Oracle® Enterprise Governance, Risk and Compliance

Installation Guide

Release 8.6.5.1000

Part No. E52268-04

June 2014

ORACLE

Oracle Enterprise Governance, Risk and Compliance Installation Guide

Part No. E52268-04

Primary Author: David Christie

Contents

Preface

This Preface introduces the guides and other information sources available to help you more effectively use Oracle Fusion Applications.

Disclaimer

The information contained in this document is intended to outline our general product direction and is for informational sharing purposes only, and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Other Information Sources

My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.

Oracle Enterprise Repository

Oracle Enterprise Repository provides visibility into service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production, and changes. In Oracle Fusion Applications, you can use the Oracle Enterprise Repository for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Publishing other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

The Oracle Fusion Applications information is provided as a solution pack that you can upload to your own deployment of Oracle Enterprise Repository. You can document and govern integration interface assets provided by Oracle with other assets in your environment in a common repository.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww@oracle.com. You can use the Send Feedback to Oracle link in the footer of Oracle Fusion Applications Help.

1

Introduction

Oracle Enterprise Governance, Risk and Compliance (GRC) is a set of products that regulate activity in business-management applications. This document provides instructions for the installation (or upgrade) of the following GRC products:

- Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) forms a documentary record of a company's strategy for addressing risk and complying with regulatory requirements.
- Oracle Advanced Controls enables users to create "models" and "continuous controls." Two Advanced Controls applications run from within the GRC platform:
  - In Oracle Enterprise Transaction Controls Governor (ETCG), models and controls specify circumstances under which individual transactions display evidence of error, fraud, or other risk.
  - In Oracle Application Access Controls Governor (AACG), models and controls define conflicts among duties that can be assigned in a company's applications, and identify users who have access to those conflicting duties.

    AACG can also implement "preventive analysis" — it can evaluate controls as duties are assigned to users of the company's applications, preventing them from gaining risky access.
- Oracle Fusion Application Access Controls Governor (FAACG) is a specialized installation of AACG that applies access models and controls in Oracle Fusion Applications. If you intend to run FAACG, see the most recent edition of the *Oracle Governance, Risk and Compliance Certifications Document* to determine whether GRC 8.6.5.1000 is certified for use with Fusion. If not, revert to the most recently certified version until version 8.6.5.1000 is ready.
- Oracle Fusion GRC Intelligence (GRCI) extracts data from GRC for display in dashboards and reports.

You can install GRC on its own, or to be integrated with an OID LDAP server that manages GRC users. (OID stands for Oracle Internet Directory; LDAP for Lightweight Directory Access Protocol.)

You can embed a GRCI instance within GRC. To use GRCI, install GRC first (see chapter 2). Then integrate GRCI with GRC (see chapter 3).

Prerequisites

GRC runs on a 64-bit Linux server. Be sure the following lines exist in the /etc/security/limits.conf file:

```
*    soft    nproc     8192
*    hard    nproc     32768
*    soft    nofile    65536
*    hard    nofile    131072
```

If you are installing on Solaris, set the following configuration parameter in /etc/system to protect against exploitation of buffer overflow attacks. (There is no need to do this for OEL or other Linux variations.)

```
noexec_user_stack = 1
```

The installation of Enterprise Governance, Risk and Compliance requires that the following also be installed on the server:

- Oracle database 11.2.0.3. See "Creating GRC and DA Schemas" (page 1-3).

  The GRC database can be one in which Real Application Clusters (RAC) is enabled. To deploy GRC on a RAC instance, install an Oracle 11.2.0.3 RAC database with Single Client Access Name (SCAN) mode on two or more nodes. Also complete procedures described in "Installing a Driver for RAC" (page 2-17) and "GRC Configuration" (page 2-17).

- Java: Oracle JDK 1.7 or higher. GRC must have its own dedicated Java container. It was not designed to coexist in a container with other web applications.

- Middleware: To support GRC, use WebLogic Server 12c (12.1.2) or Tomcat Application Server 7.0.47. If you use WebLogic Server (WLS), you also need Application Development Runtime (ADR) 12.1.2 and Repository Creation Utility (RCU) 12.1.2. In the 12c release, RCU is packaged with ADR.

  These middleware components are higher-versioned than those that supported earlier releases of GRC. If you are upgrading from an earlier GRC release, and if you do not use FAACG (see the "special case," below), you must reinstall middleware components.

  If you intend to run GRCI, you also need WLS 11g (10.3.6), installed with RCU 11.1.1.7 and ADR 11.1.1.7. This is true even if you use WLS 12c to support GRC itself.

  A special case: Only if you intend to run Fusion Application Access Controls Governor, install GRC with WebLogic 11g components — WLS 10.3.6, RCU 11.1.1.7, and Service Oriented Architecture (SOA) 11.1.1.7. (The use of SOA is not supported with any other implementation of GRC 8.6.5.1000.)

- An OID LDAP server, if you intend to install GRC so that its users are managed by such a server.

On the server or a client system, the following web browsers can display the GRC interface: Microsoft Internet Explorer 8.*x* or 9.*x* (with the Adobe SVG plugin available from http://www.adobe.com/svg/viewer/install/mainframed.html) or FireFox 24.

For details about supported components, see the *Oracle Enterprise Governance, Risk and Compliance Certifications Document*.

Creating GRC and DA Schemas

For a new installation, create a GRC schema in the Oracle database for use by GRC. If you intend also to install GRCI, create a second schema, known as the Data Analytics (DA) schema. (If you are upgrading from an earlier version of GRC, you will continue to use schemas already created for the earlier version.)

First, however, the database hosting the GRC schema must be set up to use the AL32UTF8 character set. This setup occurs during database installation, as an "advanced/custom" option. To test whether the database has been set up to use this character set, execute the following command on the database server:

```
SELECT value$ FROM sys.props$ WHERE name = 'NLS_CHARACTERSET' ;
```

The return value should be "AL32UTF8." If any other value is returned, you need to reinstall the database with the AL32UTF8 character set enabled.

The following is a sample script that serves for the creation of either the GRC or DA schema. You are assumed to have created tablespaces; each schema requires its own. (The database that supports the DA schema should also have an initial temporary tablespace of 100 GB with autoextend enabled.) The values you choose for tablespace name, user (schema) name, and password would be distinct for each schema, and are represented here by *TablespaceName*, *UserName*, and *UserPassword*, respectively. Each password must contain at least six characters.

```
create user UserName identified by UserPassword default
   tablespace TablespaceName quota unlimited on TablespaceName
   quota 0k on system;

grant connect, resource to UserName;
grant create any view to UserName;
grant create any table to UserName;
grant drop any table to UserName;
grant create synonym to UserName;
```

Run the following commands as the system user:

```
ALTER SYSTEM SET open_cursors=5000 scope=spfile;
ALTER SYSTEM SET processes=3000 scope=spfile;
ALTER SYSTEM SET deferred_segment_creation=FALSE scope=spfile;
```

After running these commands, bounce the database.

Once installation is complete, users will be able to use a set of Schema Import/Export fields (available in the Properties tab of a Manage Application Configurations page) to download the GRC schema, or to upload a copy of it. To set up this feature, create a DATA_PUMP_DIR directory, which provides temporary storage for schema-file copies.

In the following commands, use a SQL editor such as SQL*Plus. Once again, *UserName* represents the original GRC schema name; *dir* represents the path to a directory that will serve as your DATA_PUMP_DIR directory.

1. Create a directory object, and grant READ and WRITE access to it.

   ```
   CREATE DIRECTORY DATA_PUMP_DIR AS dir;
   GRANT READ, WRITE ON DIRECTORY DATA_PUMP_DIR TO UserName;
   ```

2. Ensure that UserName has EXP_FULL_DATABASE and IMP_FULL_DATABASE roles. For a list of roles within your security domain, enter the following:

   ```
   SELECT * FROM SESSION_ROLES;
   ```

3. If UserName does not have these roles, execute the following commands:

```
GRANT EXP_FULL_DATABASE, IMP_FULL_DATABASE TO UserName;
GRANT CREATE SESSION TO UserName;
GRANT CREATE TABLE TO UserName;
GRANT UNLIMITED TABLESPACE TO UserName;
```

4. Grant an additional permission, required for the import operation:

```
GRANT EXECUTE ON UTL_FILE TO UserName;
```

Before a schema file can be imported, an empty schema must be created for it, and a tablespace must be created for the schema. The script shown above may be used to create the schema. The following is an example of a script that creates a tablespace if the original GRC schema and its copy will reside in the same database. *UserCopy* is the name of the schema copy, *UserCopyPassword* is the password for that user, and *UserCopyTS* is the name of the tablespace.

```
CREATE USER UserCopy IDENTIFIED BY UserCopyPassword
DEFAULT TABLESPACE UserCopyTS QUOTA UNLIMITED ON UserCopyTS;
```

Also grant the following permissions:

```
GRANT READ,WRITE ON DIRECTORY DATA_PUMP_DIR TO UserCopy;
GRANT EXP_FULL_DATABASE,IMP_FULL_DATABASE TO UserCopy;
GRANT CREATE SESSION TO UserCopy;
GRANT CREATE TABLE TO UserCopy;
GRANT UNLIMITED TABLESPACE TO UserCopy;
GRANT EXECUTE ON UTL_FILE TO UserCopy;
```

Downloading Files

Create a staging directory on your GRC server. (Throughout this document, <*grc_stage*> represents the full path to this directory.)

To install or upgrade GRC, download a file called grc865_1616.zip to <grc_stage>, and extract its contents there. To validate your download, generate a checksum and compare it with a checksum value published in *Release Notes* for the instance you are installing. To generate a checksum, run the command *md5sum grc.ear*.

If you expect to use embedded GRCI, download files called grc865_1616_OBIEE_1of3.tar.gz, grc865_1616_OBIEE_2of3.tar.gz, and grc865_1616_ OBIEE_3of3.tar.gz to <grc_stage>. (You do not need these files for standalone GRCI, or if you are upgrading from an earlier version and already used embedded GRCI with that version.)

Regardless of whether you are performing a new installation or upgrading from an earlier GRC version, you must download and install middleware components appropriate for your installation (see “Prerequisites” on page 1-2). These are available on E-Delivery. (An exception: If you are upgrading a Fusion Application Access Controls Governor instance, you can reuse middleware components already installed for your earlier version.)

2

Installing or Upgrading GRC

You can install GRC 8.6.5.1000 independently of any past release. If you intend to do so, begin here. You can instead upgrade to GRC 8.6.5 from version 8.6.4.7000, 8.6.4.8500, or 8.6.4.8900. To do so, skip ahead to "GRC Upgrade" on page 2-29.

New GRC Installation

Do you intend to run FAACG? If so, you must complete an installation procedure that uses WebLogic components not supported in other GRC 8.6.5.1000 implementations. If not, decide whether you will use WebLogic or Tomcat. (WebLogic is required if you intend to embed GRCI in your GRC instance.)

Then complete the appropriate one of the following procedures. (Summary procedures appear here, with details given in later sections of this chapter.)

If you are installing **GRC on WebLogic and will not run FAACG**:

1. Ensure that two directories, for the storage of report and ETL data generated by GRC, are ready for use.
2. Install WebLogic Server 12c, along with Application Development Runtime (which includes Repository Creation Utility).
3. Create a WebLogic domain. This entails setting up an Administration Server.
4. If you intend to install GRC so that an OID LDAP repository manages its users, configure that repository.
5. Modify memory and other settings to conform to GRC requirements, and perform configuration steps in a WebLogic Server Administration Console.
6. Perform configuration steps in a GRC ConfigUI page.
7. Run WebLogic to complete the installation.

If you are installing **GRC on WebLogic to run FAACG**:

1. Ensure that two directories, for the storage of report and ETL data generated by GRC, are ready for use.
2. Install WebLogic Server 11g, along with Repository Creation Utility and Service Oriented Architecture.

3. Create a WebLogic domain. This entails setting up an Administration Server and a "managed server" for SOA. Within the domain, install "SOA composites" and "keystores," set up security credentials, enable "embedded LDAP," and create a soaadmin user.
4. If you intend to install GRC so that an OID LDAP repository manages its users, configure that repository.
5. Modify memory and other settings to conform to GRC requirements, and perform configuration steps in a WebLogic Server Administration Console.
6. Perform configuration steps in a GRC ConfigUI page.
7. Run WebLogic to complete the installation.

If you are installing **GRC with Tomcat**:

1. Ensure that two directories, for the storage of report and ETL data generated by GRC, are ready for use.
2. Install Tomcat (as instructed in its documentation). On the GRC server, modify Tomcat memory settings, and run a Tomcat setup script provided with GRC.
3. Perform configuration steps in a GRC ConfigUI page.
4. Run Tomcat to complete the installation.

Creating GRC Repositories

Create two "repositories" — directories that store data generated by GRC. A report repository stores copies of GRC reports that users schedule to be run. A second repository stores synchronization data used for transaction analysis. Each can reside on an NFS mount or any valid directory to which the user running WebLogic or Tomcat has full permissions.

Note the paths to the repositories, as you will need to supply them later as configuration values.

Setting Up WebLogic

If you will use WebLogic, install WebLogic Server (WLS) and related components. You will need to make choices that support their use with GRC. Complete procedures, documented from here to page 2-16, that are appropriate to the installation you are performing. Then skip "Setting Up Tomcat Application Server." If your GRC database supports RAC, continue at "Installing a Driver for RAC" (page 2-17), or if it does not, continue at "GRC Configuration" (page 2-17).

If, instead, you intend to use Tomcat, skip ahead to "Setting Up Tomcat Application Server" on page 2-16.

Initial WebLogic Installation

Ensure that Oracle JDK 1.7 is in the path to install and run WebLogic Server.

Install WLS 12c as a standard default deployment if you do *not* intend to run FAACG. Also install ADR 12c, which includes RCU 12c. Consult WebLogic documentation for detailed procedures.

Once ADR 12c is installed, run RCU to create WebLogic repositories. Required RCU components include AS Common Schemas and all its subcomponents. As you run RCU, expand AS Common Schemas and verify that all subcomponents are selected.

Install WLS 11g as a standard default deployment in either of the following cases:

- You want to embed an instance of GRCI within GRC. Also install RCU 11g and ADR 11g. Install these in addition to any WebLogic 12c components you install to support GRC itself; you will have two independent WebLogic instances.
- You are installing GRC to run FAACG. In this case, do not install WebLogic 12c components.

Only if you intend to run FAACG, complete these procedures after installing WLS 11g:

1. Install Repository Creation Utility (RCU). These RCU components are required:
   - Metadata Services (MDS schema)
   - SOA Infrastructure (SOAINFRA schema)
   - Business Activity Monitoring (ORABAM schema)
   - User Messaging Service (ORASDPM schema)
2. Once RCU is installed, run it to install SOA schemas:
   a. Set an XEDB environment variable to provide connection information for your GRC database. Enter the following:

      ```
      export XEDB=Dbhost:Dbport:SID
      ```

      Replace *Dbhost* with the fully qualified domain name (FQDN) of your GRC database server, *Dbport* with the port number at which the database communicates with other applications, and *SID* with the service identifier value configured for the database in the tnsnames.ora file.

   b. Use the createRepository option in RCU to create repositories. Navigate to <RCU_HOME>/bin (in which <RCU_HOME> represents the highest-level directory in which RCU components exist). Then execute this command:

      ```
      ./rcu -silent -createRepository -connectString $XEDB
      -dbUser sys -dbRole sysdba -lockSchemas false
      -schemaPrefix EGRCM -component SOAINFRA -component MDS
      -component ORASDPM -component BAM
      ```

      As you run the script, you will be prompted to create passwords for each of SOAINFRA, MDS, ORASDPM, and BAM.
3. Install Oracle SOA Suite. Enter the value “soa” as the Oracle Home Directory on the Specify Installation Location screen.

Creating a WebLogic Domain

For any installation, create a new WebLogic domain. To do so, execute the following command to run a Fusion Middleware Configuration Wizard:

```
<MW_HOME>/wlserver/common/bin/config.sh
```

Note: <*MW_HOME*> represents the full path to the home directory of a given (12c or 11g) middleware installation — the highest-level directory in which Fusion Middle-

ware components exist, including WebLogic. Also, <*grc_domain*> represents the name you give to the domain you create for a given WebLogic instance, 12c (for use by GRC) or 11g (for use by GRCI or FAACG).

For a WebLogic 12c installation, the Wizard prompts you to select a domain location, select templates, create a domain name, create a name and password for an "administration account," and complete other steps. In most cases, you should consult WebLogic documentation to understand your options, and are free to make configuration decisions that suit your preferences. However, note the following:

- Select these four templates:

  Basic WebLogic Server Domain — 12.1.2.0 [wlserver]
  Oracle Enterprise Manager — 12.1.2.0 [em]
  Oracle JRF — 12.1.2.0 [oracle_common]
  WebLogic Coherence Cluster Extension — 12.1.2.0 [wlserver]

- When prompted, select "Production" for your Domain Mode, and ensure that the correct JDK is selected. (This is the JDK instance you confirmed to be in the path to install and run WebLogic under "Initial WebLogic Installation" on page 2-2.) If necessary, use the "Other JDK Location" option to browse.
- When prompted, choose to create an Administration Server. You need not create any managed servers.

For a WebLogic 11g installation, complete these steps:

1. Select templates.

   One template is selected automatically: "Base WebLogic Server Domain — 10.3.6.0." Also select "Oracle Enterprise Manager — 11.1.1.0." When you do, a third template, "Oracle JRF — 11.1.1.0," is selected with it.

   Only if you intend to run FAACG, select three more templates: "Oracle SOA Suite — 11.1.1.0," "Oracle WSM Policy Manager — 11.1.1.0," and "Oracle JRF Webservices Asynchronous Services — 11.1.1.0."

2. Create a name for your WebLogic domain. Use any name you wish. Accept default values in two other fields — Domain Location and Application Location.
3. At a Configure Administrator Username Password prompt, create a WebLogic Server username and password.
4. At a Configure Server Start Mode and JDK prompt, select "Production Mode." In the JDK Selection area, ensure that the correct JDK is selected. (This is the JDK instance you confirmed to be in the path to install and run WebLogic under "Initial WebLogic Installation" on page 2-2.) If necessary, use the "Other JDK" option to browse.
5. Only if you intend to run FAACG, respond to a Configure JDBC Component Schema prompt. Enter details you've already established as you used RCU to create repositories (see step 2b of "Initial WebLogic Installation" on page 2-3). When you complete this step, you should see the value "Test Successful" at a Test Component Schema prompt. If you do not intend to run FAACG, skip this step.
6. For any installation, select "Administration Server" at a Select Optional Configuration prompt.

Only if you intend to run FAACG, also select "Managed Servers, Clusters and Machines."

7. At a Configure the Administration Server prompt, enter the IP address of the machine running the WebLogic Server. Also select an unused port for it.
8. Only if you intend to run FAACG, a Configure Managed Servers prompt appears. Click the Add button. In the row that appears, enter a name for the GRC server and the IP address of the machine running the WebLogic Server. Then continue at step 9.

   If you are installing WebLogic 11g to support GRCI you need not create a managed server. The Configure Managed Servers page and several other Configuration Wizard pages do not appear. Skip ahead to step 12.
9. Skip the Configure Clusters page.
10. In a Configure Machines page, select the Unix Machine tab. Click Add. Assign any name, and accept defaults for all other fields.
11. In the Assign Servers to Machines page, select the servers listed in the left box. Move them to machine you created in step 10, which is listed in the right box.
12. In the Summary page, select Create.

