWF",
"workflowId":"0",
"statusCode":"Prop",
"groupId":"Dev",
"ownerId":"JDOE",
"priorityCode":"Urg",
"openedById":"JDOE",
"title":"CSR created by REST call",
"openDate":"2017-09-13T09:24:00",
"dueDate":"2017-09-13T09:24:00",
"closeDate":"1900-01-01T00:00:00",
"description":" sample description ",
"textDescription":" sample description ",
"resolution":"",
"textResolution":" ",
"projectCode":"PRG1",
"trackingNumber": "11",
"altNumber":"22"
}
```

To update a CSR:

PUT /api/csrs/<csrId>?sdCd=

Example:

```
{
"applicationCode":"OAP",
"customerId":"102",
"typeCode":"NWF",
"workflowId":"0",
"statusCode":"Prop",
"groupId":"Dev",
"ownerId":"JDOE",
"priorityCode":"Urg",
"openedById":"JDOE",
"title":"CSR created by REST call",
"openDate":"2017-09-13T09:24:00",
"dueDate":"2017-09-13T09:24:00",
"closeDate":"1900-01-01T00:00:00",
"description":" changed sample description ",
"textDescription":" changed sample description ",
"resolution":"",
"textResolution":" ",
"projectCode":"PRG1",
"trackingNumber": "11",
"altNumber":"22"
}
```

Responses

Response/Status Code	Description
200	application/json returns list of CSRs or a single CSR. CSR was updated successfully.
201	CSR Created
400	Any error encountered during creation/update

api/csrAttachments

Provides access to CSR Attachments by Service Domain and CSR ID.

Request

GET /api/csrAttachments?sdCd=&csrId=

GET /api/csrAttachments/<fileId>?sdCd=&csrId=

To create a CSR Attachment.

POST /api/csrAttachments

Example:

```
{
      "sdCd":"ORA",
      "csrId":"10079",
      "comments":"comments for attachment",
      "fileName":"soa.doc",
      "contentType":"application/msword"
}
parameter key for uploaded file: uploadedFile
```

To delete a CSR Attachment:

DELETE /api/csrAttachments/<file id>

Responses

Response/Status Code	Description
200	application/json returns list of CSR attachments or a single CSR attachment
201	CSR Attachment Created
204	CSR Attachment Deleted
400	Invalid Service Domain or no access to the Service Domain
404	Attachment not found

api/csrDescriptions

Provides access to the Stat CSR Description Templates by Service Domain. You may also pass Template ID as Application Code or as CSR Type to retrieve a specific Template.

Request

GET /api/csrDescriptions?sdCd=

GET /api/csrDescriptions?sdCd=&applicationCode=

GET /api/csrDescriptions?sdCd=&csrType=

Responses

Response/Status Code	Description
200	application/json returns list of Attachments for a Service Domain and CSR ID
400	Invalid Service Domain or no access to the Service Domain

api/csrResolutions

Provides access to the Stat CSR Resolution Templates by Service Domain. You may also pass the Template ID as Application Code or as CSR Type to retrieve a specific Template.

Request

GET /api/csrResolutions?sdCd=

GET /api/csrResolutions?sdCd=&applicationCode=

GET /api/csrResolutions?sdCd=&csrType=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Resolutions for a Service Domain
400	Invalid Service Domain or no access to the Service Domain

api/csrPriorities

Provides access to Stat CSR Priorities.

Request

GET /api/csrPriorities?sdCd=

GET /api/csrPriorities/<Priority ID>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Priorities or a CSR Priority for a Service Domain
400	Invalid Service Domain or no access to the Service Domain
404	CSR Priority not found

api/csrTasks

Provides access to CSR Tasks by Service Domain and CSR ID.

Request

GET /api/csrTasks?sdCd=&csrId=

GET /api/csrTasks/<activity seq>? sdCd=&csrId=

To create a CSR Task:

POST /api/csrTasks

Example:

```
{
    "sdCd":"ORA",
```

```
    "csrId":"10079",
    "activitySeq":"0",
    "activityCd":"Train",
    "activityDescr":"Training",
    "activitySrc":"User",
    "assignedUserid":"HOLMSTROM",
    "comments":"Obtain End-User approval(s) and document business decisions",
    "completeFlag":"N",
    "hrsAct":"0",
    "hrsEst":"1",
    "pctComplete":".20",
    "startDtString":"2018-01-30T13:48:10",
    "dueDtString":"2019-02-01T00:00:00",
    "taskTimes": " {\"TaskTimes\":[{\"TaskTime\":{\"hrsDt\":\"2019-01-30
    14:33:04.0\",\"hrsUserId\":\"DENSHCHIK\",\"hrsWorked\":1,\"comments\":\"less
    than one hour or so\",\"state\":1}}]} "
}
```

Valid taskTime states:

- 0 - unmodified
- 1 - new
- 3 - modified
- 4 - deleted

To update a CSR Task:

PUT /api/csrTasks/<activity seq>?sdCd=&csrId=

Example:

```
{
    "activityCd":"Train",
    "activityDescr":"Training",
    "activitySrc":"User",
    "assignedUserid":"HOLMSTROM",
    "comments":"Obtain End-User approval(s) and document business decisions",
    "completeFlag":"N",
    "hrsAct":"0",
    "hrsEst":"1",
    "pctComplete":".20",
    "startDtString":"2018-01-30T13:48:10",
    "dueDtString":"2019-02-01T00:00:00",
    "taskTimes": " {\"TaskTimes\":[{\"TaskTime\":{\"hrsDt\":\"2019-01-30
    14:33:04.0\",\"hrsUserId\":\"DENSHCHIK\",\"hrsWorked\":1,\"comments\":\"less
    than one hour or so\",\"state\":1}}]} "
}
```

To delete a CSR Task:

DELETE /api/csrTasks/<activity seq>?sdCd=&csrId=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Tasks or a single CSR Task
201	CSR Task Created
204	CSR Task Deleted
400	Invalid Service Domain or no access to the Service Domain

api/csrLogs

Provides access to CSR Logs by Service Domain and CSR ID.

Request

GET /api/csrLogs?sdCd=&csrId=

GET /api/csrLogs/<log id>? sdCd=&csrId=

To create a CSR Log:

POST /api/csrLogs

Example:

```
{
    "sdCd":"ORA",
    "csrId":"10079",
    "logSeq":"0",
    "logTopic":"Dev Topic",
    "confidentialFlag":"Y",
    "logPreview":"preview",
    "csrDetailInfo":"This is a log added from web services...."
}
```

To update a CSR Log:

PUT /api/csrLogs/<log id>?sdCd=&csrId=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Logs or a single CSR Log
201	CSR Log Created
400	Invalid Service Domain or no access to the Service Domain

api/csrTemplates

Provides access to the Stat CSR Templates.

Request

GET /api/csrTemplates?sdCd=

GET /api/csrTemplates/<Service Domain>

Responses

Response/Status Code	Description
200	application/json returns list of CSR Templates or a single CSR Template for a Service Domain
400	Invalid Service Domain or no access to the Service Domain

api/customers

Provides access to the Stat Customers.

Request

GET /api/customers

GET /api/customers/< customer id >

Responses

Response/Status Code	Description
200	application/json returns list of Customers or a single Customer
400	Any error encountered
404	Customer not found

api/customerPriorities

Provides access to Stat Customer Priorities where “Use Customer Prio” column on Service Domain is enabled.

Request

GET /api/customerPriorities?sdCd=

GET /api/customerPriorities/<Code ID>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of Customer Priorities or a single Customer Priority for a Service Domain
400	Invalid Service Domain or no access to the Service Domain
404	Customer Priority not found

api/environments

Provides access to the Stat Application Environment where the “Use Appl Env” column on the Service Domain is enabled.

Request

GET /api/environments?sdCd=

GET /api/environments?sdCd=&applicationCode=

GET /api/environments/<Environment Code>?sdCd=&applicationCode=

Responses

Response/Status Code	Description
200	application/json returns list of Environments or a single Environment for a Service Domain and Application Code

Response/Status Code	Description
400	Invalid Service Domain or no access to the Service Domain
404	Environment not found

api/projects

Provides access to Stat Projects or Projects for a Service Domain.

Request

GET /api/projects

GET /api/projects?sdCd=

GET /api/environments/<Project Code>

Responses

Response/Status Code	Description
200	application/json returns list of all Projects or list of Projects for a Service Domain
400	Error in Request
404	Projects not found

api/logTopics

Provides access to the Stat CSR Log Topics.

Request

GET /api/logTopics?sdCd=

GET /api/logTopics/<Code ID>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Log Topics or a single CSR Log Topic for a Service Domain
400	Invalid Service Domain or no access to the Service Domain
404	CSR Log Topic not found

api/serviceDomains

Provides access to the Stat Service Domains.

Request

GET /api/serviceDomains

GET /api/myServiceDomains

GET /api/serviceDomains/<Service Domain Code>

GET /api/myServiceDomains/<Service Domain Code>

Responses

Response/Status Code	Description
200	application/json returns list of Service Domains

Response/Status Code	Description
400	Bad request
404	Service Domain not found

api/statUsers

Provides access to Stat Users and a list of Users who have access to a Service Domain.

Request

GET /api/statUsers

GET /api/statUsers?sdCd=

GET /api/statUsers/<user Id>

Responses

Response/Status Code	Description
200	application/json returns list of Users
400	Bad request
404	User not found

api/csrTypes

Provides access to the Stat CSR Types.

Request

GET /api/csrTypes?sdCd=

GET /api/csrTypes/<Type Code>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Type Codes or a single CSR Type Code for a Service Domain
400	Invalid Service Domain or no access to the Service Domain
404	CSR Type Code not found

api/csrQueues

Provides access to the Stat CSR Queues.

Request

GET /api/csrQueues?sdCd=

GET /api/csrQueues?workflowId=(finds queues for starting status)

GET /api/csrQueues?workflowId=&csrStatus=(finds queues for a specific status)

GET /api/csrQueues /<queue Id>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Queues
400	Invalid Service Domain or no access to the Service Domain
404	CSR Queue not found

api/csrStatuses

Provides access to the Stat CSR Statuses.

Request

GET /api/csrStatuses?sdCd=&csrType

GET /api/csrStatuses?workflowId=(finds statuses for a workflow)

GET /api/csrQueues /<status Id>?sdCd=&csrType=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Statuses
400	Invalid Service Domain or no access to the Service Domain
404	CSR Status not found

api/workflows

Provides access to the Stat Workflows.

Request

GET /api/workflows?sdCd=

GET /api/workflows/<workflow Id>?sdCd=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Workflows
400	Invalid Service Domain or no access to the Service Domain
404	CSR Workflow not found

api/workflowTransfers

Provides access to the Stat Workflow Transfer. You can access the current Status of the Workflow and the list of available transfers (targetStatuses field) for a CSR. You can then pass the Object ID of the available transfer to the PUT request in order to perform the transfer.

Request

GET /api/workflowTransfers?sdCd=&csrId=

PUT /api/workflowTransfers/<object Id>?sdCd=&csrId=

Example:

```
{
"overrideComment":"override",
"resolution":"resolution",
"queueId":"Dev",
"userId":"DENSHCHIK"
}
```

Responses

Response/Status Code	Description
200	application/json returns list of CSR Workflow Transfers. Transfer was performed successfully.
400	Any errors encountered.
404	CSR Workflow not found

api/migrationApprovals

Provides access to the Stat Migration Approvals.

Request

GET /api/migrationApprovals?sdCd=&csrId

POST /api/migrationApprovals?sdCd=&csrId

Example:

```
{
      "status":"Approved",            -- > Approved, Rejected, Pending
      "archiveId":"3",
      "environment":"P851UDOR",
      "approverId":"JOE",
      "approverClass":"John Class",       --> "N/A", class
      "comments":"Done"
}
```

Responses

Response/Status Code	Description
200	application/json returns list of CSR Migration Approvals or a successful submission of approval
400	Any errors encountered.

api/patchApprovals

Provides access to the Stat Patch Approvals.

Request

GET /api/patchApprovals?sdCd=&csrId

POST /api/patchApprovals?sdCd=&csrId

Example:

```
{
      "status":"Approved",            -- > Approved, Rejected, Pending
      "applyId":"48",
      "objectId":"4281",
      "environment":"d12e_550_m",
      "approverId":"AA1222",
      "approverClass":"Developer",    --> "N/A", class
      "comments":"Done"
}
```

Responses

Response/Status Code	Description
200	application/json returns list of CSR Patch Approvals or a successful submission of approval
400	Any errors encountered.

api/PSupdatePwd

API to update PeopleSoft environment passwords.

Request

POST /api/PSupdatePwd

Example:

```
{
    "dbCd": "PT86PRD",
    "srvPwd": " [ENCRYPTED_SERVER_PASSWORD] ",
    "connectPwd": " [ENCRYPTED_CONNECT_PASSWORD] ",
    "dbPwd": " [ENCRYPTED_DB_PASSWORD] "

}
```

Responses

Response/Status Code	Description
200	When all correct inputs are passed and the response code is OK. (Password is successfully updated)
400	Request has corrupt data or has implemented faulty encryption
404	No rows get updated (probably because the dbCd was not found in STAT_PSDB_CONFIG table)
500	Some un-handled exception

api/transferApprovals

Provides access to the Stat Transfer Approvals.

Request

GET /api/transferApprovals?sdCd=&csrId

POST /api/transferApprovals?sdCd=&csrId

Example:

