Oracle Utilities
Distributed Grid Management

Installation and Configuration Guide

Release 2.0.0.2

E35572-01

July 2012

ORACLE

Oracle Utilities Distributed Grid Management Installation and Configuration Guide, Release 2.0.0.2

E35572-01

Contents

Preface

Read through this guide thoroughly before beginning an installation and configuration of Oracle Utilities Distributed Grid Management.

Audience

This document is intended for the administrator and the engineers responsible for installing and configuring Oracle Utilities Distributed Grid Management.

Related Documents

For more information, see the following documents in the Oracle Utilities Distributed Grid Management, Release 2.0.0.2, documentation set:

- *Oracle Utilities Distributed Grid Management Release Notes*
- *Oracle Utilities Distributed Grid Management Quick Install Guide*
- *Oracle Utilities Distributed Grid Management User's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1

Introduction

The information provided in this document is here to guide you through the successful installation and configuration of Oracle Utilities Distributed Grid Management, which provides optimal control of a microgrid or a small section of a larger distribution grid.

Oracle Utilities Distributed Grid Management has two primary components:

- **The Manager**: The Manager is the server component, which contains the business logic for the calculations and optimizations that it communicates to external systems and grid devices via project specific adapters.
- **The Viewer**: The Viewer, which is a rich client that runs on a PC, provides the user interface for operator analysis and system interaction through the Manager.

This document takes you through the installation and configuration of the Manager and the Viewer, sequentially. Oracle recommends that you read this document thoroughly before beginning your product installation and configuration. It is important that you complete these tasks in the required order before proceeding to any post-installation steps.

Before You Begin

Verify that your system's hardware and software meet the specifications prior to installing Oracle Utilities Distributed Grid Management. Oracle Utilities Distributed Grid Management hardware and software requirements are specified in the *Oracle Utilities Distributed Grid Management Quick Install Guide*.

Chapter 2

Manager Installation and Configuration

This chapter provides instructions for installing and configuring the Oracle Utilities Distributed Grid Management server component, the Manager. This chapter includes the following topics:

- **Before You Begin**
- **Installing the Manager**
- **Configuring the Manager**
- **Configuring WebLogic Server**

Before You Begin

In order to install Oracle Utilities Distributed Grid Management, your system must have the required versions of the Oracle Database and WebLogic Server installed. See the *Oracle Utilities Distributed Grid Management Quick Install Guide* "Certified and Supported Platforms" section to verify that you have installed the required versions for the prerequisite software components.

Installing the Manager

This section contains the following topics:

- **Download Oracle Utilities Distributed Grid Management**
- **Install the Manager Files**
  - **Installation User**
  - **Installing the Manager**
  - **Create Database Environment**

Download Oracle Utilities Distributed Grid Management

Oracle Utilities Distributed Grid Management is provided for electronic download from Oracle delivery and support websites.

- New installation packages are available from Oracle Software Delivery Cloud (http://edelivery.oracle.com). Only the OS-specific Package installers are available from this site; upgrade installers are not available. These files are downloaded as ZIP files.
- Upgrade installation packages are available from My Oracle Support (https://support.oracle.com/CSP/ui/flash.html). You must have a current My Oracle Support account to access the site.

Install the Manager Files

The Manager files are installed on the server in a directory accessible by WebLogic.

Installation User

The user account you use when installing Oracle Utilities Distributed Grid Management is important. Review the following information before deciding which user account to use:

- Do not run the installation program as the root user.
- When performing an upgrade to an existing Oracle Utilities Distributed Grid Management installation, you must perform the upgrade using the same user ID as was used to perform the initial installation.
- The WebLogic Server user requires read privileges to the **`microgrid`** directory created during the Oracle Utilities Distributed Grid Management installation.

Installing the Manager

1. Login using your user account.
2. At the command prompt, enter `unzip <path/filename>.zip`
   - `path` is the path to the installation package zip file.
   - `filename` is the name of the installation package zip file.