Preparing Additional Files

Complete these additional steps when the config.sh script finishes running:

1. Copy files. The source directory is <MW_HOME>/oracle_common/modules/oracle.adf.model_12.1.2 (if you use WLS 12c) or <MW_HOME>/oracle_common/modules/oracle.adf.model_11.1.1 (if you use WLS 11g). The destination directory is <MW_HOME>/user_projects/domains/<grc_domain>/lib. The files to copy are:
   - adfm.jar
   - adfdt_common.jar
   - adfmweb.jar
2. Copy the following files from <grc_stage>/lib to <MW_HOME>/user_projects/domains/<grc_domain>/lib:
   - groovy-all-2.0.5.jar if you use WLS 12c, or groovy-all-1.6.3.jar if you use WLS 11g
   - xdoparser-10.1.3.4.jar
3. Only if you intend to run FAACG, invoke the WebLogic scripting tool — wlst.sh — from <MW_HOME>/oracle_common/common/bin. Use it to apply the JRF template to the GRC managed server you created as you set up a WebLogic domain (<*grc_server*> in the following example):

   ```
   applyJRF('<grc_server>','<MW_HOME>/user_projects/domains/<grc_domain>')
   ```

   If you do not intend to run FAACG, skip this step.
4. Create a directory called grc865 (for example, <MW_HOME>/grc865). This directory should be entirely distinct from the <grc_stage> directory you created as you downloaded GRC files.

5. Navigate to <grc_stage>/dist, and locate the file grc.ear. Extract its contents to the grc865 directory.
6. Only if you have installed WebLogic 11g to support FAACG, copy <grc_stage>/dist/weblogic.xml_WLS11 to grc865/grc/WEBINF/weblogic.xml.

In addition, as you complete GRC installation procedures, you will use scripts named startWeblogic.sh and stopWeblogic.sh to start and stop the WebLogic Administration Server. First, edit the stopWeblogic.sh file as follows:

1. Open <MW_HOME>/user_projects/domains/<grc_domain>/bin/stopWeblogic.sh in a text editor.
2. Locate a line in the file similar to the following:

```
echo "shutdown('${SERVER_NAME}','Server',
ignoreSessions='true')"
>>"shutdown.py"
```

3. Edit this line to include a *force='true'* parameter:

```
echo "shutdown('${SERVER_NAME}','Server', force='true',
ignoreSessions='true')"
>>"shutdown.py"
```

4. Save and close the file.

Whenever you run the stopWeblogic.sh script, wait 30 seconds for all processes to terminate.

Configuring External OID LDAP

This section applies to you only if you intend to install GRC so that an external OID LDAP repository manages its users. If so, complete the following steps. If not, skip ahead to one of the following sections: "Installing SOA Composites" (page 2-9) if you have installed WebLogic 11g to support FAACG, or "Modifying Settings" (page 2-14) if you have installed WebLogic 12c, or WebLogic 11g to support GRCI.

1. Log in to the WebLogic Server Administration Console:

   `http://host:port/console`

   In this URL, replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.
2. Click on the "Security Realms" link in your application's Security Settings.
3. Click on the "myrealm" link in the table.
4. Click on the "Providers" tab.
5. Click on the New button and enter the following values:
   - Name: OIDAuthenticator
   - Type: OracleInternetDirectoryAuthenticator
6. Click on the "OIDAuthenticator" link and then click on the "Provider Specific" tab.
7. Supply values for properties in the "Provider Specific" screen. (Italicized entries are literal values, to be entered as they are shown.)
   - Host: The FQDN of the LDAP provider (your OID instance).

- Port: The port number at which the host communicates with other applications.
- Principal: The username for the OID administrative user, preceded by *cn=*.
- Credential: The password configured for the OID administrative user.
- Confirm Credential: The password configured for the OID administrative user.
- SSLEnabled: Leave this box unchecked.
- User Base DN: The LDAP path to the store for user information. For example: cn=FusionUsers,cn=users,dc=us,dc=oracle,dc=com
- All Users Filter*: (&(cn=*)(objectclass=person))* or *(&(uid=*)(objectclass=person)),* depending on your configuration. If you intend to run FAACG, you must select the "uid" value.
- User From Name Filter: *(&(cn=%u)(objectclass=person))* or *(&(uid=%u)(objectclass=person)),* depending on your configuration. If you intend to run FAACG, you must select the "uid" value.
- User Search Scope: *subtree*
- User Name Attribute: *cn* or *uid*, depending on your configuration. If you intend to run FAACG, you must select the "uid" value.
- User Object Class: *person*
- Use Retrieved User Name as Principal: Select this checkbox.
- Group Base DN: The LDAP path to the store for group (enterprise role) information. For example: cn=FusionGroups,cn=groups,dc=us,dc=oracle, dc=com
- All Groups Filter: *(&(cn=*)(|(objectclass=groupofUniqueNames) (objectclass=orcldynamicgroup)))*
- Group From Name Filter: *(|(&(cn=%g)(objectclass=groupofUniqueNames)) (&(cn=%g)(objectclass=orcldynamicgroup)))*
- Group Search Scope: *subtree*
- Group Membership Searching: *unlimited*
- Static Group Name Attribute: *cn*
- Static Group Object Class: *groupofuniquenames*
- Static Member DN Attribute: *uniquemember*
- Static Group DN from Member DN filter: *(&(uniquemember=%M)(objectclass= groupofuniquenames))*
- Dynamic Group Name Attribute: *cn*
- Dynamic Group Object Class: *orcldynamicgroup*
- Dynamic Member URL Attribute: *labeleduri*
- User Dynamic Group DN Attribute: Leave this field blank.
- Connection Pool Size: *6*
- Connect Timeout: *0*
- Connection Retry Limit: *1*

- Parallel Connect Delay: *0*
- Results Time Limit: *0*
- Keep Alive Enabled: Leave this box unchecked.
- Follow Referrals: Select this checkbox.
- Bind Anonymously On Referrals: Leave this box unchecked.
- Propagate Cause For Login Exception: Leave this box unchecked.
- Cache Enabled: Select this checkbox.
- Cache Size: *32*
- Cache TTL: *60*
- GUID Attribute: *orclguid*

8. Save your settings, then click on "Activate Changes" on the left, topmost panel.
9. Click the "OIDAuthenticator" link from the authenticator list, and set the Control Flag to SUFFICIENT.
10. Click the "DefaultAuthenticator" link from the authenticator list, and set the Control Flag to SUFFICIENT.
11. Click the Reorder button. Select "OIDAuthenticator" from the available providers, and move it to the top. To do so, click on the arrow on the right side, then click OK.
12. Click on "Activate Changes" from the Change Center, then log out.
13. Stop the WebLogic Administration Server and, if one is installed, the SOA Server.
14. Edit boot.properties files. There are two possibilities:
    - GRC, OID LDAP, and (if applicable to you) SOA components exist on one instance of WebLogic Server (WLS). If so, up to two boot.properties files may exist, one for the Administration Server and (if you use SOA) one for the SOA Server.

      In this case, edit each file to set a *username* value equal to your OID administrative user name — the "Principal" in step 7 of this procedure, without the *cn=* prefix. Set a *password* value equal to that user's password — the "Credentials" value in step 7 of this procedure.
    - GRC and OID LDAP exist on distinct instances of WLS. If so, SOA may be installed on either WLS instance (only if you intend to run FAACG) or is not installed at all. In this case, two or three boot.properties files exist, for the GRC Administration Server on the GRC instance of WLS, for the OID Administration Server on the OID LDAP instance of WLS, and (if you use SOA) the SOA Server on either WLS instance.

      In this case, edit boot.properties files on the OID LDAP instance of WLS to set the *username* and *password* values equal to those for the OID administrative user (as defined earlier in this step). Edit boot.properties files on the GRC instance of WLS to set the *username* and *password* values to those you created as you set up a WebLogic domain (page 2-3).

The boot.properties files exist in these locations:

- For the Administration Server, navigate to <MW_HOME>/user_projects/domains/<grc_domain>/servers/AdminServer/security/boot.properties
- For the SOA Server (if you have installed one), navigate to <MW_HOME>/user_projects/domains/<grc_domain>/servers/<SoaServerName>/security/ boot.properties

15. Start the Administration Server and (if one exists) SOA Server. Check whether LDAP is configured successfully: Log in to the WebLogic console (see step 1of this procedure), go to Security Realms → myRealm, and click on Users and Groups. You should see your LDAP users and groups.

Installing SOA Composites

Only if you intend to run FAACG, create "SOA composites." (If you do not intend to run FAACG, this does not apply; skip ahead to "Modifying Settings" on page 2-14.) In broad terms, deploy two composite files, sca_grccomposite.jar and sca_grcclientcomposite.jar. In the process of deploying the second of these, you will also deploy a GRC client ear file.

First, complete preliminary steps:

1. Ensure that the Administration Server and SOA Server are running. (The latter is the managed server created for your WebLogic domain.)
2. Create a temporary folder. (Throughout this section, <*temp*> represents the full path to this folder.)
3. Locate the file grc-soa-composite-8.6.5.1-SNAPSHOT-package.zip in <grc_stage>/dist/soa. Extract its contents in <temp>.

Next, deploy sca_grccomposite.jar:

1. Access Enterprise Manager (EM) at:

   `http://host:port/em`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.
2. From the left navigator and under your domain, expand SOA and right-click on soa-infra.
3. Select SOA Deployment → Deploy.
4. Under the Archive or Exploded Directory section, select the radio button for *Archive on the server where Enterprise Manager is running* and enter <temp>/sca_grccomposite.jar. Under Configuration Plan, select *No external configuration plan*. Then click Next.
5. On the Select Target page, select the partition in which to deploy this SOA composite application. Partitions enable you to group SOA composite applications logically into separate sections. Even if only one partition is available, you must explicitly select it. A partition named default is automatically included with Oracle SOA Suite.

   If you want to deploy to a partition that does not exist or if the server contains no partition, exit the wizard and create the partition before deploying the com-

posite. You can create partitions in the Manage Partition page, accessible from the SOA Infrastructure menu.

6. Review your selections on the Confirmation page, and select to deploy the SOA composite as the default revision. The default revision is instantiated when a new request comes in.
7. Click Deploy. Processing messages are displayed.

When deployment has completed, the home page of the newly deployed composite revision appears automatically. A confirmation message at the top of the page tells you that the composite has been deployed successfully.

Next, deploy the GRC client ear:

1. Create a new directory called grc-client-865. Locate the file grc-client-8.6.5.1-SNAPSHOT.ear in <grc_stage>/dist/soa, and extract its contents in the grc-client-865 directory.
2. Open the WebLogic Server Administration Console:

   `http://host:port/console`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.
3. In the Change Center panel, click Lock & Edit.
4. In the Domain Structure panel, click on Deployments.
5. In the Summary of Deployments panel, select the Control tab.
6. In the Summary of Deployments panel, click on the Install button.
7. In the path field of the Install Application Assistant panel, enter the full path to the grc-client-865 directory you created in step 1. Select grc-client-865 (open directory) under Current Location.
8. In the Install Application Assistant panel, press Next.
9. In the Install Application Assistant panel, choose *Install this deployment as an application* in the Choose Targeting Style section. Click Next. Then select the Administration Server if your SOA Server exists on the same domain as your Administration Server. (You are not presented with an opportunity to select a server here if your Administration Server is the only server on your domain.)
10. In the Install Application Assistant panel, choose *I will make this deployment accessible from the following location* in the Source Accessibility section. Accept all other defaults.
11. In the Install Application Assistant panel, select Finish.
12. In the Install Application Assistant panel, select Save, then Activate Changes. On the Deployment screen, the status of the grc-client-865 is Prepared.
13. Select the grc-client-865 application. Click Start, select *Servicing all requests*, and wait until the application status changes to Active.

Finally, deploy sca_grcclientcomposite.jar:

1. Go to <temp> and open the file grcclient-composite_cfgpla.xml for editing.
2. Replace all instances of *SoaServerHostName* with the FQDN of the WebLogic Administration Server in which you deployed the grc-client ear in the previous procedure.
3. Replace all instance of *PortNo* with the port number of the Administration Server in which you deployed the grc-client ear in the previous procedure.
4. Access Enterprise Manager (EM) at:

   `http://host:port/em`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.
5. From the left navigator and under your domain, expand SOA and right-click on soa-infra.
6. Select SOA Deployment → Deploy.
7. Under Archive or Exploded Directory, select the radio button for *Archive on the server where Enterprise Manager is running*. Enter <temp>/sca_grcclientcomposite.jar. Under Configuration Plan, select *Configuration plan is on the server where Enterprise Manager is running*, and enter <temp>/grcclient-composite-cfgplan.xml. Then click Next.
8. On the Select Target page, select the partition in which to deploy this SOA composite application. Even if only one partition is available, you must explicitly select it. A partition named default is automatically included with Oracle SOA Suite.
9. Review your selections on the Confirmation page, and select to deploy the SOA composite as the default revision. The default revision is instantiated when a new request comes in.
10. Click Deploy. Processing messages are displayed.

When deployment has completed, the home page of the newly deployed composite revision appears automatically. A confirmation message at the top of the page tells you that the composite has been deployed successfully.

If you need to deploy composites again at a later point, first undeploy composites, then use the procedure defined above to deploy again. To undeploy composites:

1. Log on to Enterprise Manager (see step 4 above).
2. From the left navigator and under your domain, expand SOA and right-click on soa-infra.
3. Select SOA Deployment → Undeploy.
4. Click Undeploy.

Creating Keystores

Only if you intend to run FAACG, create “keystores” once SOA composites exist. (If you do not intend to run FAACG, this does not apply; skip ahead to “Modifying Settings” on page 2-14.)

1. Stop the SOA Server and the Administration Server.

2. Use keytool to set up your keystore. (Keytool is located in <Java_Home>/bin, where <Java_Home> represents the highest-level directory in which Java components are installed.) Execute the following command:

   ```
   ./keytool -genkeypair -alias orakey -keyalg "RSA" -keystore
   default-keystore.jks -validity 3600
   ```

3. When prompted, designate a keystore password and a key password. This creates a keystore called default-keystore.jks, and a key pair with the alias orakey within that keystore.

4. Move the new keystore to a directory called fmwconfig. Execute this command:

   ```
   mv default-keystore.jks
   <MW_HOME>/user_projects/domains/<grc_domain>/config/fmwconfig
   ```

   This overwrites a pre-existing default-keystore.jks file.

5. Start the Administration Server and the SOA Server.

Setting Up Credentials

Only if you intend to run FAACG, use Enterprise Manager (EM) to set up credentials once keystores are created. (If you do not intend to run FAACG, this does not apply; skip ahead to "Modifying Settings" on page 2-14.)

1. Access EM at

   `http://host:port/em`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.

2. Click on WebLogic Domain → <grc_domain>.

3. Right-click on the <grc_domain> and select Security → Credentials.

4. On the Credentials page, click on the button labeled + *Create Map*. Enter *oracle.wsm.security* as Map Name, and click OK. A new row, oracle.wsm.security, is created.

5. Add keys to the wallet. For each key, click the button labeled + *Create Key*, then supply the following values in response to prompts:

   - basic.credentials (this contains user authentication)
     - Select Map: oracle.wsm.security
     - Key: basic.credentials
     - Type: Password
     - Username: weblogic
     - Password: weblogic
     - Description: User credentials key
   - keystore-csf-key
     - Select Map: oracle.wsm.security
     - Key: keystore-csf-key

  - Type: Password
  - Username: owsm
  - Password: Enter the keystore password you created in step 3 of "Creating Keystores" (page 2-11).
  - Description: Keystore key
- enc-csf-key
  - Select Map: oracle.wsm.security
  - Key: enc-csf-key
  - Type: Password
  - Username: orakey
  - Password: Enter the key password you created in step 3 of "Creating Keystores" (page 2-11).
  - Description: Encryption key
- sign-csf-key
  - Select Map: oracle.wsm.security
  - Key: sign-csf-key
  - Type: Password
  - Username: orakey
  - Password: Enter the key password you created in step 3 of "Creating Keystores" (page 2-11).
  - Description: Signing key

When you finish creating credentials, your domain should be running with at least the Administration Server and SOA Server.

Creating the SOA Admin User and Enabling Embedded LDAP

Only if you intend to run FAACG, create a user called *soaadmin* and enable Embedded LDAP. (If you do not intend to run FAACG, this does not apply; skip ahead to "Modifying Settings" on page 2-14.)

1. Shut down the SOA Server.
2. Log in to the WebLogic Server Administration Console at

   `http://host:port/console`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.
3. Click on Security Realms, then myrealm. Click Users and Groups. Click New, and enter *soaadmin* in the Name field. Add a description. Accept "Default Authenticator." Enter a password of your choice in the Password field, and the same value in the Confirm Password field. Click Save.

4. Click on the soaadmin user. Click on the Groups tab, and move the value *Administrators* from Available to Chosen. Then save your settings.
5. Click on <grc_domain>. Click the Security tab, then Embedded LDAP. Enter any value for Credential, and then the same value for Confirm Credential.
6. Stop the Administration Server.

Modifying Settings

For any installation, modify settings in a file called setDomainEnv.sh, which is located in the <MW_HOME>/user_projects/domains/<grc_domain>/bin directory.

1. Stop the SOA Server (if you are installing GRC to run FAACG) and the Administration Server.
2. Navigate to setDomainEnv.sh and open it in a text editor.
3. In the file, locate the following lines:

```
# IF USER_MEM_ARGS the environment variable is set, use it
to override ALL MEM_ARGS values
if [ "${USER_MEM_ARGS}" != "" ] ; then
```

Insert the following lines between those two lines:

```
case "${SERVER_NAME}" in
"AdminServer")
  USER_MEM_ARGS="-Xms4g -Xmx16g"
;;
"bi_server1")
  USER_MEM_ARGS="-Xms2g -Xmx8g"
;;
"soa_server1")
  USER_MEM_ARGS="-Xms2g -Xmx4g"
;;
"sample_server1")
  USER_MEM_ARGS="-Xms4g -Xmx16g"
;;
"sample_server2")
  USER_MEM_ARGS="-Xms4g -Xmx16g"
;;
*)
  echo "Unknown Server Detected!!. Memory set as Xms1g
Xmx2g.";
USER_MEM_ARGS="-Xms1g -Xmx2g"
;;
esac
USER_MEM_ARGS="${USER_MEM_ARGS} -XX:PermSize=256m
-XX:MaxPermSize=512m -XX:ReservedCodeCacheSize=128M
-Djava.awt.headless=true -Djbo.ampool.maxpoolsize=600000
-Dfile.encoding=UTF-8
-Djavax.xml.bind.context.factory=com.sun.xml.internal.bind.
v2.ContextFactory"
```

Replace “placeholder” names (*AdminServer*, *bi_server1*, *soa_server1*, *sample_server1*, and *sample_server2*) with the names of your Administration Server and any managed servers included in your installation.

You may use a maximum memory setting (-Xmx) larger than 16G if your server has enough memory to support the larger value.

4. Locate the following section of the file and ensure that "-da" appears after each of two "${enableHotSwapFlag}" elements:

```
if [ "${debugFlag}" = "true" ] ; then
 JAVA_DEBUG="-Xdebug -Xnoagent
 -Xrunjdwp:transport=dt_socket,address=${DEBUG_PORT},server
 =y,suspend=n -Djava.compiler=NONE"
 export JAVA_DEBUG
 JAVA_OPTIONS="${JAVA_OPTIONS} ${enableHotswapFlag} -da
 -da:com.bea... -da:javelin... -da:weblogic...
 -ea:com.bea.wli... -ea:com.bea.broker...
 -ea:com.bea.sbconsole..."
 export JAVA_OPTIONS
else
 JAVA_OPTIONS="${JAVA_OPTIONS} ${enableHotswapFlag} -da"
 export JAVA_OPTIONS
fi
```

5. Locate the EXTRA_JAVA_PROPERTIES section of the file. In it, remove the following string:

```
-Dorg.apache.commons.logging.Log=org.apache.commons.logging.
impl.Jdk14Logger
```

6. Locate the following lines in the file:

```
if [ "${PRE_CLASSPATH}" != "" ] ; then
CLASSPATH="${PRE_CLASSPATH}${CLASSPATHSEP}${CLASSPATH}"
export CLASSPATH
fi
```

   Add the following before those lines:

```
PRE_CLASSPATH="<MW_HOME>/grc865/grc/WEB-INF/lib/jython-
2.5.1.jar:${PRE_CLASSPATH}"
export PRE_CLASSPATH
```

   Replace <MW_HOME> with the actual path to your middleware home.