```
{
      "status":"Approved",            -- > Approved, Rejected, Pending
      "workflowId":"43",
      "workflowObjectId":"4",
      "approverType":"C",             --> Class, User, Queue
      "approverClass":"Dev",
      "approverId":"AA1222",
      "comments":"Done"
}
```

Responses

Response/Status Code	Description
200	application/json returns list of CSR Transfer Approvals or a successful submission of approval
400	Any errors encountered.

api/csrArchiveSets

Provides access to the Stat CSR Archive Sets.

Request

GET /api/csrArchiveSets?sdCd=&csrId=

GET /api/csrArchiveSets/<Archive ID>?sdCd=&csrId

Responses

Response/Status Code	Description
200	application/json returns list of Archive Set or a single Archive Set for a Service Domain and CSR ID
400	Invalid Service Domain or no access to the Service Domain
404	Archive Set not found

api/csrMigrations

Provides access to Stat CSR Migrations with any combination of the input parameters.

Request

GET /api/csrMigrations?sdCd=&processStatus=&migrId=&migratorId=&targetDb=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Migrations
400	Any errors encountered

api/csrMigrationObjects

Provides access to the Stat CSR Migration objects.

Request

GET /api/csrMigrationObjects?migrId=

Responses

Response/Status Code	Description
200	application/json returns list of CSR Migrations Objects
400	Any errors encountered
404	Migration not found

api/csrMigrationPlannedSubmit

Provides access to a Stat execution of a planned migration.

Request

PUT /api/csrMigrationPlannedSubmit/<migrId>

Responses

Response/Status Code	Description
200	application/json returns staus code of 0
400	Any errors encountered

api/csrObjects

Provides access to the Stat CSR Objects.

Request

GET /api/csrObjects?sdCd=&csrId=

Responses

Response/Status Code	Description
200	application/json returns list of objects in the CSR
400	Any errors encountered
404	CSR not found

api/csr-object-save

This API will be responsible to add new objects to a CSR.

Request

POST /api/csr-object-save?sdCd=<sdCd>&csrId=<csrId>&dbCode=<dbCode>

&objectType=<objectType>&objectClass=<objectClass>&envType=<envType>

&developer=<assignedDeveloper>&reserveIfLocked=<reserve if locked>

Example

```
{
"objectsToAdd" : [["ObjectColumn1Value", "ObjectColumn2Value", "ObjectColum3Value"]]
}
```

Responses

Response/Status Code	Description
200	Objects added
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
    "statusCode":  <Error Code>,
    "errorText": "<Error Message>"
```

```
}
```

Scenario	Message	Response code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. User doesn’t at least one of these rights : <RIGHT_LIST>	-5
CSR is locked by someone else	CSR is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Trying to create a final archive set in a CSR which already has a final archive set.	Final archive set is already present. Can't add more final archive sets	-10
When the user chooses a dev environment for archive sets creation and also when the user has a file object in the list of objects that they want to archive, but they haven’t picked a “files from“ value	You must select Environment, VCM or working in filesFrom field	-11
When the archive set has no objects to add	No objects added in archive set.	-12
When user is trying to add a final archive set, however the final archive set doesn’t contain all CSR belonging to the chosen environment.	A final archive set must contain all CSR objects of the selected environment.	-13

api/lock-status-update

Change the lock status of single or multiple objects.

Request

POST /api/lock-status-update?csrId=<csrId>&sdCd=<sdCd>

Example

```
{
      "lockAction": 1,
      "objList": [
            {
            "objId": 2020,
            "dbCd": "P857UP17"
            }
      ]
}
}
```

Responses

Response/Status Code	Description
200	Lock status changed
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. <user> doesn’t have the rights to perform the following operation	-5
CSR is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Assigned developer doesn't have access to that object	Assigned developer does not have access to the selected object type	-7
When another process is running in that CSR	Objects in process so You can't perform following action	-8

api/csr-objects/remove

When this API is called, these objects will be removed from the CSR and all archive sets. The removal of the objects from the archive sets will be asynchronous.

Request

DELETE /api/csr-objects/remove?csrId=<csrId>&sdCd=<sdCd>

Example

```
{
"objList":
[
   {
            "objId": 2028,
            "dbCd": "PS857DEV"
```

```
    }
]
}
```

Responses

Response/Status Code	Description
200	Lock status changed
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. <user> doesn’t have the rights to perform the following operation	-5
CSR is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Assigned developer doesn't have access to that object	Assigned developer does not have access to the selected object type	-7
When another process is running in that CSR	Objects in process so You can't perform following action	-8

api/csr-objects-reassign

With this API you can add objects of another CSR in your current CSR.

Request

POST /api/csr-objects-reassign?csrId=<csrId>&sdCd=<sdCd>&reserveIfLocked=<reserveIfLocked>&lockOption=<lockOption>&developer=<developer>&dbCode=<dbCode>

Example

```
{
    "sourceCsr": {
        "csrId": 1,
        "sdCd": "Dm1"
```

```
    },
"objIds": [
        2020,
        2021
]
}
```

Responses

Response/Status Code	Description
200	Objects reassigned. Look out for partial failure scenarios which can happen when only some of the objects have been assigned successfully
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. <user> doesn’t have the rights to perform the following operation	-5
CSR is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Assigned developer doesn't have access to that object	Assigned developer does not have access to the selected object type	-7
When another process is running in that CSR	Objects in process so You can't perform following action	-8

api/csr-remove-archiveset/remove

Remove archive sets from your CSR.

Request

DELETE /api/csr-remove-archiveset/remove?csrId=<csrId>&sdCd=<sdCd>&swatId=<swatId>&module=<module>

Responses

Response/Status Code	Description
200	Objects reassigned. Look out for partial failure scenarios which can happen when only some of the objects have been assigned successfully
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. <user> doesn’t have the rights to perform the following operation	-5
CSR is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9

api/csr-create-archiveset

Creates archive sets in your CSR.

Request

POST /api/csr-create-archiveset?sdCd=<sdCd>&csrId=<csrId>

Example

```
{
      "environment":<Environment>,
      "archiveType":<ArchiveType>,
      "shortDescr":<ShortDescr>,
      "comments":<Comments>,
      "filesFrom":<FileFromWork>,
      "releaseDesc":<ReleaseName>,
      "vcmOption": <VcmOption>,
      "objects":[id1, id2, id3]
```

```
}
```

Responses

Response/Status Code	Description
200	Archive set created
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. <user> doesn’t have the rights to perform the following operation	-5
CSR is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
When the archive set has no objects to add	No objects added in archive set.	-12
When user is trying to add a final archive set, however the final archive set doesn’t contain all CSR belonging to the chosen environment.	A final archive set must contain all CSR objects of the selected environment.	-13

api/archiveset-logs

This API is responsible to fetch all the logs of archive set.

Request

GET /api/archiveset-logs?sdCd=<service_domain>&csrId=<CSR_Id>&swatId=<swat_id>

Responses

Response/Status Code	Description
200	Archive set logs fetched
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Wrong Archive ID provided	Invalid archive set id. Make sure archive is not deleted	-9
User is trying to access a CSR to which they don't have read access	You do not have access to perform read operations on this CSR.	-31

api/csr-ready-to-migr-archiveset

This API will be responsible to enable or disable the ready to migrate flag of archive set.

Request

POST /api/csr-ready-to-migr-archiveset?sdCd=<sdCd>&csrId=<csrId>

&swatId=<swatId>&migrFlag=<migrFlag>

Responses

Response/Status Code	Description
200	"Ready to migrate" flag changed
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4

Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
Approvals are present	This action is not allowed. There are approvals present.	-14
Trying to change the ready to migrate flag to its current value.	A final archive set must contain all CSR objects of the selected environment.	-16

api/archiveset-logs-export

Downloads the archive set logs in TEXT/PLAIN format.

Request

GET /stat/api/archiveset-logs-export?sdCd=<sdCd>&csrId=<csrId>&swatId=<archiveSetId>

Responses

Response/Status Code	Description
200	Logs will be downloaded.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3

api/archiveset-logs/remove

Delete/Clear archive set logs.

Request

DELETE /api/archiveset-logs/remove?sdCd=<sdCd>&csrId=<csrId>

&swatId=<swatId>

Responses

Response/Status Code	Description
200	Logs will be cleared.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode": <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9

api/csr-archiveset/setDefMigrOrder

Changes the migration order of objects to default migration order.

Request

POST /api/csr-archiveset/setDefMigrOrder?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

Example

```
[
      {
      "statusCode": 1,
      "objectId": <objectId>,
      "migrationOrder": <migrationOrder>,
      "message": null
      }
]
```

Responses

Response/Status Code	Description
200	Archive set object's migration order will be changed to default migration order. Look out for partial failure scenarios where the API worked for only some of the objects.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
User doesn't have the rights to do the specific operation	Access denied. User doesn't at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	CSR is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
Invalid Obj Id provided	One or more object Ids is invalid.	-18

api/csr-archiveset/setMigrOrder

Set migration order of archive set objects.

Request

PATCH /api/csr-archiveset/setMigrOrder?sdCd=<sdCd>&

csrId=<csrId>&swatId=<swatId>

Example

```
{
  "request": [
{
   "objId": <objId>,
"migrOrder": <migrOrder>
},
   {
```

```
   "objId": <objId>,
"migrOrder": <migrOrder>
   }
]
}
```

Responses

Response/Status Code	Description
200	Archive set object's migration order will be changed to the requested migration order. Look out for partial failure scenarios where the API worked for only some of the objects.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn't have the rights to do the specific operation	Access denied. User doesn't at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
Invalid object ID provided	One or more object Ids is invalid.	-18

api/csr-add-objs-archiveset

Add Objects in Archive Set .

Request

POST /api/csr-add-objs-archiveset?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

Example

```
{
   "syncPsObjFlag": <syncPsObjFlag>,
   "objIds": [<objId1>, <objId2>]
```

}

Responses

Response/Status Code	Description
200	Archive set objects will be added. Look out for partial failure scenarios where the API worked for only some of the objects.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. User doesn’t at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
Invalid object ID provided	One of the object IDS is either invalid or the user doesn't have permission to its object type.	-18

api/archiveset-objs-export

Export the list of archive set objects in plain text format.

Request

GET /stat/api/archiveset-objs-export?sdCd=<sdCd>&csrId=<csrId>&swatId=<archiveSetId>

Responses

Response/Status Code	Description
200	Exported list of archive set objects as a txt file
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9

api/csr-rearchive-objects

Re-archive those objects which are eligible to re-archive the objects.

Request

POST /api/csr-rearchive-objects?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

Example

```
{
"objIds": [<objId1>,<objId2>]
}
```

Responses

Response/Status Code	Description
200	Archive set objects will be added. Look out for partial failure scenarios where the API worked for only some of the objects.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4

User doesn’t have the rights to do the specific operation	Access denied. User doesn’t at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
Invalid object ID provided	One of the object IDS is either invalid or the user doesn't have permission to its object type.	-18
If archive set type is base and objects has not been locked.	One or more of the selected objects are not locked in this CSR.	-22
Objects need to honor either of these conditions to be fit for re-archival • Archive status should be Archive/Warn or Archive/Error • Already archived object’s are only eligible if its a base archive set.	This object is unfit for Re-archive object operation.	-23

api/csr-objs-archiveset/remove

Delete archive set objects

Request

DELETE /api/csr-objs-archiveset/remove?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

Example

```
{
   "objIds": [<objId1>,<objId2>]
}
```

Responses

Response/Status Code	Description
200	Archive set objects will be deleted. Look out for partial failure scenarios where the API worked for only some of the objects.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. User doesn’t at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
Invalid object ID provided	One of the object IDS is either invalid or the user doesn't have permission to its object type.	-18
If archive set’s type is base or final	Base archive set error message: Objects for a baseline Archive Set are managed dynamically. You cannot manually remove objects. Final archive set error message: Objects for a final Archive Set are managed dynamically. You cannot manually remove objects.	-21

api/archiveset-objects-migration-flag

Modify the action and upgrade values for eligible archive set objects.

Request

PATCH api/archiveset-objects-migration-flag?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

Example

```
{
    "request": [
        {
        "objectId" : 2,
        "action" : "delete",
        "upgrade" : "N"
        },
    ]
}
```

Responses

Response/Status Code	Description
200	Archive set objects' migration flag will be updated. Look out for partial failure scenarios where the API worked for only some of the objects.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn't have the rights to do the specific operation	Access denied. User doesn't at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
Invalid object ID provided	One or more object Ids is invalid.	-18
User is trying to update the migration flag for those objects which are not eligible	This object is unfit for archive set objects migration flags modification	-27
If user has provided CopyProp action value but it doesn't fit with that object	This object doesn't fit for CopyProp action	-28

api/csr-copy-archiveset

Copy an existing archive set .

Request

POST api/csr-copy-archiveset?sdCd=<sdCd>&csrId=<csrId>&sourceSwatId=<source Swat Id>

Example

```
{
      "environment":<Environment>,
      "archiveType":<ArchiveType>,
      "shortDescr":<ShortDescr>,
      "comments":<Comments>,
```

```
    "filesFrom":<filesFrom>,
    "releaseDesc":<releaseDesc>,
    "vcmOption": <VcmOption>,
    "syncPsObjFlag": <syncPsObjFlag>
}
```

Responses

Response/Status Code	Description
200	Archive set will be copied.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
    "statusCode":  <Error Code>,
    "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. User doesn’t at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6
Trying to create a final archive set in a CSR which already has a final archive set.	Final archive set is already present. Can't add more final archive sets	-10
When the user chooses a dev environment for archive sets creation and also when the user has a file object in the list of objects that they want to archive, but they haven’t picked a “files from“ value	You must select Environment, VCM or working in filesFrom field	-11
When the archive set has no objects to add	No objects added in archive set.	-12
When user is trying to add a final archive set, however the final archive set doesn’t contain all CSR belonging to the chosen environment.	A final archive set must contain all CSR objects of the selected environment.	-13

api/csr-edit-archiveset

Edit an existing archive set details.

