Navigating the Oracle Diagnostics Security Model

Joseph Imbimbo
Carnegie Mellon University

Marijo Erickson
Oracle Corporation
Hiran Patel
Oracle Corporation

Abstract

The concept of the "Diagnostics Role" has been introduced to secure access to data, test groups, and reports generated in Oracle Diagnostics. This paper will document the three diagnostics roles of this new security model and discuss the components that facilitate deployment of Oracle Diagnostics in custom responsibilities and custom applications. A real time demonstration of Release 12.1 features will illustrate the new functionality and required set ups.

The primary goals of the paper and conference presentation include:

- A brief review of the components of Oracle Diagnostics and their utility to data base administrators, developers, and functional users.
- Presentation of the security model currently deployed and one that will be deployed in e-Business Suite release 12.1
- Documentation of the setups necessary to provide access to the Diagnostics Tool test groups.
- Review of functionality that permits the extension of test groups to custom applications and responsibilities.
- Conference demonstration of the Oracle Diagnostics Tool employed in e-Business Suite 12.1.

I. The Components and Utility of Oracle Diagnostics

e-Business Suite diagnostics are comprised of two components: the Remote Diagnostic Agent (RDA) and the Oracle Diagnostics. The former is available for the data base server and the latter is the diagnostics engine for the oracle applications. Both components are delivered as patches that may be installed with minimal pre-requisites in 11i and Release 12. The diagnostics tests are grouped by the major products such as Oracle Applications DBA, Receivables, or Payables, to name a few. These tests may be used to extract information about the versions of packages, java servlets, and patch levels pertaining to specific functional modules. The may also be utilized to trouble shoot issues with invoices, purchase orders, and data integrity. Support analysts handling metalink service requests use the output from these tests to determine action plans. Many sites run the tests to proactively identify issues resulting from changes to setups and system profile settings. There are seeded tests that analyze the data base and the AOL side of e-Business Suite to determine if minimal best practice security recommendations have been implemented. As tests are created, these are installed via patches. A catalog of most of the tests provided for 11i and release 12 installations may be referenced in Metalink note 342459.1. Figure 1 provides an overview of the diagnostic test groups in the release 12.0 RUP 4 diagnostics patch. Figure 2 details the specific test groups in the Oracle Payables product group resulting from a mouse click of that link in Figure 1. Mouse clicking on the note number to the right of Internet Expenses Report Status provides the details concerning the inputs and outputs of these tests displayed in Figure 3. Metalink note 167000.1 provides administrators with the installation instructions for both Release 11i and Release 12 e-Business Suite. In Release 12.0, as well as earlier releases, test groups were assigned a low, medium, or high sensitivity level. This feature enables restricting medium and high marked tests to diagnostic roles of a more privileged nature. In Release 12.1, the sensitivity level will be assigned to the individual tests themselves and achieves the same goal while providing a greater degree of control.

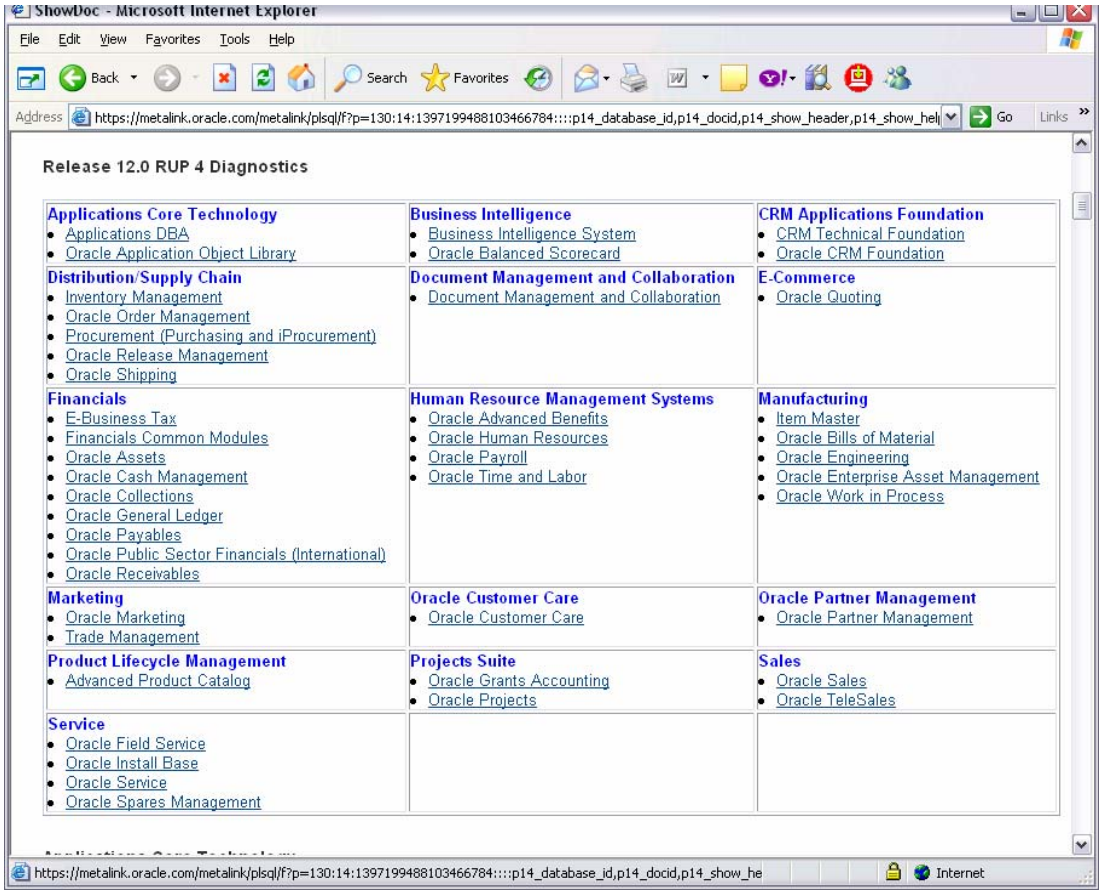

Figure 1

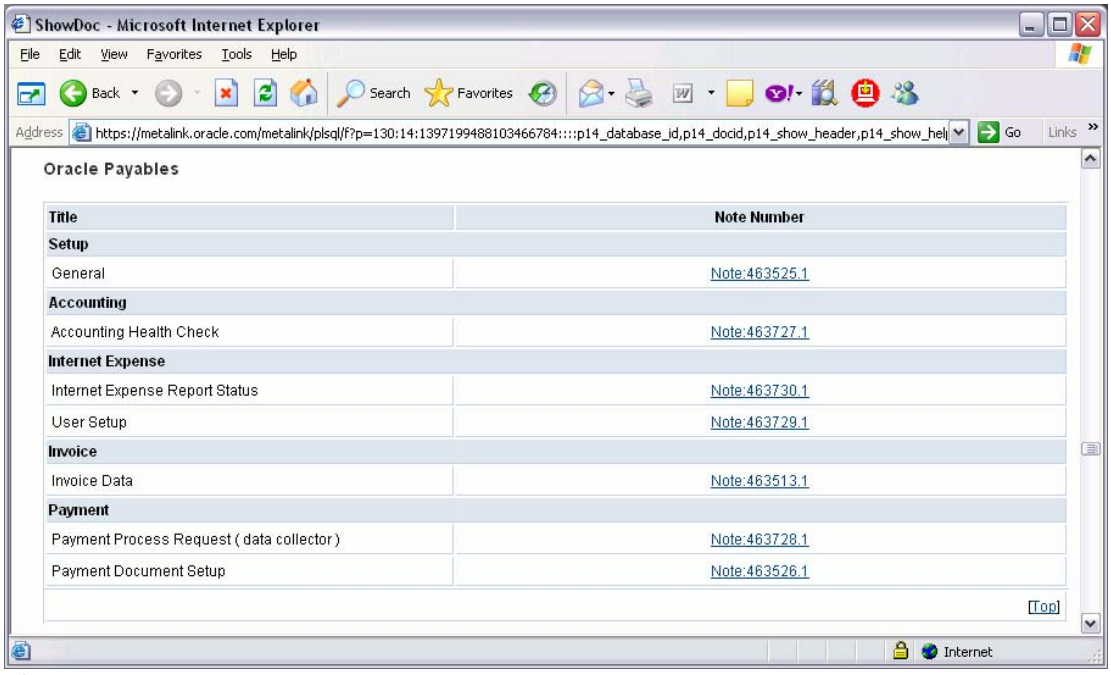

Figure 2

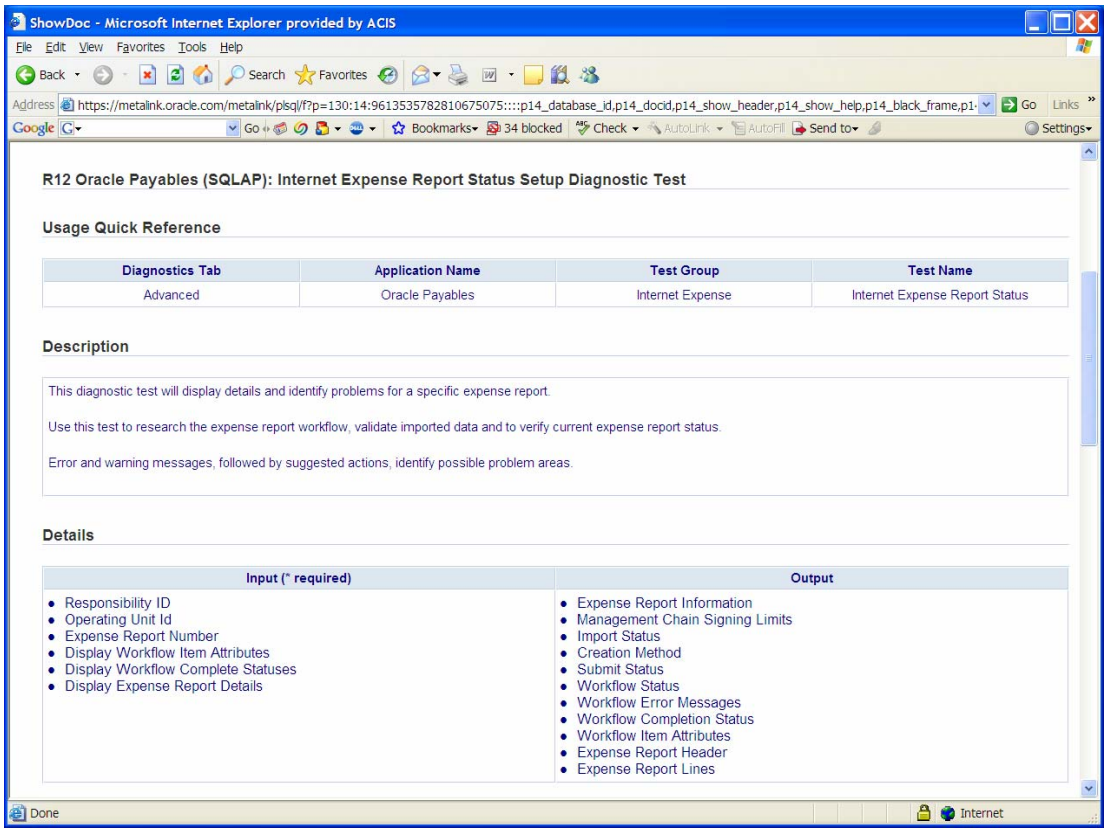

Figure 3

II. Current Oracle Diagnostics Security Model

Oracle Diagnostics has employed role-based security since the introduction of Oracle Diagnostics version 2.5 in January, 2007. Users running diagnostics are associated with diagnostic roles. Responsibilities are assigned to roles. The four "out of the box" roles provided consist of End User, Application Super User, Diagnostics Super User, and Anonymous User. As a result, user access to a test is determined by the responsibility assigned to the user as well as the diagnostic roles assigned to the responsibility. This permits more granularity than the predecessor "function security" model.