After unzipping the distribution file, you will see a directory called `dgm`. This directory will be referred to as **`MICROGRID_HOME`**, which is a system property required by the Manager. Using an account with suitable privileges, add **`MICROGRID_HOME`** as an environment variable.

Create Database Environment

The Manager installation requires the availability of a database.

> **Note:** Oracle Database 11g Release 2 (11.2) must be installed and running on a server that is accessible to the server where the Manager is installed; it does not have to be installed on the same server.

The following steps ask you to modify and then run three SQL files needed to configure the database environment.

Modify and run UserSetup.sql:

1. Modify the `$MICROGRID_HOME/config/manager/sql/oracle/UserSetup.sql` file to suit your environment.
2. Run `$ sqlplus user/password@db_name < $MICROGRID_HOME/config/manager/sql/oracle/UserSetup.sql`

Modify and run AdminUserSchemaSetup.sql

1. Modify the `$MICROGRID_HOME/config/manager/sql/oracle/AdminUserSchemaSetup.sql` file to suit your environment.
2. Run `$ sqlplus user/password@db_name < $MICROGRID_HOME/config/manager/sql/oracle/AdminUserSchemaSetup.sql`

Modify and run AppUserSchemaSetup.sql

1. Modify the `$MICROGRID_HOME/config/manager/sql/oracle/AppUserSchemaSetup.sql` file to suit your environment.
2. Run `$ sqlplus user/password@db_name < $MICROGRID_HOME/config/manager/sql/oracle/AppUserSchemaSetup.sql`

Configuring the Manager

This section contains the following topics:

- **Understanding Data Preparation**
- **Editing the Manager Configuration File**
- **Defining User Roles**

Understanding Data Preparation

Oracle Utilities Distributed Grid Management engineering data contains network information regarding devices and device attributes. The information is maintained in the **Engineering Workbook**.

About the Engineering Workbook

The Engineering Workbook is an Excel spreadsheet (*Engineering_Workbook.xls*) that contains data obtained from the Oracle Utilities Network Management System's network data.

> **Note:** You should copy the workbook that comes with the product to use as a template.

The engineering workbook holds the following data:

- **Conductor type catalog:** impedance per unit length. Supported units: ohms per foot, yard, mile, meter, or kilometer
- **Conductor limits:** in amperes.
- **Generators:** data associated with generators required, primarily, for DER optimization purposes.
- **Energy Storage:** data associated with energy storage devices needed for resource optimization.
- **Cost Curves:** data associated with quadratic and segmented cost curves for generators.
- **Controllable equipment:** control actions available for each equipment. [no need to enter equipment that is not controllable].
- **Measured Values:** types of measured values available for each equipment [no need to enter equipment that does not have any associated measured value].
- **Sources:** Specification for 'extra' sources, such as grid supply points, that are not already defined in the system model data.
- **IslandController:** data associated with islanding. Data required for islanding includes:
  - External device identifier for the grid source.
  - External device identifiers for the matching DER (or DERs) that will provide frequency control and regulation when the system is islanded.
  - External device identifier for switches that need to be opened to isolate the microgrid from the main grid.

> **Note:** the data descriptions above do not directly correlate to the spreadsheet tab names.

The engineering workbook spreadsheet has a built in macro that can be invoked from the "overview" tab that exports the data from the spreadsheet to an XML file. The user can provide a file name and location. This file must be moved to `$MICROGRID_HOME/data/manager`, and the file name must be assigned to the key *Data.engFile* in `$MICROGRID_HOME/config/manager/config.xml` file.

Network Model Information

Oracle Utilities Distributed Grid Management reads model data in a format compatible with the Oracle Utilities Network Management System ***.mb** file format (or equivalent XML format) along with associated class data in an XML format. Typically the network data will be one or more Oracle Utilities Network Management System partitions representing a small section of system to be controlled by Oracle Utilities Distributed Grid Management. For customers not using the Oracle Utilities Network Management System, model data must be converted into this format or hand populated using the Microsoft Office Visio tool, which is shipped with Oracle Utilities Distributed Grid Management. The network model information must, ultimately, be contained in the following two files.