Request

PATCH /api/csr-edit-archiveset?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

Example

```
{
      "shortDescr": {
      "value": <short description>
},
      "comments": {
      "value": <short description>
},
      "releaseDesc": {
      "value": <short description>
}
}
```

Responses

Response/Status Code	Description
200	Archive set details will be updated.
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode":  <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can’t be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Value not allowed	<Parameter_Name> value is invalid	-4
User doesn’t have the rights to do the specific operation	Access denied. User doesn’t at least one of these rights : <RIGHT_LIST>	-5
Csr is locked by someone else	Csr is locked by {LOCKED_BY_USER_ID}. User can't perform the following operation	-6

Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
If User doesn't provide value for shortDescr, comments or releaseDesc	At least one of the value is required	-26

api/archiveset-download-objects

Edit an existing archive set details.

Request

GET /stat/api/archiveset-download-objects?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

&objectId=<objectId> PATCH /api/csr-edit-archiveset?sdCd=<sdCd>&csrId=<csrId>&swatId=<swatId>

Responses

Response/Status Code	Description
200	Archive set object will be downloaded
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
      "statusCode": <Error Code>,
      "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
Compulsory parameter missing	<Parameter_Name> value Can't be null or empty	-2
Wrong CSR, Service domain value provided	Provided value for csrId or sdCd is invalid	-3
Invalid archive set ID provided	Invalid archive set id. Make sure archive is not deleted	-9
User is trying to download non archived or not eligible object	This object is unfit to download	-29

api/EBSupdateDbPwd

API to update STAT repository password (reference KB - 4280263).

Request

POST /api/EBSupdateDbPwd

Example

```
{
  "dbCd": "EBS_DEV",
  "srvPwd": " [ENCRYPTED_SERVER_PASSWORD] ",
```

```
"connectPwd": " [ENCRYPTED_CONNECT_PASSWORD] ",
"dbPwd": " [ENCRYPTED_DB_PASSWORD] "
}
```

Responses

Response/Status Code	Description
200	When all correct inputs are passed and the response code is OK. (Password is successfully updated)
400	Request has corrupt data or has implemented faulty encryption
404	No rows get updated (probably because the dbCd was not found in STAT_PSDB_CONFIG table)
500	Some un-handled exception

api/statRepoUpdatePwd

API to update STAT repository password (reference KB - 4280263).

Request

POST /api/statRepoUpdatePwd

Example

```
{
"currentPwd":"[ENCRYPTED_CURRENT_PASSWORD]",
"newPwd":"[ENCRYPTED_NEW_PASSWORD]"
}
```

Responses

Response/Status Code	Description
200	When all correct inputs are passed and the response code is OK. (Password is successfully updated)
400	Any errors encountered. Probably due to incorrect user input
500	Some unhandled exception

Error Handling

Example error response body

```
{
    "statusCode": <Error Code>,
    "errorText": "<Error Message>"
}
```

Scenario	Message	Error code
When any one or both password is null.	Current or New password should not be null	400
When current password is not correct.	Invalid Current Password	400

When current and new password both are same	Current and New Password should not be same	400
When user doesn’t have the rights to update the STAT password.	User doesn't have the rights to change the password of STAT database	400
Any other error which hasn’t been handled specifically by the SCA.	<Specific runtime exception>	500
When config.update.allowIPlist property is not set or is empty or IP address not motioned in stat-config.properties file, then access will be denied.	"Access denied."	200

H

Appendix: SOAP-Based Web Services API

Stat provides programmatic access to CSR information via a Web Service API.

The Stat Web Services are available when the Stat Central Agent is live.

API calls represent specific operations that your client applications can use to retrieve or update data, such as:

- Query the data in your Stat repository that is required to create or update a CSR.
- Add a CSR
- Add or delete attachments to/from a CSR
- Query a CSR
- Update a CSR

The following information is intended for developers and system administrators who want to use Stat Web Services to develop an interface to one or more of their in house applications, specifically for managing CSRs.

NOTE: Stat Web Services have been tested for Microsoft .NET Framework (2.0 or higher) and Java (JDK 1.5 or higher) development environments. They have not been validated on any other development environments.

Stat Web Services are implemented using the JAX-WS 2.0 technology available in JBoss application servers. When developing the interface for Web Services, the Top-Down approach (also known as WSDL-first approach) is used. All WSDL files are created using the Document/Literal Wrapped strategy.

NOTE: Sample code for Stat Web Services APIs is available on the Stat installation media under the folder web_services_sample.

Users accessing Stat through Web Services must establish a valid connection. The Stat Central Agent maintains a list of valid connections, which are refreshed each time a user makes a call to any service. The user should close the connection after making all the desired service calls. If a connection is left open longer than a specified period of time, the Stat Central Agent automatically closes the connection and the user will have to establish a new connection for any future service calls. The default session timeout value is set for 30 seconds (30000) in the System Maintenance window. For more information, see Parameters Tab on page 51.

Services and Exposed Methods

This section documents the Login Service, CSR Service, and Approval Service and their exposed Methods.

Login Service

The URL for the wsdl file of this service is located at:

http://hostname:port/stat/WSLoginService?wsdl

long connect(String userId, String password) throws WSLoginFault;

User has to establish a valid connection in order to interact with Stat through Web Services. Connections are validated the same way a normal login into the Web Client is validated. Upon successful connection, a valid Connect ID is returned to the user, which will be used in subsequent method calls to validate user's connection. Also proper rows are written into CONNECTION_MGMT and CONNECT_HIST tables. A list of valid connections is stored on the server and the connection is refreshed each time a valid Web Service Method is executed. This connection will have to be either closed by User or it will expire after a time-out period.

void disconnect(long connectId);

This method terminates an established connection through Web Services.

CSR Service

The URL for the wsdl file of this service is located at: http://hostname:port/stat/WSCsrService?wsdl

Save a New CSR

The server throws an exception if user does not have Add CSR or Add Attachment rights or if any of the fields in the csr bean is invalid.

Method	long saveNewCSR(long connectId, CSRType csr, List<AttachmentType> attachments) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • csr - A bean representing all the values in a CSR. (See Class Definitions, part 3 for CSRType definition) • attachments - List of attachments. For more information, see AttachmentType Bean on page 298.
Return Parameter	A long value representing the CSR Id of the new csr is returned.

Retrieve the Content of a CSR from Stat

Method	CSRType retrieveCSR(long connectId, String sdcd, long csrId) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	A csr bean representing the retrieved csr is returned. For more information, see CSRType Bean on page 298.

Update an Existing CSR in Stat

The csr parameter bean will contain all the original values in the CSR in addition to the updated values.

The server throws an exception in the following circumstances:

- In the case of an invalid service domain, or CSR Id parameters.
- If another user has the lock on the CSR.

- If user has restriction to the Application.
- If the CSR is in a Closed Status and user does not have proper rights.
- If the CSR is assigned to another user and the current user does not have proper override rights.
- If the user does not have change rights to any of the fields in CSR.
- If any of the values in CSR are invalid.
- If the CSR has objects and user is attempting to change to an Application that results in a change of Module.
- If the CSR has objects and user is attempting to change to a CSR Type that invalidates the current Workflow.
- If the CSR has objects and user is attempting to change to a Workflow that invalidates the current migration path.

Before updating the CSR, a row is inserted into CSR_LOCK_STATUS and is removed after the update.

CSR History records are inserted for the updated fields.

Method	void updateCSR(long connectId, CSRType csr) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • csr - A csr bean representing the retrieved csr is returned. For more information, see CSRType Bean on page 298.

Retrieve a CSR by Tracking Number

Query Stat for the CSR based on the Tracking Number field.

Method	List<CSRType> retrieveCSRByColumn(connectId, columnName, columnValue)
Input Parameters	• connectId - a valid connection Id • columnName - valid values are TRACKING_NUMBER and ALTERNATE_NUMBER • columnValue - the value you are searching for
Return Parameter	List of CSRType records

Retrieve a List of Active Service Domains

Method	List<RecordType> getServiceDomainList(long connectId) throws WSCsrFault;
Input Parameters	connectId - A valid connect Id obtained by calling WSLoginService.connect
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Service Domains the Current User Can Access

The connectId parameter has the information about the current user.

The server throws an exception in case of an empty return list.

Method	List<RecordType> getServiceDomainForUserList(long connectId) throws WSCsrFault;
Input Parameters	connectId - A valid connect Id obtained by calling WSLoginService.connect
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Customers

The server throws an exception in case of an empty return list.

Method	List<RecordType> getCustomerList(long connectId) throws WSCsrFault;
Input Parameters	connectId - A valid connect Id obtained by calling WSLoginService.connect
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Projects for a Specific Service Domain

The server throws an exception in case of an invalid service domain parameter.

The server throws an exception in case of an empty return list.

Method	List<RecordType> getProjectList(long connectId, String sdcd) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Users for a Specific Service Domain

The server throws an exception in case of an invalid service domain parameter.

The server throws an exception in case of an empty return list.

Method	List<RecordType> getOpenedByList(long connectId, String sdcd) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Customer Priorities for a Specific Service Domain

The server throws an exception in case of an invalid service domain Parameter.

The server throws an exception in case of an empty return list.

The server throws an exception if Customer Priority is disabled at the service domain level.

Method	List<RecordType> getCustomerPriorityList(long connectId, String sdcd) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Applications for a Specific Service Domain

The server throws an exception in case of an invalid service domain parameter or an empty return list.

This method verifies any possible restricted access to applications for current user.

Method	List<RecordType> getApplicationList(long connectId, String sdcd) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Environments for a Specific Service Domain and Application

The server throws an exception in case of an invalid service domain or Application Code parameters or in case of an empty return list.

The server throws an exception if Application Environment is disabled at the service domain level.

Method	List<RecordType> getEnvironmentList(long connectId, String sdcd, String applicationCode) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • ApplicationCode - Application Code
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active CSR Types for a Specific Service Domain

The server throws an exception in case of an invalid service domain parameter or an empty return list.

Method	List<RecordType> getCSRTypeList(long connectId, String sdcd) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Priorities for a Specific Service Domain

The server throws an exception in case of an invalid service domain parameter or an empty return list.

Method	List<RecordType> getPriorityList(long connectId, String sdcd) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Users for a Queue in a Specific Service Domain

The server throws an exception in case of an invalid service domain or Queue Id parameters or in case of an empty return list.

Method	List<RecordType> getAssignedToList(long connectId, String sdcd, String queueId) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • queueId - Queue Id
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Workflows for an Application Code and a CSR

Type in a specific service domain.

The server throws an exception in case of an invalid service domain, Application Code or CSR Type Code parameters.

The server throws an exception in case of an empty return list.

Method	List<RecordType> getWorkflowList(long connectId, String sdcd, String applicationCode, String typeCode) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • applicationCode - Application Code • typeCode - CSR Type Code
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Status Records for a Workflow Id in a Specific Service Domain

If Workflow Id is a null value, a list of all Status records for the passed CSR Type is returned.

The server throws an exception in case of an invalid service domain, CSR Type Code, or Workflow Id parameters.

The server throws an exception in case of an empty return list.

Method	List<RecordType> getStatusList(long connectId, String sdcd, String typeCode, String workflowId) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • typeCode - CSR Type Code • workflowId - Workflow Id
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Retrieve a List of Active Queue Assignments for a Specific Service Domain.

If workflowId and statusCode are also passed, the method returns selected Queue Assignments on the particular Status of the passed Workflow.

If workflowId and statusCode are null values, the method returns all the Queue Assignments for the passwd service domain.

The server throws an exception in case of an invalid service domain, Workflow Id or Status Code parameters.

The server throws an exception in case of an empty return list.

Method	List<RecordType> getQueueList(long connectId, String sdcd, String workflowId, StatusCode) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • workflowId - Workflow Id • statusCode - Status Code
Return Parameter	List of values. For more information, see RecordType Bean on page 297.

Add attachments to an Existing CSR in Stat

The server throws an exception in the following circumstances:

- In the case of an invalid service domain, or CSR Id parameters.
- If another user has the lock on the CSR.
- If the user has restrictions to the Application.
- If the CSR is in a Closed Status and user does not have proper rights.
- If the CSR is assigned to another user and the current user does not have proper override rights.
- If the user does not have proper right to add Attachments.
- If the attachment list is empty.

Before updating the CSR, a row is inserted into CSR_LOCK_STATUS and is removed after the update.

CSR History records are inserted for added attachments.

Method	void addCSRAttachments(long connectId, String sdcd, long csrId, List<AttachmentType> attachments) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id • attachments - List of attachments. For more information, see AttachmentType Bean on page 298.

Delete attachments from an Existing CSR in Stat.

File Ids may be retrieved by calling the retreiveCSRAttachments method.

The server throws an exception in the following circumstances:

- In the case of an invalid service domain, or CSR Id parameters.
- If another user has the lock on the CSR.
- If the user has restrictions to the Application.
- If the CSR is in a Closed Status and user does not have proper rights.
- If the CSR is assigned to another user and the current user does not have proper override rights.
- If the user does not have proper right to delete Attachments.
- If the attachment list is empty.

Before updating the CSR, a row is inserted into CSR_LOCK_STATUS and is removed after the update.

CSR History records are inserted for deleted attachments.

Method	void deleteCSRAttachments(long connectId, String sdcd, long csrId, List<Long> fileIds) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id • fields - List of file Ids for attachments.

Retrieve a List of Attachments in a CSR

If there are no attachments in the CSR, a null value is returned. For more information, see AttachmentType Bean on page 298.