7. Save and close the file. Start the Administration Server and (if appropriate) SOA Server.

Using the WebLogic Console to Deploy the GRC Application

For any installation, use the WebLogic Server Administration Console to complete additional configuration steps:

1. Log in to the WebLogic Server Administration Console at

   `http://host:port/console`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.

2. In the Change Center pane, click Lock & Edit.
3. In the Domain Structure pane, click on Deployments.
4. In the Summary of Deployments pane, select the Control tab.
5. In the Summary of Deployments pane, click on the Install button.
6. In the Path field of the Install Application Assistant pane, enter the full path to the grc865 directory you created earlier (see step 4 of "Preparing Additional Files" on page 2-5). Select "grc865 (open directory)" under Current Location.
7. In the Install Application Assistant pane, press next.
8. In the Install Application Assistant pane, choose *Install this deployment as an application* in the "Choose targeting style" section.
9. In the Install Application Assistant pane, press Next. Then:
   - If you are installing GRC to run FAACG, select the GRC managed server you created in as you set up a WebLogic domain.
   - If you do not intend to run FAACG, you are not presented with an opportunity to select a server here. Skip to step 10.
10. In the Install Application Assistant pane, choose *I will make this deployment accessible from the following location* in the "Source accessibility" section. Accept all other defaults.
11. In the Install Application Assistant pane, press Next.
12. In the Install Application Assistant pane, choose *Yes, take me to the deployment's configuration screen* in the "Additional configuration" section.
13. In the Install Application Assistant pane, press Finish.
14. In the Install Application Assistant pane, press Save, then Activate Changes. On the Deployments screen, the state of the grc865 application will be Prepared.
15. Select the grc865 application. Click Start, select *Servicing all requests*, click *Yes* on Start Application Assistant, and wait until the application status changes to Active.

Setting Up Tomcat Application Server

If you prefer to use Tomcat Application Server rather than WebLogic, disregard all the WebLogic information on pages 2-2 through 2-15, and complete this section instead. Then, if your GRC database supports RAC, continue at "Installing a Driver for RAC" (page 2-17), or if it does not, continue at "GRC Configuration" (page 2-17).

To install GRC with Tomcat:

1. For a new installation, download and install Tomcat generally as its documentation instructs you to do.
2. Shut down the Tomcat application server.
3. Modify Tomcat settings. In <TomcatHome>/bin, create the file setenv.sh. (Note: Throughout this document, <*TomcatHome*> represents the full path to the highest-level directory in which Tomcat components are installed.) Include the following lines in setenv.sh:

```
CATALINA_OPTS="-Xss512k -Xms256M –Xmx16G -XX:MaxPermSize=256m
-XX:+UseParallelGC -Djava.awt.headless=true
-XX:-UseGCOverheadLimit -XX:ReservedCodeCacheSize=128M
-Doracle.mds.cache=simple -Dfile.encoding=UTF-8"

export CATALINA_OPTS
```

You may use a maximum memory setting (-Xmx) larger than 16G if your server has enough memory to support the larger value.

4. Navigate to <grc_stage>/dist. From there, run the file grc_tomcat_setup.sh Supply the paths to <grc_stage>/dist subdirectory, <TomcatHome>, and the full path to your Java home as parameters:

   ```
   cmd> ./grc_tomcat_setup.sh <grc_stage>/dist <TomcatHome>
   JavaHomePath
   ```

5. Start the Tomcat application server.

Installing a Driver for RAC

If Real Application Clusters (RAC) is enabled in your GRC database, you must set up a jdbc-oci driver. (If you do not use RAC, this section does not apply; skip ahead to the next section, "GRC Configuration.")

1. Shut down your web application server (WebLogic administration server and, if installed, managed server; or Tomcat application server).
2. In a web browser, go to http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html. Select the Instant Client link for the platform on which you are installing, then find the Basic download for 11.2.0.3.0.
3. Download and unzip the package into a single directory, such as "instantclient."
4. Set the library loading path in your environment to this directory before starting the application. On many Linux platforms, LD_ LIBRARY_PATH is the appropriate environment variable.
5. Copy the file ojdbc6.jar from the instant client to <TomcatHome>/webapps/grc/WEB-INF/lib if you installed GRC to run with Tomcat, or to grc865/grc/WEB-INF/lib if you installed GRC to run with WebLogic. (In the latter case, you created grc865 as a home directory for your GRC installation in step 4 of "Preparing Additional Files" on page 2-5.)
6. Restart your web application server.

GRC Configuration

Regardless of whether you use WebLogic or Tomcat, open a ConfigUI page to perform GRC-specific configuration:

1. Access GRC at

   ```
   http://host:port/grc
   ```

   In this URL, replace *host* with the FQDN of your GRC server. Select one of the following values for *port*:

   - If you use WebLogic 11g and are installing GRC to run FAACG, enter the port number you chose for the GRC managed server as you created a WebLogic domain.

- If you use WebLogic 12c (and do not intend to run FAACG), enter the port number you chose for the Administration Server as you created a WebLogic domain.
- If you use Tomcat, replace *port* with 8080 (if you accepted the default value when you installed Tomcat) or your configured value (if you changed the default during Tomcat installation).

2. A ConfigUI page appears. In the Installation Configuration section, type or select appropriate property values:
   - User Name: Supply the user name for the GRC database.
   - Password: Supply the password for the GRC database.
   - Confirm Password: Re-enter the password for the GRC database.
   - Port Number: Supply the port number at which the GRC database server communicates with other applications.
   - Service Identifier: Supply the service identifier (SID) for the GRC database server, as configured in the tnsnames.ora file. Or, if your GRC database supports RAC, enter the RAC service name configured for your RAC database.
   - Server Name: Supply the FQDN of the database server. Or, if your GRC database supports RAC, enter RAC@<SCAN_NAME>, where <SCAN_NAME> is the IP address/host name of the SCAN address configured for your RAC database.
   - Maximum DB Connections: Default is 50. You can edit this value.
   - Report Repository Path: Supply the full path to the Report Repository directory discussed in "Creating GRC Repositories" on page 2-2.
   - Log Threshold: Select a value that sets the level of detail in log-file entries. From least to greatest detail, valid entries are *error*, *warn*, *info*, and *debug*.
   - Transaction ETL Path: Enter the full path to the directory you created to hold ETL data used by Enterprise Transaction Controls Governor (see "Creating GRC Repositories" on page 2-2).
   - App Server Library Path: Enter the full path to the library subdirectory of your web application server (for use in the upload of custom connectors for AACG). If you are installing GRC to run FAACG, set this value to <grc865>/grc/WEB-INF/lib. If you use Tomcat Application server and intend to enable parallel processing (see step 4 below), set this field to the "lib/adf" subdirectory of the Tomcat home directory.
3. In the Language Preferences section of the ConfigUI page, select check boxes for up to twelve languages in which you want GRC to be able to display information to its users. "English (U.S.)" should be selected by default; do not deselect it.
4. In the Performance Configuration section of the ConfigUI page, select or clear check boxes:
   - Optimize Appliance-Based Operation: Select the check box to optimize performance if the GRC application and GRC schema reside on the same machine. Do not select this check box if the GRC application and schema

do not reside on the same machine. When you select this check box, an ORACLE_HOME Path field appears. In it, enter the full, absolute path to your Oracle Home — the directory in which you have installed the Oracle database that houses the GRC schema.

- Enable Graph Synchronization Date Limit: "Data synchronization" enables GRC to recognize data changes in each business application subject to models and controls. Although the process applies to AACG and ETCG, it works differently for the two applications.

  Either application recognizes "business objects," each of which is a set of related fields from a "datasource" (business application). ETCG distinguishes among three categories of business object — Transaction (in which records are created or updated frequently), and Operational and Configuration (consisting of master-data or setup records that change infrequently).

  For ETCG only, select the Enable Graph Synchronization Date Limit check box to cause the synchronization of Transaction business objects to operate only on records created or updated in datasources on or after a specified date.

  The setting of this check box has no effect on ETCG Operational or Configuration business objects, for which a synchronization run encompasses all records, no matter when they were created or updated. Moreover, AACG does not distinguish among business-object categories, and the setting of this check box has no effect on AACG synchronization runs.

  When you select the check box, a Transactions Created As Of field appears. In it, enter the cutoff date for the synchronization of ETCG Transaction business objects. When you click in the field, a pop-up calendar appears. Click left- or right-pointing arrows to select earlier or later months (and years), and then click on a date in a selected month.

- Externalize Report Engine: Select the check box to enable the reporting engine to run in its own java process, so that the generation of large reports does not affect the performance of other functionality. But select the check box only if you have installed GRC on hardware identified as "certified" in the *Oracle Enterprise Governance, Risk and Compliance Certifications Document*; clear the check box if you use hardware identified as "supported."

- Enable Parallel Processing: Select this check box to enable multiple jobs to run simultaneously. When you select the Enable Parallel Processing check box, two fields appear:

  In a Number of Cores Available for Processing field, enter the number of processor cores you wish to devote to parallel processing. GRC uses one core for each job, until as many cores as you specify here are in use.

  In a Maximum Megabytes of Physical RAM Available field, specify an amount of memory for use in parallel processing. Ensure that this value is at least 4,096 MB times the number of cores. GRC then divides the memory value by the core value to determine the actual amount of memory per core. As a rule of thumb, enter total RAM minus 8 GB; you may need to adjust this value if other processes run slowly.

- Enforce Allocated Analysis Time Per Filter: Select this check box, and enter a number in the Minutes field, to limit the time that transaction models and controls can run.

  A model or control consists of filters, each of which defines some aspect of a risk and selects transactions that meet its definition. When the Allocated Analysis Time feature is enabled, each filter runs no longer than the number of minutes you specify. If time expires, the filter passes records it has selected to the next filter for analysis, but ignores records it has not yet examined. So a filter may not capture every record that meets its definition, and the model or control results are labeled "partial" in GRC job-management pages.

  Once enabled here, this feature may be disabled for individual models (and for the controls developed from those models). This feature applies only to transaction models and controls, not to access models and controls, and not to EGRCM objects.

5. In the ConfigUI page, click on Actions → Save. GRC tests the values you've entered and, if they are valid, saves them. (If any are invalid, an error message instructs you to re-enter them.)
6. Exit the ConfigUI page.

Completing the Installation

With components in place and properly configured, complete the installation, in effect by running your web application server.

1. Shut down your server — the Administration Server if you're using WebLogic, or the Tomcat application server if you're using Tomcat. Then restart the server.
2. In a web browser, enter the GRC URL (see step 1 of "GRC Configuration" on page 2-17).
3. Wait for a progress bar to indicate that initialization is complete.
4. You are redirected to a GRC logon page. Log on to the application. For a new installation, use the default logon values *admin* for user ID and *admin* for password. GRC requires you to change the password the first time you log on. (For an upgrade, you can use the password established for the previous version.)

If you do not intend to run FAACG (you have installed GRC without SOA), and if you have not set up an external OID LDAP repository to manage users, basic GRC installation is complete. (You may, however, choose complete other procedures described later.)

If you do intend to run FAACG (you have installed GRC to run with SOA), or if you have set up an OID LDAP repository, complete these additional steps:

1. If you use SOA, ensure that the SOA Server is up and running.
2. In GRC, select Navigator → Setup and Administration → Setup → Manage Application Configurations.
3. If you need to configure SOA, select the Worklist tab and enter these values:
   - Worklist Server User Name: Keep the default value, *soaadmin*.

- Worklist Server Password. Enter the password you created for the soaadmin user (see step 3 of "Creating the SOA Admin User and Enabling Embedded LDAP" on page 2-13).
- Confirm Password: Re-enter the Worklist Server Password.
- Worklist Server URL: http://*host*:*port*, in which *host* is the IP address of your SOA server, and *port* is its port number.
- Worklist Server Protocol: Select the communications protocol —SOAP or RMI — used by the GRC application to send and receive SOA requests.

4. If you need to configure external OID LDAP, select the User Integration tab and enter the following values:
   - Enable Single Sign On: See "Integrating with Single Sign On Authentication" on page 2-22.
   - Enable Integration: Select the check box to permit integration with LDAP to occur.
   - User Name: Supply the user name (common name) to log in to the LDAP server. This user should have admin privileges. (This is the value specified for "Principal" in step 7 of "Configuring External OID LDAP," page 2-6.)
   - Password: Enter the password for the user identified in the User Name field (established in step 7 of "Configuring External OID LDAP").
   - Confirm Password: Re-enter the password for the user identified in the User Name field.
   - Port: Enter the port number at which the LDAP server communicates with other applications (established in step 7 of "Configuring External OID LDAP").
   - Server Name: Enter the host name of the LDAP server. (This is the "Host" value from step 7 of "Configuring External OID LDAP.")
   - Bind DN Suffix: Enter the "User Base DN" from step 7 of "Configuring External OID LDAP."
   - Enable SSL Authentication: Select the box to allow GRC to access the LDAP server through SSL. The LDAP server must be configured to support SSL.
   - Perform LDAP Recursive Search: Select the check box to search recursively for users in subfolders along with those in the base path specified in the Bind DN Suffix field.
   - Unique User Identifier: uid
5. In the Manage Application Configurations page, click on Actions → Save. Then log off of GRC.
6. Stop the GRC Deployment in the WebLogic Console:
   a. Log in to the WebLogic Console at

      `http://host:port/console`

      Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.

   b. From the Domain Structure menu, select Deployments.

c. From the Deployment page, locate the GRC deployment and verify the state is Active.

d. Click the checkbox next to the GRC deployment.

e. From the toolbar, click Stop → Force Stop Now.

7. Start the GRC Deployment in the WebLogic Console:

a. From the Domain Structure menu, select Deployments.

b. From the Deployment page, locate the GRC deployment and verify the state is Prepared.

c. Click the checkbox next to the GRC deployment.

d. From the toolbar, click Start → Servicing All Requests.

Integrating with Single Sign On Authentication

Rather than use the GRC authentication system to authenticate GRC users, you can integrate GRC with Oracle Access Management (OAM) Single Sign On (SSO). To do so, you must have installed GRC to run with WebLogic; SSO is not supported in a GRC instance that runs with Tomcat. Moreover, you require not only OAM 11g, but also Oracle HTTP Server (OHS) 11g WebGate for OAM.

First, register OHS WebGate 11g Agent for OAM 11g:

1. Log on to the OAM console. Its URL is `http://<oam_host>:<oam_port>/oamconsole`, in which <*oam_host*> is the host name of the OAM server, and <*oam_port*> is its port number.

2. In the SSO Agent panel, click on New OAM 11g WebGate.

3. In the Create OAM 11g WebGate tab, enter the following values:

   - Name: Enter any value to create a name for the agent.
   - Base URL: Enter `http://<host>:<port>`, in which <*host*> is the host name of the machine where Oracle HTTP Server 11g WebGate is installed, and <*port*> is its port number.
   - Security: Select *Open*.
   - Host Identifier: Enter either the Name or the Base URL value.
   - Select the Auto Create Policies check box.
   - In the Protected Resource List, add */grc*.

   Leave the Access Client Password and User Defined Parameters fields blank, and leave the Virtual Host and IP Validation checkboxes unselected.

4. Click the Apply button.

Once the agent is created, update the authentication scheme to your LDAP scheme:

1. Select the Policy Configuration tab

2. Click Application Domains → <agent_name> → Authentication Policies → Protected Resource Policy.

3. Click the Open icon.

4. Select your LDAP authentication scheme.
5. Click the Apply button.

Next, modify OHS to redirect to GRC.

1. On the server on which you've installed OHS, navigate to <MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1.
2. Open the mod_wl_hos.conf file in a text editor and add the following information to it:

```
<IfModule weblogic_module>
  Debug ON
  WLLogFile /tmp/weblogic.log
</IfModule>

<Location /grc>
  SetHandler weblogic-handler
  WebLogicHost <GRC_HOST_NAME>
  WebLogicPort <GRC_PORT_NUMBER>
</Location>
```

   Replace <GRC_HOST_NAME> with the fully qualified domain name of your GRC server. Replace <GRC_PORT_NUMBER> with the port of your GRC managed server (if you created one to run FAACG) or your Administration Server (if you did not create a managed server).
3. Save and close the mod_wl_hos.conf file.
4. Restart the OAM server and WebGate.

Next, add the OAM Identity Asserter to the GRC domain:

1. Log in to the WebLogic Server Administration Console:

   `http://host:port/console`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server.
2. Click Lock and Edit.
3. Click Security Realms (on the left under Domain Structure), then click myrealm.
4. In the Providers tab, click the New button, and enter *OAM Identity Asserter* for both Name and Type. Then click the OK button.
5. In the Providers tab, click the newly created OAM Identity Asserter.
6. In the Common tab, select:
   - ControlFlag: Required
   - Active Types — Choose: OAM_REMOTE_USER (deselect ObSSOCookie)

   Click the Save option.
7. Return to the Providers tab, click on DefaultAuthenticator, change the ControlFlag to SUFFICIENT, and click the Save option.
8. In the Providers tab, reorder the authentication providers so that OAM Identity Asserter is first, DefaultAuthenticator is second, and DefaultIdentityAsserter is third. Then click the OK button.

9. Click Activate Changes and restart the application server.

Finally, enable SSO in GRC:

1. Log on to GRC and select Navigator → Setup and Administration → Setup → Manage Application Configurations. Select the User Integration tab.
2. Select the Enable Single Sign On check box. (You are presumed to have already set OID LDAP values on this page, as described in step 4 on page 2-21.)
3. Select the Save option from the Actions menu.
4. Select Navigator → Setup and Administration → Security → Manage Users Application Configurations. Select the Import from LDAP option from the Actions menu and import users.fs

GRC and SSL

Once GRC in installed, you can set it up to support Secure Sockets Layer (SSL). This is a prerequisite if you intend to use Application Access Controls Governor, and intend to install preventive enforcement agents (PEAs) so that they support SSL. (For more on PEAs, see chapter 6.) Otherwise, GRC support for SSL is optional. The procedure you use depends on whether you have installed GRC to run with WebLogic or Tomcat.

Implementing SSL if GRC Runs with WebLogic

To install and configure SSL support for a GRC instance that runs with WebLogic, first create custom certificates, then enable and configure SSL.

To create custom certificates:

1. Navigate to the config directory of your WebLogic domain — <MW_HOME>/user_projects/domains/<grc_domain>/config.
2. Create a self-signed keystore. Run the following command. (Here and throughout this section, replace <Java_Home> with the full path to the highest-level directory in which Java components are installed.)

   ```
   <Java_Home>/bin/keytool -genkey -alias grc -keyalg RSA
   -keysize 1024 -dname "CN=KeyMachine,OU=Unit, O=Org,
   L=Locality, ST=StateProvince, C=CountryCode" -keypass
   KeyPassword -keystore KeyFileName.jks -storepass StorePassword
   ```

   In this command, replace italicized values as follows (and enter other values as they are shown).

   - -alias: Accept *grc*, or enter any other value. (If you choose a value other than *grc*, be sure to use that same value where you need to supply the alias in subsequent commands in this procedure.)
   - -dname parameters:

     CN stands for Common Name. Replace *KeyMachine* with the fully qualified domain name of the machine on which the keystore is being generated (the GRC server).

