Oracle® Enterprise Governance, Risk and Compliance

Installation Guide

Release 8.6.6.3000

Part No. E80459-01

October 2016

ORACLE

Oracle Enterprise Governance, Risk and Compliance Installation Guide

Part No. E80459-01

Primary Author: David Christie

Contents

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 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

You can install GRC 8.6.6.3000 only as an upgrade to version 8.6.6.2000. GRC runs on a 64-bit Linux server and requires the following. It's assumed you will continue to use components already installed for version 8.6.6.2000.

- An Oracle 12.1.0.2 (12*c*) database, by preference. During earlier upgrades, you may have retained an Oracle 11.2.0.4 or 11.2.0.3 database. You can continue to use that database with version 8.6.6.3000.

  In the database, a GRC schema must be created. If you implement GRCI, a data analytics (DA) schema must exist as well. The database that supports the GRC schema must use the AL32UTF8 character set.

  If you want to upgrade to the 12*c* database, follow this sequence to install GRC 8.6.6.3000: Upgrade your database to 12*c*, import your GRC schema to the 12*c* database, upgrade GRC, then point your GRC instance to the new database (see "GRC Configuration" beginning on page 8).

- 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 12*c* (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 12*c* release, RCU is packaged with ADR.

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

As an option, an OID LDAP server can manage GRC users.

On the server or a client system, the following web browsers can display the GRC interface: Microsoft Internet Explorer 11*x* or FireFox 38.5 or 43.04.

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

Recording Configuration Values

Make a note of certain configuration values for version 8.6.6.2000, as you will need to re-enter them for version 8.6.6.3000. All these values are displayed in the GRC Manage Application Configurations page. (Start the GRC 8.6.6.2000 instance, then select Navigator → Setup and Administration → Setup → Manage Application Configurations).

- Select a Properties tab and note values you will need to enter in a ConfigUI page during 8.6.6.3000 installation.

- If you have set up GRC to work with an OID LDAP repository, select a User Integration tab and note the values entered there.

- If you use GRCI, select an Analytics tab and note the values entered there.

Downloading Files

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

To upgrade GRC, download a file called grc866_3050.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 have not embedded GRCI in your 8.6.6.2000 instance, but wish to do so for 8.6.6.3000, you can do so only if you created a Data Analytics (DA) schema for GRC 8.6.6.1000 and upgraded it (reconnected it to GRC) for release 8.6.6.2000. If so, download files called grc865_1_OBIEE_ 1of3.tar.gz, grc865_ 1_OBIEE_2of3.tar.gz, and grc865_1_OBIEE_3of3.tar.gz to <grc_stage>.

For you to embed GRCI in GRC, your instance must run with WebLogic. If you use Tomcat, you can run GRCI only as a standalone application. You do not need the three grc865_1_OBIEE files for standalone GRCI, or if you have already embedded GRCI in your 8.6.6.2000 instance.

2

Upgrading GRC

In broad terms, the upgrade to GRC 8.6.6.3000 involves these steps:

1. Ensure that two directories, for the storage of GRC report data and ETL data, are ready for use.
2. Remove some files installed for your GRC 8.6.6.2000 instance, and run a setup script.
3. Restart the WebLogic or Tomcat application server, then perform configuration steps in a GRC ConfigUI page.
4. Restart your application server to complete the installation.

No matter whether you use WebLogic or Tomcat, you will (as noted in chapter 1) reuse Java and middleware components installed for GRC 8.6.6.2000.

You may continue to use the database installed for your 8.6.6.2000 instance or, if that database is 11.2.0.3 or 11.2.0.4, you may upgrade to 12*c*. If so, perform the upgrade and import your GRC and DA schemas to the new database before completing the procedures in this chapter.

Back up your database, schema, middleware components, and report and transaction ETL repositories.

GRC Repositories

For your earlier version of GRC, you should have 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.

Reuse these repositories for GRC 8.6.6.3000. 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.