The Diagnostics Super User role as the name suggests has unrestricted privileges inside Oracle Diagnostics. This role is the default granted to the "System Administrator" and "CRM and HTML Administration" responsibilities.

The Application Super User role may only configure test inputs, execute tests, and view reports for test groups within its own application (for example, Payables). This role can execute tests labeled high, medium, and low sensitivity within its own test groups, as well as tests marked as having low and medium sensitivity in other applications.

The End User role permits users to configure test inputs, execute tests, and view reports for test groups marked as having low sensitivity for tests in the application to which the responsibility belongs. This role is the default granted to the "Oracle Diagnostics Tool" responsibility.

As an example of how this works, let's assume that the user, LARRYE, has been assigned to the AP Manager responsibility. If we have granted the "Application Super User" role to the AP Manager responsibility, then the user, LARRYE, will be permitted to execute high, medium, and low sensitivity tests

in the Accounts Payable application. Additionally the user, LARRYE will only be capable of running medium and low sensitivity tests in all other applications such as General Ledger, Inventory, and Receivables. The higher sensitivity level tests in these other applications are blocked.

The Anonymous User role is implicitly assigned if none of the user's responsibilities have any association with the previously described roles. It is the "bit bucket" where unassigned responsibilities remain until they are explicitly assigned. Most documents provided by Oracle do not reference this role and in fact this role will be disabled in Release 12.1.

The existing model is unable to accommodate custom responsibilities residing within custom applications. Release 12.1 will provide this capability as well as the capability to create custom roles, taking advantage of the latest industry standards in role based access control.

III. Oracle Diagnostics Security Model in Release 12.1

The Oracle Diagnostic security model in Release 12.1 is based upon. Role Based Access Control (RBAC), an ANSI standard supported by the National Institute of Standards and Technology. The Oracle implementation of this standard first appeared within Oracle User Management in Release 11.5.10 for a subset of modules. As noted in the previous section of this paper, a limited implementation of RBAC has been available in Oracle Diagnostics since January, 2007. The complete implementation will first be made available in Release 12.1 in 2008. A definition of some of the terms as well as a brief explanation of the concepts employed the security model follow.

In the full implementation of the model, roles, both seeded and custom, are grouped categorically. For example, Security Administration, Information Technology, Training, and Territory Management Task Roles are major groupings. Custom role categories may be created by administrators to bundle roles and responsibilities in ways that make sense for their own organization. Roles discussed within this paper are grouped inside the category known as Diagnostic Roles.

Permission sets provide a means of grouping related permissions together. Permission sets are granted to users or roles independently of responsibilities. These are best described as functions inside of menus that users or roles require access to.

Grants may be of a functional or data security nature. Functional grants specify permission sets. Data security grants specify a data object and an instance set or specific instance. An instance set corresponds to a set of rows for the database object. It may be thought of as a SQL WHERE clause on the attributes of an object. Specific instances are a single row in the data base. Function and Data Security are implemented within the Oracle Application Object Library. Functional security restricts user access to menus, forms, and HTML pages. Data Security extends Function Security by controlling user access to data sets and/or the actions that they can perform on the data sets.

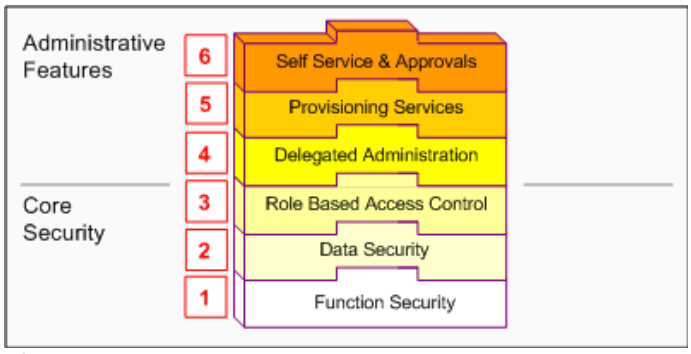

Figure 4

Figure 4 is taken from the Oracle Applications System Administrator's Guide – Security and illustrates the relationships among the various components of the security model. The administrative features are beyond the scope of this paper.

At the top of the security model sits Role Based Access Control. A role can be configured to acquire and/or inherit responsibilities, permissions, function security, and data security policies required to perform their duties. Members of an organization may be assigned more than one role.

Roles can be defined inside of role inheritance hierarchies. This allows higher level role to inherit all of the properties of lower level or subordinate roles. An obvious example is that of a member of an organization who is in a managerial role. That person retains specific functions as a manager but also assumes the capabilities of an employee since a manager is also an employee.

IV. Oracle Diagnostics Setup and Navigation in Release 12.1

A. Background

The model's key concepts will be highlighted with displays of the relevant setup screens but by no means should this paper be considered a comprehensive "how to" that will replace Oracle Corporation's formal documentation. Three seeded responsibilities are involved with setup and configuration of the security model as it applies to Oracle Diagnostics. The System Administrator responsibility is required to create custom responsibilities for custom applications as well as to assign users to these responsibilities. The User Management responsibility (Figure 5) creates role categories and custom roles if business requirements require. The Functional Administrator responsibility (Figure 6) is where permission sets and grants are duplicated from the seeded versions. As is always the case, Oracle recommends that seeded functionality never be directly modified. Duplicating the components with custom names or labels is always the best practice to prevent software patches from overwriting customizations made directly to the seeded components.

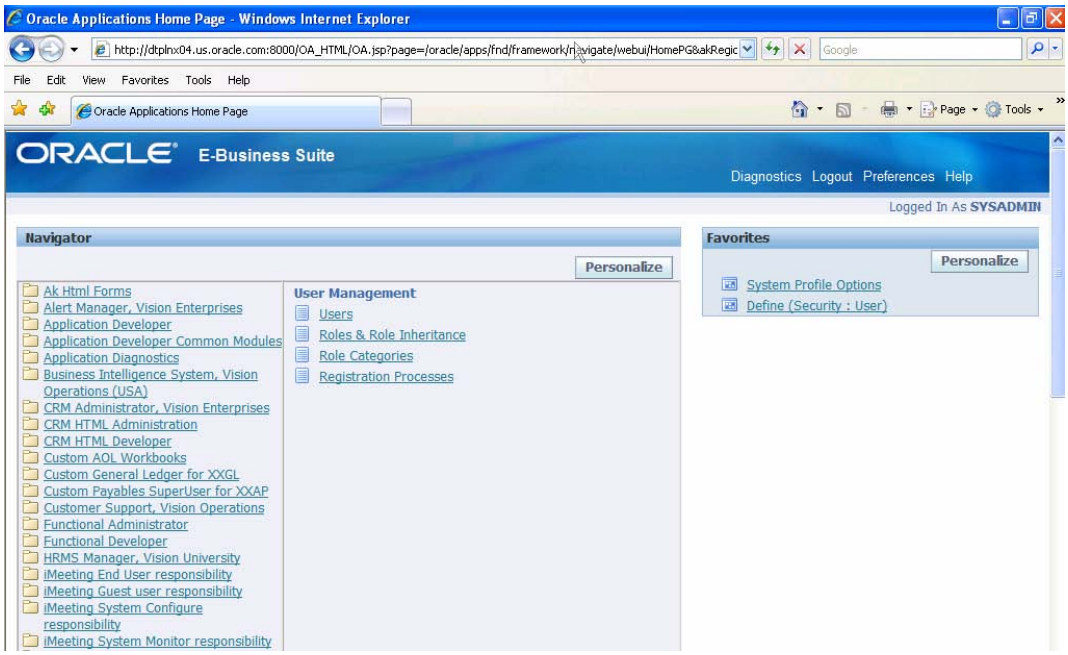

Figure 5 User Management

.

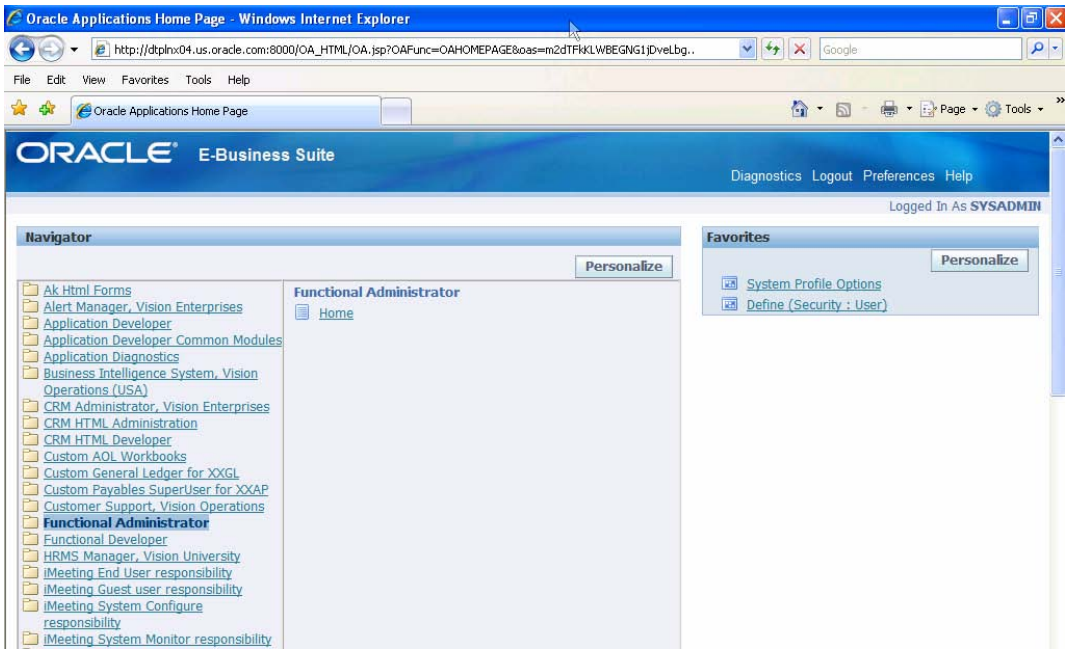

Figure 6 Functional Administrator

B. Illustration of Setups and Concepts

1. Duplication of a Seeded Role

The application, Custom Payables, assigned a short name of XXAP and created inside of a VISION demo data base will be referenced to illustrate how customizations at the application level may be integrated into the Oracle Diagnostics security model.

Figure 7a illustrates the three seeded grants that are packaged with the Application Super User role, itself an Oracle supplied role. Note the presence of three grants, two of which deal with data security and one with functional security. These grants are maintained via the Functional Administrator responsibility and can be cloned if the grants do not reflect business requirements of the user company.