OU and O: Replace *Unit* with the name of an organizational unit, and *Org* with the name of the parent organization of that unit. You can supply any values you choose.

L, ST, and C: Replace *Locality* with the name of a city or municipality; *StateProvince* with the name of a state, province, or other political subdivision of a country; and *CountryCode* with a two-letter country code.

- -keypass and -storepass: Replace *KeyPassword* and *StorePassword* with passwords that you create as you run this command. It's recommended that you use the same value for both passwords. (These values, established here, will be used in subsequent commands.)
- -keystore: Replace *KeyFileName* with any name for a keystore file. (The file extension must be .jks, and the name, established here, will be used in subsequent commands.)

3. Self-sign the certificate. Run the following command.

```
<Java_Home>/bin/keytool -selfcert -v -alias grc -keypass
KeyPassword -validity 8000 -keystore KeyFileName.jks
-storepass StorePassword -storetype jks
```

Again, replace italicized values as follows (and enter other values as they are shown).

- -alias: Replace *grc* with the alias you created in step 2 (or use *grc* if you accepted that value in step 2).
- -keypass and -storepass: Replace *KeyPassword* and *StorePassword* with the passwords you created in step 2.
- -keystore: Replace *KeyFileName* with the keystore file name you created in step 2.

4. Export the root certificate. Run the following command:

```
<Java_Home>/bin/keytool -export -v -alias grc -keystore
KeyFileName.jks -storepass StorePassword -file rootCA.der
```

Again, replace italicized values as follows (and enter other values as they are shown).

- -alias: Replace *grc* with the alias you created in step 2 (or use *grc* if you accepted that value in step 2).
- -keystore: Replace *KeyFileName* with the keystore file name you created in step 2.
- -storepass: Replace *StorePassword* with the password you created in step 2.
- -file: Replace *rootCA* with a file name of your choosing. (The file extension must be .der, and the name, established here, will be used in a subsequent command.)

5. Import the root certificate into a trusted keystore. Run the following command:

```
<Java_Home>/bin/keytool -import -v -trustcacerts -alias grc
-keystore trust.jks -storepass StorePassword -file rootCA.der
```

Again, replace italicized values as follows (and enter other values as they are shown):

- -alias: Replace *grc* with the alias you created in step 2 (or use *grc* if you accepted that value in step 2).
- -keystore: Replace *trust* with a new keystore name. This must not be the same as the -keystore value entered in earlier steps, but otherwise may be any value you wish. (The file extension must be .jks.)
- -storepass: Replace *StorePassword* with the password you created in step 2.
- -file: Replace *rootCA* with the file name you created in step 4. (The file extension must be .der.)

When prompted "Trust this certificate? [no]," enter yes to confirm the key import.

To enable SSL:

1. Log in to the WebLogic Server Administration Console at

   `http://host:port/console`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server as you set up a WebLogic domain.

   In the left panel of the Console, expand Environment and select Servers.
2. Click the name of the Administration Server on which GRC is installed.
3. In the Change Center of the Administration Console, click Lock & Edit.
4. Select the Configuration tab and then the General subtab.
5. Select the checkbox next to SSL Listen Port Enabled.
6. Enter a port number in the SSL Listen Port textbox.
7. Select Save. Click Activate Changes in the Change Center of the Administration Console.

Repeat this procedure for any managed servers.

To configure SSL:

1. Still in the Administration Console, expand Environment and select Servers.
2. Click the name of the Administration Server on which GRC is installed.
3. In the Change Center of the Administration Console, click Lock & Edit.
4. Select the Configuration tab and then the Keystores subtab.
5. In the Keystore row, click the Change button. From the drop-down list, select Custom Identity and Custom Trust.
6. In the Custom Identity Keystore field, enter the full path to your keystore file (the .jks file you created at step 2 in the procedure for creating custom certificates, page 2-24).
7. Enter JKS as the value for Custom Identity Keystore Type.

8. For the Custom Identity Keystore Passphrase, enter the value you chose for the -storepass parameter at step 2 in the procedure for creating custom certificates (page 2-24).
9. Re-enter the -storepass value in the Confirm Custom Identity Keystore Passphrase field.
10. In the Custom Trust Keystore field, enter the full path to your trusted keystore file (the .jks file you created at step 2 in the procedure for creating custom certificates, page 2-24).
11. Enter JKS as the value for Custom Trust Keystore Type.
12. For the Custom Trust Keystore Passphrase, enter the value you chose for the -storepass parameter at step 2 in the procedure for creating custom certificates (page 2-24).
13. Reenter the -storepass value in the Confirm Custom Trust Keystore Passphrase field.
14. Select Save. Click Activate Changes in the Change Center of the Administration Console.
15. In the Change Center of the Administration Console, click Lock & Edit.
16. Click on the SSL subtab, to the right of the Keystore subtab.
17. Ensure that the Identity and Trust Locations value is set to "Keystores." If not, change it to this value.
18. Set the value of the Private Key Alias to the value you chose for the -alias parameter at step 2 in the procedure for creating custom certificates (page 2-24).
19. For the Private Key Passphrase, enter the values you chose for the -keypass parameter at step 2 in the procedure for creating custom certificates (page 2-24).
20. Reenter that -keypass value in the Confirm Private Key Passphrase field.
21. Expand the Advanced options of the SSL subtab by clicking on the Advanced pane title.
22. Select the Use JSSE SSL checkbox.
23. Select Save. Click Activate Changes in the Change Center of the Administration Console.
24. Log out of the WebLogic Administration Console: click on the Log Out link at the top of the console page.
25. Bounce the Administration Server, then ensure there are no SSL-related errors in the server log.
26. Navigate to https://*host:SSLport*/console to test your latest changes. (The SSLport is the value you selected in step 6 of the procedure for enabling SSL, page 2-26.)

Repeat this procedure for any managed servers.

Implementing SSL if GRC Runs with Tomcat

To install and configure SSL support for a GRC instance that runs with Tomcat, prepare a certification keystore, then modify a server.xml file.

To prepare the certification keystore, which contains a single self-signed certificate:

1. Execute the following command from a terminal command line.

```
<Java_Home>/bin/keytool -genkey -alias grc -keyalg RSA
-keystore <TomcatHome>/conf/keystore -storetype pkcs12
```

This command creates a new file, named "keystore," in the conf directory of your <TomcatHome>.

2. In response to a prompt, create a keystore password. (Note that you will need to specify this password later as you edit the server.xml file.)
3. In response to a prompt, confirm the password you just created.
4. In response to prompts, provide general information about the certificate, such as company, contact name, and so on. (This information is displayed to users who attempt to access a secure page in your application.)

To modify the server.xml file:

1. Navigate to <TomcatHome>/conf, and open the server.xml file for editing.
2. In the file, locate a Connector element that looks like the following:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
     This connector uses the JSSE configuration, when using
     APR, the connector should be using the OpenSSL style
     configuration described in the APR documentation -->

<!--
     <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
     maxThreads="150" scheme="https" secure="true"
     clientAuth="false" sslProtocol="TLS" />

-->
```

3. From the second block of text, delete the comment tags (<!-- and -->).
4. Accept the default value for the port attribute (8443), or change it to any other value. This is the TCP/IP port number on which Tomcat listens for secure connections. Note that special setup (outside the scope of this document) is necessary to run Tomcat on port numbers lower than 1024 on many operating systems.

   If you change the port number, also change the value for the redirectPort attribute on the non-SSL connector you use. This lets Tomcat redirect users who attempt to access a page with a security constraint specifying that SSL is required.
5. Add values to the connector element — keystoreFile, keystorePass, keyAlias, and keystoreType attributes. A completed connector element looks like the following (in which you would replace *YourKeystorePassword* with the password you created as you prepared the certification keystore):

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<TomcatHome>/conf/keystore"
keystorePass="YourKeystorePassword" keyAlias="grc"
keystoreType="PKCS12" />
```

6. Restart Tomcat.

Accessing GRC

After configuring SSL successfully, access the GRC application at https://*host*:*SSLport*/grc, in which *host* is the FQDN of your GRC server, and

SSLport is the port you selected to support SSL. (If you use WebLogic, see step 6 of the procedure for enabling SSL on page 2-26. If you use Tomcat, see step 4 above.)

Because you are using a self-signed certificate, which is not signed by an official Certificate Authority, you get a security warning when you open GRC at this URL.

- For Internet Explorer, the warning reads, "There is a problem with this website's security certificate." Dismiss this warning by choosing "Continue to this website (not recommended)."
- For Firefox, the warning reads, "This Connection is Untrusted." Dismiss this warning by clicking "I Understand the Risks," and then "Add Exception."

GRC Upgrade

You can upgrade from version 8.6.4.7000, 8.6.4.8500, or 8.6.4.8900. If you upgrade from 8.6.4.7000, ETCG results are not carried forward, although AACG results are (if analysis has not been run in version 8.6.4.8000 or 8.6.4.8500). If you upgrade from version 8.6.4.8500 or from 8.6.4.8900, ETCG and AACG results are included.

However, unless your earlier GRC instance runs FAACG, you need to upgrade middleware components, so to upgrade GRC, you essentially perform a new installation in which you reuse GRC and DA schemas from the earlier instance. You can also reuse your database and Java if your earlier instance used 8.6.5.1000-compatible versions (11.2.0.3 and JDK 1.7); otherwise you need to replace these as well. See "New GRC Installation" on page 2-1.

Back up your database schema and report and transaction synchronization directories before performing the upgrade.

If you use GRC Advanced Controls (AACG or ETCG), you must perform certain procedures after you complete an upgrade. See chapter 4, "Additional Advanced Controls Configuration."

GRC Repositories

For earlier versions of GRC, you created two repositories — directories that store data generated by GRC. A report repository stores copies of GRC reports that users schedule to be run. A second repository stores synchronization data used for transaction analysis. (See "Creating GRC Repositories" on page 2-2.)

Reuse these repositories for GRC 8.6.5.1000. Retain the contents of the transaction synchronization repository. Note the paths to the repositories, as you will need to supply them later as configuration values.

FAACG Upgrade

If you are upgrading a GRC instance in which you run FAACG, you will reuse the database, Java, and (WebLogic 11g) middleware components already installed for your earlier instance. Complete the following steps:

1. Stop the WebLogic Administration Server and managed servers.

2. During installation of earlier GRC releases, a directory called grc864 was created, typically as a subdirectory of your middleware home directory (represented in this document as <MW_HOME>). Delete the contents of this directory.
3. Create a new directory called grc865; typically, once again, this would be a sub-directory of your middleware home directory.
4. Navigate to <grc_stage>/dist, and locate the grc.ear file.
5. Extract the contents of grc.ear into the grc865 directory.
6. Navigate to <grc_stage>/dist. From there, run the file grc_wls_setup.sh. Supply the path to the grc865 directory (into which you extracted the contents of the grc.ear file in step 5). For example:

   ```
   cmd> ./grc_wls_setup.sh <MW_HOME>/grc865
   ```

7. Remove content from the following directories. (In these paths, <grc_domain> represents the name of the WebLogic domain created for GRC, and <managed_server> is the name of a WebLogic managed server, if one was created.)

   <MW_HOME>/user_projects/domains/<grc_domain>/servers/AdminServer/logs
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/AdminServer/cache
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/AdminServer/tmp
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/<managed_server>/logs
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/<managed_server>/cache
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/<managed_server>/tmp

8. Restart the WebLogic servers.
9. To finish the upgrade, perform several procedures that are the same as they would be for a new installation. If your database is one in which Real Application Clusters is enabled, begin with “Installing a Driver for RAC” (page 2-17). In any case, also execute procedures described in “GRC Configuration” (page 2-17) and “Completing the Installation” (page 2-20). Finally, if they apply to your instance, execute procedures described in “Integrating with Single Sign On Authentication” (page 2-22) and “GRC and SSL” (page 2-24).

Again, see chapter 4, “Additional Advanced Controls Configuration,” for procedures to be completed after an upgrade.

3

Integrating GRCI

Oracle Fusion GRC Intelligence (GRCI) makes use of Oracle Business Intelligence Enterprise Edition (OBIEE) and a Data Analytics (DA) schema. (The database that supports the DA schema should have an initial temporary tablespace of 100 GB with autoextend enabled.)

If you have performed a new installation of GRC 8.6.5.1000, you can create a DA schema and install GRCI 8.6.5.1000 as well. Do so even if you do not immediately intend to use GRCI, but anticipate using it with a future upgrade of GRC. (With an upgrade-only version of GRC, you can upgrade GRCI, but cannot install it.)

If you are upgrading to GRC 8.6.5.1000, you may install or upgrade GRCI, depending on whether a GRCI instance or DA schema exists in your earlier GRC version:

- If you upgrade to GRC 8.6.5.1000 from an instance in which GRCI is running, then you can upgrade GRCI as well. (See "GRCI Upgrade" on page 3-15.)
- If you upgrade to GRC 8.6.5.1000 from an instance in which GRCI is not running, but in which a DA schema has been in place, then you can install GRCI and capture data both from the 8.6.5.1000 instance and from earlier GRC instances.
- If you upgrade to GRC 8.6.5.1000 from an instance in which GRCI is not running, and in which no DA schema is in place, you can create a DA schema and install GRCI, but you will capture data only from the 8.6.5.1000 instance, not from the earlier instances.

New GRCI Installation

In broad terms, a new GRCI installation is a three-step process:

- You are assumed to have created a Data Analytics (DA) schema for use by GRCI (see "Creating GRC and DA Schemas," page 1-3). Set up connections to the DA schema in a GRC Analytics page.
- Set up OBIEE for use with GRC.
- Select and optionally rename GRCI dashboards that are to appear in the GRC instance.

If you've installed GRC with WebLogic, you can embed your GRCI instance within GRC. If you've installed GRC with Tomcat, you must install OBIEE (and so GRCI) as a standalone application.

Connecting to the DA Schema

The GRC schema used by GRC supplies data to the DA schema used by GRCI. For this to happen, you need to enter connectivity information in GRC.

1. Log on to GRC (see step 1 of "GRC Configuration" on page 2-17). Select Navigator → Tools → Setup and Administration → Setup → Manage Application Configurations → Analytics.
2. In the Data Analytics Configuration section, enter values that identify the DA schema you set up in "Creating GRC and DA Schemas" (page 1-3).
   - User Name: Supply the user name for the DA database.
   - Password: Supply the password for the DA database.
   - Confirm Password: Re-enter the password for the DA database.
   - Port Number: Supply the port number at which the database server communicates with other applications.
   - Service Identifier: Supply the service identifier (SID) for the database server.
   - Server Name: Supply the fully qualified domain name of the database server.
3. When you finish entering property values, click on Actions → Save. GRC tests the values you've entered and, if they are valid, saves them. (If any are invalid, an error message instructs you to re-enter them.)
4. Look for the prompt, "Successfully saved configuration values."

After that message appears, a one-time process runs in the background. It creates the DA schema tables and views. This process takes approximately fifteen minutes. Do not stop your WebLogic or Tomcat server during this period.

Once you have connected to the DA schema, set a schedule on which the schema is refreshed — on which the DA schema reads from the GRC schema. No data exists in the schema until the first scheduled refresh occurs. You can modify a schedule at any time. (A refresh can take up to 90 minutes to finish.) To create the schedule:

1. Select the Analytics tab of the Manage Applications Configurations page.
2. Click on the Schedule Data Analytics Update button.
3. A Schedule Parameter dialog opens. Enter values that set the name of the schedule, its start date and time, the regularity with which the DA schema should be refreshed, and an end date (if any). Then click on the Schedule button.
4. Click on Actions → Save.

To view the status of a scheduled refresh, go to Tools → Setup and Administration → Manage Jobs. To view the Data Analytics schedule, go to Tools → Setup and Administration → Manage Scheduling.

Setting Up OBIEE in GRC with WebLogic

If you installed GRC to run with WebLogic, complete procedures documented from here to page 3-7. Then skip "Setting Up OBIEE in GRC with Tomcat," and continue at "Repository and WebCat Configuration" on page 3-8.

GRCI requires WebLogic 11g — WLS 10.3.6, ADR 11.1.1.7, and RCU 11.1.1.7. Install these components, and create a WebLogic domain for use by GRCI and OBIEE. (See "Initial WebLogic Installation," "Creating a WebLogic Domain," and "Preparing Additional Files" on pages 2-2 through 2-6 as well as "Using the WebLogic Console to Deploy the GRC Application" on page 2-15).

Note: You may be upgrading from a GRC instance for which you had installed 11.1.1.7 components to support GRC. If so, you cannot repurpose these components for use with GRCI 8.6.5.1000; you must install a fresh set of middleware components.

Start the WebLogic instance (run the startWeblogic.sh script, and supply the username and password created during domain configuration). Once the instance goes successfully into running mode, stop it (run the stopWeblogic.sh script). Ensure that a VNC server is running on your GRC host (the machine on which you installed GRC in chapter 2), and use a VNC client of your choosing to start a VNC session.

Perform the OBIEE installation on the GRC host.

Preparing Files

Locate the files grc865_1616_OBIEE_1of3.tar.gz, grc865_1616_OBIEE_2of3.tar.gz, and grc865_1616_OBIEE_3of3.tar.gz in your <grc_stage> directory (see "Downloading Files," page 1-4). Extract their contents in the 11g < MW_HOME>. This overwrites some files under the oracle_common directory.

Running the Installation Script

Run an installation script, which prompts you for settings that apply to your instance. The entire process is logged to <MW_HOME>/installation.log.

Note: Ensure that GRCI RCU schemas are installed on the database were GRC and DA schemas have been created.

Pay attention to script output on your monitor. Some installation stages may cause errors or may require your attention. Should errors occur, check the log file. Also, refer to "Troubleshooting" (page 3-13).

To run the script, execute the following command in your 11g <MW_HOME>:

```
./install_obiee.sh
```

The script determines whether X Server is running. (If not, the script directs you to start X Server, then exits. In a later step, you will use a graphical user interface, and X Server is required for that interface to be displayed.) Next, the script reminds you to shut down your administration and managed servers, and prompts for confirmation.

Complete these steps:

1. Type 1 and press Enter if you are ready to continue with setup. If, however, you need to shut down your servers, type 2 and press Enter to quit.
2. Assuming you pressed 1 in step 1, the script prompts you to enter these values:
   - MW_HOME: The full path to the home directory of the GRCI middleware installation.
   - JAVA_HOME: The full path to the Java deployment used for the middleware installation (the JDK instance you confirmed to be in the path to install and run WebLogic under "Initial WebLogic Installation" on page 2-2.)

- RCU_HOME: The full path to the highest-level directory in which the RCU 11.1.1.7 component exists.
- DOMAIN: The full path to the WebLogic domain you created for GRCI: <MW_HOME>/user_projects/domains/<grc_domain>.
- ADMIN_SERVER_NAME: Your WebLogic Administration Server name.
- HOST_PORT: The port number configured for your Administration Server.
- HOST: The fully qualified domain name for the host on which you are performing the GRCI installation.