Method	List<AttachmentType> retrieveCSRAttachments(long connectId, String sdcd, long csrId) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	A list of attachments for the csr is returned. For a definition of AttachmentType refer to Class Definitions, part 2.

Retrieve any possible CSR Template Values for the Current User

If there are no CSR Template values, a null Object is returned.

Method	CSRType getCSRTemplateValues(long connectId, String sdcd) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	A csr bean representing the retrieved csr is returned. For more information, see CSRType Bean on page 298.

Retrieve any Possible Description Template for a Specific Application Code

If there are no Templates present, a null String is returned.

Method	String getApplicationDescriptionTemplate(long connectId, String sdcd, String code) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • code - Application Code
Return Parameter	A string of template is returned.

Retrieve any Possible Resolution Template for a Specific Application Code.

If there are no Templates present, a null String is returned.

Method	String getApplicationResolutionTemplate(long connectId, String sdcd, String code) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • code - Application Code
Return Parameter	A string of template is returned.

Retrieves any Possible Description Template for a Specific CSR Type Code

If there are no Templates present, a null String is returned.

Method	String getCSRTypeDescriptionTemplate(long connectId, String sdcd, String code) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • code - Application Code
Return Parameter	A string of template is returned.

Retrieve any Possible Resolution Template for a Specific CSR Type Code

If there are no Templates present, a null String will be returned.

Method	String getCSRTypeResolutionTemplate(long connectId, String sdcd, String code) throws WSCsrFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • code - Application Code
Return Parameter	A string of Resolution template is returned.

Add or Update a Log on a CSR

Method	List<CSRLogType> updateCSRLogs(long connectId, String sdcd, long csrId, CSRLogType detailLog)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id **NOTE:** This method is called for adding a new CSRlogs and updating an existing CSRlog. When adding a new CSRlog, logSequence of the CSRLogType record is zero. When updating an existing CSRlog, logSequence of the CSRLogType record is not zero. For more information, see CSRLogType Bean on page 298.

Retrieve the Logs for a CSR

Method	List<CSRLogType>retrieveCSRLogs(connectId, sdcd, csrId)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	List of CSR logs

Retrieve a Log record by sequence ID for a CSR

Method	List<CSRLogType>retrieveCSRLog(connectId, sdcd, csrId)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id • seqId - sequence Id
Return Parameter	A single CSR log record

Retrieve a List of CSR Log Topics for a Service Domain

Method	List<string>retrieveLogTopicList(connectId, sdcd)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain
Return Parameter	List of CSR log topics for a service domain

Retrieve the Tasks (including times) for a CSR

Method	List<CSRTaskType>retrieveCSRTasks(connectId, sdcd, csrId)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	List of CSR tasks and times. For more information, see CSRTaskType Bean on page 298.

Add or Update a Task on a CSR

Method	void updateCSRTasks(long connectId, String sdcd, long csrId, CSRTaskType taskType)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	**NOTE:** This method is called for adding a new task and updating an existing task. When adding a new task, activitySeq of the CSRTaskType record is zero. When updating an existing task, activitySeq of the CSRTaskType record is not zero. The list of tasks should always be retrieved first before making any changes to the task or time records. CSRTimeType records have state field with the following values: Zero means unmodified, one means new, three means modified, 4 means deleted. For more information, see CSRType Bean on page 298.

Retrieve the list of Status available for Transfer for a CSR

Method	CSRWorkflowType retrieveWorkflowStatusList(connectId, sdcd, csrId)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId – CSR Id
Return Parameter	List of available status based on the current state of the workflow in the CSR. The actual list can be accessed by calling the getTargetStatuses () method of CSRWorkflowType bean. For more information, see CSRType Bean on page 298.

Transfer the Status in Workflow

Method	void transferToStatus(connectId, sdcd, csrId, overrideComment, resolution, workflow, targetStatus)
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId – CSR Id • overrideComment – required comment in case of an override transfer • resoluiton – required resolution if needed • CSRWorkflowType – current workflow in the CSR • CSRWorkflowStatusType – target status that the workflow is being transferred to
Return Parameter	**NOTE:** If status does not need Queue and User, pass the status (CSRWorkflowStatusType) without any Queues. If status needs a Queue and User, add the target Queue to the status, and pass the status. In all cases, if you are overriding the transfer, pass a comment. For more information, see CSRWorkflowType Bean, CSRWorkflowStatusType Bean, CSRWorkflowStatusQueueType Bean, and CSRWorkflowStatusQueueMemberType Bean on page 300.

Approval Service

The URL for the wsdl file of this service is located at: http://hostname:port/stat/WSApprovalService?wsdl

Retrieve a List of all Transfer Approvals for CSRs that are Not Closed

Method	List<TransferApprovalType> getTransferApprovalList(long connectId) throws WSApprovalFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	List of all Transfer Approvals for CSRs that are not closed

Retrieve a List of all Transfer Approvals for a CSR

Method	List<TransferApprovalType> getTransferApprovalForCsrList(long connectId, String sdcd, long csrId) throws WSApprovalFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	List of all Transfer Approvals for a CSR

Retrieve a List of all Transfer Approvals for a CSR with Specific Status Code From to Status Code To

Method	List<TransferApprovalType> getTransferApprovalForCsrByStatusList(long connectId, String sdcd, long csrId, String statusCodeFrom, String statusCodeTo) throws WSApprovalFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id • statusCodeFrom - CSR status code • statusCodeTo - CSR status code
Return Parameter	List of all Transfer Approvals for a CSR with specific status code From to status code To

Change the Status of a Single Transfer Approval Record

NOTE: Valid values for TransferApprovalType.status are Approved, Rejected, Pending. Valid values for TransferApprovalType.approverType are Class, User, Queue.

Method	void submitTransferApproval(long connectId, TransferApprovalType approval) throws WSApprovalFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • TransferApprovalType approval - Transfer approval type

Retrieve a List of all Migration Approvals for CSRs that are Not Closed

Method	List<MigrationApprovalType> getMigrationApprovalList(long connectId) throws WSApprovalFault;
Input Parameters	connectId - A valid connect Id obtained by calling WSLoginService.connect
Return Parameter	List of all Migration Approvals for CSRs that are not closed

Retrieve a List of all Migration Approvals for a CSR

Method	List<MigrationApprovalType> getMigrationApprovalForCsrList(long connectId, String sdcd, long csrId) throws WSApprovalFault
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	List of all Migration Approvals for a CSR

Change the Status of a Single Migration Approval Record

NOTE: Valid values for MigrationApprovalType.status are Approved, Rejected, Pending.

Method	void submitMigrationApproval(long connectId, MigrationApprovalType approval) throws WSApprovalFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • MigrationApprovalType approval - Transfer approval type

Retrieve a List of all Patch Approvals for CSRs that are Not Closed

Method	List<PatchApprovalType> getPatchApprovalList(long connectId) throws WSApprovalFault;
Input Parameters	connectId - A valid connect Id obtained by calling WSLoginService.connect
Return Parameter	List of all Patch Approvals for CSRs that are not closed

Retrieve a List of all Patch Approvals for a CSR

Method	List<PatchApprovalType> getPatchApprovalForCsrList(long connectId, String sdcd, long csrId) throws WSApprovalFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • sdcd - service domain • csrId - CSR Id
Return Parameter	List of all Patch Approvals for a CSR

Change the Status of a Single Patch Approval Record

NOTE: Valid values for PatchApprovalType.status are Approved, Rejected, Pending.

Method	public void submitPatchApproval(long connectId, PatchApprovalType approval) throws WSApprovalFault;
Input Parameters	• connectId - A valid connect Id obtained by calling WSLoginService.connect • PatchApprovalType approval - Transfer approval type

Class Definitions

RecordType Bean

```
public class RecordType {
 protected String code;
 protected String description;
}
```

AttachmentType Bean

```
public class AttachmentType {
    protected String filename;
    protected String contentType;
    protected String comments;
    protected DataHandler content;
}
```

CSRType Bean

```
public class CSRType {
    protected String sdcd;
    protected long csrId;
    protected String applicationCode;
    protected String environmentCode;
    protected String customerId;
    protected String csrTypeCode;
    protected String workflowId;
    protected String statusCode;
    protected String queueId;
    protected String assignedToId;
    protected String priorityCode;
    protected String openedById;
    protected String title;
    protected XMLGregorianCalendar openDate;
    protected XMLGregorianCalendar dueDate;
    protected XMLGregorianCalendar closeDate;
    protected String description;
    protected String textDescription;
    protected String resolution;
    protected String textResolution;
    protected String projectCode;
    protected String customerPriorityCode;
    protected String trackingNumber;
    protected String altNumber;
}
```

CSRLogType Bean

```
public class CSRTimeType {
    protected String sdcd;
    protected long csrId;
    protected long activitySeq;
    protected XMLGregorianCalendar hrsDt;
    protected String hrsUserId;
    protected double hrsWorked;
    protected String comments;
    protected XMLGregorianCalendar updateDt;
    protected String updateUserid;
    protected int state;}
```

CSRTaskType Bean

```
public class CSRTaskType {
```

```
    protected String sdcd;
    protected long csrId;
    protected long activitySeq;
    protected double pctComplete;
    protected String activityCd;
    protected String activitySrc;
    protected String activityDescr;
    protected String assignedUserid;
    protected String comments;
    protected XMLGregorianCalendar completeDt;
    protected String completeFlag;
    protected XMLGregorianCalendar dueDt;
    protected double hrsAct;
    protected double hrsEst;
    protected XMLGregorianCalendar startDt;
    protected XMLGregorianCalendar updateDt;
    protected String updateUserid;
    protected List<CSRTimeType> timeEntries;
}
```

CSRTimeType Bean

```
public class CSRTimeType {
    protected String sdcd;
    protected long csrId;
    protected long activitySeq;
    protected XMLGregorianCalendar hrsDt;
    protected String hrsUserId;
    protected double hrsWorked;
    protected String comments;
    protected XMLGregorianCalendar updateDt;
    protected String updateUserid;
    protected int state;
}
```

CSRWorkflowType Bean

```
public class CSRWorkflowType {
    protected String overrideComment;
    protected boolean hasChangeCSRStatusRight;
    protected boolean hasTransferOverrideRight;
    protected boolean resolutionEntered;
    protected List<CSRWorkflowStatusType> targetStatuses;
}
```

CSRWorkflowStatusType Bean

```
public class CSRWorkflowType {
    protected long objId;
    protected long transferRuleObjId;
    protected String objname;
    protected String objcode;
    protected boolean canUserTransfer;
    protected boolean transferRulesComplete;
    protected boolean closedStatus;
```

```
    protected boolean resolutionRequiredRule;
    protected List<CSRWorkflowStatusQueueType> queues;
}
```

CSRWorkflowStatusQueueType Bean

```
public class CSRWorkflowStatusQueueType {
    protected String id;
    protected String descr;
    protected List<CSRWorkflowStatusQueueMemberType> members;
}
```

CSRWorkflowStatusQueueMemberType Bean

```
public class CSRWorkflowStatusQueueMemberType {
    protected String userId;
    protected String fullName;
}
```

Appendix: Troubleshooting Chart

Appendix H provides detailed explanations of some error messages you may receive while using Stat, along with possible solutions. The information is categorized according to the application component or function that the errors concern. For problems not listed in this section, please contact Quest Technical Support.

- Stat Database
- Stat Central Agent
- Stat Oracle Agent
- Login/Connection
- Administrative Utilities
- CSRs
- Stat Web
- Archiving and Migrating
- Printing
- Miscellaneous

Stat Database

Problem	Explanation/Solution
PeopleSoft Staging Database: There exists more than one staging script. What values do I need to enter in the script for the tablespaces?	Confer with your DBA as to which tablespaces he or she created in the PeopleSoft AUD environment (staging database)
Receive the following error when archiving large sets of objects: “Select error: ORA-03232: unable to allocate an extent....”	Have your DBA re-size the temporary segments in the database to a minimum size of 1 MB initially and increase by increments of 1 MB if problem recurs.

Stat Central Agent

Problem	Explanation/Solution
Receive the following error when starting the Stat Central Agent on AIX: “The parameter or environment lists are too long”	The default buffer size on AIX is 6, which may be too low. To change the buffer size to 10, enter the following: chdev -1 sys0 -a ncargs= 10 If 10 is still too low, try increasing the buffer size in increments of 10 until the problem is resolved.
Receive the following warning even when logging is turned off for the server: “WARN [TxConnectionManager] Prepare called on a local tx. Use of local transactions on a jta transaction with more than one branch may result in inconsistent data in some cases of failure”.	This warning is generated because JDBC datasource does not support two phase commit and does not support XA. This warning can be ignored.
Receive the following error when saving the Stat configuration page: “Access denied”	To prevent unauthorized access to the configuration page, the Stat administrator needs to edit the *stat-config.properties* file in $STAT_HOME/config. For example, you can grant user John the permission by appending his computer's IP address (e.g.192.168.244.130) to the list. You can add multiple IPs to the list and use a comma to separate them.