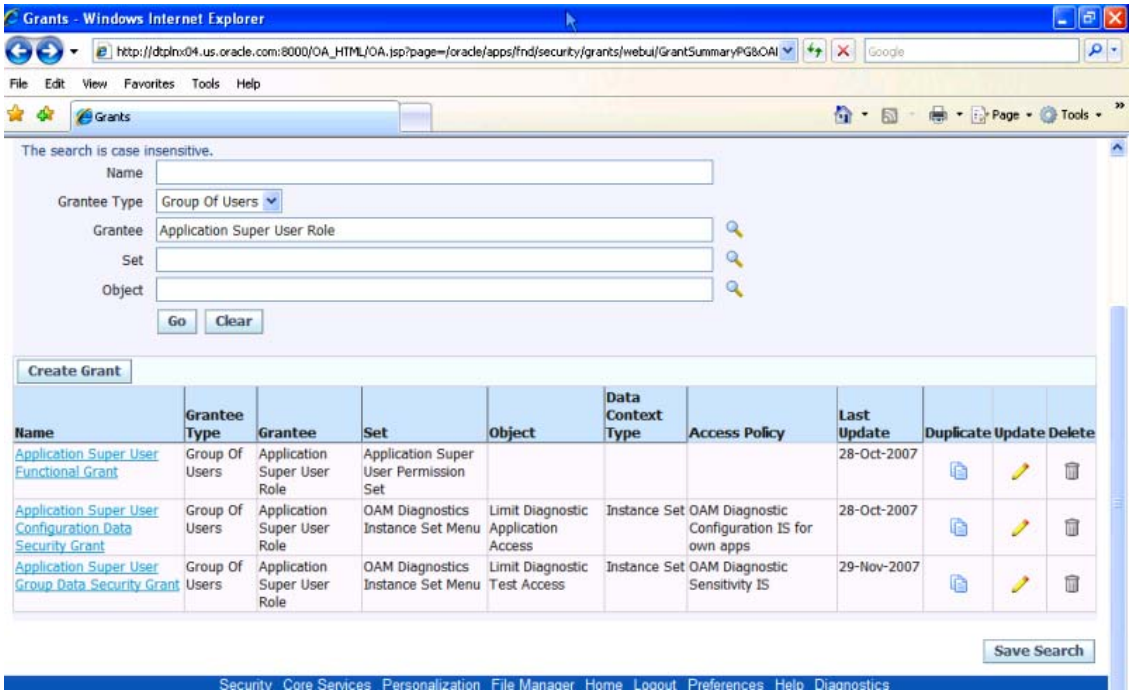

Figure 7 Seeded Application Super User Role

The Application Super User Role illustrated in Figure 7 may be cloned to establish a custom version as shown in Figure 8. Details concerning modifications to the three grants in the cloned role are provided later in this paper.

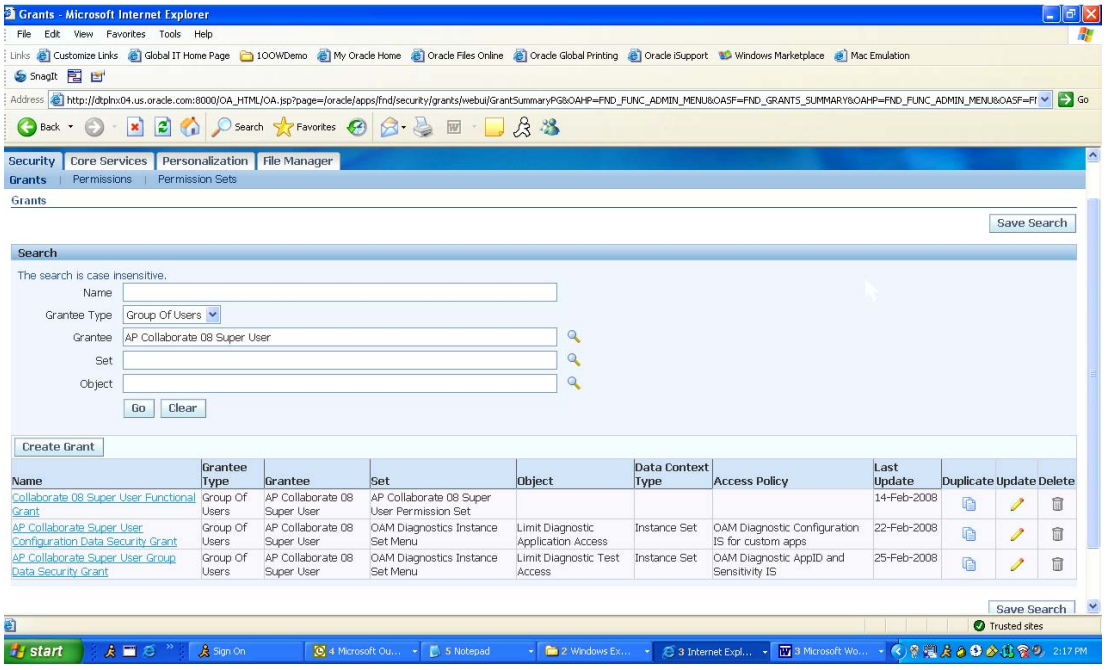

Figure 8

2. Roles and Inheritance

Figure 9 is a snapshot of the Role Categories form accessed via the Functional Developer responsibility. Note the existence of the Diagnostics Roles grouping.

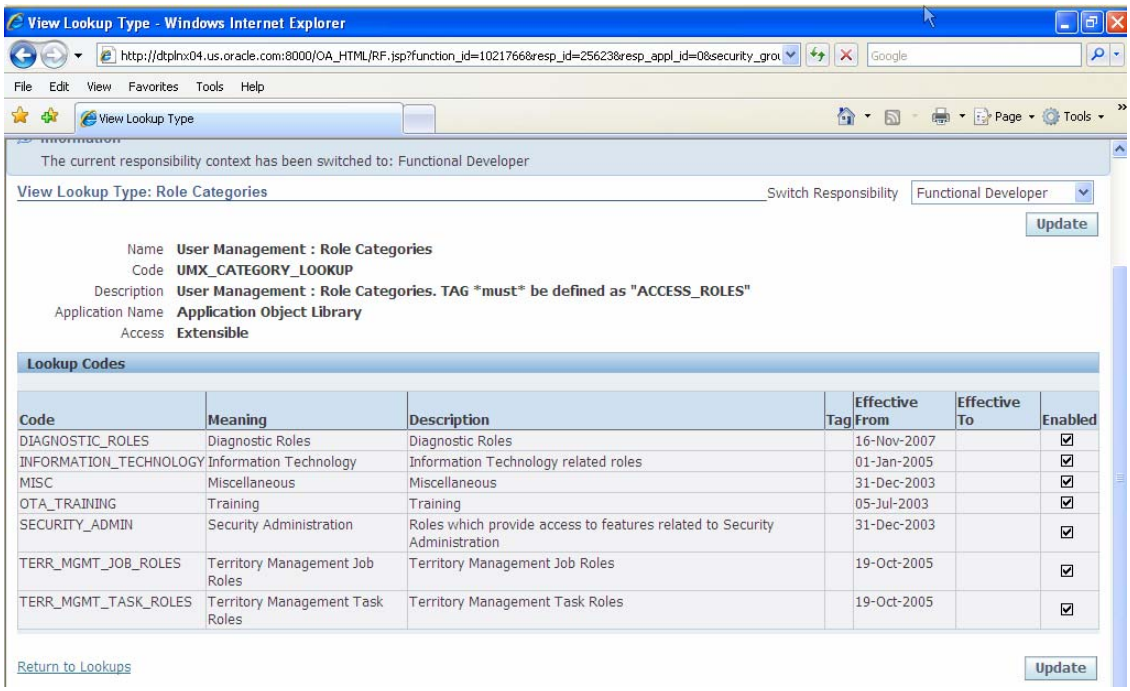

Figure 9

Figures 10a 10b, and 10c provide drill down views of the concept of Role Inheritance as it pertains to the AP Collaborate 08 Super User Role within the Diagnostic Role category. Figure 10c is a hierarchical view visible after mouse clicking on the 'GO" button in Figure 10a and mouse clicking on "View Hierarchy" in Figure 10b What we see is that the Custom Payables Super User will inherit the capabilities of the AP Collaborate 08 Super User Role as well as the capabilities of the Oracle Diagnostics responsibility. The convention utilized when this information is displayed is that FND is a tag for a responsibility while UMX tags roles.