3. The script attempts to extract the HOST_IP — the IP address of the machine on which GRCI is being installed. Verify that the value is detected correctly.
4. The script prompts you to enter these additional values:
   - DB_HOST : The fully qualified domain name for the machine that hosts the database that in turn hosts the DA schema.
   - DB_PORT : The listen port number for the database that hosts the DA schema.
   - SID : The instance name for the database that hosts the DA schema.
   - DB_NAME: The service name for the database that hosts the DA schema.
   - SYS_PASSWORD: The SYS user's password for the database that hosts the DA schema.
   - WLS_ADMIN_USER: The administrator user name for the WebLogic instance dedicated to GRCI.
   - WLS_ADMIN_PASSWORD: The administrator password for the WebLogic instance dedicated to GRCI.
5. The script performs string replacements inside installation files based on the setting values you've supplied, and it creates two RCU schemas.
6. The script launches a GUI wizard in which you can extend the domain you created for GRC. To do so, follow steps in "Extending Your Domain" (page 3-5). Then continue this procedure at step 7.
7. Open another terminal window. In it, open <MW_HOME>/user_projects/domains/<grc_domain>/bin/setDomainEnv.sh in a text editor, and locate the following lines:

   ```
   # IF USER_MEM_ARGS the environment variable is set, use it
   to override ALL MEM_ARGS values

   if [ "${USER_MEM_ARGS}" != "" ] ; then
   ```

   Insert the following between those two lines:

   ```
   case "${SERVER_NAME}" in
   "AdminServer")
     USER_MEM_ARGS="-Xms2g -Xmx2g"
   ;;
   "bi_server1")
     USER_MEM_ARGS="-Xms2g -Xmx8g"
   ;;
   *)
     echo "Unknown Server Detected!!. Memory set as Xms1g
   ```

```
Xmx2g.";
USER_MEM_ARGS="-Xms1g -Xmx2g"
;;
esac
USER_MEM_ARGS="${USER_MEM_ARGS} -XX:PermSize=256m
-XX:MaxPermSize=512m -XX:ReservedCodeCacheSize=128M
-Djava.awt.headless=true -Djbo.ampool.maxpoolsize=600000
-Dfile.encoding=UTF-8"
```

You may use a maximum memory settings (-Xmx) larger than the values shown above if your server has enough memory to support the larger values.

8. Return to the window in which the script is running, enter the value *1*, and press the Enter key so that the script continues. The installation script continues to perform automated installation operations.
9. Complete the "Repository and WebCat Configuration" section (page 3-8) to update the rpd file with correct connection values.
10. Complete the "Deploying GRCDiagnostic.rpd and Updating Scheduler Credentials" section (page 3-10).
11. Test the installation to verify it was successful. See "Testing the Installation" (page 3-12).

Extending Your Domain

While install_obiee.sh runs, it presents a GUI wizard in which to extend the WebLogic domain you created for GRCI. Follow these steps to extend your domain.

OWSM MDS and EPM schemas are the only two schemas you need to modify in the following steps.

1. Select *Extend an existing WebLogic domain*.
2. Click Next.
3. Select to extend the <MW_HOME>/user_projects/domains/<grc_domain> directory.
4. Click Next.
5. Click Extend my domain using an existing extension template.
6. Click Browse.
7. Navigate to <MW_HOME>/Oracle_BI1/common/templates/applications/ and select oracle.bi_base_enterprise_template_11.1.1.jar.
8. Click OK.
9. Click Next.
10. Select both OWSM MDS and EPM schemas and enter the following values:
    - Vender: Oracle
    - DBMS/Service: The service name for the GRC database.
    - Driver: Accept the default value.
    - Host Name: The fully qualified domain name for the machine that hosts the GRC database.

- Schema Password: grc
- Port: The port number at which the GRC database communicates with other applications.

11. Unselect OWSM MDS Schema while leaving EPM Schema selected. As Schema Owner, enter the value EGRCM_BIPLATFORM.
12. Unselect EPM Schema and select OWSM MDS Schema. As Schema Owner, enter the following value: EGRCM_MDS.
13. Click Next.
14. If the connection tests for both schemas succeed, click Next. Otherwise, click Previous and enter correct values.
15. Select *Managed Servers, Clusters and Machines*.
16. Click Next.
17. Modify the Listen address field for bi_server1 to the IP address of the machine on which you are installing GRCI.
18. Click Next.
19. Click Next.
20. Click Next.
21. Click Next.
22. Click Extend.
23. Click Done.
24. The GUI wizard closes and another one launches to extend the domain with further Oracle Business Intelligence features. Select Extend an existing WebLogic domain.
25. Click Next.
26. Select to extend the <MW_HOME>/user_projects/domains/<grc_domain> directory.
27. Click Next.
28. Select Oracle BI Enterprise Edition — 11.1.1.7.0. Additional products are selected automatically.
29. Click Next.
30. Click Next.
31. Click Next.
32. Select Deployments and services.
33. Select bi_cluster from the Target pane in the left.
34. Unselect the following Applications (clear the checkmark next to each):
    - DMS Application#11.1.1.1.0
    - wsil-wls

- ESSAPP
- wsm-pm
- bilocaladmin#11.1.1
- bicontentserver#11.1.1
- bicomposer#11.1.1
- asyncadminserver#11.1.1
- jbips#11.1.1
- bioffice#11.1.1
- biofficeclient#11.1.1
- analytics#11.1.1
- bimiddleware#11.1.1
- bisearch#11.1.1
- bisecurityadmin#11.1.1
- bisecurity#11.1.1
- mapviewer#11.1.1
- adminservice#11.1.1
- biadminservlet#11.1.1

35. Select bi_server1 from the Target pane in the left.
36. Check the applications listed in step 34.
37. Click Next.
38. Click Next.
39. Click Extend.
40. Click Done.

Return to step 7 on page 3-4.

Setting Up OBIEE in GRC with Tomcat

If you installed GRC to run with Tomcat, disregard the GRC-with-WebLogic information on pages 3-2 through 3-7, and complete this section instead. Then continue with “Repository and WebCat Configuration on page 3-8.

A GRC-Tomcat installation requires that you install OBIEE in a standalone configuration. Install OBIEE 11.1.1.7 and related components generally as their documentation instructs you to do.

As you perform the installation, keep the following points in mind:

- You will create RCU schemas to be used by OBIEE. As you do, use *EGRCM* as your schema prefix, and *grc* as the password for the MDS and BIPLATFORM schemas.
- Unless directed otherwise, accept default values.

- Select *Enterprise Insall* as your installation type.
- On the screen titled Create or Scale Out BI System, select *Create New BI System*. Make a note of the username and password you choose. Accept the default domain name.
- On the screen titled Specify Installation Location, set the Oracle Middleware Home path to the absolute path for your Oracle Middleware home. Specify either an empty directory or a directory that does not exist. (If the directory does not exist, the installer creates it for you.) Note the path to this directory; you will need it for a later configuration step. Throughout this document, <OBIEE_MW> will represent this path. Do not set the value for any other empty field; all will be populated based on your middleware home path.
- On the port-configuration screen, specify ports appropriate for your environment, or accept the default ports.
- Be sure to take note of paths and URLs displayed on a screen titled Installation Completed. You will need them later. These values include Oracle Enterprise Manager URL, Business Intelligence Enterprise Edition URL, and the port number used in the Business Intelligence Enterprise Edition URL.

After installation is complete, shut down your Administration Server, BI Server, and BI components. Run the following commands:

```
<OBIEE_MW>/user_projects/domains/bifoundation_domain/bin/stopManagedWebLogic.sh bi_server1

<OBIEE_MW>/user_projects/domains/bifoundation_domain/bin/stopWebLogic.sh

<OBIEE_MW>/instances/instance1/bin/opmnctl stopall
```

Then, prepare files:

1. Open <OBIEE_MW>/instances/instance1/config/OracleBIPresentationServices Component/coreapplication_obips1/instanceconfig.xml for editing.
2. Locate the <Security> tag. On the line immediately below it, insert the following:

   ```
   <InIFrameRenderingMode>allow</InIFrameRenderingMode>
   ```

3. Save and close the instanceconfig.xml file.
4. Copy tnsnames.ora from the Oracle database home for the database that hosts your DA schema (ORACLE_HOME/NETWORK/ADMIN/) to <OBIEE_MW>/Oracle_BI1/network/admin.

Repository and WebCat Configuration

Extract and copy custom files that are consumed by GRCI dashboards and reports:

- Locate the file grc-reportservices-8.6.5.1-SNAPSHOT-obiee-artifacts.zip in your <grc_stage>/dist directory (see “Downloading Files” on page 1-4). Extract its contents into a temporary directory. (Throughout this document, <OBIEE_TEMP> represents the full path to this directory.)

- If your GRC installation uses Tomcat, copy <OBIEE_TEMP>/Webcat/GRCDWebcat to <OBIEE_MW>/instances/instance1/bifoundation/OracleBIPresentationServices Component/coreapplication_obips1/catalog. (Use the R option of the cp command.)
- If your GRC installation uses WebLogic, copy <OBIEE_TEMP>/Webcat/GRCDWebcat to <MW_HOME>/instances/ instance1/ bifoundation/OracleBI PresentationServicesComponent/ coreapplication_obips1/catalog. (Use the R option of the cp command.)

Modify a file called GRCDiagnostic.rpd, and then use it to configure repositories. To do so, you must use a tool that runs only on a Windows-based computer.

Throughout this section (as before), *host* is the FQDN of your GRC server, and *port* is the number you selected for the WebLogic Administration Server.

1. On a Windows machine, open an FTP client and connect to *host*.
   - Navigate to <OBIEE_TEMP>/repository.
   - Download the file GRCDiagnostic.rpd to you Windows machine. Then close the FTP client.
2. On the Windows machine, go to http://www.oracle.com/technetwork/ middleware/bi-enterprise-edition/downloads/bus-intelligence-11g-165436.html. From that site, download and install Oracle Business Intelligence Developer Client Tools Installer (11.1.1.7.0).
3. When the installation is complete, ODBC Data Source Administrator opens. Press Cancel to close it (it is not needed for this procedure.)
4. Open the Oracle BI Administration Tool: From the Start menu, navigate to Oracle Business Intelligence Enterprise Edition Plus Client → Administration.
5. Navigate to File → Open → Offline. Select the GRCDiagnostic.rpd file you downloaded in step 1. Enter *Admin123* as the Repository Password.
6. Navigate to Manage → Variables.
   - In the left pane, expand Repository and select Variables.
   - In the right pane, double-click on GRI_DSN. Under Default Initializer, enter the service identifier (SID) for the Oracle database that hosts your DA schema, inside the single quotation marks. Press OK.
   - Double-click on GRI_USER_ID. Under Default Initializer, enter the schema name used by your DA schema, inside the single quotation marks. Press OK.
   - Close the Variable Manager.
7. In the main window under the Physical section, right-click on GRC Diagnostics and select Properties.
   - Click on the Connection Pools tab and double-click on GRCI Connection Pool.
   - Under the Shared Logon section, enter the schema password used by your DA schema.
   - Press OK, re-enter the schema password in the confirmation pop-up, and then press OK again.

- Double-click on INIT BLOCK Connection Pool, and make the same password update as you made for the GRCI Connection Pool.
- Press OK to close the Properties window.

8. Navigate to File → Save and answer No to "Do you wish to check global consistency?"
9. Exit the Oracle BI Administration Tool.

Deploying GRCDiagnostic.rpd and Updating Scheduler Credentials

If you installed GRC to run with Tomcat, start your Administration Server, BI Server, and BI components. Run the following commands:

```
<OBIEE_MW>/user_projects/domains/bifoundation_domain/bin/start
WebLogic.sh
```

```
<OBIEE_MW>/user_projects/domains/bifoundation_domain/bin/start
ManagedWebLogic.sh bi_server1
```

```
<OBIEE_MW>/instances/instance1/bin/opmnctl startall
```

If you installed GRC to run with WebLogic, the installation script has already started all necessary servers and components.

No matter which web server you use, complete the following steps:

1. Still on the Windows machine
   - If your GRC installation uses WebLogic, go to http://*host*:*port*/em. Log in to the host with your WebLogic Administration username and password.
   - If your GRC installation uses Tomcat, go to your Oracle Enterprise Manager URL. Log in with your WebLogic Administration username and password. (You noted the URL, user name, and password as you completed "Setting Up OBIEE in GRC with Tomcat," page 3-7).
2. From the left menu, expand Business Intelligence and double-click on *coreapplication*.
3. Select the Deployment tab.
4. Select the Scheduler tab.
5. Press *Lock and Edit Configuration*.
6. Close the confirmation pop-up.
7. Update the username to EGRCM_BIPLATFORM.
8. Update the password and confirm password fields to *grc*.
9. Click the Apply button.
10. Click on the Activate Changes button on top.
11. Click on Close after the changes are activated.
12. Press *Lock and Edit Configuration*.
13. Select the Repository tab.

14. Under *Upload BI Server Repository*, click the Browse button and select the GRCDiagnostic.rpd that you modified and saved on your Windows machine in "Repository and WebCat Configuration" (page 3-8). Enter *Admin123* in both of the Repository Password and Confirm Password fields.
15. Under *BI Presentation Catalog*, enter the following as the *Catalog Location*:
    - If your GRC installation uses WebLogic: <MW_HOME>/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog/GRCDWebcat
    - If your GRC installation uses Tomcat: <OBIEE_MW>/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/ catalog/GRCDWebcat
16. Click on the Apply button.
17. Click on the Activate Changes button on top.
18. Click on Close after the changes are activated.
19. Navigate to Business Intelligence → Core Application → Capacity Management → Performance. There, ensure that the cache is disabled (that the Enable BI Server Cache check box is cleared).
20. Press the *Restart to apply recent changes* button on top.
21. Click on the Restart button.
22. Select Yes.
23. Click on Close after the restart completes.

As long as the following BI components are up and running, warnings or errors related to any other components can be ignored. You can verify the status of these components by clicking on the Availability tab. If any of them are down, see the Troubleshooting section.

- BI Presentation Services
- BI Servers
- BI Schedulers
- BI Cluster Controllers
- BI Java Hosts

Configuring Intelligence in GRC

Within the GRC application, you need to enter values than enable GRC to connect to OBIEE, and you need to select "dashboards" in which GRC displays reports.

1. Log on to GRC (see step 1 of "GRC Configuration" on page 2-17). Select Navigator → Tools → Setup and Administration → Setup → Manage Application Configurations → Analytics.
2. In the GRC Intelligence Configuration section, supply the following values:
    - OBIEE Server Username: If your GRC installation uses WebLogic, the user name configured for the WebLogic Administration Server. If your GRC

installation uses Tomcat, the WebLogic Administration username you noted in "Setting Up OBIEE in GRC with Tomcat."

- OBIEE Server Password: The password for the GRCI Administration Server Username.
- OBIEE Server Port: If your GRC installation uses WebLogic, *9704*. If your GRC installation uses Tomcat, the port number noted under Setting Up OBIEE in GRC with Tomcat."
- OBIEE Server Host: If your GRC installation uses WebLogic, the fully qualified domain name for the machine on which you installed GRCI. If your GRC installation uses Tomcat, the fully qualified domain name for the machine on which you installed OBIEE under "Setting Up OBIEE in GRC with Tomcat."
- Root Context: *analytics*

Leave the Enable SSL Authentication check box unchecked.

3. An Intelligence Page Configuration section displays a row for each dashboard you can display for GRC. (Each is identified as a "subtab" of an Intelligence tab that appears in, or in reference to, a major GRC page, such as the home page or an overview page for an object such as risk or continuous control.)
   - To enable a dashboard, click in its field in the Enable column until a check mark appears. To disable it, double-click until the check mark disappears.
   - To modify the display name of a dashboard, double-click in its field in the Display Label column. The field becomes write-enabled; enter the name you want to use.
4. A GRCI Intelligence Standard Mode Link Configuration section contains a single field, GRCI Intelligence Standard Mode URL. If you have installed a standalone instance of OBIEE, enter the URL for that instance.
5. When you finish entering values, click on Action → Save. If you've modified settings in the GRC Intelligence Configuration section, GRC tests the values you've entered and, if they are valid, saves them. (If any are invalid, an error message instructs you to re-enter them.)
6. Look for the prompt, "Successfully saved configuration values."

In addition, each GRC user who is to have access to GRCI must be granted one or more of three GRC job roles: GRC Intelligence Administrator Job Role, GRCM Embedded Intelligence Viewer Job Role, and CCM Embedded Intelligence Viewer Job Role. For information on adding job roles to GRC user accounts, see the *Enterprise Governance, Risk and Compliance User Guide*.

Testing the Installation

As a first test, ensure that you can open OBIEE:

- If your GRC installation uses WebLogic, open a browser and go to http://*host*:9704/analytics (in which *host* is the FQDN of the machine on which you installed GRCI). Log in with your GRCI WebLogic Administration username and password.

- If your GRC installation uses Tomcat, open a browser and go to your Business Intelligence Enterprise Edition URL. Log in with your WebLogic Administration username and password. (You noted the URL, user name, and password as you completed "Setting Up OBIEE in GRC with Tomcat.")

Second, ensure that the GRCI dashboard loads with no errors in your GRC application:

1. Ensure that the DA schema has been refreshed (see page 3-2).
2. Log on to GRC (see step 1 of "GRC Configuration" on page 2-17). Use the logon credentials of a user who has been assigned GRCI job roles.
3. Click on the Intelligence tab for each of the home and overview pages in which you've enabled a GRCI dashboard. (See step 3 of "Configuring Intelligence in GRC," page 3-12.)

If you see no errors, the integration has been successful.

Troubleshooting

As you install GRCI, you may encounter the following problems:

- An invalid property value is entered, and the installation script has run through the string replacement stage.

  You must start over. However, before running the installation script, you must either remove the obiee.properties and installation.stages files from your <MW_HOME> directory, or find the invalid value in obiee.properties and fix it after deleting the installation.stages file.

- An invalid property value is entered, and the installation script has not run through the string replacement stage.

  Simply remove the obiee.properties and installation.stages files from your <MW_HOME> directory and start the script over to go through the properties questionnaire.

- The installer skips through a stage that needs to be redone.

  Edit the installation.stages file and remove the line that has the flag corresponding to the stage you are trying to redo.

- After BI components are restarted, one or more of them are not running.

  Depending on which component fails to start, look in <MW_HOME>/instances/instance1/diagnostics/logs/<OracleBIComponentName> coreapplication_obis1 and examine the log files that were modified most recently. They will contain information you can use to resolve the startup issue.

- You see SQL errors in GRCI dashboards, or any of your OBIEE components fail to start.

  Check the following logs for more information on the errors.

  – Presentation Services Log: <MW_HOME>\instances\instance1\diagnostics\logs\OracleBIPresentationServicesComponent\coreapplication_obips1\sawlogo.log

- BI Server Component:
  <MW_HOME>\instances\instance1\diagnostics\logs\OracleBIServerComponent\coreapplication_obis1\nqquery.log
  <MW_HOME>\instances\instance1\diagnostics\logs\OracleBIServerComponent\coreapplication_obis1\nqserver.log
- BI Scheduler Component:
  <MW_HOME>\instances\instance1\diagnostics\logs\OracleBISchedulerComponent\coreapplication_obisch1\nqscheduler.log
- BI Cluster Component:
  <MW_HOME>\instances\instance1\diagnostics\logs\OracleBIClusterControllerComponent\coreapplication_obiccs1\nqcluster.log
- Java host Component:
  <MW_HOME>\instances\instance1\diagnostics\logs\OracleBIJavaHostComponent\coreapplication_obijh1\jh.log

- After the RPD is deployed and BI components are restarted, only the BI Presentation Services Component is down and the following appears in <MW_HOME>\instances\instance1\diagnostics\logs\OracleBIPresentationServicesComponent\coreapplication_obips1\sawlogo.log:

  ```
  Unable to create a system user connection to BI Server
  during start up. Trying again.
  ```

  and

  ```
  Error connecting to the Oracle BI Server: Could not connect
  to the Oracle BI Server because it is not running or is
  inaccessible.  Please contact your system administrator.
  ```

  Wait a few minutes. Then complete these steps to restart just the BI Presentation Services Component:

  1. Follow step 1 and 2 of "Deploying GRCDiagnostic.rpd and Updating Scheduler Credentials" (page 3-17) to log in to the Enterprise Manager and open the coreapplication settings page.
  2. Click on the Availability tab.
  3. Click on BI Presentation Services to select it.
  4. Click Restart Selected.
  5. Click Yes to confirm.
  6. Press Close.