Stat Oracle Agent

Problem	Explanation/Solution
Could not find agent identifier for environment code.	The environment code name that is entered in the stat.conf file on the Stat OraApps computer has to exactly match (case sensitive) the **Environment Cd** value under **Maintenance | General | Oracle Applications Connect**. Select **Maintenance | General | Oracle Applications Connect** and double-click the ENV in question or highlight it and click the Servers tab. The name of the server that is entered in Stat needs to be an exact match to the actual hostname of the host computer. To check the hostname, login to the host and type “hostname” at a command prompt. Then compare that hostname with the name that is entered in Stat. They need to be exactly the same. If hostname does not work then enter the ip address.
Stat Central Agent connection unavailable	1 Verify the Stat Central Agent is up running. 2 Look at the stat.conf file and verify the stat.central_agent.server parameter. Is the hostname or ip address pointing to the correct stat central agent? 3 Query for select * from STAT_AGENT to get the central agent hostname and ip address. Pay attention to the hostname and ip address and compare this with the stat.conf file. 4 If the ip address returns 127.0.0.1 as the loopback address then have Network Admin verify what the ip address should be. 5 Modify the /etc/host file to have the additional ip address instead of just the loopback ip address.
ERROR - IOException : No more data to read from socket	This is a port error. Possibilities include: • Wrong port assigned • Firewall port closed • Some other application has grabbed the port
ERROR - Stat's working directory does not exist on server FATAL - Fatal: Stat validation of environment failed. Unable to start Stat Oracle Agent	1 Login to Stat windows client and go to **Maintenance | General | Oracle Applications Connect.** 2 Highlight the desired Environment then open the Servers tab, scroll to the right and you will see the Working Directory column. Make sure you define the location of the working directory.

Login/Connection

Problem	Explanation/Solution
Receive the following error message when logging in: “Unable to complete ‘First Pass’ login.... Invalid username/password.”	Verify that the login ID field in the Stat.ini is correct. Normally, this is “STATLOGIN.” Verify that the STATLOGIN account is defined at the environment level.
Receive the following error message when logging in: “Unable to complete ‘First Pass’ login.... DBMS (073/MSS) is not supported on your current installation.”	Re-install Stat, making sure that you install the appropriate native environment connectivity drivers. Verify that the appropriate environment client software is installed on the workstation (i.e., SQL Net or SQL Server client). In the case of Oracle, verify that the oracle/bin directory is part of the workstation’s path.
Receive the following error message when logging in: “TNS: Could not resolve service name.”	Verify that the **Server Name** field in the Stat.ini file matches a valid TNSnames.ora entry
Receive the following error message when logging in: “Unable to complete ‘Second Pass’ login.... Invalid user name/password....”	This error indicates that the LOGINID and/or LOGINPWD fields in the STAT_LOGIN table do not match those of the environment owner. Check the password in the stat.ini file.

Administrative Utilities

Problem	Explanation/Solution
Data Replicator: After adding a new service domain using the Data Replicator, unable to access **Applications** in the **Domain Specific** menu and rceive the following error message: “An application error has occurred. Please note the following information and notify the System Administrator. Error: (3) Array boundary exceeded, Winmenu: nvo_security_manager, Object: nvo_security_manager, Script: has right, Line: 21, Version 5.0.0 Click OK to continue…”	This error message indicates that the user has not been granted access to the newly added service domain. Contact your system administrator and request access to the new service domain. To grant a user access to a new service domain, refer to Chapter 3, “Stat Security.” Users receive this error message when they have not been granted access to any service domains.
Stat INI File Editor: Receive the following error message when attempting to save a record in the Stat INI File Editor: “Error: Some fields need to be completed!!!”	One of the fields in the Stat INI Editor has not been completed. All fields must contain a value with the exception of the Other DB Parms field.

CSRs

Problem	Explanation/Solution
CTRL+F Usage: The CTRL+F keystroke that advances the user to the next entry field in the Description Tab of the CSR is not functioning.	This is caused when a space is inserted between the adjoining greater than/less than <> brackets in the Application/CSR Template. Access the template which is failing, and verify that no spaces exist between the two brackets.
Deleting CSRs: Is there a way to delete CSRs from the environment?	With proper security rights, you can use the CSR Purge Wizard to permanently delete CSRs from the Stat Repository. Before deleting a CSR, however, it is recommended that you first use the wizard to export the CSR to a file for backup purposes.
Deleting Objects and Archive Sets from CSRs: How do I delete objects and archive sets from existing CSRs?	Please contact Quest Software Support for instructions on how to proceed.
CSR Locks: After logging in to Stat, opened an existing CSR and received the following message: “This message has been locked by...”	This warning message indicates that the CSR is locked by the user noted in the message. You will also receive this error message when a user closes Stat and fails to close the CSR first. Ensure that all CSRs are closed prior to closing Stat. Not doing so will not remove the lock status in the environment and will cause this warning message to appear when another user tries to access the CSR.
The **Read Project**, **Read CSR, Read File**, and **Add Objects** buttons are greyed out in the Objects tab	The CSR may have a workflow that invokes object control, restricting the status where objects may be added to the CSR. 1 Open the workflow tab of the CSR. 2 Double-click on the current status. If the Allow Object Add/lock rule exists, you should be able to add objects. If the Allow Object Add/lock rule does not exist go to maintenance to determine if the overall Object Control feature is turned on. 1 Go to **Maintenance | Domain Specific | Workflow**. 2 Locate the workflow that the csr is using and look for the column called obj control. If this option is check then this functionality is enable. 3 Double-click on the workflow | right click at the workflow status and select status rule. If the option allow object add/lock is not check then the read csr, read project, add object will be grey out at that particular status of the workflow. **NOTE:** If you do not want to use this feature then the obj control option need to be uncheck at the workflow level. Changes will be effective on new CSRs. Changes made now will not affect existing CSRs.

Stat Web

Problem	Explanation/Solution
For users running the Stat Central Agent on Unix, graphical workflow diagrams do not display properly in Stat Web.	This problem may occur when either: • The machine hosting the Stat Central Agent doesn't have a windowing system installed in the operating system, as specified in the Stat system requirements • You are connecting to the Stat Central Agent using a telnet session that doesn't have graphical display capability The solution to the second case is to start the Stat Central Agent in a background mode through the telnet session. To do this, execute the following command: `./run.sh &`

Archiving and Migrating

Problem	Explanation/Solution
Base Archive Sets: Base archive set status remains stuck in In Process.	First, verify that the objects in the Base archive set are from the Base Object Source (Base Final). Also, verify that you selected the All on Migration Path radio button in the Lock in Environment box on the Objects tab in the *PeopleSoft Change Management* window. A base archive set may remain in process if: Any objects are locked in another CSR (for example, you have a reservation for an object in the Base database) The Stat Central Agent lost connectivity to the environment and/or the network There are no objects that can be archived for the base environment on the CSR.
Receive the following error in the archive log for PeopleSoft: "Error creating SQL - [ERROR] Database is not available, please check db info".	1 Confirm that the database is up and running. 2 Go to **Maintenance | General | Peoplesoft Connect**. 3 Hold down the ctrl key to select multiple PeopleSoft db for testing. If you are getting error verify connection error--io exception: unknown host specified driver: oracle or verify connection error--listener refused the connection on the Central Agent Results, check the hostname, service name and db listener port settings in the Peoplesoft Connect window.
Receive a CSR error when migrating forms fmb object types.	Refer to the following for more information: https://support.software.Quest.com/stat/kb/104980 Or https://support.oracle.com/epmos/faces/SearchDocDisplay?_adf.ctrlstate=agtl9ty5e_23&_afrLoop=138616630525556 (Oracle document 431324.1)

Printing

Problem	Explanation/Solution
When changing the printer (**File | Print Setup**) to generic text only, the font for the open description on CSRs changes to Roman 10cpi. This is the only available font listed until changing the printer back and re-opening the CSR.	Unfortunately, Stat has no control over font displays. This is a function of Windows. Similar behavior occurs in Microsoft Word.
Receive the following error message from the Stat Central Agent when printing a scheduled report “-9 error opening print job in Stat Central Agent scheduled report”	Verify that the printer to which you are trying to print your scheduled job exists on the machine where the Stat Central Agent is running. Also verify that the Host Printer name on the Stat Central Agent matches the printer name on the machine. For more information on the Stat Central Agent Printers, see Chapter 6, Configuring the Stat Central Agent on page 163.

Miscellaneous

Problem	Explanation/Solution
User Class Security: I would like to configure my service domains in such a way that HR dept. users cannot view FIN dept. users' CSRs and vice versa, even though they are all members of the same service domain.	The only way to do this is to set up two service domains; one for HR and one for FIN. This way, they cannot view each other's CSRs. If you have some users who need to view CSRs from both service domains, you can configure this at the user ID level; e.g., give user X access to both service domains. For information on granting access to multiple service domains, please see Stat Security on page 29.

Appendix: Oracle Agent: Stat.conf and log4j2.xml configuration

The stat_ora.zip file includes a default stat.conf file and log4j2.xml file, which after installation are located in the user's home directory under STAT_HOME>/conf. All the mandatory parameters and most commonly used parameters are included in these default configuration files. Additional parameters listed in this section may not be included in the default stat.conf file and, if applicable, will need to be defined by the user. The syntax for all parameters is name:value pair. Comments begin with a “#” character and end with the end of the line.

The following table lists all valid parameters. Some parameters apply to all instances of an agent (e.g. parameters to identify the Stat Repository), while others apply to each instances of an agent (e.g. parameters specific for an Oracle E-Business Suite environment).

Parameters prefixed with “stat” apply to all instances of an agent and should only be defined once in the configuration file. Parameters prefixed with <ENV> refer to an instance of the Stat Oracle Agent for a particular Oracle E-Business Suite environment. The <ENV> must be replaced with the environment code used to define that Oracle E-Business Suite environment in Stat.

When the Stat Oracle Agent is started, the stat.conf configuration parameters are cached in memory. You need to restart the agent before a parameter change can take effect.

<ENV>.adadmin_timeout 309
<ENV>.admin_port 309
<ENV>.autopatch_timeout 310
<ENV>.command_timeout 310
<ENV>.db_init_sql 310
<ENV>.DB_ORACLE_HOME 310
<env>.env.ADOP_LOG_PATTERN 310
<ENV>.env.APPLFENV 310
<ENV>.env.APPLREP 310
<ENV>.env.APPLTMP 310
<ENV>.env.APPL_TOP 310
<ENV>.env.<BaseDirCode> 310
<ENV>.env.CONTEXT_FILE 311
<ENV>.env.CONTEXT_NAME:<sid_hostname> 311
<ENV>.env.CUSTOM_OAF_DIR 311
<env>.env.CUSTOM_PRODUCTS 311
<ENV>.env.JAVA_TOP 311
<ENV>.env.NLS_LANG 311
<ENV>.env.ORACLE_HOME 311
<ENV>.env.<parameter> 311
<ENV>.env.PLSQL_ERROR_EXPRESSION 312
<ENV>.env.<ProductCode> 312

<ENV>.env.set_escape_processing 312
<ENV>.env.SHARED_PRODUCTS 312
<env>.env.ssh_disabled 312
<ENV>.env.SQLPLUS_PREPROCESSORS 312
<ENV>.env.USE_DATABASE_CHARACTERSET 312
<ENV>.env.TWO_TASK 313
<ENV>.env.XMLIMPORTER_OPTIONAL_PARMS 313
<ENV>.env.XMLEXPORTER_OPTIONAL_PARMS 313
<ENV>.event_processors 313
<ENV>.event_timeout 313
<ENV>. java.naming.factory.initial 313
<ENV>.maintmode_script 313
<ENV>.maintmode_timeout 314
<ENV>.migration_order_timeout 314
<ENV>.servername 314
<ENV>.sqlplus_options 314
<ENV>.shutdown_services_timeout 314
<ENV>._skip_object_generation 314
<ENV>.skip_show_errors 315
<ENV>._sqlplus_timeout 315
<ENV>.WFLOAD.upload_mode 315
stat.central_agent.disconnect_action 315
stat.central_agent.name_port 315
stat.central_agent.server 315
stat.db.name 315
stat.db.jdbc_driver 315
stat.db.password 316
stat.db.port 316
stat.db.server 316
stat.db.username 316
stat.central_agent.protocol 316
STAT_HOME>/conf/log4j2.xml 316

<ENV>.adadmin_timeout

Minutes the Stat Oracle Agent will wait for an adadmin command to produce an output. The Stat Oracle Agent will fail the Adadmin session if the inactivity (i.e., no output) exceeds this parameter. Default is 5 minutes.

<ENV>.admin_port

Port on local server for administering the Stat Oracle Agent processes for <ENV> Oracle E-Business Suite environment. Any unused port greater than 1024 can be used (e.g., 5501, 5502). The parameter for each environment on the server must be unique.

<ENV>.autopatch_timeout

Minutes the Stat Oracle Agent will wait while monitoring AutoPatch activity. The Stat Oracle Agent will fail the AutoPatch session if the inactivity (i.e., no output) exceeds this parameter. Default is 5 minutes. Larger patches may require up to 15 minutes.

<ENV>.command_timeout

This timeout is used when an internal command processor is run to execute commands. Default is 5 minutes.

<ENV>.db_init_sql

This parameter can be set to an anonymous PL/SQL block. When the Oracle Agent connects to the Oracle Apps database, this anonymous PL/SQL block will be executed to initialize the connection. This is useful to initialize a database session. For example, if the database language in not American English: “<env>.db_init_sql:declare begin dbms_session.set_nls('nls_language', 'AMERICAN') end.”

<ENV>.DB_ORACLE_HOME

(optional parameter)

Configures the Stat Oracle Agent to use the specified path for sqlplus.

<env>.env.ADOP_LOG_PATTERN

Default pattern for capturing Patch logs is "(.*\\.log)|(.*\\.lgi), meaning all files with .log and .lgi extensions. Users may add other extension by changing the regular expression. For example to additionally capture files with .out extension change the pattern to (.*\\.log)|(.*\\.lgi)|(.*\\.out)

<ENV>.env.APPLFENV

<ENV> environment file name (filename only) (Optional for R12 and R12.1)

<ENV>.env.APPLREP

<ENV> reports directory. This parameter should be set to “reports”, unless the default reports directory name has been changed. (Optional for R12 and R12.1)

<ENV>.env.APPLTMP

<ENV> temporary directory. Used to temporarily store generated forms. (Optional for R12 and R12.1)

<ENV>.env.APPL_TOP

<ENV> APPL_TOP directory for server. (Optional for R12 and R12.1)

<ENV>.env.<BaseDirCode>

Directory for the base directory code used with generic file types. For more information, see the section, “Object Compare Support for Form Library Files” in the Install Guide.