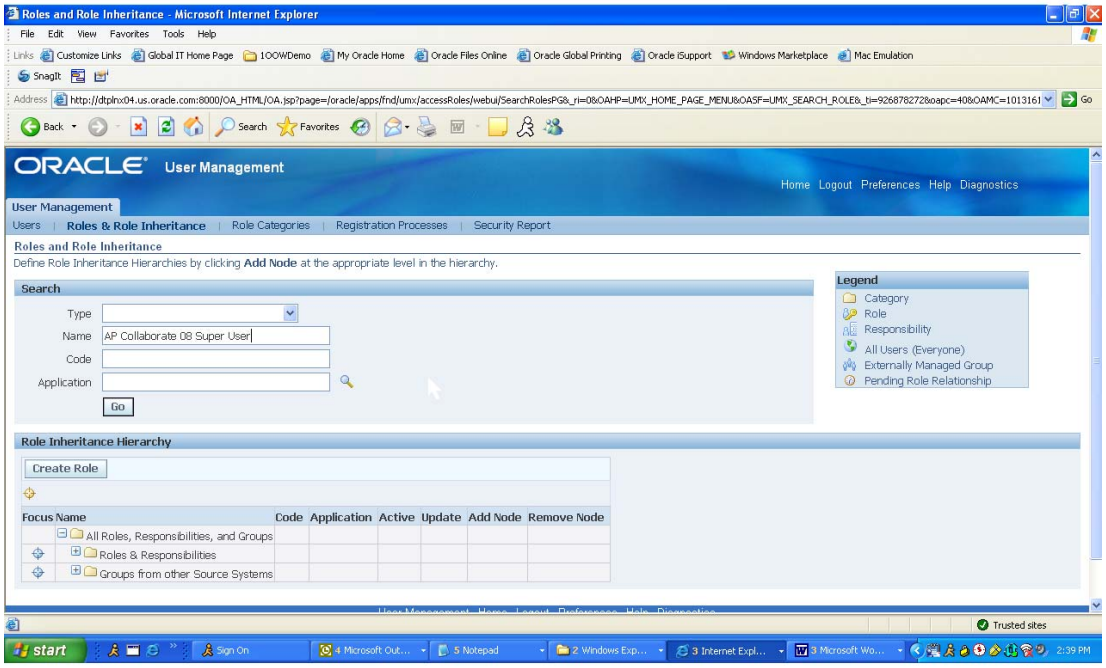

Figure 10a

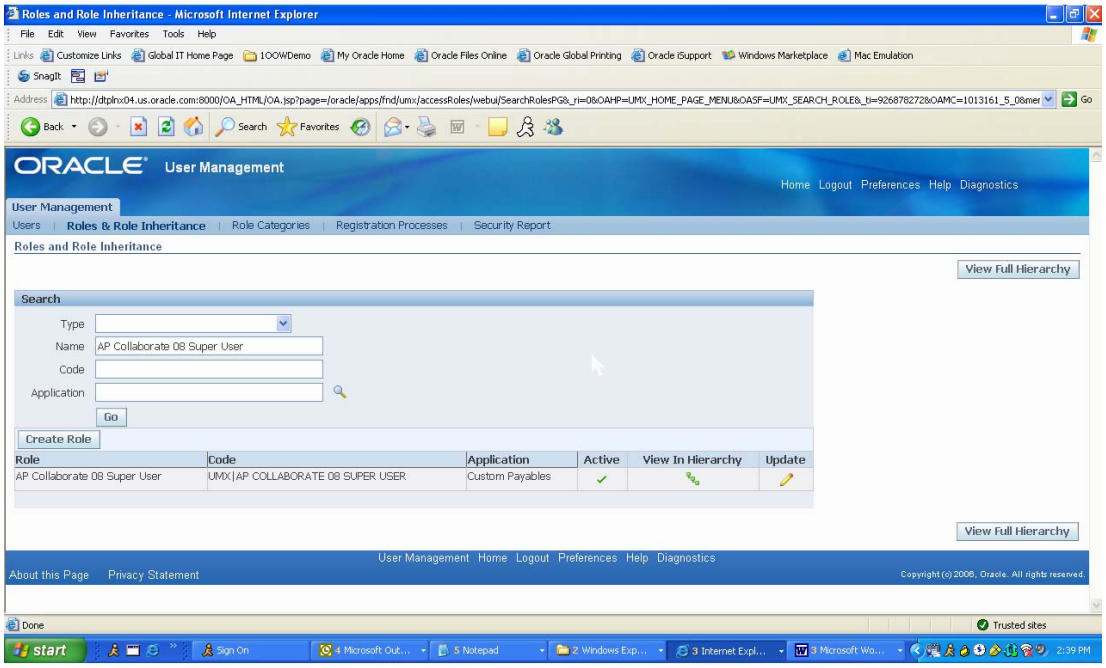

Figure 10b

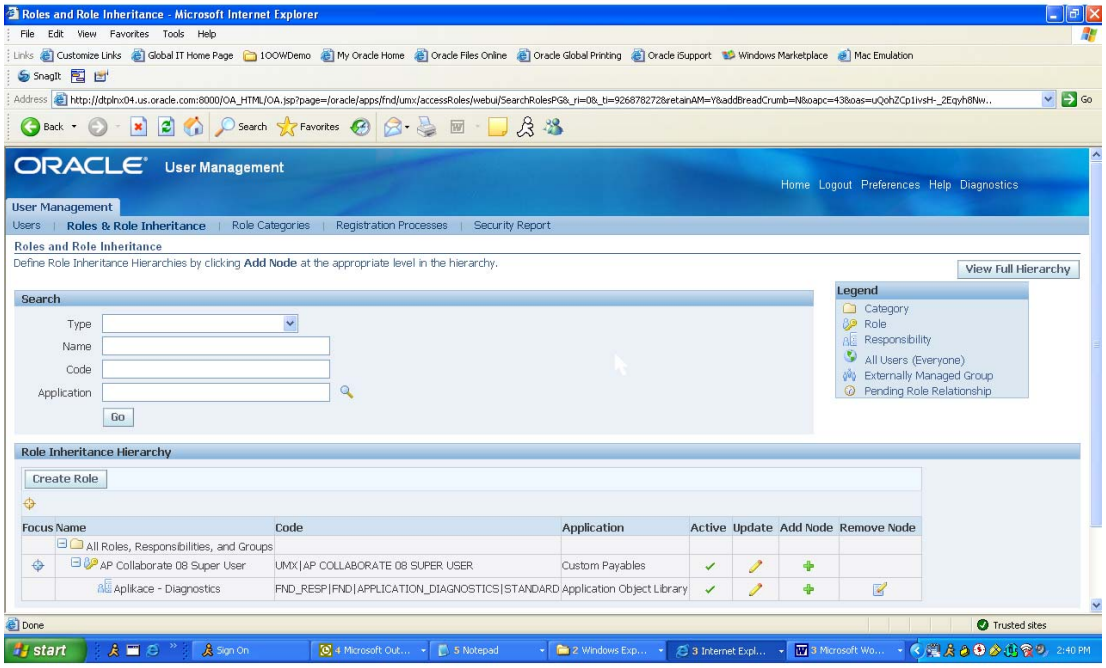

Figure 10c

3. Grants

The customization below in Figure 11, "AP Collaborate Super User Configuration Data Security Grant," is an example of how one maps a custom application, XXAP in this case, to a seeded application, SQLAP, the short name for Oracle Payables. This is accomplished within the instance set, "OAM Diagnostic Configuration IS (as in instance set) for Custom apps." With this configuration, users who have been assigned, the custom responsibility for XXAP AP Super User will be able to run all SQLAP (the short name for AP Payables provided by Oracle Corp) diagnostic tests.

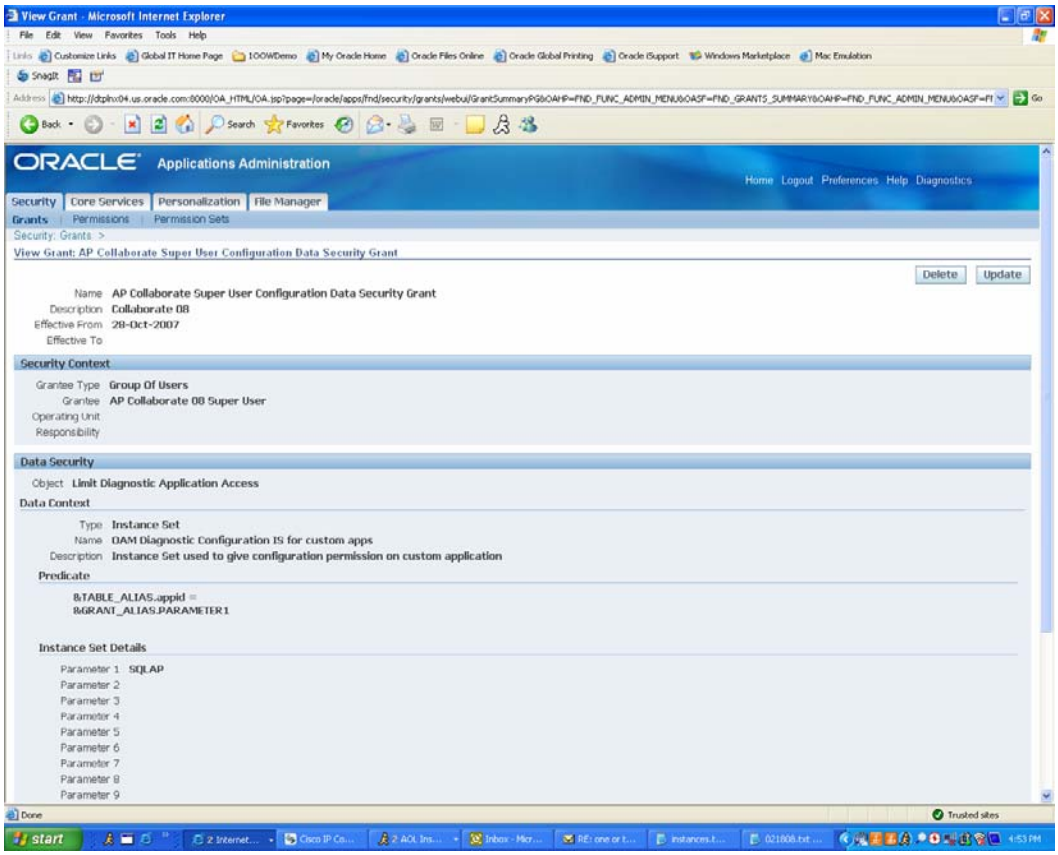

Figure 11

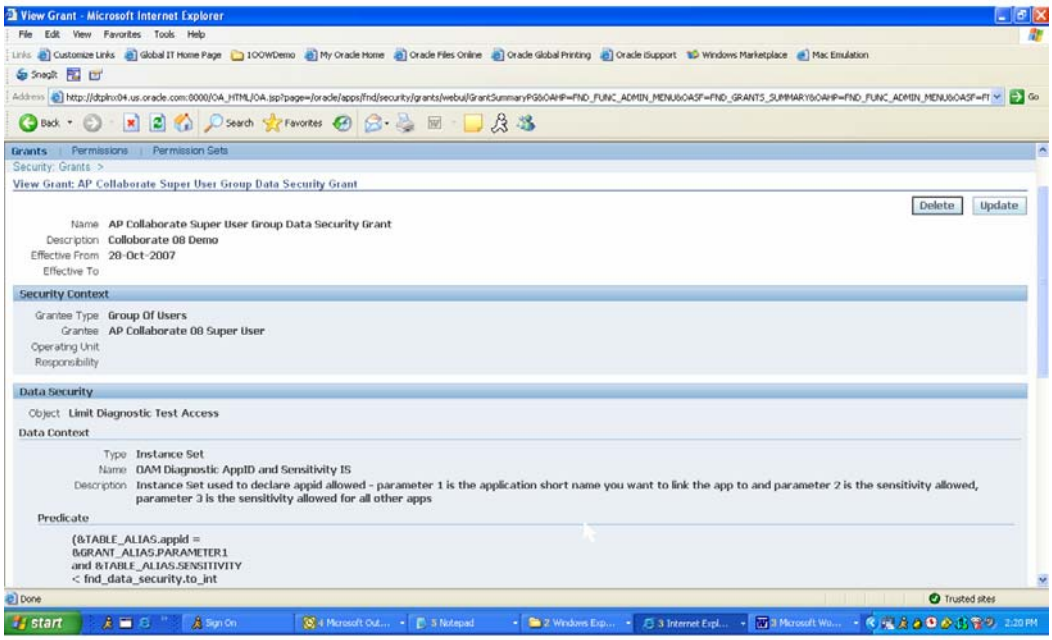

Figure 12a

The Super User Group Data Security Grant permits super users to set sensitivities for their own applications as well as other applications (Figure 12a). The details are supplied in Figure 12b. Parameter 1 is the application short name you want to link the role to. Parameter 2 is the declared sensitivity for this application which all users assigned to this role will inherit. Parameter 3 is the declared sensitivity allowed for all other applications. In order to view all tests of low, medium, and high sensitivity, the parameters must have a value of four. To view low and medium sensitivity tests, the values must be set to three. To restrict execution and viewing to low sensitivity tests, the value should be set to two. To prevent all tests from being accessible, the value is set to 1.