GRC with WebLogic

If you installed GRC to run with WebLogic Server, complete the following steps:

1. Stop the WebLogic Administration Server and (if any exist in your installation) managed servers.
2. During installation of earlier GRC releases, a directory called grc866 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. Navigate to <grc_stage>/dist, and locate a grc.ear file.
4. Extract the contents of grc.ear into the grc866 directory.
5. Navigate to <grc_stage>/dist. From there, run the file grc_wls_setup.sh. Supply the path to the grc866 directory (into which you extracted the contents of the grc.ear file in step 4). For example:

   ```
   cmd> ./grc_wls_setup.sh <MW_HOME>/grc866
   ```

6. Remove content from the following directories. (In these paths, <grc_domain> represents the name of the WebLogic domain created for GRC during installation of version 8.6.6.1000, and <managed_server> is the name of a WebLogic managed server, if one was created during installation of version 8.6.6.1000.)

   <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

7. Copy the files jython-2.5.1.jar and xdoparser-10.1.3.4.jar from <grc_stage>/lib to <MW_HOME>/user_projects/domains/<grc_domain>/lib.
8. Navigate to the file setDomainEnv.sh, and open it in a text editor. The file is located in the <MW_HOME>/user_projects/domains/<grc_domain>/bin directory.
9. In setDomainEnv.sh, locate the following lines:

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

10. Add the following before those lines:

    PRE_CLASSPATH="<MW_HOME>/user_projects/domains/<grc_domain>/lib/jython-2.5.1.jar:${PRE_CLASSPATH}" export PRE_CLASSPATH

    (Replace <MW_HOME> and <grc_domain> with the specific values appropriate for your environment.)

11. Restart the WebLogic servers.

GRC with Tomcat

If you installed GRC to run with Tomcat Application Server, complete the following steps:

1. Shut down the Tomcat Application Server.
2. Remove the directory <TomcatHome>/webapps/grc and all its contents.
3. Remove the Catalina directory from the Tomcat work area (<TomcatHome>/work/Catalina). Delete the contents of <TomcatHome>/temp. Also delete Tomcat logs, located at <TomcatHome>/logs. (You may want to save them to another location.)
4. Navigate to <TomcatHome>/webapps and delete the grc.war file.
5. Navigate to <grc_stage>/dist. From there, run the file grc_tomcat_setup.sh. Supply the paths to the <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>
   ```

6. Copy the file xdoparser-10.1.3.4.jar from <grc_stage>/lib to <TomcatHome>/webapps/grc/WEB-INF/lib.
7. Start the Tomcat application server.

GRC Log-On URL

When you installed release 8.6.6.1000 of GRC, you may have set it up to support Secure Sockets Layer (SSL). How you log on to GRC depends on whether it does or does not support SSL.

If you have not set up GRC to use SSL, log on with the following URL:

`http://host:http_port/grc`

Replace *host* with the fully qualified domain name (FQDN) of your GRC server. Select one of the following values for *http_port*:

- If you use WebLogic 12*c*, enter the port number you chose for the Administration Server as you created a WebLogic domain.
- If you use Tomcat, enter 8080 (if you accepted the default value when you installed Tomcat) or your configured value (if you changed the default during Tomcat installation).

If you have set up GRC to use SSL, log on with the following URL:

`https://host:https_port/grc`

Again, replace *host* with the FQDN of your GRC server. Select one of the following values for *https_port*:

- If you use WebLogic 12*c*, enter the port number you selected as the SSL Listen Port when you set up SSL for GRC.
- If you use Tomcat, enter the port number you selected as the Connector Port when you set up SSL for GRC.

GRC Configuration

Regardless of whether you use WebLogic or Tomcat, perform GRC-specific configuration:

1. Open a ConfigUI page: Navigate to your GRC log-on URL. If prompted, supply the *admin* user ID along with a password established for that user ID during installation of version 8.6.6.1000.
2. 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.
   - Server Name: Supply the FQDN of the database server.
   - 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 “GRC Repositories” on page 5.
   - 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*, *debug*, and *trace*. Select *trace* only if Oracle Support instructs you to do so.
   - Transaction ETL Path: Enter the full path to the directory you created to hold ETL data used by Enterprise Transaction Controls Governor (see “GRC Repositories” on page 5).
   - 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 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 concept applies to AACG and ETCG, the process 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:

  Number of Cores Available for Processing: 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.

  Maximum Megabytes of Physical RAM Available: Specify an amount of memory for use in parallel processing. Ensure that this value is at least 16 GB times the number of cores. GRC then divides the memory value by the core value to determine the actual amount of memory per core.

  This value is in addition to what is already allocated to the WebLogic Admin server or Tomcat server. Review the amount of memory allocated to other processes (such as Linux or database management) before allocating memory to parallel processing. **Important:** Allocating more memory than what is available causes disk swapping, which causes poor performance during peak load.

- 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 "GRC Log-On URL," page 7).
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. Use the *admin* user ID, with a password established for that user ID during the installation of version 8.6.6.1000.

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 have set up an OID LDAP repository, complete these additional steps:

1. In GRC, select Navigator → Setup and Administration → Setup → Manage Application Configurations.
2. 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 11.
   - 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.
- Password: Enter the password for the user identified in the User Name field.
- 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.
- Server Name: Enter the host name of the LDAP server.
- Bind DN Suffix: Enter the "User Base DN."
- 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

3. In the Manage Application Configurations page, click on Actions → Save. Then log off of GRC.
4. 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.
5. 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 11*g*, but also Oracle HTTP Server (OHS) 11*g* WebGate for OAM.

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

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 11*g* WebGate.
3. In the Create OAM 11*g* 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 11*g* 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 FQDN of your GRC server. Replace <GRC_PORT_NUMBER> the number of your HTTP Port if SSL is not enabled, or your HTTPS Port if SSL is enabled. See "GRC Log-On URL" (page 7) for more information on identifying these port numbers.

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 2 on page 10.)
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.

GRC and SSL

When you installed release 8.6.6.1000 of GRC, you may have set it up to support Secure Sockets Layer (SSL). If so, complete the following steps to ensure that GRC communicates properly with preventive enforcement agents (PEAs) installed in Oracle E-Business Suite instances subject to AACG analysis.

1. Copy the file axis2.xml from <grc_stage>/conf to:
   - <MW_HOME>/user_projects/domains/<grc_domain>/grc/WEB-INF/conf, if you installed GRC to run with WebLogic.
   - <TomcatHome>/webapps/grc/WEB-INF/conf, if you installed GRC to run with Tomcat.
2. Copy the file addressing-1.7.3.mar from <grc_stage>/modules to:
   - <MW_HOME>/user_projects/domains/<grc_domain>/grc/WEB-INF/modules, if you installed GRC to run with WebLogic.
   - <TomcatHome>/webapps/grc/WEB-INF/modules, if you installed GRC to run with WebLogic.
3. Open the axis2.xml file in a text editor. In it, search for the following text:

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
      <parameter name="port"><add HTTP Port></parameter>
</transportReceiver>

<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
   <parameter name="port"><add HTTPS Port></parameter>
</transportReceiver>
```

4. In that passage:
   - Replace the phrase “add HTTP Port” with the number of the port GRC would use if SSL were not enabled.
   - Replace the phrase “add HTTPS Port” with the number of the port GRC uses once SSL is enabled.

   See “GRC Log-On URL” (page 7) for more information on identifying these port numbers.

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.)

You can run GRCI only if the DA schema was created for a release of GRC that could be installed independently of earlier releases — in this case, 8.6.6.1000, then reconnected to GRC for each subsequent upgrade-only release of GRC (in this case, 8.6.6.2000). You are assumed (for the purposes of this chapter) to be upgrading an instance of GRCI already present in GRC 8.6.6.2000.