<ENV>.env.CONTEXT_FILE

The Oracle Agent resolves product top environment variables using the context file defined by this parameter. The context file is an XML file used by AutoConfig normally located in the *$APPL_TOP/admin* directory. The parameter value should be a fully qualified file name for the context file. When the agent needs the value for a product top variable, it checks the following in the order listed:

- The <env>.env.<productTop> parameter in the stat.conf configuration file for the Oracle Agent.
- If the <env>.env.CONTEXT_FILE agent configuration parameter is set, the value is parsed from the context file.
- The environment file defined by the <env>.env.APPLFENV agent configuration parameter is parsed for the value.
- The adovars file is parsed for the value.

NOTE: This parameter is optional for Release 12 and recommended for 11.5.10 and higher since the environment file will no longer explicitly set product top variables.

<ENV>.env.CONTEXT_NAME:<sid_hostname>

sid_hostname is the usually configuration for this value. Yours may be different. Ask your DBA

<ENV>.env.CUSTOM_OAF_DIR

This parameter is used to support OAF object types and is set to the name of the custom directories (example: XXQuest,XXQUEST).

<env>.env.CUSTOM_PRODUCTS

For R12.2, when a custom top is created using adsplice, a new Product's status is not set to 'L'. This parameter keeps track of custom products. Value is a comma separated list of custom products, for example (XXQuest,XXQUEST).

<ENV>.env.JAVA_TOP

This parameter is used to support OAF object types and is set to the value of $JAVA_TOP variable on the environment. (Optional for R12 and R12.1; not used in R12.2)

<ENV>.env.NLS_LANG

This parameter defines the NLS_LANG environment variable for the Oracle Agent. NLS_LANG is only used for archiving and migrating AK objects.

<ENV>.env.ORACLE_HOME

<ENV> Oracle Home for Oracle Developer.(Optional for R12 and R12.1)

<ENV>.env.<parameter>

When defining new Custom Object types, users may also define a Generation command to be run at the end of migration.

If a user needs to pass a user-defined environment parameter to the Generation command, they may do so by defining that parameter in Stat.conf.

<ENV>.env.PLSQL_ERROR_EXPRESSION

When compiling file objects using SQLPlus, we looks for the expression 'Warning: (.*) created with compilation errors.' in order to capture any possible errors. Customer may use this parameter to change the value of this expression.

For example, if user needs to pass a version number, they will enter %%VERSION%% in the Generation command, and they will define an <ENV>.env.VERSION:1.2 in stat.conf.

<ENV>.env.<ProductCode>

Directory for a product top. This parameter can be used to define the top directory for custom products. Additionally, this parameter can be used for standard products when the context file is not used and product tops are not defined explicitly in the environment file. For more information, see the section, “Custom Products and File Locations” in the Install Guide.

<ENV>.env.set_escape_processing

By default Escape Processing is set to false for Oracle agent. If for any reason customer needs to set this option to true, they may use < env>.env.set_escape_processing:Y.

<ENV>.env.SHARED_PRODUCTS

If a product is a shared product but is listed on the E-Business product table as not installed (N), the product can be added to the stat.conf file. Use commas to list separate products.

Example: <ENV>.env.SHARED_PRODUCTS:'JA','JE'

<env>.env.ssh_disabled

In a Multi-node environment, by default, Stat assumes that the ssh utility is running between the Admin node and all other nodes. To override this, set this parameter to 'n'.

<ENV>.env.SQLPLUS_PREPROCESSORS

The following preprocessors are passed to SQLPlus by default:

SET VERIFY OFF

WHENEVER SQLERROR EXIT FAILURE ROLLBACK;

WHENEVER OSERROR EXIT FAILURE ROLLBACK;

Customers may use this parameter if they need to change this list. For example:

<env>.env.SQLPLUS_PREPROCESSORS:SET DEFINE OFF\n WHENEVER SQLERROR EXIT FAILURE ROLLBACK;\n WHENEVER OSERROR EXIT FAILURE ROLLBACK;\n SET LINESIZE 999\n

Customers may also ignore the passing of any preprocessors by setting the value of this parameter to no value. For example:

<env>.env.SQLPLUS_PREPROCESSORS:

<ENV>.env.USE_DATABASE_CHARACTERSET

When archiving a multi-language aol record, the database character set is used. The database has to use UTF8 or AL32UTF8 character set or the archive will not have correct characters in it.

By default we use the database character set using the following query:

select value from NLS_DATABASE_PARAMETERS where parameter=”NLS_CHARACTERSET”;

users can disable this by setting this parameter to “N.” For example, <env>.env.USE_DATABASE_CHARACTERSET:n)

In this case we will use the characterset specified in fnd_languages_vl view.

<ENV>.env.TWO_TASK

If your DBA has set the two_task variable, enter it here. This is typically a DB instance name. (Optional for R12 and R12.1)

<ENV>.env.XMLIMPORTER_OPTIONAL_PARMS

(optional parameter)

This parameter is used to support OAF object types and is used to pass extra parameters to XMLImporter commands.

<ENV>.env.XMLEXPORTER_OPTIONAL_PARMS

(optional parameter)

This parameter is used to support OAF object types and is used to pass extra parameters to XMLExporter commands.

<ENV>.event_processors

Number of <ENV> message processing threads for non-patch requests. This parameter controls the degree of concurrency for processing events. Recommended initial value is 2.

<ENV>.event_timeout

(optional parameter)

If maintenance mode is used when applying patches, rolling back patches or migrating custom objects in multi-node environments, an agent will wait until all other agents have finished processing the event before maintenance mode is disabled. This parameter defines the number of minutes an agent will wait before failing the event. If this parameter is not defined, the default is 60 minutes.

NOTE: This parameter is applicable after an event has been processed, while the parameter <env>.maintmode_timeout is applicable before processing an event.

<ENV>. java.naming.factory.initial

Naming Context for JBoss Application Server

For JBoss: java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory

<ENV>.maintmode_script

(optional parameter)

This parameter can be used to specify a script to enable/disable maintenance mode. The Oracle Agent on the database server will pass a single parameter, “ENABLE” to enable maintenance mode and “DISABLE” to disable maintenance mode. If the script specified by this parameter has a “.sql” file extension, it will be executed with sqlplus. Otherwise, the script specified by this parameter will be executed as a command. If this parameter is not

defined, the Oracle Agent will use the FND_APPS_MODE_UTIL package by default to enable/disable maintenance mode.

NOTE: Only the agent on the database server will enable/disable maintenance mode. In multi-node environments, the other agents monitor the profile option Applications Maintenance Mode to determine the state for the environment.

<ENV>.maintmode_timeout

(optional parameter)

In multi-node environments, only the Stat Oracle Agent on the database server will enable/disable maintenance mode. However, all agents will wait until maintenance mode is enabled before processing the request. This parameter defines the number of minutes agents will wait before failing the request. If this parameter is not defined, the default is 5 minutes

NOTE: This parameter is applicable before an event is processed, while the parameter <env>.event_timeout is applicable after an event is processed.

<ENV>.migration_order_timeout

If migration order is used for objects in a multi-node environment, an agent may have to wait for other agents to finish processing objects with a lower migration order. This parameter defines the number of minutes an agents wait for other agents. Default is 15 minutes.

<ENV>.servername

(optional parameter)

This parameter defines the logical servername for <ENV> environment. When this parameter is not used, the Stat Oracle Agent uses the physical servername and environment code to identify itself with the Stat repository. This parameter can be used with HA architectures that require a virtual hostname.

<ENV>.sqlplus_options

When set (envCode.sqlplus_options:-s), enables the agent to use sqlplus to execute sql scripts and packages.

<ENV>.shutdown_services_timeout

When applying E-Business patches, all services will be stopped before the patch apply starts. Stat will wait for a response from each server indicating it is down. This parameter indicates the amount of time Stat should wait for services to shutdown. If that time is exceeded without response from the service, Stat will assume that it is down.

<ENV>._skip_object_generation

A comma-separated list of file objects for which generation will be skipped. Valid values are:

- RDF - Report Files
- FMB - Form Files
- PLL - Form File Libraries
- PKH - (PL/SQL Spec) File
- PKB - (PL/SQL Body) File
- PLS - PL/SQL File
- SQLS - SQL Scripts

- MMB - Menu File

<ENV>.skip_show_errors

When compiling package headers, package bodies, PLS objects, or SQL Scripts, a SHOW ERRORS is pasted to the end of the script. If user wants to skip this step, they can set this parameter to “Y.”

<ENV>._sqlplus_timeout

Minutes the Stat Oracle Agent will wait for a sqlplus command to produce an output. The Stat Oracle Agent will fail the sqlplus session if the inactivity (i.e., no output) exceeds this parameter. Default is 5 minutes.

<ENV>.WFLOAD.upload_mode

This parameter defines the upload mode for Oracle's WFLOAD utility when migrating WFT files. The value can be set to UPGRADE (default), UPLOAD or FORCE.

UPGRADE - Customizations to seed workflow data is preserved. Only process definitions that have not been previously customized are loaded.

UPLOAD - WFLOAD will use the access levels specified in the WFT file when uploading the workflow.

FORCE - The entire workflow definition will be loaded, regardless of an object's protection level.

stat.central_agent.disconnect_action

Determines how the Stat Oracle Agent handles a lost connection with the Stat Central Agent. No events are lost when the connection is lost.

Retry - When set to “retry”, the Stat Oracle Agent attempts to re-establish the connection to the Stat Central Agent every 10 seconds indefinitely. The agent can be shutdown at anytime using statctl.sh.

Terminate (default) - When set to “terminate”, the Stat Oracle Agent immediately terminates when the connection to the Stat Central Agent is lost. This is the default process if the parameter is not set or is invalid.

stat.central_agent.name_port

JNDI port of the Stat Central Agent server. If JBoss is used as the application server, 1099 is the default naming port. If the application server is configured for a different naming port, the Oracle Agent should be updated with the correct port.

stat.central_agent.server

Server or IP hosting the Stat Central Agent server.

stat.db.name

(optional parameter)

Stat Repository database name. For Oracle, this is the service name.

stat.db.jdbc_driver

(optional parameter)

The JDBC driver class name for the Stat Repository. This parameter must be set to “oracle.jdbc.driver.OracleDriver” since Oracle is the only supported database platform for the agent. Note the class does not include a “com.” prefix.

NOTE: This parameter is optional except in the case of NATTED environments, in which case it is required and should be the IP address.

stat.db.password

(optional parameter)

Stat Repository database password.

NOTE: This parameter is in clear text and can be removed.

stat.db.port

(optional parameter)

Stat Repository database listener port.

NOTE: This parameter is optional except in the case of NATTED environments, in which case it is required.

stat.db.server

(optional parameter)

Stat Repository server name.

NOTE: This parameter is optional except in the case of NATTED environments, in which case it is required.

stat.db.username

(optional parameter)

Stat Repository database username.

NOTE: This parameter is optional except in the case of NATTED environments, in which case it is required.

stat.central_agent.protocol

(optional parameter)

Running protocol for Stat Central Agent. By default the running protocol is http. If Stat Central Agent is running on https, this parameter needs to be set to https.

STAT_HOME>/conf/log4j2.xml

The section explains how to configure the log4j2.xml

NOTE: Rename log4j2.xml to the name of the instance/environment. For example, if the name of the instance/environment is VISDB-PROD then re-name the log4j2.xml as VISDB-PROD.xml

The customers running in the multiple environment scenarios, must duplicate the log4j2.xml file as many copies as the #n of the instances. For example, you must perform the above steps for each instance resulting in the structure below:

After making the required changes, re-start the Oracle Agents.

The following sections describe how to configure the log4j2 properties.

<Property name="log-path">log-path</Property>

It is a mandatory property. Please provide the directory path where the log file will be created.

Here is an example to understand the configurable values. The values to be configured are highlighted.

```
<?xml version="1.0" encoding="UTF-8"?>

<Configuration status="INFO">

   <Properties>
      <Property name="log-path">/home/applmgr/log4jupgrade/log</Property>
   </Properties>
   <Appenders>
      <RollingFile name="RollingFile" fileName="${log-path}/oraDev.log"
filePattern="${log-path}/oraDev-%d{yyyy-MM-dd}-%i.log" >
         <PatternLayout>
            <pattern>%d%7p[%t](%F:%L)-%m%n</pattern>
         </PatternLayout>
         <Policies>
            <TimeBasedTriggeringPolicy interval="1"/>
            <SizeBasedTriggeringPolicy size="10MB" />
         </Policies>
         <DefaultRolloverStrategy max="4"/>
      </RollingFile>
   </Appenders>
   <Loggers>
      <Logger name="root" level="DEBUG" additivity="false">
         <appender-ref ref="RollingFile" level="DEBUG"/>
      </Logger>
   </Loggers>
</Configuration>
```

<RollingFile name="RollingFile" fileName="${log-path}/Demo.log" filePattern="${log-path}/Demo-%d{yyyy-MM-dd}-%i.log" >

Replace Demo.log with name of log file in above line. The name of the file where log information is written.

<Logger name="root" level="INFO" additivity="false">
<appender-ref ref="RollingFile" level="INFO"/>
</Logger>

Update log level in place of INFO. Level of detail logged by Stat Oracle Agent for <ENV> Oracle E-Business Suite environment. Set this parameter to one of the following values: off, fatal, error, warn, info, detail, verbose or trace. Levels are cumulative and listed indegree of detail printed in log file (i.e. “error” includes all log records for “fatal” as well as some additional records). A value of “info” is suggested.