- **<network_name>.xml:** this file is obtained by converting a corresponding ***.mb** file (or equivalent).
- **ClassCatalog.xml:** this file contains mapping between class names to numbers and types

Both of the above files must be moved to the Oracle Utilities Distributed Grid Management server at location `$MICROGRID_HOME/data/manager`, and the file names must be assigned to the *Data.ModelFiles* section, and the *Data.classFile*, respectively, in `$MICROGRID_HOME/config/manager/config.xml` file.

Load Curve Data

Oracle Utilities Distributed Grid Management also requires Load Curves data. to represent the variation of load over time for forecasting purposes. This data is populated in a CVS file. The Load Curves data file must also be placed in `$MICROGRID_HOME/data/manager` folder, and the file name must be assigned to key *Data.loadCurveFile* in `$MICROGRID_HOME/config/manager/config.xml` file.

Generator Curve Data

Oracle Utilities Distributed Grid Management also reads Generator Curve Data from a csv file. This is the generation forecast for renewable resources such as wind turbines or solar panels. This data is in the same format as that of the load curves data. The data file must be placed in `$MICROGRID_HOME/data/manager` folder and the file name must be assigned to key *Data.GeneratorCurveFile* in `$MICROGRID_HOME/config/manager/config.xml`.

Distributed Energy Resource Scheduling Data

The DER scheduling functionality is capable of using time varying generator cost curves. These curves can be provided in a csv file. This file must be placed at the same location as that of other data files. The file name must be assigned to key *Data.generatorCostCurveFile* in `$MICROGRID_HOME/config/manager/config.xml`.

Editing the Manager Configuration File

The Manager configuration file (`$MICROGRID_HOME/config/manager/config.xml`) controls a range of configuration options for the Manager. The content is arranged hierarchically so that main sections exist for major functional areas and individual settings are contained in elements within the sections. The root (**`config`**) element contains the following sections:

- **Manager**
- **Command**
- **Data**
- **Forecast**
- **Modes**
- **Persistence**
- **Optimization**
- **Alerts**
- **Adapters**

Manager

The primary Manager application parameters.

Key	Default	Values	Description
`batchSize`	10		Upper limit of the number of device update messages to process as a batch.
`cycleTime`	30	10-600	Seconds to wait between Manager updates if no new incoming measurements / status data
`sessionTimeout`	300	30-600	Seconds to wait on web session
`Authentication`	LDAP authentication settings		
`dsEnabled`	false	true/false	True if LDAP authentication should be used
`dsName`	Localmspiota	LDAP ds name	Name of LDAP provider set up in WebLogic
`vendor`	OpenDS	LDAP vendor	Name of vendor
`basedn`	dc=tugbu, dc=org	Base dn	Base dn value

Command

Settings for device action command timing.

Key	Default	Values	Description
`timeout`	30	30-1800	Seconds to wait for a command to be completed before it is identified as Timed Out
`Unapproved`	Contains the time-out for unapproved commands		
`timeout`	60	30-1800	Seconds to wait for a command requiring manual Approval to be completed before it is identified as *Timed Out*

Data

Data for defining the microgrid area.

Key	Default	Values	Description
`builder`	0	0,13,33,1-5000	Values other than zero load test system data
`classFile`	filename		Filename from NMS data containing device class data in XML format
`engFile`	filename		Filename containing engineering data. Normally exported from the DGM Engineering Data workbook.
`loadCurveFile`	filename		CSV text file containing load curve data for each load in the system
`generatorCurveFile`	filename		Optional CSV text file containing generator curve data for each non-dispatchable DER in the system
`generatorCostCurveFile`	filename		Text file containing time-specific DER cost curve data. This is unnecessary if the DER cost curves are fixed. Useful for importing ISO data for grid tie costs.
`lengthUnit`	FOOT	FOOT, YARD, METER	Length unit used to represent conductor lengths in the model data