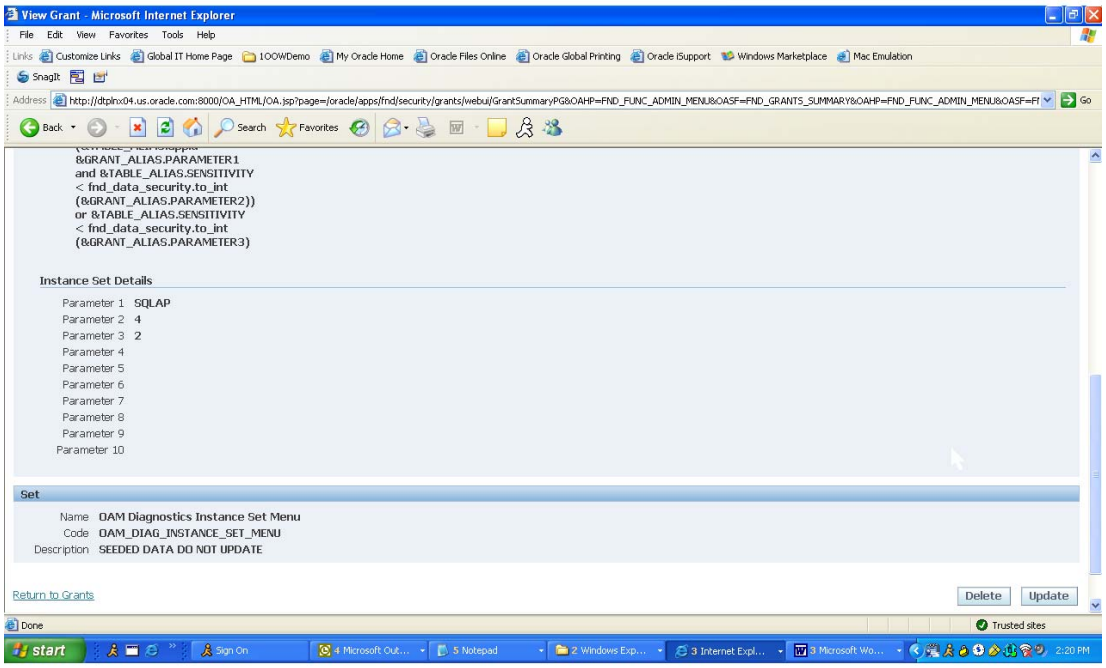

Figure 12b

4. Assigning Sensitivity Levels

In Release 12.1, one may register a custom application within Oracle Diagnostics, supply custom tests, and assign sensitivity levels to these custom tests. This functionality is accessible using the Application Diagnostics responsibility and clicking on the "Configuration" menu as displayed in Figure 13. Figure 14 displays the available applications registered in Diagnostics. The example provided demonstrates navigation using a seeded test in a Vision demo data base where these tests have not been locked down. In a real installation, seeded tests provided by Oracle Corporation for Oracle Diagnostics in Release 12 will be locked down and administrators will not be able to alter the sensitivity levels of tests residing in the supplied product groups. The actual release of this product will have the Update icons grayed out except for custom tests installed by system administrators, functional administrators, or data base administrators.

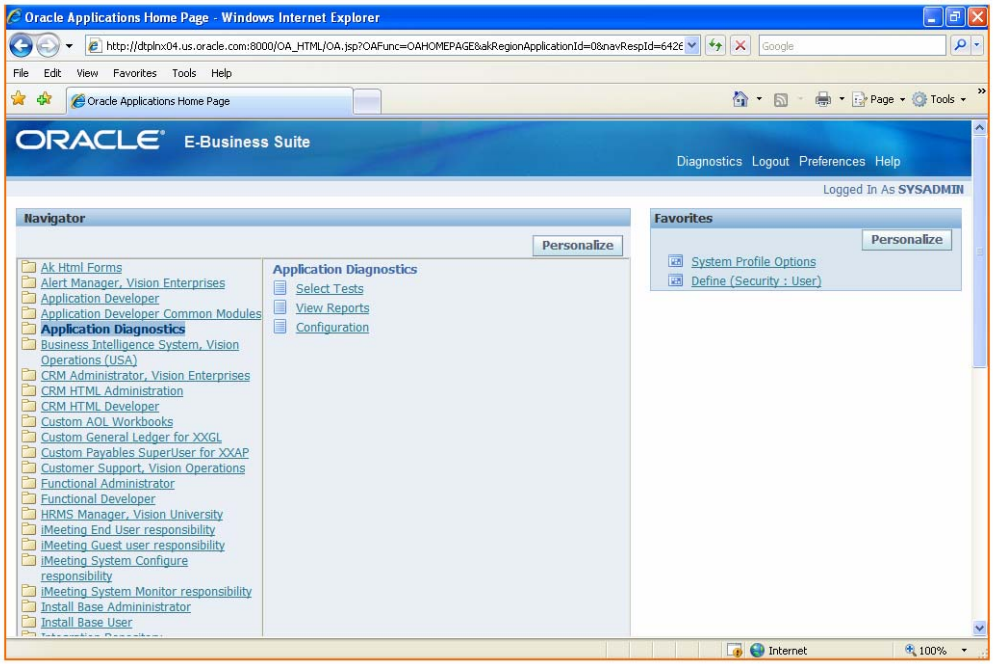

Figure 13

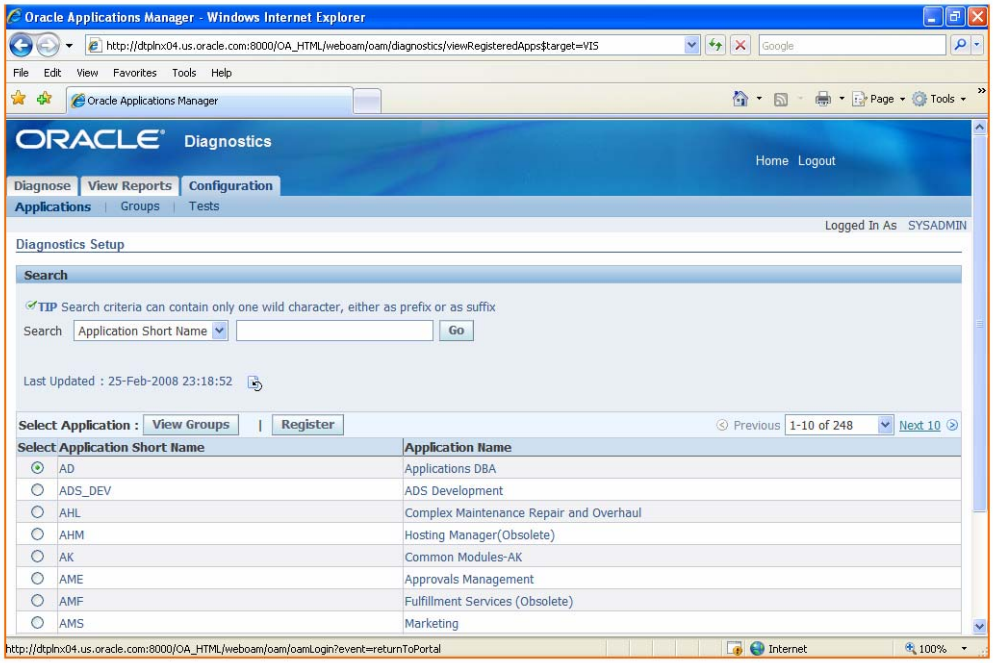

Figure 14

We select Payables and see several test groups (Figure 15) with a count of the number of tests registered within that group. For example, the Internet Expense grouping contains two registered tests.

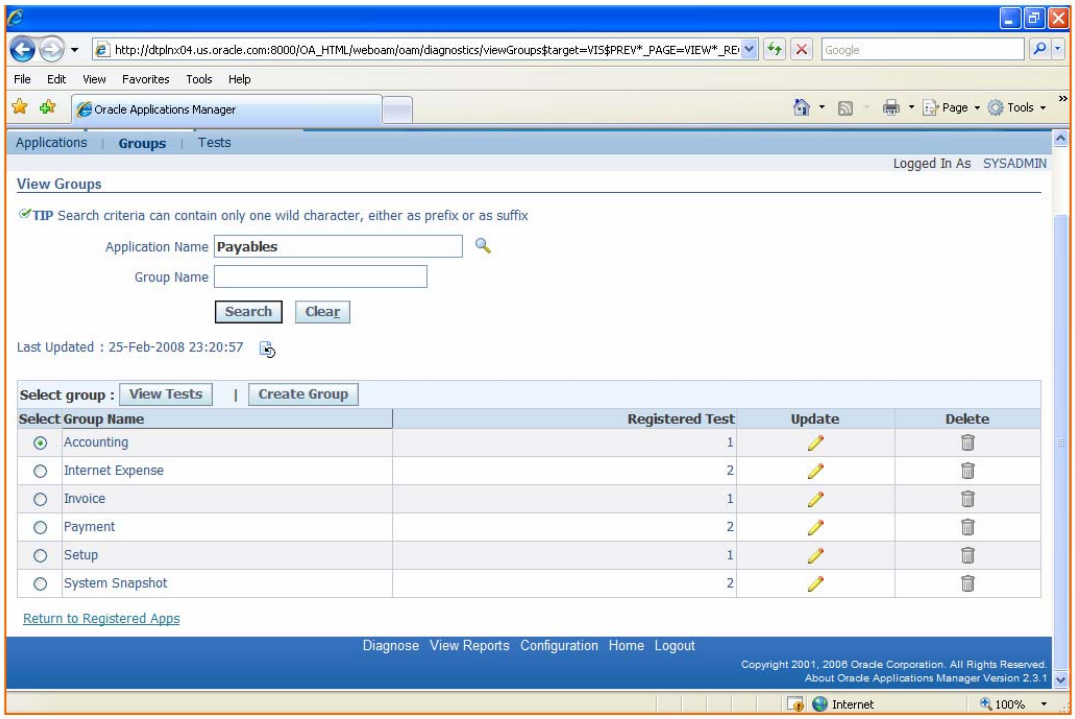

Figure 15

We select the Accounting test group and click on the Update icon in Figure 16. Figure 17 illustrates the sensitivity pull down menu where the sensitivity level may be toggled as desired.