- Other problems.

  Check <MW_HOME>/installation.log or <MW_HOME>/instances/instance1/diagnostics/logs/<OracleBIComponentName>coreapplication_obis1. Look for an error message to help you gather more information on the problem and possibly lead you to its resolution.

GRCI Upgrade

If you have upgraded to GRC 8.6.5.1000 from an instance in which GRCI operated, you can upgrade your GRCI instance. As noted earlier, GRCI makes use of Oracle Business Intelligence Enterprise Edition (OBIEE), which in turn is supported by WebLogic middleware components.

- If your GRC instance runs with WebLogic, you completed an "embedded" GRCI installation. (You may also have installed a second, standalone OBIEE instance, for use in customizing GRCI.)
- If your GRC instance runs with Tomcat, you completed a "standalone" GRCI installation

If your existing GRCI implementation uses versions of WebLogic components required for GRCI -5.6.5.1000 — WLS 10.3.6, ADR 11.1.1.7, and RCU 11.1.1.7 — you can reuse them as you upgrade. If not, review installation procedures earlier in this chapter (in particular, "Setting Up OBIEE in GRC with WebLogic" or "Setting Up OBIEE in GRC with Tomcat").

In any case, identify the following to complete the upgrade procedure:

- <MW_HOME>: The complete path to the middleware home that serves GRCI. If you run GRC with WebLogic, this is also the middleware home for your previous GRC instance. If you run GRC with Tomcat, this is the middleware home for the WebLogic components that exist independently of the Tomcat components that support GRC.
- If you run GRC with WebLogic, the host name and port number of the GRC server for the instance from which you are upgrading. (This is typically the WebLogic Administration server, although if you run FAACG it is a managed server.)
- If you run GRC with Tomcat, the Oracle Enterprise Manager URL and the Business Intelligence Enterprise Edition URL; the host name and port number for the WebLogic Administration server that supports OBIEE and GRCI; the fully qualified domain name for the machine on which OBIEE is installed. (These values were set, and reported in an "Installation Completed" screen, during installation of middleware components that support standalone OBIEE and GRCI. Ideally, they were noted as your earlier GRC version was installed.)
- The service identifier (SID) and schema name for the Data Analytics (DA) database schema that supports GRCI.

Beginning the Upgrade

To begin to upgrade GRCI to version 8.6.5.1000:

1. Stop OBIEE components.
2. Create a temporary directory. (Throughout this document, <obiee_temp> represents the full path to this directory.)
3. Locate the file grc-reportservices-8.6.5.1-SNAPSHOT-obiee-artifacts.zip in your <grc_stage>/dist directory. Extract its contents in <obiee_temp>.

4. Back up your GRCDWebcat folder, which is a subdirectory of <MW_HOME>/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog. Rename it or move it to another folder.
5. Copy <obiee_temp>/Webcat/GRCDWebcat to <MW_HOME>/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog.

Repository Configuration

When GRCI was set up for your earlier GRC version, an OBIEE client was installed on a Windows system. Use that system to complete the following steps:

1. Using ftp, transfer <obiee_temp>/repository/GRCDiagnostic.rpd to the Windows system.
2. On the Windows system, open the Oracle BI Administration Tool: From the Start menu, navigate to Oracle Business Intelligence Enterprise Edition Plus Client → Administration.
3. Navigate to File → Open → Offline. Select the GRCDiagnostic.rpd file you transferred in step 1. Enter *Admin123* as the Repository Password.
4. Navigate to Manage → Variables.
   - Double-click on GRI_DSN. Under Default Initializer, enter the SID for the Oracle database that hosts your DA schema, inside single quotation marks. Press OK.
   - Double-click on GRI_USER_ID. Under Default Initializer, enter the schema name used by your DA schema, inside single quotation marks. Press OK.
   - Close the Variable Manager.
5. In the main window under the Physical section, right-click on GRC Diagnostics and select Properties.
   - Click on the Connection Pools tab and double-click on GRCI Connection Pool.
   - Under the Shared Logon section, enter the schema password used by your DA schema.
   - Press OK, re-enter the schema password in the confirmation pop-up, and then press OK again.
   - Double-click on INIT BLOCK Connection Pool, and make the same password update as you made for the GRCI Connection Pool.
   - Press OK to close the Properties window.
6. Navigate to File → Save and answer No to "Do you wish to check global consistency?"
7. Exit the Oracle BI Administration Tool.

Deploying GRCDiagnostic.rpd and Updating Scheduler Credentials

Deploy the new GRCDiagnostic.rpd:

1. Start the Administration Server, BI Server, and BI components.
2. Still on the Windows machine
   - If your GRC installation uses WebLogic, go to http://*host*:*port*/em. Log in to the host with your WebLogic Administration username and password.
   - If your GRC installation uses Tomcat, go to your Oracle Enterprise Manager URL. Log in with your WebLogic Administration username and password.
3. From the left menu, expand Business Intelligence and double-click on "coreapplication."
4. Select the Deployment tab.
5. Press *Lock and Edit Configuration*.
6. Select the Repository tab.
7. Under *Upload BI Server Repository*, click the Browse button and select the GRCDiagnostic.rpd that you modified and saved on your Windows machine in "Repository Configuration" (page 3-16). Enter *Admin123* in both of the Repository Password and Confirm Password fields.
8. Under *BI Presentation Catalog*, enter the following as the *Catalog Location*: <MW_HOME>/instances/instance1/bifoundation/OracleBIPresentationServices Component/coreapplication_obips1/catalog/GRCDWebcat.
9. Click on the Apply button.
10. Click on the Activate Changes button on top.
11. Click on Close after the changes are activated.
12. Navigate to Business Intelligence → Core Application → Capacity Management → Performance. There, ensure that the cache is disabled (that the Enable BI Server Cache check box is cleared).
13. Press the *Restart to apply recent changes* button on top.
14. Click on the Restart button.
15. Select Yes.
16. Click on Close after the restart completes.

It is ok if all the BI system components are up and running, but there are warnings or errors.

Completing the Upgrade

To complete the upgrade, perform procedures that are the same as they would be for a new installation. Execute procedures described in "Connecting to the DA Schema" (page 3-2), "Configuring Intelligence in GRC" (page 3-11), and "Testing the Installation" (page 3-12).

`

4

Additional Advanced Controls Configuration

Once you've installed or upgraded GRC 8.6.5.1000, complete additional configuration procedures as needed if you intend to use AACG or ETCG:

- Define information with which GRC creates "global users." Business applications subject to models and controls may have user-account information that varies from one application to the next. GRC maps each person's business-application IDs to a global-user ID. You can determine what information GRC uses to do so. You must change the default setting if you run FAACG.

  If you are upgrading, version 8.6.5.1000 inherits the global-user definition from your earlier version. If you are satisfied with your configuration for the earlier version, you need not redefine it for version 8.6.5.1000.
- Decide whether to implement a Page Access Configurations business object, which enables AACG users to build models and controls that take PeopleSoft user preferences into account. This feature is enabled by default. If your access models and controls do not cite PeopleSoft user preferences, you can disable this feature to improve performance and reduce memory requirements.
- Set up datasources — connections to business applications in which GRC is to perform analysis. However, if you are upgrading, version 8.6.5.1000 inherits datasources configured for your earlier version. For version 8.6.5.1000, you need to set up only new datasources.
- For a new installation, synchronize data from all AACG datasources.

If you have upgraded to GRC 8.6.5.1000, you must complete the following procedures in the order indicated:

1. Perform access synchronization on all datasources used for AACG analysis (see "How to Synchronize Data," page 4-7).
2. Perform a graph rebuild on all datasources used for ETCG analysis (again, see "How to Synchronize Data" on page 4-7).
3. Run all controls that compile data for user defined objects (controls for which the result type is "Dataset").
4. Run all models and all controls that generate incidents (controls for which the result type is "Incidents").

Note, however, that if you are upgrading through several releases (for example, from version 8.6.4.6000 to 8.6.4.7000 to 8.6.5.1000), then synchronize access data,

rebuild the graph for transaction data, and run controls and models only once, after the final upgrade is complete. For information on running models and controls, and distinguishing between control types, see the user guides for AACG and ETCG.

Configuring Global Users

Implement one of the following options to determine the information GRC uses to create global users. Important: Select an option that identifies each person uniquely.

- EMAIL_ONLY: Match the global user to email addresses from distinct data-sources (or within one datasource). This is the default.
- EMAIL_AND_USERNAME: Match the global user to email address plus username from distinct datasources (or within one datasource). This option is required for FAACG implementations. Because PeopleSoft implementations often do not use the email address for users, customers who implement PeopleSoft usually select this option as well.
- EMAIL_AND_ALL_NAMES: Match the global user to email address, username, given name, and surname from distinct datasources (or within one datasource).

GRC users regularly synchronize data and analyze controls to produce "incidents" (records of control violations). If no data has been synchronized and no controls have been analyzed (in version 8.6.5.1000 or, for an upgrade, any version beginning with 8.6.4.5000), complete the following three steps to change a global-user configuration.

1. Use SQL*Plus, or any other tool with the ability to execute SQL commands on a database, to connect to the GRC schema.
2. Run the following SQL statement:

```
DELETE FROM GRC_PROPERTIES
WHERE NAME like 'GLOBAL_USER_CONFIG';
COMMIT;
```

3. Run *one* of the following SQL statements, depending on the global-user format you want to implement:

   For email and username, run the following statement:

```
Insert into GRC_PROPERTIES (NAME, VALUE, DESCRIPTION, DEFAULT_VALUE,
VISIBLE, CONFIGURABLE, DATA_TYPE_ID)Values ('GLOBAL_USER_CONFIG',
'EMAIL_AND_USERNAME', 'Global User configuration. Possible values:
EMAIL_ONLY, EMAIL_AND_USERNAME, EMAIL_AND_ALL_NAMES', 'EMAIL_ONLY',
0, 0, 0);

COMMIT;
```

   For email, username, given name, and surname, run the following statement:

```
Insert into GRC_PROPERTIES (NAME, VALUE, DESCRIPTION, DEFAULT_VALUE,
VISIBLE, CONFIGURABLE, DATA_TYPE_ID) Values ('GLOBAL_USER_CONFIG',
'EMAIL_AND_ALL_NAMES', 'Global User configuration. Possible values:
EMAIL_ONLY, EMAIL_AND_USERNAME, EMAIL_AND_ALL_NAMES', 'EMAIL_ONLY',
0, 0, 0);

COMMIT;
```

   For email only, run the following statement. (As already noted, email-only is the default configuration. Run this statement only if you have changed your global-user configuration to one of the other formats, and want to change back.)

```
Insert into GRC_PROPERTIES (NAME, VALUE, DESCRIPTION, DEFAULT_VALUE,
VISIBLE, CONFIGURABLE, DATA_TYPE_ID) Values ('GLOBAL_USER_CONFIG',
'EMAIL_ONLY', 'Global User configuration. Possible values: EMAIL_ONLY,
EMAIL_AND_USERNAME, EMAIL_AND_ALL_NAMES', 'EMAIL_ONLY', 0, 0, 0);

COMMIT;
```

A second possibility is that data has been synchronized, but controls have not been analyzed. If so, changing your global-user configuration wipes out all existing global-user data.

1. Complete the steps outlined above for the first global-user-configuration scenario (in which data synchronization and control analysis have not occurred).
2. Sill logged on to your SQL tool, also run the following SQL statement:

```
TRUNCATE TABLE GRC_SRC_USER_MAPPING;
TRUNCATE TABLE GRC_GLOBAL USER;
COMMIT;
```

A third possibility is that data has been synchronized, controls have been analyzed, and incidents have been generated. In this case, when you change your global-user configuration, all existing incidents become invalid, and all existing global-user data is wiped out.

1. Log on to GRC (see page 2-17). Select Setup and Administration under Tools in the Navigator, then Manage Application Configurations under Setup. Select the Maintenance tab, and from the Maintenance page, purge *all* existing incidents. (For detailed instructions on purging incidents, see the *Governance, Risk and Compliance User Guide*.)
2. Still logged on to GRC, go to the Manage Results page. (Select Manage Incident Results from the Result Management tasks available under Continuous Control Management in the Navigator.) Select Incident Result in the View By list box, and confirm that no incidents exist.
3. Log off of GRC and shut down the application server.
4. Complete the steps outlined above for the first global-user-configuration scenario (in which data synchronization and control analysis have not occurred).
5. While logged on to your SQL tool, also run the following SQL statement:

```
TRUNCATE TABLE GRC_SUM_CTRL_INC;
TRUNCATE TABLE GRC_SRC_USER_MAPPING;
TRUNCATE TABLE GRC_GLOBAL USER;
COMMIT;
```

6. Clear the contents of your Transaction ETL Path folder. (This folder is specified as GRC properties are set. See page 2-17).

Enabling or Disabling Page Access Configurations

An access model or control may include filters that serve as conditions — they specify users or other objects that are exempt from analysis. Like any other access filter, a condition filter specifies a business object — a set of related fields from a datasource (business application). A business object called Page Access Configurations makes PeopleSoft user-preference values available for use in condition filters. By default, processing of data provided by this business object is enabled.

If your site does not use PeopleSoft user-preference values in access models and controls, you may choose to disable the processing of Page Access Configurations data. This improves performance and reduces memory requirements.

Important Note: If you disable Page Access Configurations data processing, the business object will nevertheless appear to be available for use in models. Users may create filters that cite this object, but GRC will ignore those filters. This may cause models (and controls developed from those models) to return results that differ from those that users expect. If you disable Page Access Configurations data processing, alert users not to use the Page Access Configurations business object as they create models.

To disable Page Access Configurations data processing:

1. Shut down the GRC application server.
2. Use SQL*Plus, or any other tool with the ability to execute SQL commands on a database, to connect to the GRC schema.
3. Run the following SQL statement

```
update GRC_PROPERTIES set VALUE = 'FALSE' where NAME =
'grc.access.user.preferences';
COMMIT;
```

4. Restart the GRC application server.

Configuring Datasources and Synchronizing Data

Connect GRC to datasources (instances of business-management applications that are to be subject to GRC models or controls). Also synchronize data for each datasource — collect information required for AACG or ETCG analysis.

Synchronization and Global Users

The order in which you synchronize access data from datasources determines how GRC creates global-user IDs: It adopts the ID configured for each user in the first datasource to be synchronized. When data from a second datasource is synchronized, GRC matches users who also exist in the first datasource to their already-existing global-user IDs. For each user who did not exist in the first datasource, GRC adopts the user ID from the second datasource as the user's global ID. And so on.

AACG pages display the global-user ID for each business-application user. You may prefer to set IDs from a particular datasource as the global-user IDs.

During an upgrade, GRC inherits the global-user IDs existing on the earlier version. If you have upgraded to version 8.6.5.1000, global-user IDs are initially the same as they were for your earlier GRC version.

However, when you complete a new installation of version 8.6.5.1000, global users do not yet exist. Or, if you modify the global-user configuration (see page 4-2), existing global-user IDs are wiped out. In either of these cases, or as you add new datasources, consider the following:

Configure all datasources in which you expect to apply AACG models and controls before you synchronize data for any of them. Next, choose a datasource from which you want GRC to adopt IDs as global-user IDs, and synchronize that datasource first. Establish an order for the remaining datasources, each of which sets global IDs for users who do not exist in the datasources for which synchronization has already been completed. Then synchronize the remaining datasources in that order.

To configure datasources or to synchronize their data, log on to GRC (see page 2-17). Select Setup and Administration under Tools in the Navigator, then Manage Application Datasources under Setup.

Special Cases Involving SQL Server

You must install the Microsoft JDBC Driver 4.0 for SQL Server if your GRC instance connects to a Microsoft SQL Server datasource and if either of the following is true:

- Your GRC instance runs with Tomcat Application Server.
- Your GRC instance runs with WebLogic and implements Secure Sockets Layer (see "GRC and SSL" on page 2-24).

Install the driver before you synchronize data for the SQL Server datasource. However, if you are upgrading and have already competed this procedure for your earlier GRC version, you need not reinstall the driver.

On the GRC server:

1. Download the UNIX version of the JDBC driver — sqljdbc_*.tar.gz — from http://msdn.microsoft.com/en-us/data/aa937724.aspx.
2. Shut down your application server.
3. From the download file, extract the JDBC driver for SQL Server 2005 and newer — sqljdbc4.jar. (A SQL Server 2000 driver is also included in the download file, but is not supported by GRC.)
4. Copy the sqljdbc4.jar file to a directory appropriate for your application server:
   - If you use Tomcat, the directory is <TomcatHome>/webapps/grc/WEB-INF/lib.
   - If you use WebLogic, the directory is <MW_HOME>/user_projects/domains/<grc_domain>/lib
5. If you use WebLogic, edit the setDomainEnv.sh file, which is located in the <MW_HOME>/user_projects/domains/<grc_domain>/bin directory.

   Locate the following line:

   ```
   if [ "${PRE_CLASSPATH}" != "" ] ; then
   ```

   Immediately before that line, add the following line:

   ```
   PRE_CLASSPATH="<MW_HOME>/user_projects/domains/<grc_domain>
   /lib/sqljdbc4.jar"
   ```

   (Skip this step if you use Tomcat.)
6. Restart your application server.

How to Configure Datasources

To configure a datasource, complete these steps. However, if you have upgraded to version 8.6.5.1000, remember that it inherits datasources configured for your earlier GRC version, and you need not reconfigure them. (To set up a Fusion datasource, see page 5-5.)

1. In the GRC Manage Application Datasources page click on Actions → Create New. A Create Datasource window opens. Enter the following values:
   - Datasource Name: Create a name for the datasource.
   - Description: Type a brief description of the datasource (optional).
   - Application Type: Select the type of business application to which you are connecting, such as EBS or PeopleSoft.
   - Application Type Version: Select the version number of the business-management application to which you are connecting.
   - Default Datasource: Select the checkbox to make the datasource you are configuring the default for use in transaction models. Only one datasource can have this value selected.
   - Connector Type: For an Oracle EBS or PeopleSoft datasource, select Default. For any other application, you would need to have created and uploaded a custom connector; select it.
   - Connector Properties: Enter values required for the connector you specified in Connector Type. Values vary by connector. They may include:
     – ERP Database Type: Select the type of database — Oracle, Oracle RAC, MS SQL Server, DB2, or MySQL — used by the business-management application being configured as a datasource.
     – Hostname: For Oracle EBS or PeopleSoft, supply the fully qualified domain name (FQDN) for the machine that hosts the database used by the business-management application. Or, if the database is RAC-enabled, enter RAC@<SCAN_NAME>, where <SCAN_NAME> is the IP address/host name configured for the RAC database.
     – Service Name: For Oracle EBS or PeopleSoft, supply the SID value configured for the business-application database in the tnsnames.ora file. Or, if the database is RAC-enabled, enter the RAC service name configured for the RAC database.
     – Port: For Oracle EBS or PeopleSoft, enter the port number that the business-application database uses to communicate with other applications.
     – Username: For Oracle EBS or PeopleSoft, supply the user name for the business-application database. (For an Oracle database, this is the same as Schema Name; for an Oracle EBS instance, this is typically APPS.)
     – Password: Supply the password that authenticates the user name for the business-application database.
2. After entering values, click on the Test Connection button.
3. When the test completes successfully, click the Save or Save and Close button. A row representing the datasource appears in the Manage Application Datasources grid.

How to Synchronize Data

For a new installation or an upgrade, you must synchronize data from every datasource used for access analysis. For an upgrade, you must also "rebuild the graph" for every datasource used for transaction analysis. Perform these operations even on datasources inherited from an earlier GRC version.