> **NOTE:** Performance is impacted modestly with each increase in the logging level. Levels with high degree of logging (e.g.) should be used only during the initial deployment and troubleshooting to minimize the performance impact.

<pattern>%d %7p [%t] (%F:%L) - %m%n</pattern>

Format mask of the log file records for <ENV> Oracle E-Business Suite environment.

Following is an example value that captures the date and message for each log record.

```
%d{yyyy-MM-dd HH:mm:ss} - %m%n
```

Following is an example value that captures additional detail, such as the class, line number and thread, for each record.

```
%d{yyyy-MM-dd HH:mm:ss} %20F:%4L %15t - %m%n
```

<TimeBasedTriggeringPolicy interval="1"/>

The TimeBasedTriggeringPolicy causes a rollover once the date/time pattern no longer applies to the active file. This policy accepts an interval attribute which indicates how frequently the rollover should occur based on the time pattern and a modulate boolean attribute.

Example values: Value of interval depends on date pattern. With a date pattern having hours as the most specific item, an increment of four rollovers would occur every four hours if interval value is set to 4. The default value is 1.

<SizeBasedTriggeringPolicy size="10MB" />

This parameter defines the size of the log file (in bytes) before it will be archived. When the size of the log file reaches the size defined by this parameter, it will be archived to a new file with ".1" extension. The value must be an integer in the range 0 to 2^63 (default is 10MB).

The size can be specified in bytes, with the suffix KB, MB or GB, for example 20MB. The size may also contain a fractional value such as 1.5 MB.

Appendix: Custom Report Files

Appendix J describes how use Jaspersoft Studio, a 3rd party reporting tool, to format the .jrxml files used to create Stat reports. It is not intended to be a comprehensive how-to guide; Instead, it points out required items and offers tips to make designing reports easier.

About Stat Report Files

All Stat reports are created with a tool called Jaspersoft Studio. This is a GUI based tool that allows you to format your report and store it in a .jrxml file. Although some knowledge of XML may be necessary to handle the finer details, Jaspersoft Studio does most of the formatting work for you. It is available at http://sourceforge.net/projects/jasperstudio/files/JaspersoftStudio-6.1.1/ at no charge. All Stat reports were created with Jaspersoft Studio 6.1.1. We suggest using the same version of Jaspersoft Studio or set the compatibility version to 6.1.1.

You may copy a Stat report that contains embedded SQL as a starting point for designing you own report. When creating a report, be aware of the following:

- You must give the report file a new unique name
- You must change the name inside the .jrxml file to reflect the new name
- You are not allowed to edit the existing files in their current locations. These files are the property of Quest Software and will be overlaid with each release of Stat.
- Once the report has been created, use the maintenance tool to upload your .jrxml file into the Stat Central Agent repository. For more information, see Stat Report Definition Maintenance on page 115.
- The tool adds the report to the STAT_REPORT_DEFN table and will insert the file into <STAT_HOME>/report/custom on the agent server
- It is recommended that you archive your custom files into your Stat repository and/or backup the <STAT_HOME>/report/custom folder on a regular basis.

Define Data Adapter for Stat Datasource

To connect to the Stat Repository, you need to create a new Data Adapter using JasperSoft Studio.

To create a new Data Adapter:

1. In JasperSoft Studio, navigate to the Repository Explorer and create a new adapter.
2. Select **JDBC Connection**, and click **Next** to open the Data Adapter Wizard.
3. Specify the JDBC driver. For example, if the Stat Repository is on Oracle, select oracle.jdbc.driver.OracleDriver.
4. Enter a valid JDBC URL, user name, and password.
5. Select a Driver Classpath, and click **Add** to add the proper JDBC driver. For example, for Oracle, the driver would be ojdbc6.jar.

Report Parameters

Jaspersoft Studio provides for several different types of Report Parameters.

- Parameters provided by Jaspersoft Studio for internal workings of the report start with REPORT_, JASPER_REPORT, plus a couple others all in capital letters.
- Stat supplies a few global parameters that may be used to populate data on your report. This includes the date/time that the report was created, the Report Title as stored in the Report Library and a Watermark on the report
- Stat Reports use a series of prompt parameters that may be used in your custom reports. They can be used to filter data on your reports.
- You may define your own custom parameters that prompt for data. Their names must be different than the predefined list below.
- You may also define custom global parameters. These must start with P_. These may be used in combination or as replacements for the Stat delivered global parameters.

Stat Predefined Global Parameters

Stat has a series of predefined global parameters. The values associated with these parameters are owned by Quest and should not be modified.

- CurrentTime - Displays the date/time that report was created
- CompanyReserve - Displays Quest's copyright
- ReportTitle - Displays the 40 character Report description from the Stat database
- BACKGROUND_TEXT - Displays the watermark as defined in report.properties

Stat Predefined (prompt) Parameters

This is a list of predefined parameters defined in Stat reports. These parameters are defined to prompt the user for a value that will filter the data on the report.

Name	Description	Parameter Class
APPL_CD	CSR Application	java.lang.String
ARCHIVE_SET	Archive Set ID	java.lang.Long
ASSIGNED_USERID	CSR Assigned User	java.lang.String
CHGMGMT_FLAG	Change Management Module	java.lang.String
CLOSED_STATUS_FLAG	Closed Status	java.lang.String
CSR_ID_START	CSR ID Start	java.lang.Long
CSR_ID_END	CSR ID End	java.lang.Long
CSR_STATUS_CD	CSR Status	java.lang.String
CSR_TYPE	CSR Type	java.lang.String
CUST_ID_START	Customer ID Start	java.lang.Long
CUST_ID_END	Customer ID End	java.lang.Long
DEPARTMENT	Department	java.lang.String
DUE_DT_START	CSR Due Date Start	java.sql.Timestamp
DUE_DT_END	CSR Due Date End	java.sql.Timestamp
MIGR_CD	Migration Path	java.lang.String
OBJECT_CLASS	Object Class	java.lang.String
OBJECT_DEVELOPER	Developer	java.lang.String

Name	Description	Parameter Class
OBJECT_NAME	Object Name	java.lang.String
OBJECT_TYPE	Object Type	java.lang.String
OPEN_DT_START	CSR Open Date Start	java.sql.Timestamp
OPEN_DT_END	CSR Open Date End	java.sql.Timestamp
PRIORITY_CD	Priority	java.lang.String
PROJ_CD	Project Code	java.lang.String
PS_DATABASE	Application Database	java.lang.String
MIGR_DB	Application Database	java.lang.String
QUEUE_ID	CSR Assigned Queue	java.lang.String
RECORD_STATUS	Record Status	java.lang.String
RELEASE	Release	java.lang.String
SD_CD	service domain	java.lang.String
STATISTICAL_STATUS_FLAG	Closed for Stats	java.lang.String
STATUS_CD	Status Code	java.lang.String
WRKFLW_START	Workflow ID Start	java.lang.Long
WRKFLW_END	Workflow ID End	java.lang.Long

For each predefined parameter Stat Report Wizard has a corresponding control with specific rules. It could be a dropdown for example with pre-populated list of values. Default parameter descriptions can be overridden by specifying a value in parameter description property of the report itself.

Custom (prompt) Parameters

Report parameters which are not selected from the list of predefined parameters are considered to be custom parameters. The custom parameters class may be selected from these three data types:

- java.lang.String
- java.lang.Long
- java.sql.Timestamp

Depending on the selected class, the Report Wizard will provide the corresponding selector for entering string, numeric or date values. Report Wizard parameter selectors will be displayed in the order that the corresponding parameters are defined in a given report.

Custom Global Parameters

You may define your own custom global parameters.

Custom global parameters must start with prefix P_. The “Use as Prompt” should be off. The names and values are defined in the report.properties file which is located in the <Stat_home>/report folder. Global parameters do not appear in the Report Wizard nor in report cover page. They are valid for all the reports on which they are defined. If the report.properties file is modified, the Stat Central Agent must be restarted to enact the change.

Watermarks

You may add a watermark to your reports. Watermarks display on the right side of the report. The text runs from bottom to top. All reports will have the same watermark.

1 Locate the file <Stat_home>/report/report.properties where is Stat Central Agent is installed.

2 Open the file.

3 Locate the statement: #BACKGROUND_TEXT=For internal use only.

4 Remove the #.

5 Modify the right side of the equation as desired.

6 Save and close the file.

7 Re-start the Stat Central Agent to enable file modifications.

Copyright

Reports delivered by Quest are copyrighted by Quest. If you copy a Quest report it will reflect the Quest Copyright.

To add your own copyright to your custom report. There are two methods to handle this.

1 Remove the parameter $P{CompanyReserve} from the bottom of the report

2 Add a static field that includes your copyright information. This static text field must be defined on each report, but can be a different value on each report if desired.

3 Alternatively, define your own custom global parameter. This allows you to place the same information on several reports and modify it in a single location.

   The naming convention is P_X where X is whatever you wish. Parameter class should be <java.lang.String>.

   a Place the parameter in the appropriate location on the report

   b Open <STAT_HOME>/report/report.properties and define the parameter at the end of this file under the global parameters comment.

      Example P_Company=(c)2011 MyCompany

   c Re-start the Stat Central Agent to enable file modifications

Report Variables

Jaspersoft Studio also has a series of predefined variables that allow you add information to your reports. For example: PAGE_COUNT AND PAGE_NUMBER allow you to specify page 3 of 10 on your page. These variables may be viewed in the Variables section of the Report Inspector.

Text Field Expressions

Sometimes you may wish to reformat the data coming from the database. For example, a check box on is stored as a 1 and off is stored as a 0. You may wish to format this on the report to on/off or yes/no. This is done in the Text Field Expressions box. Click on the ellipsis to expand the field and add you formatting. Some examples are listed below.

- Date time

  ""+(new SimpleDateFormat("ddMMMyyyy HH:mm")).format(new java.sql.Date($P{CurrentTime}.getTime()))

- Simple if statement when the value may be null

  $F{APPL_CD}==null?"All":$F{APPL_CD}
  If APPL_CD is null then print All, otherwise print the actual APPL_CD value.

- Simple if statement

(($F{OA_VERSION_ID}.equals("1"))?"11i" : "R12")
If OA_VERSION_ID = 1 the print 11i, otherwise print R12

- If statement with 5 options

  (($F{OA_CUSTOM}.equals("B"))?"Custom with Lang" : (($F{OA_CUSTOM}.equals("P"))?"Custom w/o Lang":($F{OA_CUSTOM}.equals("Y"))?"Generic":($F{CUSTOM_TYPE}.equals("N"))?"Predefined":"Unk"))

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

Glossary

A

Activity or Activity codes

A category of tasks and auto tasks. Example: Invoicing or documentation.

Application

A subdivision of a service domain. Example: PeopleSoft or MS Office.

Archive Set

A snapshot of a set of objects that have been grouped together for archiving purposes. There are three types of archive sets: Base, Interim, and Final.

Assigned User

The Stat user who has been assigned to a CSR. Available users depend on the queue selected.

Auto Tasks

Tasks that Stat automatically adds to a CSR. They are triggered by the selection of Applications, Types, and Statuses.

B

Base Archive Set

The original snapshot of the objects in the Base environment. Objects in the base archive set always originate in the Base environment. Only one base archive set exists per CSR.

Base Environment

The source environment from which the base archive set originates. All objects in the base archive set are from the Base environment. This is a PeopleSoft environment.

Business Rule

A rule that triggers an email to a distribution list when a CSR corresponds to the user-defined event.

C

Change Management Module

The change management support modules provided by Stat for PeopleSoft, Oracle Applications, and generic applications.

CSR

Stands for Change/Service Request. This a request made by a customer or user that is documented and resolved in Stat. A CSR can belong to only one service domain and can have an unlimited number of tasks defined on it.

Customer

The person who reported the request/problem. Customers may or may not be Stat users. Depending on the business environment, customers can be internal or external.

D

Data Object

User-defined or third party data sets developed for specific application environments.

Department

The business division or organization to which the customer belongs. This can be an outside company name or an internal department within a business.

Development Environment

The environment in which object development occurs.

E

Environment

A database as well as the file servers and file paths associated with it. Also, a subdivision of an application. Its use is optional by application. Example: A/R for PeopleSoft application or Excel for MS Office application.

F

File Objects

File type objects (also called flat files), such as SQL and COBOL files. In Stat, file objects (as well as PeopleSoft proprietary objects) can be included in an archive set and migrated from one PeopleSoft database or generic application environment to another.

Final Archive Set

The final snapshot of all objects taken from the Development environment. The final archive set should be created after all changes have been approved. The final archive set should be migrated to all environments on the migration path so they are all in sync. Only one final archive set exists per CSR.

G

Generic Application

Any file-based application connected to Stat

H

History

A record of value changes maintained by Stat. These values can include transfers of CSR ownership, CSR status transfers, triggering of business and personal rules, and other of changes.

I

Interim Archive Set

An interim snapshot of objects while they are in the process of being modified. An unlimited number of interim archive sets can be created. Interims should be created from the environments in which objects were modified which would probably be Development. Interim archive sets should be migrated to one or many target environments for testing and evaluation.

L

List Group

A grouping of tabs displayed on the Support Console.

O

Object

A term used in Stat to refer to both PeopleSoft proprietary objects and file objects.

P

PeopleSoft Proprietary Object

An object native to PeopleSoft, such as pages and records. In Stat, PeopleSoft proprietary objects (as well as file objects) can be included in an archive set and migrated from one PeopleSoft environment to another.