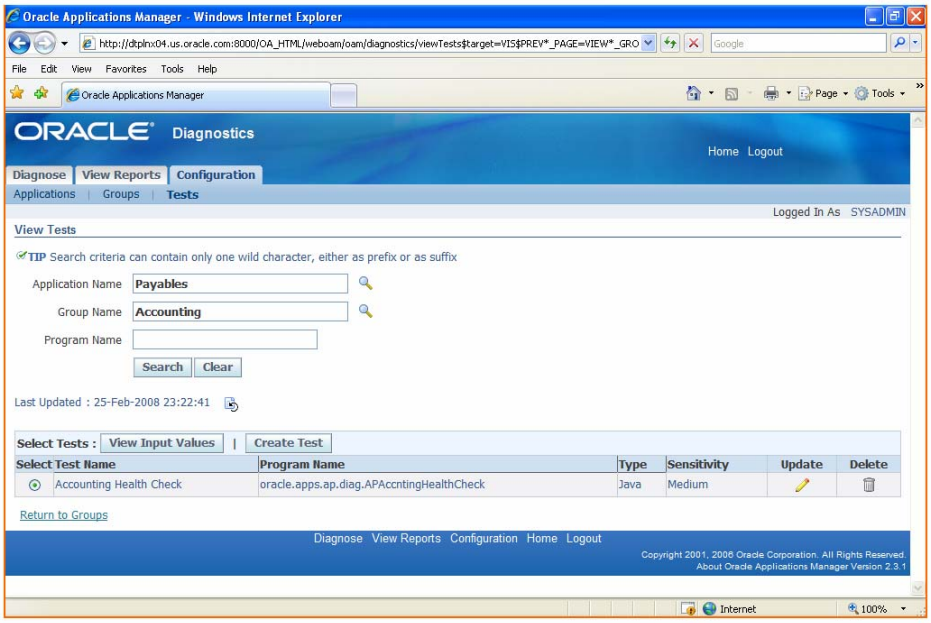

Figure 16

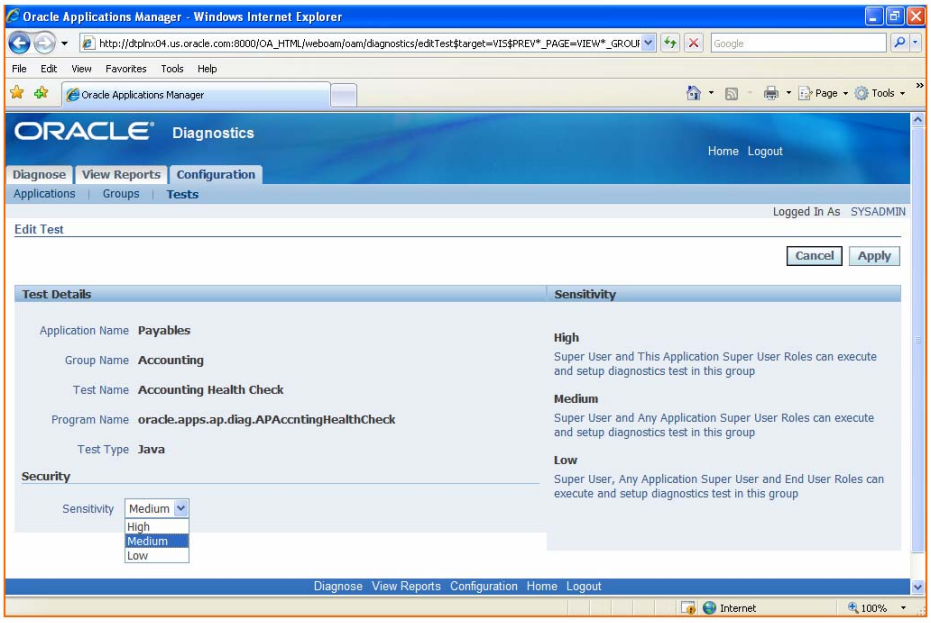

Figure 17

5. Test Execution

The login id, JOEI, assigned the custom responsibility "Custom Payables for XXAP" will be the user for the diagnostic test runs. Figure 18a is a view of the capabilities of this user as seen in the User Management responsibility. Figure 18b shows the responsibilities assigned. Note that this user is NOT assigned any of the seeded Payables responsibilities provided by Oracle. To run the tests, the responsibility, "Application Diagnostics" is selected with navigation to "Select Tests" in Figure 18c.

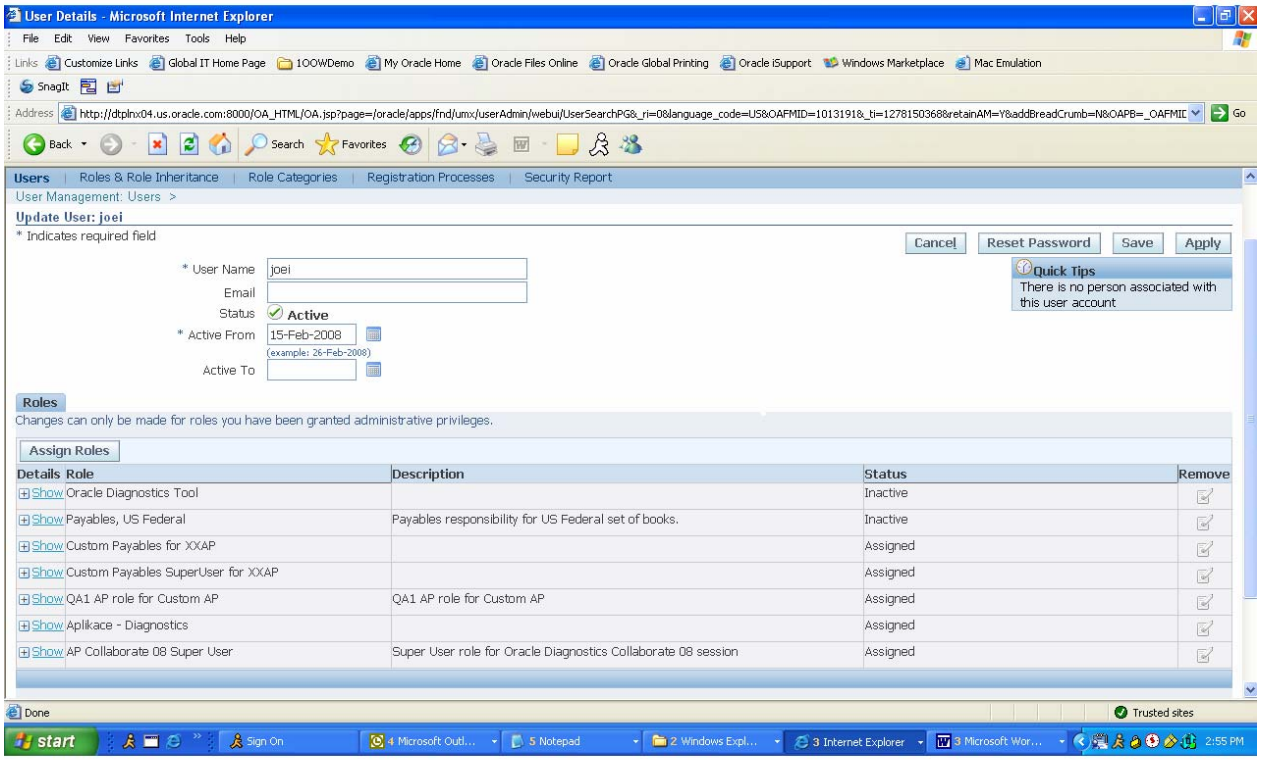

Figure 18a

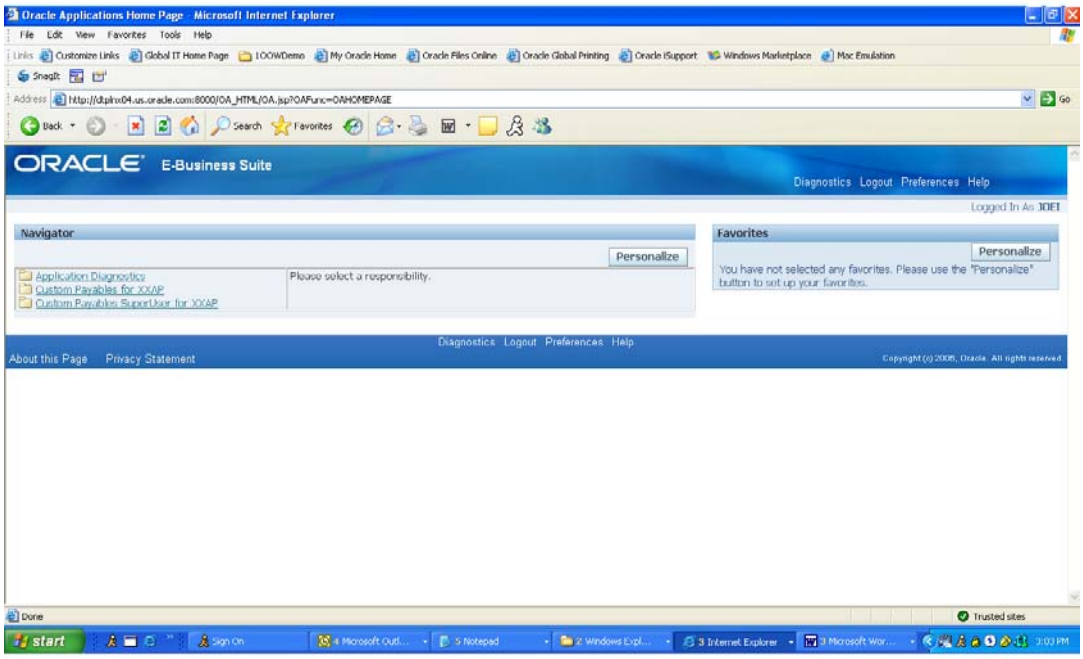

Figure 18b

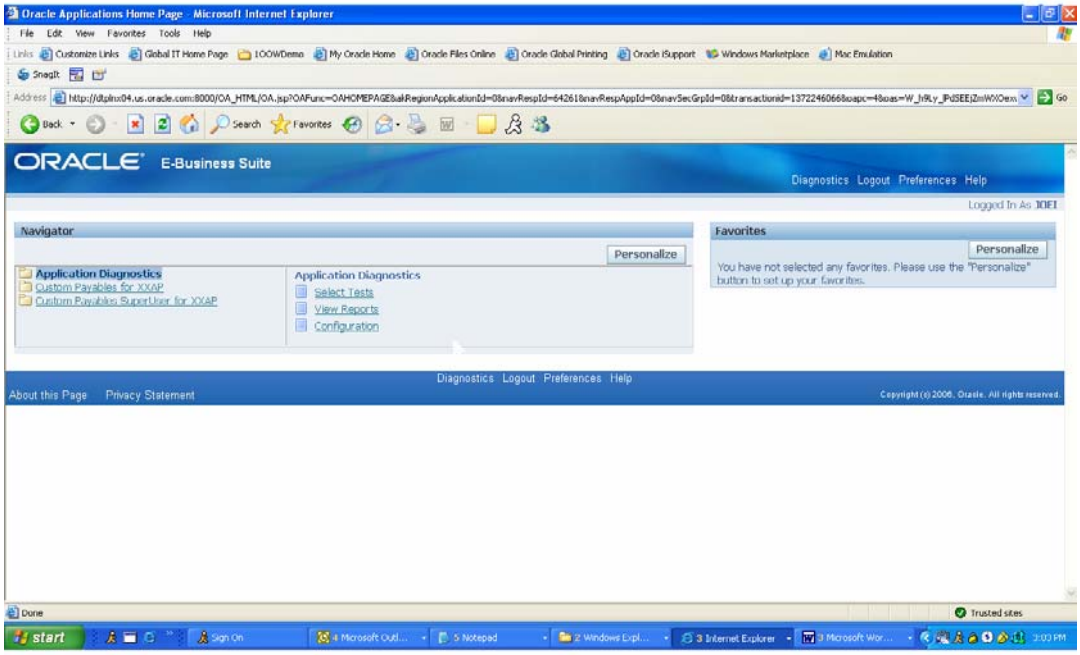

Figure 18c

In Figure 19, tests assigned to the Payables Applications are selected by the user id, JOEI. Because the sensitivity level (parameter 2) for SQLAP (parameter 1) for the diagnostic role, "AP Collaborate 08 Super User," in Figure 12b has been set to level 4, and JOEI has been assigned to this diagnostic role, this user is capable of executing all AP tests. This is indicated by the PLUS icons to the left of the various test groups (Accounting, Internet Expense, Invoice, Payment, Setup, and System Snapshot)