An ordinary synchronization run is incremental — it creates or updates only records that are new or have changed since the previous synchronization. A graph rebuild deletes all data for a given datasource and replaces it with a complete set of current data. This typically takes longer than ordinary synchronization.

(There is an option to synchronize transaction data, and this is the preferred operation for routine use of ETCG. However, a graph rebuild is required after an upgrade. Because a transaction synchronization or graph rebuild has an effect only if at least one transaction model or control exists, neither operation is needed for a new installation.)

To synchronize access data, complete these steps:

1. In the Manage Application Datasources page, select the row for the datasource with which you want to synchronize data.
2. Click on Actions → Synchronize Access.
3. A confirmation message appears; click its OK button.

To "rebuild the graph" for transaction data, complete these steps:

1. In the Manage Application Datasources page, select the row for a transaction datasource.
2. Select Actions → Rebuild Graph.
3. A confirmation message appears; click its OK button.

Each time a datasource is synchronized, GRC updates fields in the row for that datasource: Last Access Synchronization Date and Last Access Synchronization Status show the date of the most recent access synchronization, and its completion status. Last Transaction Synchronization Date and Last Transaction Synchronization Status do the same for the most recent transaction synchronization or graph rebuild.

Determining Datasource IDs

When you configure a datasource, GRC assigns an ID number to it. If you intend to implement preventive analysis for an Oracle EBS or PeopleSoft datasource, you need to know its datasource ID. To determine the number, configure the datasource, then complete the following steps:

1. In the Manage Application Datasources page, select View > Columns.
2. A list of available columns appears. In it, select Datasource ID.
3. The Manage Application Datasources page now displays a Datasource ID column. In it, note the ID number assigned to the datasource you've configured.

If, having determined the datasource IDs for your datasources, you wish to remove the Datasource ID column from view, repeat this procedure but clear the Datasource ID selection.

5

Setting Up FAACG

If you have installed Enterprise Governance, Risk and Compliance so that you can use Application Access Controls Governor to perform segregation-of-duties analysis in Oracle Fusion Applications, complete the procedures in this chapter. (If not, this chapter does not apply to you.)

As prerequisites, Fusion Human Capital Management (HCM) and Oracle Identity Manager(OIM) must be installed, through the Fusion Applications provisioning process. In conjunction with this, Oracle Internet Directory (OID) must be set up as the LDAP repository whose identity store is managed by OIM. In addition, you must have installed GRC to run with WebLogic 11g (see chapter 2 of this document).

To set up Fusion Application Access Controls Governor (FAACG), change the GRC "global user" configuration to EMAIL_AND_USERNAME (see page 4-2). Then install a "connector" within your GRC instance. (The connector collects data from a Fusion instance and provides it in a format that GRC recognizes.) Finally , use Fusion Setup Manager to perform GRC setup.

Installing the Connector

To install a connector, you use a Manage Application Libraries page available in GRC. Before doing so, however, you must complete several preliminary configuration steps — associate the GRC domain with OID, create an OIDAuthenticator, and grant permission to the GRC code base.

If you are upgrading from an earlier FAACG instance, you've already completed these steps and need not repeat them; skip ahead to "Upload the Connector" on page 5-4. For a new installation of GRC to support FAACG, begin at the next section, "Associate the GRC Domain with OID."

Associate the GRC Domain with OID

Associate your GRC domain (set up in "Creating a WebLogic Domain" on page 2-3) with a "security store" maintained by OID.

1. Invoke the WebLogic scripting tool — wlst.sh — from <MW_HOME>/oracle_common/common/bin.

2. Enter the following command:

```
reassociateSecurityStore(domain="fusion_domain",
  servertype="OID", ldapurl="host:port", jpsroot="cn=nodename",
  admin="cn=adminuser", password="adminpassword", join="true")
```

In this command:

- *fusion_domain* is the name of the Fusion policy store (which is, in turn, the branch of the security store that identifies privileges that can be granted within applications). This value is identified beneath the "cn=JPSContext" entry in the OID LDAP tree.
- *host* is the FQDN of the LDAP provider (your OID instance), and *port* is the port number at which it communicates with other applications.
- *nodename* is the root node for your policy store within the OID LDAP tree.
- *adminuser* is the username for the OID administrative user.
- *adminpassword* is the password configured for the OID administrative user.

3. Bounce the WebLogic Administration Server and managed servers.

Create an OIDAuthenticator

Next, create an OIDAuthenticator. (However, skip this section if you installed GRC so that an external OID LDAP repository manages its users — if you completed the "Configuring External OID LDAP" section beginning on page 2-6.)

1. Log in to the WebLogic Server Administration Console:

   `http://host:port/console`

   In this URL, replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server.

2. Click on the "Security Realms" link in your application's Security Settings.
3. Click on the "myrealm" link in the table.
4. Click on the "Providers" tab.
5. Click on the New button and enter the following values:
   - Name: OIDAuthenticator
   - Type: OracleInternetDirectoryAuthenticator
6. Click on the "OIDAuthenticator" link and then click on the "Provider Specific" tab.
7. Supply values for properties in the "Provider Specific" screen. (Italicized entries are literal values, to be entered as they are shown.)
   - Host: The FQDN of the LDAP provider (your OID instance).
   - Port: The port number at which the host communicates with other applications.
   - Principal: The username for the OID administrative user, preceded by *cn=*.
   - Credential: The password configured for the OID administrative user.

- Confirm Credential: The password configured for the OID administrative user.
- SSLEnabled: Leave this box unchecked.
- User Base DN: The LDAP path to the store for user information. For example: cn=FusionUsers,cn=users,dc=us,dc=oracle,dc=com
- All Users Filter: *(&(uid=*)(objectclass=person))*
- User From Name Filter: *(&(uid=%u)(objectclass=person))*
- User Search Scope: *subtree*
- User Name Attribute: *uid*
- User Object Class: *person*
- Use Retrieved User Name as Principal: Select this checkbox.
- Group Base DN: The LDAP path to the store for group (enterprise role) information. For example: cn=FusionGroups,cn=groups,dc=us,dc=oracle, dc=com
- All Groups Filter: *(&(cn=*)(|(objectclass=groupofUniqueNames) (objectclass=orcldynamicgroup)))*
- Group From Name Filter: *(|(&(cn=%g)(objectclass=groupofUniqueNames)) (&(cn=%g)(objectclass=orcldynamicgroup)))*
- Group Search Scope: *subtree*
- Group Membership Searching: *unlimited*
- Static Group Name Attribute: *cn*
- Static Group Object Class: *groupofuniquenames*
- Static Member DN Attribute: *uniquemember*
- Static Group DN from Member DN filter: *(&(uniquemember=%M)(objectclass= groupofuniquenames))*
- Dynamic Group Name Attribute: *cn*
- Dynamic Group Object Class: *orcldynamicgroup*
- Dynamic Member URL Attribute: *labelеduri*
- User Dynamic Group DN Attribute: Leave this field blank.
- Connection Pool Size: *6*
- Connect Timeout: *0*
- Connection Retry Limit: *1*
- Parallel Connect Delay: *0*
- Results Time Limit: *0*
- Keep Alive Enabled: Leave this box unchecked.
- Follow Referrals: Select this checkbox.
- Bind Anonymously On Referrals: Leave this box unchecked.
- Propagate Cause For Login Exception: Leave this box unchecked.
- Cache Enabled: Select this checkbox.

- Cache Size: *32*
- Cache TTL: *60*
- GUID Attribute: *orclguid*

8. Save your settings, then click on "Activate Changes" on the left, topmost panel.
9. Click the "OIDAuthenticator" link from the authenticator list, and set the Control Flag to SUFFICIENT.
10. Click the "DefaultAuthenticator" link from the authenticator list, and set the Control Flag to SUFFICIENT.
11. Click the Reorder button. Select "OIDAuthenticator" from the available providers, and move it to the top. To do so, click on the arrow on the right side, then click OK.
12. Click on "Activate Changes" from the Change Center, then log out.
13. Bounce the WebLogic Administration Server and managed servers.

Grant Permission to the GRC Code Base

Use the WebLogic scripting tool to grant necessary permissions.

1. Invoke the WebLogic scripting tool — wlst.sh — from <MW_HOME>/oracle_common/common/bin.
2. Execute the grantPermission command twice, as shown below. In the commands, replace <*grc865*> with the full path to the grc865 directory created in step 4 of "Preparing Additional Files," on page 2-5. All other arguments to the commands are literal values, to be entered as shown.

```
grantPermission(codeBaseURL= "file:/<grc865>/WEB-INF/-",
permClass="oracle.security.jps.service.policystore.PolicySt
oreAccessPermission", permTarget="context=SYSTEM",
permActions="getConfiguredApplications")

grantPermission(codeBaseURL= "file:/<grc865>/WEB-INF/-,
permClass="oracle.security.jps.service.policystore.PolicySt
oreAccessPermission", permTarget="context=APPLICATION,
name=*", permActions="getApplicationPolicy")
```

3. Bounce the WebLogic Administration Server and managed servers.

Upload the Connector

The Fusion connector is provided in a file called grc-connector-fusion-8.6.5.1-SNAPSHOT-connectorsetup.zip. To upload it to GRC:

1. Log on to GRC. In a web browser, enter the following URL, in which *host* is the FQDN of your GRC server, and *port* is the number you chose for the GRC managed server as you created a WebLogic domain.

   `http://host:port/grc`

2. In the Navigator, select Setup and Administration → Setup → Manage Application Libraries. Click the Connectors tab.
3. Click on Actions → Import.

4. A Import File pop-up window opens. Click on its Browse button.
5. A file-upload dialog opens. In it, navigate to, and select, grc-connector-fusion-8.6.5.1-SNAPSHOT-connectorsetup.zip, which is among the files in <grc_stage> directory (see "Downloading Files" on page 1-4). The path and name of the file then populate the field next to the Browse button in the Import File window.
6. Click on the Upload File button. A pop-up message reports the status of the upload operation. Click on its OK button to clear it, and then click on the Close button in the Import File window.
7. Log off of GRC.
8. Ensure that the following files do not exist in the library subdirectory of your web application server:
   - tika-app-0.9.jar
   - dom4j-1.6.1.jar
   - idxuserrole-1.0.jar
   - org.openliberty.arisid-1.1.jar
   - org.openliberty.arisidbeans-1.1.jar
9. Restart both the Administration Server and the GRC managed server. (Before doing so, be sure that the file tika-app-0.9.jar does not exist in the library subdirectory of your web application server).

Create and Synchronize a Datasource

Having uploaded the connector, you will need to configure a datasource that associates your Fusion instance with the connector:

1. Log on to GRC once again.
2. Navigator → Setup and Administration → Setup → Manage Application Datasources.
3. Click on Actions → Create New. A Create Datasource window opens. Enter the following values:
   - Datasource Name: Create a name for the datasource.
   - Description: Type a brief description of the datasource (optional).
   - Application Type: Select the type of business application to which you are connecting — in this case, Fusion.
   - Application Type Version: Select the version number of the Fusion instance to which you are connecting.
   - Default Datasource: Clear this check box.
   - Connector Type: For Fusion, select the Fusion connector you installed prior to working in this Manage Application Datasources page; the correct value is *FusionConnector*.
4. Click the Save or Save and Close button. A row representing the datasource appears in the Manage Application Datasources grid.

Finally, perform a data synchronization. In the Manage Application Datasources page, select the row you've just created for the Fusion datasource. Then either click on Actions → Synchronize Access, or click on the Synchronize button in the tool bar, then on a Run Now option, and then on an Access option.

Performing GRC Setup in Fusion Setup Manager

Once the Fusion connector is installed, create an implementation project for GRC in Fusion Setup Manager (FSM).

It's assumed you are familiar with use of the Fusion Setup Manager, and with terms such as *offerings*, *activities*, *tasks*, and *tasklists*. If not, see the *Oracle Fusion Application Installation Guide* and the *Fusion Setup Manager Administrator's Guide*.

Portlet Registration

Begin by ensuring that GRC is registered successfully in FSM. With FSM open, select Manage Portlet Registration under Implementations in the Tasks list (along the left of the interface). If the Manage Portlet Registration page does not show that GRC is registered, search for the "GRC Setup" Enterprise-Application and perform the portlet registration. Refer to the *FSM Administrator's Guide* for instruction on how to perform portlet registration.

Configure Offerings

Because seeded offerings are not GRC-enabled by default, use a Configure Offerings page to enable GRC for the desired offering.

1. Open the page: Select Configure Offerings under Implementations in the Tasks list.
2. Click on the Select Feature Choices icon for the selected offering. For example, selecting the icon for the Customer Data Management offering displays a screen in which Enterprise Governance, Risk and Compliance is listed.
3. Select the Enterprise Governance, Risk and Compliance entry — click on it so that a check mark appears in its check box.
4. Click Save and Close.

Implementation Project

To display a GRC-Setup screen within FSM, create one or more implementation projects. You can base a project on the offerings enabled for GRC, or you can directly add GRC-Setup tasks (and tasklists). In either case, expanding a node will display a "Go to Task" icon for the selected task within the node, and clicking on it will render the GRC-Setup screen.

Create a GRC Setup Master Record

When you select a Go-to-Task icon, a Manage Setup Configurations screen enables you to create new GRC setup records or to search for, update, or delete existing records.

Click the Create New icon to open a Configuration screen, in which you can create or register a new GRC Setup configuration master record.

In this page, supply the following values:

- Code: A code that uniquely identifies the master record being created, for example GRC_HCM.
- Name: Short name to describe the code, for example "GRC Setup Data for Human Capital Management."
- Description: Full description, for example, "This is the master record to define GRC Setup data to enforce separation of duties mandate for HCM."

Click the Save and Continue button to save the date prior to creating detail records. (Clicking on Save and Close would return you to the Manage Setup Configurations screen.)

Create a GRC Setup Detail Record

In the Configuration (master-record) screen, locate the Configuration Details panel and click on its Create New icon. A Configuration Details screen opens, in which you can create detail records for the master record.

In this page, enter the following values:

- Detail Name: Code that uniquely identifies the detail record being created.
- Name: Short name to describe the code.
- Description: Full description.
- Status: Optional field to specify the status of the detail record. It typically contains Active or Inactive.
- Services URL: http://*host*:*port*/grc/Services/GrcService, in which *host* is the FQDN of your GRC server, and *port* is the number you chose for the Administration Server as you created a WebLogic domain.
- User Name: The user name for a user granted the Admin role defined in the GRC UI.
- Password: The password for the user granted the Admin role.
- Confirm Password: The same password, entered for verification.
- GRC Data Source: The name of the datasource configured under "Create and Synchronize a Datasource" on page 5-5.

Click on Save and Close to return to the Configuration screen.

Publish Configuration

When detail records are complete, they must be published to Oracle Identity Management. From the Configuration (master-record) screen, select (click on) a detail record in the Configuration Details panel. Then select the Publish to OIM icon (it looks like an arrow pointing upwards).

A Publish Configuration to OIM pop-up window opens. In it, enter these values:

- Protocol: The protocol used for communication with the OIM managed server. Either https or t3s is recommended, but you may use any protocol the OIM managed server accepts.
- OIM Hostname: The name of the host of the OIM managed server.
- Port Number: The port of the OIM managed server.
- OIM User Name: The name of the user with admin role on the OIM managed server. (This user must be able to invoke MBean operations.)
- OIM Password: The password of the OIM user.

6

Installing PEAs

In support of the AACG preventive analysis feature, install a Preventive Enforcement Agent (PEA) on each Oracle EBS or PeopleSoft instance that is to be subject to AACG analysis. If you are upgrading, however, you need not reinstall a PEA on an EBS or PeopleSoft instance where the PEA for an earlier GRC release already exists.

There are distinct PEAs (and installation procedures) for EBS and PeopleSoft. See the *Oracle Enterprise Governance, Risk and Compliance Certifications Document* for supported versions of Oracle EBS and PeopleSoft.

PEAs and SSL

You can install a PEA (on Oracle EBS or PeopleSoft) so that it supports Secure Sockets Layer (SSL). To do so, you must first set up GRC itself to support SSL (see "GRC and SSL" on page 2-24). Then, in the OEBS or PeopleSoft instance on which you are installing a PEA, run the following command:

```
keytool -import -alias <host name> -file <certificate file>
-keystore <name of truststore>
```

In this command:

- Replace <host name> with the host name of the GRC server.
- Replace <certificate file> with the SSL certificate file from the GRC server.
- Replace <name of truststore> with the name of a truststore on the EBS or PeopleSoft server. Supply the name of an existing truststore, or supply an unused name to create a new truststore.

As you run this command, you are prompted to supply a password for an existing truststore, or to create a password for a new one.

Move the file created by the keytool command to the $ORACLE_HOME directory for the EBS or PeopleSoft server database.

Installing the Oracle PEA

On each EBS instance for which you want to enable preventive analysis, you must install version 7.3.3 of Preventive Controls Governor (PCG) before installing version 8.6.5.1000 of the PEA.

Keep the following in mind:

- You can install GRC 8.6.5.1000 on its server without first having installed PCG on any EBS instance. If so, however, AACG would not be able to apply preventive analysis to Oracle EBS instances. You can implement preventive analysis subsequently; to do so, you would first install PCG, then the PEA, on each EBS instance for which you want to enable preventive analysis.
- Even after preventive analysis is enabled, you may choose to reinstall PCG on an EBS instance. If so, you must also reinstall the PEA on that instance.
- A single instance of GRC can connect to multiple EBS instances (once PEAs are installed on those instances). However, a given EBS instance cannot connect to multiple GRC instances.

There are both an automated PEA installer and a manual PEA installation process. If the Oracle EBS concurrent manager server and forms server reside on the same instance, attempt automated installation first, as it's simpler. If not, or if the automated installer fails, use the manual process. In either case, first complete some preliminary steps that apply to both automated and manual installations.

Preliminary Steps

If you run your Oracle EBS instance in the Linux operating system, you must set a display option. To do so, execute the following command:

```
export DISPLAY=localhost:1.0
```

As you install the PEA, you must supply the username and password of a GRC user. It's recommended that you create a user called *wsclient*, and specify that user during PEA installation. For information on creating users, see the *Enterprise Governance, Risk Governance, Risk and Compliance User Guide*.

When you configure an Oracle EBS instance as a datasource, GRC generates a datasource ID number. You must supply that number as you install the PEA. Thus sequence matters: Install GRC on its server and configure each EBS instance as a datasource (see page 4-4) before you install the PEA on any EBS instance.

In the Oracle EBS instance on which you are installing the PEA, navigate to the custom application TOP (conventionally called XXLAAPPS_TOP) created on the Preventive Controls Governor forms server. Execute a directory listing to determine if it has a subdirectory named *mesg*. If not, create the subdirectory:

```
mkdir mesg
```

Downloading and Preparing Files

Create a staging directory on the server that supports Oracle E-Business Suite. When this directory is created, complete the following steps:

1. In <grc_stage> (see page 1-4), locate grc-peainstallation-8.6.5.1-SNAPSHOT-ebs-package.zip. Extract its contents. This should produce subdirectories called db, fndload, Forms, and lib, each of which contains files. Also, files called grc-peainstallation-8.6.5.1-SNAPSHOT.jar, install.properties, and pea.properties reside in the staging directory.

2. To perform the automated installation, use a text editor to open and edit the install.properties file in the staging directory. (For a manual installation, this step is unnecessary.) Provide values for the following properties:

   - APPS_USER_NAME = *APPS*

     Supply the username for the database schema that supports your Oracle EBS instance. Typically, this value is *APPS*.

   - APPS_PASSWORD = *apps_schema_password*

     Supply the password for the Oracle EBS database schema identified in the previous property.

   - XXLAAPPS_USER_NAME = *XXLAAPPS*

     Supply the username for the database schema that supports PCG, installed on your Oracle EBS instance. Typically, this value is *XXLAAPPS*.