You may install a "fresh" instance of GRCI only if a DA schema was created for release 8.6.6.1000, then reconnected to GRC for release 8.6.6.2000. If so, obtain version 8.6.6.1000 of the *GRC Installation Guide* and follow its instructions for installing OBIEE and supporting middleware components.

Preparing for the Upgrade

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.

Regardless of whether you installed GRC to run with WebLogic 12*c* or Tomcat Application Server, you will have installed GRCI to run with WebLogic 11*g* components. As you upgrade to 8.6.6.3000, you will reuse the OBIEE and WebLogic 11*g* components. To complete the procedure, identify the following:

- <MW_HOME>: The complete path to the 11*g* middleware home that serves GRCI. (If you installed GRC to run with WebLogic, this is not the same as the 12*c* middleware home that serves 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.)
- 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 GRCI 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 8.6.6.3000:

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-8.6.6.3-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 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.

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 "GRC Log-On URL," page 7). 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. (These are values that you noted earlier. See "Recording Configuration Values" on page 2.)
   - 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. You can modify a schedule at any time. (A refresh can take up to 90 minutes to finish.)

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.

Configuring Intelligence in GRC

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

1. Log on to GRC (see "GRC Log-On URL," page 7). Select Navigator → Tools → Setup and Administration → Setup → Manage Application Configurations → Analytics.
2. In the GRC Intelligence Configuration section, supply the following values. (Again, these are values you noted earlier. See "Recording Configuration Values" on page 2.)
   - OBIEE Server Username: The user name configured for the WebLogic Administration Server.
   - OBIEE Server Password: The password for the OBIEE Server Username (the password configured for the WebLogic Administration Server).
   - OBIEE Server Port: If your GRC installation uses WebLogic, *9704*. If your GRC installation uses Tomcat, the port number configured for the 11*g* WebLogic Administration Server used for GRCI.
   - 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.
   - 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
- 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.

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 18).
2. Log on to GRC (see "GRC Log-On URL," page 7). 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 "Configuring Intelligence in GRC," page 19.)

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

4

Additional Advanced Controls Configuration

Once you've upgraded to GRC 8.6.6.3000, 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.

  If you are upgrading, version 8.6.6.3000 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 8.6.6.3000.
- 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 8.6.6.3000 inherits datasources configured for your earlier version. For version 8.6.6.3000, you need to set up only new datasources.
- 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 27).
  2. Perform a graph rebuild on all datasources used for ETCG analysis (again, see "How to Synchronize Data" on page 27).
  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 8.6.6.1000 to 8.6.6.2000 to 8.6.6.3000), 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 datasources (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). 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 8.6.6.3000 or any earlier version), 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 "GRC Log-On URL," page 7).
2. From the Navigator, select Tools → Setup and Administration → Setup → Manage Application Configurations. 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*.)
3. Still logged on to GRC, select Navigator → Continuous Control Management → Results Management → Manage Incident Results. In a Manage Results page, select Incident Result in the View By list box. Confirm that no incidents exist.
4. Log off of GRC and shut down the application server.
5. Complete the steps outlined above for the first global-user-configuration scenario (in which data synchronization and control analysis have not occurred).
6. 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;
```

7. Clear the contents of your Transaction ETL Path folder. (This folder is specified as GRC properties are set. See "GRC Configuration," page 8.)

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.

However, during an upgrade, GRC inherits the global-user IDs existing on the earlier version. For version 8.6.6.3000, global-user IDs are initially the same as they were for version 8.6.6.2000.

If you modify the global-user configuration (see page 22), existing global-user IDs are wiped out. In that case, 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 "GRC Log-On URL," page 7). 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.

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. (Skip this step if you use Tomcat.)

   The setDomain Env.sh file is located in the <MW_HOME>/user_projects/domains/<grc_domain>/bin directory. In it, 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:${PRE_CLASSPATH}" export PRE_CLASSPATH
   ```

   Replace <MW_HOME> and <grc_domain> with the specific values appropriate for your environment.
6. Restart your application server.