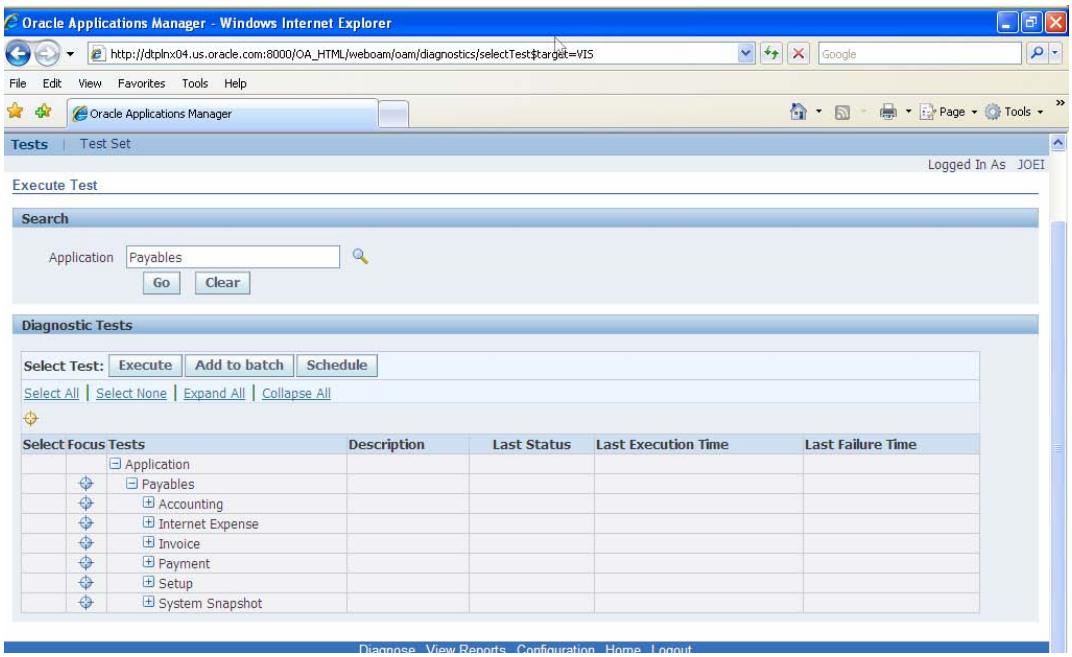

Figure 19

Now suppose that the user, JOEI, wishes to run tests in the Receivables product group. The user, JOEI does not have access to a diagnostic role or a responsibility related to this product group. Figure 20 is a view of the two tests within the Collections test group of the Receivables product group displayed by the SYSADMIN user. Note that the "Balance Forward Billing Data" and the "Statements" tests have sensitivities set to High and Medium, respectively. Also note that the update icons are "live." Figure 21 provides details about these two tests displayed by the SYSADMIN user.

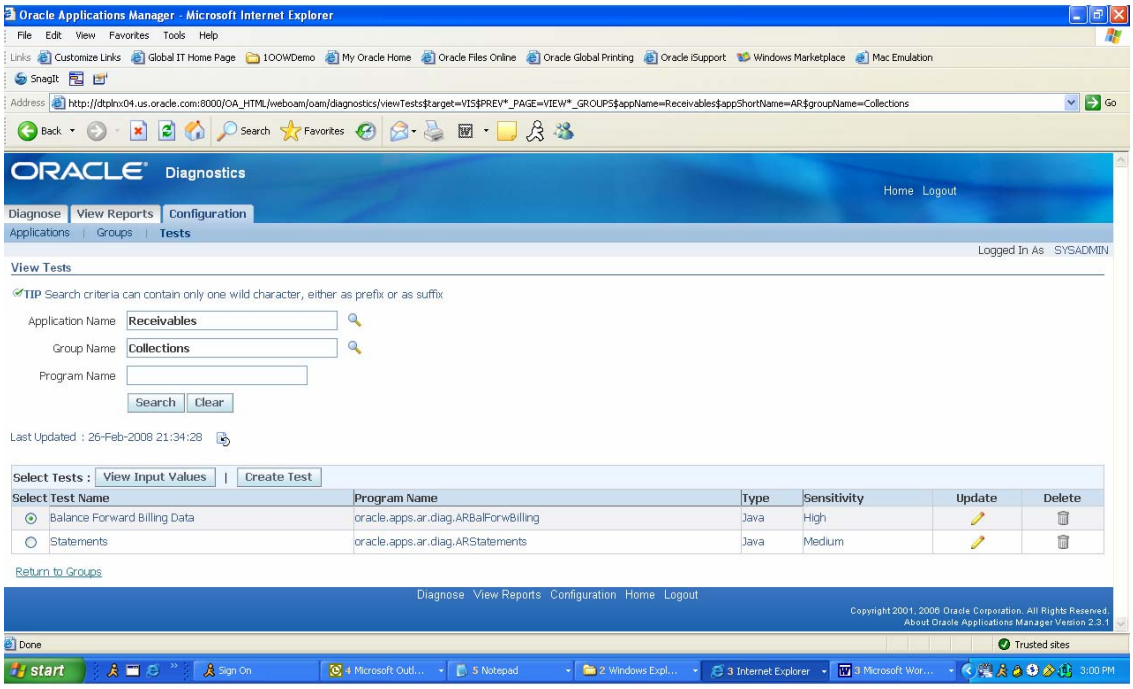
Oracle Applications Manager - Microsoft Internet Explorer
ORACLE Diagnostics
Home Logout
Diagnose View Reports Configuration
Applications Groups Tests
Logged In As SYSADMIN
View Tests
TIP Search criteria can contain only one wild character, either as prefix or as suffix
Application Name Receivables
Group Name Collections
Program Name
Search Clear
Last Updated : 26-Feb-2008 21:34:28
Select Tests : View Input Values | Create Test
Select Test Name
Program Name
Type
Sensitivity
Update
Delete
Balance Forward Billing Data
oracle.apps.ar.diag.ARBalForwBilling
Java
High
Statements
oracle.apps.ar.diag.ARStatements
Java
Medium
Return to Groups
Diagnose View Reports Configuration Home Logout
Copyright 2001, 2006 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1
Done
Trusted sites
start
3:00 PM

Figure 20

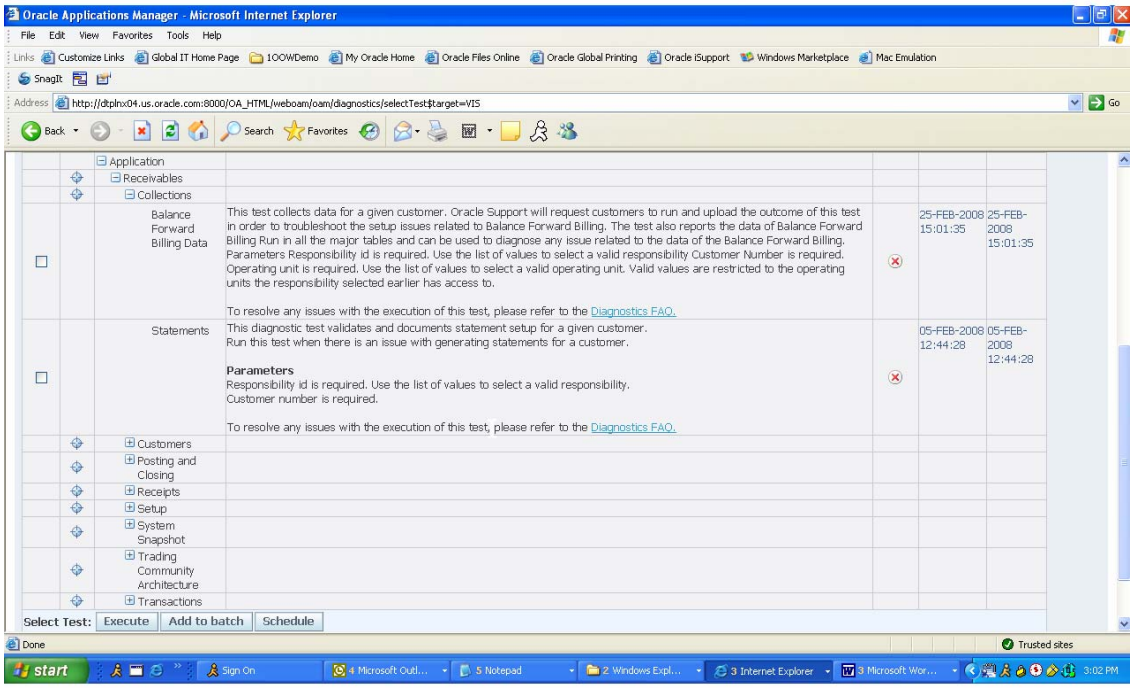
Oracle Applications Manager - Microsoft Internet Explorer
Application
Receivables
Collections
Balance Forward Billing Data
This test collects data for a given customer. Oracle Support will request customers to run and upload the outcome of this test in order to troubleshoot the setup issues related to Balance Forward Billing. The test also reports the data of Balance Forward Billing Run in all the major tables and can be used to diagnose any issue related to the data of the Balance Forward Billing. Parameters Responsibility id is required. Use the list of values to select a valid responsibility Customer Number is required. Operating unit is required. Use the list of values to select a valid operating unit. Valid values are restricted to the operating units the responsibility selected earlier has access to.
To resolve any issues with the execution of this test, please refer to the Diagnostics FAQ.
25-FEB-2008 15:01:35
25-FEB-2008 15:01:35
Statements
This diagnostic test validates and documents statement setup for a given customer.
Run this test when there is an issue with generating statements for a customer.
Parameters
Responsibility id is required. Use the list of values to select a valid responsibility.
Customer number is required.
To resolve any issues with the execution of this test, please refer to the Diagnostics FAQ.
05-FEB-2008 12:44:28
05-FEB-2008 12:44:28
Customers
Posting and Closing
Receipts
Setup
System Snapshot
Trading Community Architecture
Transactions
Select Test: Execute Add to batch Schedule
Done
Trusted sites
start
3:02 PM

Figure 21

If the user, JOEI accesses the Receivables product group, that user will not be able to expand the Collections test group (Figure 22). The icon to the left of the Collections appears as a minus. Figure 23 displayed by the user, JOEI is unable to modify the sensitivity of these tests as the Update icons are grayed out. However, Figure 22 indicates that JOE can expand the "Customers" test group containing one test, "Customer Data." The Configuration tab (Figure 24) illustrates that the Update icon is accessible to JOEI as well.

One might question why we would let JOEI update the sensitivity level of this Receivables test. Figure 25 presents the various capabilities inside the "AP Collaborate 08 Super User Permission Set." The "Diagnostics Setup Function" which is part of the role via this permission set, would have to be modified to prevent sensitivity level updates. These can be modified using the Functional Administrator responsibility. Oracle Development has indicated that this will not be the case in the formal rollout of Version 12.1 Diagnostics. Seeded tests will be locked down and grayed out so that end users will not be able to modify the sensitivity level of these tests. What's more, every administrator is aware that any modifications to Oracle seeded components have the chance of being lost during a subsequent patch installation.