   - XXLAAPPS_PASSWORD = *XXLAAPPS_passsword*

     Supply the password for the PCG database schema identified in the previous property.

   - HOST = *hostname*

     Supply the host name for the Oracle EBS database server.

   - PORT = *number*

     Supply the port number at which the Oracle EBS database server communicates with other applications.

   - SID = *service_identifier*

     Supply the service identifier (SID) for the Oracle EBS database server.

   - FREQUENCY = 30

     Supply a number that sets the interval, in minutes, at which two PEA concurrent programs are to run. GRCC User Provisioning Poll handles the approval or rejection of preventive analysis requests in the Oracle EBS instance. GRCC User Provisioning Request Recovery transmits stored requests to GRC when communications with the EBS instance have been interrupted, then restored. The recommended value for both programs is 30.

3. Execute the environment file, if it is not included in the profile. Run this command:

   ```
   . $APPL_TOP/$APPLFENV
   ```

Automated Installation

Once you have downloaded files and prepared them, execute the following steps to complete an automated installation:

1. Navigate to your staging directory.
2. Run the installation file. Execute the following command:

   ```
   java -jar grc-peainstallation-8.6.5.1-SNAPSHOT.jar -ebs
   ```

The installation program prompts for property values required by the PEA:

- Enter GRCC user name

  If you created a wsclient user on your GRC instance, supply the value *wsclient* here. If not, supply the user name configured for any GRC user.

- Enter GRCC password

  Enter the password for the user identified in the previous property.

- Enter GRCC server name

  Supply the fully qualified server name of the server on which GRC is installed. To verify, ping the GRC server from the server where the PEA is being installed.

- Enter GRCC port number

  Supply the port number at which the GRC server communicates with other applications.

- Enter GRCC web services URL

  This property specifies the URL of the webservice where the GRC instance is installed. This URL should be */grc/services/GrcService/*.

- Enter GRCC web services timeout

  Enter a timeout, in seconds, for communication with the Oracle EBS server. The default value is 60.

- Enter datasource ID

  Supply the datasource ID assigned by GRC to the Oracle EBS instance in which you are installing the PEA. (This value is available in the GRC Manage Application Datasources page; see "Determining Datasource IDs," page 4-7).

3. After you enter the datasource ID, the installation program presents the prompt, "Connect to GRC server using SSL? (Yes/No)."

   - If you select No, PEA installation proceeds without support for SSL.
   - If you select Yes, the installation program prompts for an SSL truststore name and an SSL truststore password. Enter the values you created as you ran the keytool command (see "PEAs and SSL" on page 6-1).

4. When the file finishes running, review its log file: In the staging directory, use a text editor to open the file *debugInstall.log*. It notes status for several installation stages (Status of Packages, Status of Concurrent Programs, Status of Load Java, and Status of Forms), as well as for overall installation.

   - If the status for each is *Success*, PEA is installed. Ignore the manual installation procedure.
   - Otherwise, the debugInstall.log file lists errors that have occurred at each stage. Either resolve the errors and retry the automated installation process, or complete the manual installation process (see the next section).

Manual Installation

If your Oracle EBS concurrent manager server and forms server reside on separate instances, or if the automated PEA installation has failed, execute a manual installation instead. Once you have downloaded files and prepared them, complete the following sections.

Forms Installation

First, install forms. The PEA uses forms in twelve languages, for which you will need to know language codes as you perform the installation. These codes include:

D	German	**KO**	Korean
DK	Danish	**NL**	Dutch
E	Spanish	**PTB**	Brazilian Portuguese
F	French	**US**	American English
I	Italian	**ZHS**	Simplified Chinese
JA	Japanese	**ZHT**	Traditional Chinese

Complete the following steps:

1. Navigate to your staging directory.
2. Execute the following command to execute the package (PKS).

   (Here and in subsequent steps, *appsSchemaName* and *appsSchemaPassword* are the user name and password for the database schema used by Oracle E-Business Suite.)

   ```
   sqlplus appsSchemaName/appsSchemaPassword
   @db/grcc_provdb_pkg.pks
   ```

3. Execute the following command to execute the package body (PKB).

   ```
   sqlplus appsSchemaName/appsSchemaPassword
   @db/grcc_provdb_pkg.pkb
   ```

4. To set the environment variable, execute one of the following commands, once for each language. As you do, replace the placeholder *CODE* with the appropriate language code (see above).

   If you use Oracle E-Business Suite Release 12:

   ```
   export FORMS_PATH=$FORMS_PATH:$AU_TOP/forms/CODE
   ```

   If you use an earlier version of Oracle EBS:

   ```
   export FORMS60_PATH=$FORMS60_PATH:$AU_TOP/forms/CODE
   ```

5. Execute one of the following commands to compile the library:

   For Oracle E-Business Suite Release 12:

   ```
   frmcmp_batch module=Forms/GRCC_PROV.pll module_type=library
   userid=appsSchemaName/appsSchemaPassWord
   ```

   For earlier versions of Oracle EBS:

   ```
   f60gen module=Forms/GRCC_PROV.pll module_type=library
   userid=appsSchemaName/appsSchemaPassWord
   ```

6. Execute the following command to copy the compiled library.

   ```
   cp Forms/GRCC_PROV.* $AU_TOP/resource
   ```

7. To compile the forms, execute one of the following commands, once for each language. Again, as you do, replace the placeholder *CODE* with the appropriate language code (see page 6-5):

   For Oracle EBS Release 12:

   ```
   frmcmp_batch module=Forms/CODE/LAASCAUS.fmb
   userid=appsSchemaName/appsSchemaPassWord
   ```

   For earlier versions of Oracle EBS:

   ```
   f60gen module=Forms/CODE/LAASCAUS.fmb
   userid=appsSchemaName/appsSchemaPassWord
   ```

8. To back up the compiled forms, execute the following command, once for each language. Again, as you do, replace the placeholder *CODE* with the appropriate language code (see page 6-5):

   ```
   cp $XXLAAPPS_TOP/forms/CODE/LAASCAUS.fmx
   $XXLAAPPS_TOP/forms/CODE/LAASCAUS.fmx.orig
   ```

   (If you followed recommendations as you installed Preventive Controls Governor, you selected XXLAAPPS as the application short name, and the environment variable shown in this command — $XXLAAPPS_TOP — is correct. If you chose another application short name as you installed Preventive Controls Governor, make sure the environment variable in this command and the next reflects the application short name you created.)

9. To copy the compiled form, execute the following command once for each language. Again, as you do, replace the placeholder *CODE* with the appropriate language code (see page 6-5):

   ```
   cp Forms/CODE/LAASCAUS.fmx
   $XXLAAPPS_TOP/forms/CODE/LAASCAUS.fmx
   ```

Concurrent Programs Installation

Change to your staging directory and, from it, run the following commands to set up concurrent programs that support preventive analysis. In these commands:

- *appsSchemaName* and *appsSchemaPassword* are the user name and password for the database schema used by Oracle E-Business Suite.
- *XXLAAPPSUserName* is the user name for the database schema that supports Preventive Controls Governor. This value is case-sensitive.
- *frequency* is a number setting the interval, in minutes, between scheduled runs of concurrent programs (see the description of the FREQUENCY option on page 6-3).

Execute the following command to run the User Provisioning Poll concurrent program:

```
sqlplus appsSchemaName/appsSchemaPassword
@db/grccexecutable.sql XXLAAPPSUserName frequency
```

Execute the following command to run the User Provisioning Request Recovery concurrent program:

```
sqlplus appsSchemaName/appsSchemaPassword
@db/grccexecrecover.sql XXLAAPPSUserName frequency
```

Once this initial setup is complete, execute the following command once for each of the eleven supported languages, so that concurrent-program messages, parameter names, and descriptions are available in each language. As before:

- Replace the placeholder *CODE* with the appropriate language code (see page 6-5).
- *appsSchemaName* and *appsSchemaPassword* are the user name and password for the database schema used by Oracle E-Business Suite.
- *stagedir* is the path to the staging directory in which you copied and extracted PEA files.

```
FNDLOAD appsSchemaName/appsSchemaPassword 0 Y UPLOAD
$FND_TOP/patch/115/import/afcpprog.lct stagedir/fndload/CODE/
AACG_CONCURRENT_PROGRAMS.ldt
```

Load Java

Complete the following steps:

1. Set the DB environment of APPS (the Oracle EBS database) and execute the installation program, specifying a "manual" argument:

   ```
   Java –jar grc-peainstallation-8.6.5.1-SNAPSHOT.jar -ebs
   –manual
   ```

   This prepares the pea.properties file to be loaded into the database (as specified in step 5).

2. Execute the following commands. These commands should not error out:

   ```
   dropjava
   loadjava
   ```

3. Execute the following commands. In steps 3–5, *appsUserName* and *appsPassword* are the user name and password for the Oracle E-Business Suite database.

   ```
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grcc-encryption-8.6.4.5-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grcc-peacommon-8.6.4.5-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grcc-peaebs-8.6.4.5-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grcc-encryption-8.6.4.6-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grcc-peacommon-8.6.4.6-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grcc-peaebs-8.6.4.6-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-encryption-8.6.4.7-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-peacommon-8.6.4.7-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-peaebs-8.6.4.7-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-encryption-8.6.4.8-SNAPSHOT.jar
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-peacommon-8.6.4.8-SNAPSHOT.jar
   ```

```
dropjava –user appsUserName/appsPassword –verbose –resolve
-genmissing lib/grc-peaebs-8.6.4.8-SNAPSHOT.jar
dropjava –user appsUserName/appsPassword –verbose –resolve
-genmissing grc.properties
dropjava –user appsUserName/appsPassword –verbose –resolve
-genmissing pea.properties
```

4. Execute the following commands to load the pea jar into the database.

```
loadjava –user appsUserName/appsPassword –verbose –resolve
lib/grc-encryption-8.6.5.1-SNAPSHOT.jar
loadjava –user appsUserName/appsPassword –verbose –resolve
lib/grc-peacommon-8.6.5.1-SNAPSHOT.jar
loadjava –user appsUserName/appsPassword –verbose –resolve
lib/grc-peaebs-8.6.5.1-SNAPSHOT.jar
```

5. Execute the following commands to load the modified pea.properties file into the database:

```
loadjava –user appsUserName/appsPassword –verbose –resolve
grc.properties
loadjava –user appsUserName/appsPassword –verbose –resolve
pea.properties
```

Postinstallation Steps

Regardless of whether you used the automated or manual installation process, run the Generate Messages concurrent program once for each language.

1. Log in to Oracle E-Business Suite as any user with the Application Developer responsibility.
2. Select the Application Developer responsibility, and select the Requests: Run option in the Application Developer Navigator.
3. The Submit a New Request window appears. In it, select Single Request and click on the OK button.
4. The Submit Request window appears. In its Name field, query for Generate Messages. (Press the F11 key; type the value *Generate Messages* in the Name field; press Ctrl+F11.)
5. A Parameter window appears. In it, enter the following:
   - Language: With each run of the concurrent program, enter one of the language codes shown on page 6-5.
   - Application: GRC Controls Custom
   - Mode: DB_TO_RUNTIME

   Click on the OK button.
6. In the Submit Request window, click on the Submit button.
7. A pop-up window informs you of an ID number for the concurrent request. Make a note of the number, and then click on the OK button to close the message.

8. Optionally, verify that the request has been completed successfully:
   a. Click on View in the menu bar, then on Requests in the View menu.
   b. A Find Requests form opens. In it, click on the Specific Request radio button. Type the ID number of your concurrent request in the Request ID field, and click on the Find button.
   c. A Requests form opens. In the row displaying information about your request, ensure that the entry in the Phase field is *Completed* (you may need to click on the Refresh Data button), and the entry in the Status field is *Normal*.
   d. Close the Request form: Click on the × symbol in its upper right corner.

Installing the PeopleSoft PEA

You can install GRC 8.6.5.1000 on its server without installing the PEA on PeopleSoft instances. If so, however, AACG would not be able to apply preventive analysis to PeopleSoft instances. To implement preventive analysis subsequently, install the PEA on each PeopleSoft instance for which you want to enable preventive analysis. (For PeopleSoft instances, there is no requirement to install an application comparable to Preventive Controls Governor, which is necessary in Oracle EBS instances.)

As you install the PEA, you must supply the username and password of a GRC user. It's recommended that you create a user called *wsclient*, and specify that user during PEA installation. For information on creating GRC users, see the Enterprise *Governance, Risk and Compliance User Guide*.

When you configure a PeopleSoft instance as a datasource, GRC generates a datasource ID. You must supply that number as you install the PEA. Thus sequence matters: Install GRC on its server and configure each PeopleSoft instance as a datasource (see page 4-4) before you install the PEA on any PeopleSoft instance.

Downloading and Preparing Files

Create a staging directory on the server that supports a PeopleSoft Financials or HR instance. When this directory is created, complete the following steps:

1. Locate the Enterprise Governance, Risk, and Compliance Disk in your Oracle media pack. On it, locate grc-peainstallation-8.6.5.1-SNAPSHOT-ps-package.zip. Copy it to the staging directory, and extract its contents into that directory.

   The extraction should produce subdirectories of the staging directory called lib, GRCC_AGENT_86_PS_FIN90, and GRCC_AGENT_86_PS_HR90, each of which contains files. Also, files called grc-peainstallation-8.6.5.1-SNAPSHOT.jar, pea.properties, and log4j.properties reside in the staging directory.

2. Execute the installation program to update the pea.properties file:

   ```
   java –jar grc-peainstallation-8.6.5.1-SNAPSHOT.jar -psft
   ```

   The installation program prompts for property values required by the PEA:

   - Enter GRCC user name

     If you created a wsclient user on your GRC instance, supply the value *wsclient* here. If not, supply the user name configured for any GRC user.

- Enter GRCC password

  Enter the password for the user identified in the previous property.

- Enter GRCC server name

  Supply the fully qualified server name of the server on which GRC is installed. To verify, ping the GRC server from the server where the PEA is being installed.

- Enter GRCC port number

  Supply the port number at which the GRC server communicates with other applications.

- Enter GRCC web services URL

  This property specifies the URL of the webservice where the GRC instance is installed. This URL should be */grc/services/GrcService/*.

- Enter GRCC web services timeout

  Enter a timeout, in seconds, for communication with the Oracle EBS server. The default value is 60.

- Enter datasource ID

  Supply the datasource ID assigned by GRC to the PeopleSoft instance in which you are installing the PEA. (This value is available in the GRC Manage Application Datasources page; see "Determining Datasource IDs," page 4-7).

- Enter PeopleSoft SID

  Supply the service identifier (SID) for the PeopleSoft database server.

- Enter PeopleSoft port:

  Supply the number for the port at which the PeopleSoft database server communicates with other applications.

- Enter PeopleSoft FQDN

  Supply the fully qualified domain name of the PeopleSoft database server.

- Enter PeopleSoft user name

  Supply the user name for the PeopleSoft database schema.

- Enter PeopleSoft user password

  Supply the password configured for the username identified in the previous property.

- Enable PeopleSoft PEA? (y/n)

  Enter the value *y* to enable the PEA, or the value *n* to disable the PEA.

- Enter log4j properties location

  Specify the path to a directory in which the log4j.properties file will reside — *PS_HOME*/appserv/classes/log4j.properties, in which *PS_HOME* represents the full path to the highest level directory in which PeopleSoft components are installed.

(In step 5, you'll edit a copy of this file that's located in your staging directory. During installation, the file will be copied from the staging directory to a place where it can be used, and this property tells where it should be copied.)

- Enter PEA log location

  Set the path an name of a log file that records information about communications between PeopleSoft and GRC. The path is *PS_HOME*/appserv/*APP*/LOGS/grcc-peapsclient.log, in which *PS_HOME* represents the full path to the highest level directory in which PeopleSoft components are installed, and *APP* is replaced by FIN or HR, depending on whether the PEA is being install on an instance of PeopleSoft Financials or Human Resources.

- Enter interval for PEA poller

  Set a time interval, in minutes, at which an "GRCC poller" may be scheduled to run. The poller updates role assignments for PeopleSoft when the assignments have been resolved in the GRC Manage Access Approvals page. In the Roles panel of the PeopleSoft User Profiles page, a user may select a link labeled "Schedule GRCC Poller"; if so, the poller runs at intervals defined by this parameter.

3. The installation program presents the prompt, "Connect to GRC server using SSL? (Yes/No)."

   - If you select No, PEA installation proceeds without support for SSL.
   - If you select Yes, the installation program prompts for an SSL truststore name and an SSL truststore password. Enter the values you created as you ran the keytool command (see "PEAs and SSL" on page 6-1).

4. The installation program generates a temporary folder in the staging directory; it contains grcc-peaps-865.jar for installation of PEA on PeopleSoft.

5. In the staging directory, use a text editor to open and edit the log4j.properties file. Set the following property:

   ```
   log4j.appender.file.File = PS_HOME/appserv/APP/LOGS/grcc-peapsagent.log
   ```

   In this value, replace *PS_HOME* with the full path to the highest level directory in which PeopleSoft components are installed, and *APP* with FIN or HR, depending on whether the PEA is being install on an instance of PeopleSoft Financials or Human Resources.

   Do not modify the values of other properties in the log4j.properties file.

Installing the PEA

Once you have downloaded files and prepared them, execute the following steps:

1. Stop the PeopleSoft application server.

   To do so, use the psadmin utility: To start it, execute the command *PS_HOME/appserv/psadmin*. In either case, replace *PS_HOME* with the full path to the highest-level directory in which PeopleSoft components are installed. If necessary, see PeopleSoft documentation for information on using the psadmin utility.

2. From the PS_HOME/appserv/classes directory, remove any jar files that start with "grcc," "ag," or "aacg."
3. Copy the following files from the lib subdirectory of your staging directory to the *PS_HOME*/appserv/classes directory:

```
grcc-peacommon-8.6.5.1-SNAPSHOT.jar
grcc-encryption-8.6.5.1-SNAPSHOT.jar
commons-logging-1.1.jar
log4j-1.2.14.jar
ojdbc14-10.2.0.3.jar
```

4. Copy the following file from the your staging directory to the *PS_HOME*/appserv/classes directory:

```
grc-peaps-8.6.5.1-SNAPSHOT.jar
```

5. Copy the log4j.properties file from your staging directory to the directory you specified for it in the "Enter log4j properties location" property when you ran the grc-peaps-8.6.5.1-SNAPSHOT.jar file.
6. Use the psadmin utility to restart the PeopleSoft application server. (See step 1 for information on running the psadmin utility.)

Importing a Project

To complete the PEA installation, import a PeopleTools project:

1. Open the PeopleTools Application Designer. Log in as a user who has the PeopleSoft administrator role.
2. Navigate to Tools > Copy Project > From File…
3. A Copy From File dialog opens. In a field labeled "Look in:" navigate to your staging directory. This causes subdirectories of the staging directory to appear in the large, unlabeled field below the "Look in:" field, and the names GRCC_AGENT_86_PS_FIN90 and GRCC_AGENT_86_PS_HR90 to appear in the a field labeled "Select Project from the List Below." A Select button also becomes active.
4. For PeopleSoft 9.0 or 9.1 Financials, select GRCC_AGENT_86_PS_FIN90 in the "Select Project" field, and click on the Select button. For PeopleSoft 9.0 or 9.1 HR, select GRCC_AGENT_86_PS_HR90 in the "Select Project" field, and click on the Select button.
5. When the Copy from File dialog appears, click on the Copy button. After the Progress dialog disappears, confirm that application objects appear in the Application Designer project window and click on the Save All icon or File > Save All.

It's important to follow instructions in the PeopleSoft *Application Import/Update Installation Guide* when you apply an application import/update project to your database. Failure to do so could corrupt your database and cause you to lose customizations that you have made to your database.