Personal rule

A rule that triggers an email to the user who created the rule when a CSR corresponds to the user-defined event. An email generated by a personal rule can only be sent to the creator of the rule.

Priority

The level of urgency associated with the CSR. The priority sets the due date of the CSR.

Project (in Stat)

A larger business process that groups an unlimited number of CSRs and tasks from various service domains. A project can be used to track a number of related CSRs from one location.

Q

Queue

A group of users that possess a similar skill set. The assigned user must be a member of the current queue. Throughout the life of a CSR, ownership can be transferred to various queues. A queue is associated with a specific service domain. All members of the queue must have access to the associated service domain.

S

Schema Object

A schema object definition supported by Stat. Stat supports locking, archiving, and migrating schema object definitions on Oracle databases version 9i or higher and on MS SQL Server 2005/2008.

Service Domain

Service domains allow you to divide your business into logical units. CSRs can only belong to one Service domain and cannot be reassigned.

Source File Location

The file server plus the file path where file objects originally reside for an environment.

Stat Central Agent

The Stat component that does the actual processing of many behind-the-scenes activities, such as object locking and creating archive sets.

Stat Oracle Agent

A background daemon that runs on each Oracle Applications server. It receives requests from the Stat Central Agent, processes the requests, and sends resulting information back to the Stat Central Agent.

Status

The current phase of a CSR.

T

Target Environment

An environment to which interim archive sets are migrated for testing and evaluation purposes. Examples of target environments are QA, Testing, and Training.

Task

An individual step required to complete a CSR. A CSR can include many tasks. A task can be manually or system generated (auto task). Tasks cannot exist outside of a CSR.

Template

A predefined data entry field on the Description tab. Templates are triggered by Applications and Types. They help save time and ensure data consistency.

Type

The categorization of a CSR.

U

User

A person who uses Stat. A user can also be a customer.

User Class

A security level which determines a user's access within a Service Domain. A user class is assigned rights. Rights exist for a variety of functions from editing fields on a CSR, creating archive sets, and accessing wizards.

W

Workflow

Sets of rules that regulate the sequence and conditions by which CSRs can change from one status to another.

Working Directory

The file servers plus the file paths that are defined for individual users.

Index

A

Activating record changes
re-caching codes, 17
Activity Code Maintenance table, 123
Administrative utilities
Connection Manager, 45
Data Replicator, 25
PS ObjectMover Instruction Update Utility, 27
Table Dump Utility, 26
Application access, 39
Application Environment Maintenance table, 124
Application Maintenance table, 123
Application Template Maintenance table, 151
Applications
restricting user access, 39
Approvals
generic apps migration approvals, 103
PeopleSoft migration approvals, 85
transfer approval lists, 156
Auto Task Maintenance table
by CSR Status, 125
by CSR Type, 125

B

Business Rule Maintenance table, 126
Business rules
copying, 132
defining, 127
disabling, 132
e-mail content, 130
e-mail distribution list, 130
history, 133
rule criteria, 128
trigger events, 127

C

CLI functionality
distribution environments, 142
COBOL compilers, 72
Color Selection dialog box, 17
Connection history, 46
Connection Manager, 45
Copying
business rules, 132
generic application environment definitions, 106
Oracle Applications environment definitions, 100
PeopleSoft environment definitions, 88
user definitions, 34
workflows, 161
Country Maintenance table, 57
CSR Priority Maintenance tables, 133
CSR Status Maintenance table, 135
CSR Type Maintenance table, 134
CSR Type Template Maintenance table, 151
CSRs
inbound e-mail triggers, 178
unlocking, 168
workflows, 152
Customer Maintenance table, 58
Customer Priority Maintenance tables, 136
Customers
Customer Maintenance table, 58
inbound e-mail configuration, 182

D

Data Object Maintenance table, 106
Data objects
application version numbers, 107
Edit Data Objects window, 107
Data Replicator, 25
Database Management System (DBMS), 11
Databases
connecting, 21
connection history, 46
copying data, 25
database engine, 11
INI parameters, 21
passwords, 30, 36
profiles, 24
DataMover Scripts, 148
Default working directories, 73
Department Maintenance table, 55
Distribution environments, 138, 141, 144, 145

E

Edit Template window, 151

E-mail, 174
business rule distribution list, 130
configuration, 174, 175, 176
CSRs triggered by inbound e-mail, 178
default values, 179
defining for business rules, 130
Electronic Mail Interface window, 174
error notification, 126
inbound e-mail configuration, 178
outbound e-mail addresses, 130
outbound e-mail configuration, 176
reply messages, 187
Environments
copying PeopleSoft environment definitions, 88
distribution environments, 138, 141, 144, 145
Generic application environment connections, 100
PeopleSoft build scripts, 148
PeopleSoft environment connections, 80
Error notification, 126
Stat Central Agent jobs, 169
Escalation events, 127
Exporting
maintenance tables, 18

F

File object security, 196, 199
File objects
case sensitivity, 74
COBOL compilers, 72
default working directories, 73
file directories, 38, 60, 65
file templates, 67
file type directories, 38
file types, 38, 60
name conversion, 74
security, 196, 199
servers, 60, 67
source file locations, 65, 84
user default directories, 73
user working directories, 60
File path syntax, 73
File servers, 60, 67
syntax, 73
Unix file servers, 72
validating connections, 66
File templates, 67
File type directories, 38, 60
File types
user working directories, 66

G

Generic Application Environment Connection Maintenance table, 100
Generic Application Migration Path Maintenance table, 136
Generic applications
copying environment definitions, 106
Distribution environments, 138, 145
migration approval lists, 103
source file locations, 65

H

H2_Heading2
Pre and Post Migration Steps, 146
History
business rules, 133
Stat Repository, 46

I

Importing
maintenance tables, 18
ObjectMover instructions, 27
Inbound e-mail configuration
about, 178
CSR fields, 186
CSRs triggered by e-mail, 178
defining, 179
finding customers, 182
parameters, adding, 181, 185, 187
parameters, removing or editing, 182, 186, 187
reply messages, 187
special processing, 180
INI files
editing profiles, 24
printing, 24

J

Job Monitor, 169
filtering and sorting, 171
Jobs tab, 170
logs, 170
scheduling, 170

L

Languages
Oracle Applications, 91
License Manager, 45
Locking
physical lock exclusions, 85
Login IDs, 30
Login security, 29

M

Maintenance tables
- about, 12
- Activity Code Maintenance table, 123
- Application Environment Maintenance table, 124
- Application Maintenance table, 123
- Application Template Maintenance table, 151
- Business Rule Maintenance table, 126
- Color Selection dialog box, 17
- Country Maintenance table, 57
- CSR Priority Maintenance table, 133
- CSR Status Maintenance table, 135
- CSR Type Maintenance table, 134
- CSR Type Template Maintenance table, 151
- Customer Maintenance table, 58
- Customer Priority Maintenance table, 136
- Data Object Maintenance table, 106
- Department Maintenance table, 55
- editing, 17
- exporting, 18
- Generic Application Environment Connection Maintenance table, 100
- Generic Application Migration Path Maintenance table, 136
- importing, 18
- Oracle Application Maintenance table, 92
- Oracle Applications Configuration, 90
- Oracle Applications Migration Path Maintenance table, 143
- PeopleSoft Employee Search Configuration maintenance table, 111
- PeopleSoft Environment Connection Maintenance table, 80
- PeopleSoft Migration Path Maintenance table, 140
- Reports Maintenance table, 151
- Service Domain Maintenance table, 54
- service domain-specific tables, 122
- standard maintenance window, 13
- Stat Report Definition Maintenance table, 115
- System Maintenance table, 47
- template maintenance tables, 151
- User Class Maintenance table, 31
- User Maintenance table, 33
- Vendor Maintenance table, 151
- Workflow maintenance table, 152

Manager, 45

Migration Approval lists
- generic applications, 103
- PeopleSoft, 85

Migration paths
- generic applications, 136
- Oracle Applications, 143
- PeopleSoft, 140

O

Object type access, 40

Objects
- file objects, 38
- PeopleSoft object locking, 85
- PeopleSoft object security, 189
- restricting user access, 40

Operating system commands
- defining, 167

Operator IDs, 36

Oracle Application Maintenance table, 92

Oracle Applications
- copying definitions, 100
- distribution environments, 144
- languages, 91
- patch types, 90
- patches, 90
- platforms, 91
- product families, 90
- servers, 94
- Stat Oracle Agent, 64
- updating products, 91, 100

Oracle Applications Configuration maintenance table, 90

Oracle Applications Migration Path Maintenance table, 143

Outbound e-mail configuration, 176
- Object Lock event, 177
- Request for Info event, 177

P

Parameters
- pre/post migration steps, 88

Passwords
- databases, 30
- PeopleSoft passwords, 36
- resetting, 35

Patches
- Oracle Applications Configuration maintenance table, 90
- Oracle Applications languages, 91
- Oracle Applications patch types, 90
- Oracle Applications platforms, 91
- Oracle Applications product families, 90
- updating Oracle Applications products, 91, 100

PeopleSoft
- CLI functionality, 142
- COBOL compilers, 148
- DataMover script, 148
- Distribution environments, 141

environment connections, 80
migration approvals, 85
object locking, 166
operator IDs, 36
passwords, 36
project build scripts, 148
PS Config file, 81, 83
source file locations, 65, 84
user connections, 85
PeopleSoft Employee Search Configuration maintenance table, 111
PeopleSoft Employee Search Configuration table
exclusions, 115
special considerations, 112
PeopleSoft Environment Connection Maintenance table, 80
source file locations, 84
user connections, 85
PeopleSoft Migration Path Maintenance table, 140
PeopleSoft object security, 189, 197, 202
FAQs, 194
PeopleSoft ObjectMover Instruction Update Utility, 27
PeopleSoft objects
physical locking exclusions, 85
security, 189
Post migration steps
Create Project Build Script, 148
custom commands, 148
PeopleSoft Compile COBOL, 148
PeopleSoft Run DataMover Script, 148
Pre/Post migration steps
parameters, 88
Pre/Post Migration Steps Parameters Maintenance table, 88
Printing
INI files, 24
Stat Central Agent printers, 169

Q

Queue Maintenance table
editing queue membership, 39, 152

R

Re-caching codes, 17
Reports
e-mailing, 165
printing, 165
Reports Maintenance table, 151
REST API Resources, 249

S

Scheduling, 170
Stat Central Agent jobs, 168
Security, 12, 30
application access, 39
Connection Manager, 45
database passwords, 30
file object security, 196, 199
login IDs, 30
login security, 29
object type access, 40
PeopleSoft objects, 189
service domain-specific tables, 123
Stat users, 32
user classes, 31
Servers
Oracle Applications, 94
service domain access, 30
Service Domain Maintenance table, 54
Service domains
security, 30
Service Domain Maintenance table, 54
Service domain-specific maintenance tables, 122
security considerations, 123
Source file locations, 65
PeopleSoft, 84
Standard maintenance window, 13
Stat
Connection, 45
License Manager, 45
security, 12
Stat reports, 115
System Maintenance table, 47
upgrading, 13
users, 32
Stat Central Agent, 12
business rules, 127
defining operating system commands, 167
e-mail configuration, 174
e-mail processing, 174, 175, 176
inbound e-mail configuration, 178
inbound e-mail processing, 180
logs, 170
monitoring on the web, 169
outbound e-mail configuration, 176
printers, 169
scheduling, 170
starting and stopping, 163
Stat Central Agent jobs, 170
Check for Past Due Items, 165
class parameters, 165
defining, 164
E-mail Reports and Print Reports, 165
error notification, 169

Log Off and Wait, 166
monitoring, 170
PS Object locking, 166
Purge Error Log Tables, 166, 167
Purge Event Tables, 167
Run Operating System Command, 167
scheduling, 168
Unlock Locked CSRs, 168
Stat INI Editor
database connections, 21
editing profiles, 24
printing INI files, 24
Stat Oracle Agent
base directories, 64, 79
Stat Report Definition Maintenance table, 115
Stat Repository
copying data, 25
Status rules, 160
Syntax
file paths, 73
System Maintenance table, 47

T

Table Dump Utility, 26
Template maintenance tables
Application Template Maintenance table, 151
CSR Type Template Maintenance table, 151
Edit Template window, 151
Templates
application templates, 151
CSR Type templates, 151
editing, 151
file templates, 67
workflow templates, 154, 161
Transfer rules, 155
approval lists, 156
Trigger events, 127
Troubleshooting
PS ObjectMover Instruction Update Utility, 27
Table Dump Utility, 26

U

Unix, 72
Upgrading Stat, 13
User Access Information window, 35
User class rights, 209
editing, 32
User classes, 31
User Class Maintenance table, 31
user class rights, 32, 209
User file directories, 38
User working directories
default directories, 73
file types, 66
Users, 32
application access, 39
connecting to PeopleSoft environments, 85
Connection Manager, 45
copying user definitions, 34
file directories, 38
LDAP passwords, 34
object type access, 40
PeopleSoft operator IDs, 36
PeopleSoft passwords, 36
resetting Stat passwords, 35
synchronizing user access information, 41
User Maintenance table, 33
working directories, 38

V

Validating
file server connections, 66
Vendor Maintenance table, 151
Version Control Management Maintenance table, 117

W

Windows
Connection Manager, 45
Edit Data Objects window, 107
Edit Template window, 151
Electronic Mail Interface window, 174
File Object Maintenance window, 60
standard maintenance windows, 13
User Access Information, 35
Workflow
copying, 161
status rules, 160
templates, 154
transfer approval lists, 156
transfer rules, 155
Workflow Maintenance table, 152
Working directories, 38, 60