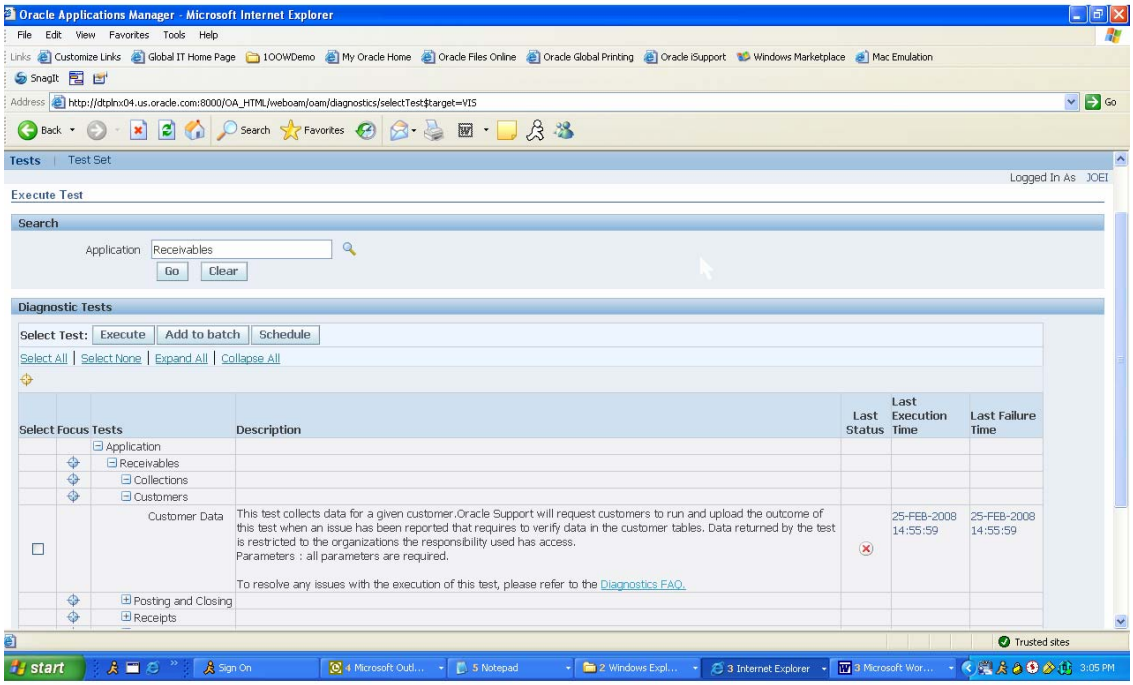

Figure 22

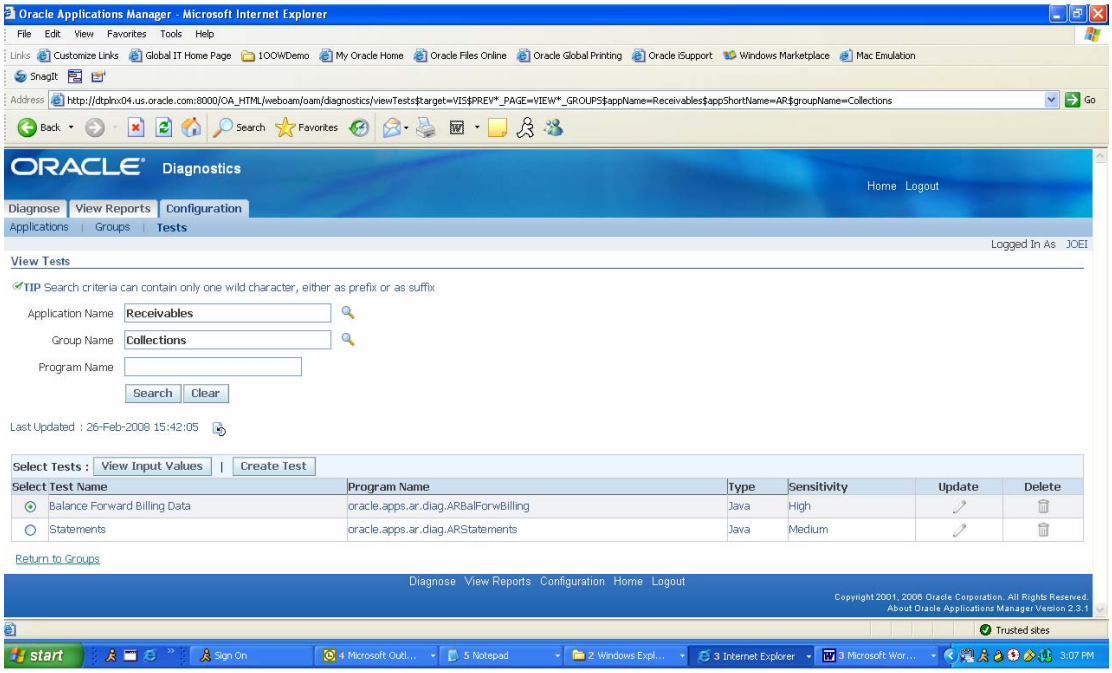

Figure 23

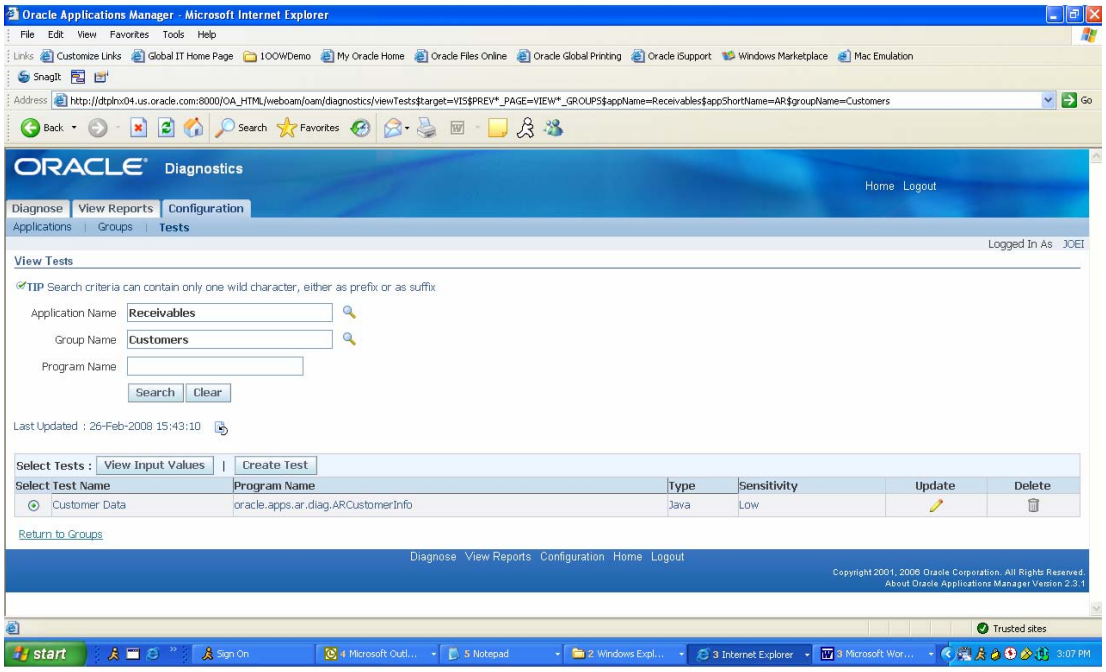

Figure 24

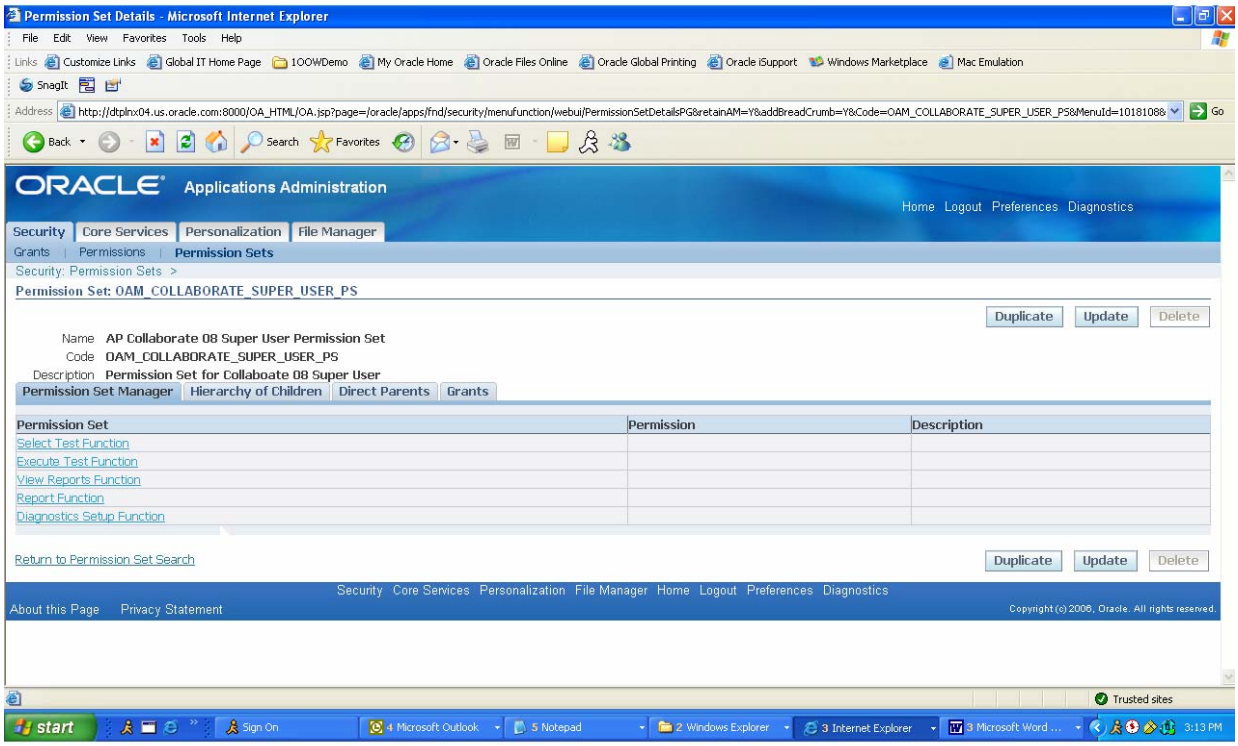

Figure 25

V. Concluding Remarks

Those utilizing Oracle Diagnostics in supported 11i and 12.0 releases of e-Business Suite currently do not have all of the functionality presented in this paper. The security model and functionality presented is currently undergoing quality assurance. One additional capability that has not been highlighted in this paper is the integration of Oracle Diagnostics with Business Intelligence (BI) Publisher to permit users to create reports in Excel, Word, HTML, Rich Text, or PDF formats.

The extension of the RBAC model to Oracle Diagnostics is another example of Oracle Corporation's commitment to standards based software development and implementation. The RBAC was introduced in 11i Oracle Diagnostics in January, 2007 but did not contain all of the detail and granularity presented in this paper. That implementation also did not provide for the running of tests by users assigned custom responsibilities in custom applications. The new model establishes sensitivity level definition at the test level rather then the test group level providing additional flexibility and control.

Because the Release 12.1 version of Oracle Diagnostics has not been officially released, the Collaborate 08 presentation of this paper will include generous time for a real time demonstration off new capability that could not be documented prior to the publication deadline.