How to Configure Datasources

To configure a datasource, complete these steps. However, remember that GRC version 8.6.6.3000 inherits datasources configured for your earlier GRC version, and you need not reconfigure them.

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 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

You must synchronize data from every datasource used for access analysis, and "rebuild the graph" for every datasource used for transaction analysis — even datasources inherited from your earlier GRC version.

An ordinary synchronization run 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.

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.

There is an option to synchronize transaction data; it's the preferred option for routine use of ETCG. However, do not use it in this instance. During a GRC upgrade, you must perform a graph rebuild on transaction datasources.

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 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

Installing PEAs

In support of the AACG preventive analysis feature, install a Preventive Enforcement Agent (PEA) on each Oracle EBS instance that is to be subject to AACG analysis.

A new PEA is available for EBS. If an earlier PEA exists on an EBS instance, you must replace it with the new one. Installation instructions for the new PEA follow.

See the *Oracle Enterprise Governance, Risk and Compliance Certifications Document* for supported versions of Oracle EBS.

PEAs and SSL

You can install a PEA so that it supports Secure Sockets Layer (SSL). To do so, you must first have set up GRC itself to support SSL. Then, in the OEBS 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 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 server database.

Installing the Oracle PEA

On each EBS instance for which you want to enable preventive analysis, version 7.3.3 of Preventive Controls Governor (PCG) must be installed before you install version 8.6.6.3000 of the PEA.

Keep the following in mind:

- You can install GRC 8.6.6.3000 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 24). Then identify the ID for each datasource (see page 27). Only then should you install the PEA on the 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>/dist/ (see page 3), locate grc-peainstallation-8.6.6.3-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-8.6.6.3-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-8.6.6.3-SNAPSHOT.jar –ebs
   ```

3. Respond to 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. This is the HTTPS Port value if you set up GRC to support SSL, or the HTTP Port value if not. See "GRC Log-On URL" (page 7) for more information on identifying these port numbers.
   - 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 27.)
4. Respond to a prompt presented by the installation program: "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 29).
5. Next, the installation program presents the prompt, "Enable MOAC (Yes/No)?" If you are installing the PEA in an EBS R12 instance set up to use MOAC, select Yes. Otherwise, select No.
6. 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 33):

   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 33):

   ```
   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 33):

   ```
   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 31).

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 33).
- *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 your environment for the Oracle EBS database and execute the installation program, specifying a "manual" argument:

   ```
   Java –jar grc-peainstallation-8.6.6.3-SNAPSHOT.jar -ebs
   -manual
   ```

   This prepares the pea.properties file to be loaded into the database. The installation program prompts for property values required by the PEA. See steps 3 through 5 of "Automated Installation" (beginning on page 31).

2. If the PEA has been installed previously, execute the following commands. If not, skip ahead to step 3. In these commands, replace *appsUserName* and *appsPassword* with the user name and password for the Oracle E-Business Suite database. Wildcard characters (*) represent the version number of your earlier PEA.

   ```
   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-encryption-*.*.*.*-SNAPSHOT.jar

   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-peacommon-*.*.*.*-SNAPSHOT.jar

   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing lib/grc-peaebs-*.*.*.*-SNAPSHOT.jar

   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing grc.properties

   dropjava –user appsUserName/appsPassword –verbose –resolve
   -genmissing pea.properties
   ```

3. Execute the following commands to load the pea jar into the database. You can ignore any ORA-00942 error on dropping JAVA$CLASS$MD5$TABLE.

   ```
   loadjava –user appsUserName/appsPassword –verbose –resolve
   lib/grc-encryption-8.6.6.3-SNAPSHOT.jar

   loadjava –user appsUserName/appsPassword –verbose –resolve
   lib/grc-peacommon-8.6.6.3-SNAPSHOT.jar

   loadjava –user appsUserName/appsPassword –verbose –resolve
   lib/grc-peaebs-8.6.6.3-SNAPSHOT.jar
   ```

4. 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 33.
   - 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.