Key	Default	Values	Description
ModelFiles	One or more File[n] sections each representing settings for a data model file.		
File[n]	Settings for an individual data files.		
name	filename	filename	Filename of NMS mb format system data file
scale	1.0,1.0		Optional field. X and Y scaling of coordinates in this model file
referencePoint	x,y		Optional field. Original X and Y coordinate of point in original model file.
destinationPoint	x,y		Optional field. New X and Y coordinate of referencePoint coordinate.

Forecast

Settings for load forecasting periods. Child elements:

- **LoadScalingWindow**
- **Timeline**

Key	Default	Values	Description
LoadScalingWindow	Period during the forecast for which to apply current measurement data effects on loading		
fadingHours	12	0-48	Hours over which to reduce scaling from measured values to historical values. Starts after the nonFadingHours period
nonFadingHours	12	0-48	Hours into the future for which to apply full scaling factors derived from difference between historical values and measured values

Key	Default	Values	Description
`Timeline`	Settings for determining the number of time slots to keep track of for both future forecasts and recent past data Contains: `PreferredHour`, `Future`, and `Past`.		
`PreferredHour`	12	0-23	Hour of the data for which to run forecasts for daily intervals
`Future`	Time slot configuration for future forecasts.		
`IntervalInfo[n]`	Number and spacing of time slots for future forecasts		
`spacing`	1	1+	Number of units of time between time slots
`unit`	MINUTE	MINUTE, HOUR, DAY	Unit of time for time slot interval
`quantity`	10	1+	Number of time slots of this spacing and unit to use
`Past`	Time slot configuration for historical data		
`IntervalInfo[n]`	Number and spacing of time slots for past data		
`Threshold`	1	1+	Number of units of time that must pass in order to keep a past time slot
`unit`	MINUTE	MINUTE, HOUR, DAY	Unit of time for time slot interval
`quantity`	10	1+	Number of time slots of this spacing and unit to use

Modes

The Modes section contains settings for *system modes* that define what device actions and optimizations are enabled or disabled when that mode is active.

Key	Default	Values	Description
`defaultMode`		Mode name	The name of the default mode when the system starts. Must match one of the Mode[n] names.
`Mode[n]`	One or more sections each representing settings for a mode.		
`name`			Name of the mode.
`description`			Description of the mode.
`DeviceActions`	Device action definitions for the mode.		
`requireUserPermission`		true, false	Determines if device actions require user permission before they are sent to the device. *`true`*: all device actions require user permission before they can be sent. *`false`*: device actions are sent without requiring user approval.
`restrictions`			Comma delimited list of restricted device actions.

restrictions values

- **`SWITCH_STATUS:`** Switch status change is not allowed
- **`DER_ON:`** Turning on of DERs is not allowed
- **`DER_POWER:`** Change in power set point of DERs is not allowed
- **`DER_MODE_AUTO:`** DERs cannot be put into auto mode
- **`CAP_STEP:`** Capacitor step change is not allowed
- **`CAP_MODE_AUTO:`** Capacitors cannot be put in auto mode
- **`TRANS_TAP:`** Tap changes on transformer are not allowed
- **`TRANS_MODE_AUTO:`** Transformer cannot be put in auto mode
- **`REG_TAP:`** Regulator tap change is not allowed
- **`REG_MODE_AUTO:`** Regulators cannot be put into auto mode

Key	Default	Values	Description
OptimizationsNotRun			Comma delimited list of optimizations that will not run when the mode is active.
			OptimizationsNotRun values • **OPT_VOLTVAR:** Volt var optimization is disabled • **OPT_SWITCH:** Switch reconfiguration is disabled • **OPT_SCHEDULING:** Resource scheduling is disabled • **OPT_DISPATCH:** Dispatch optimization is disabled

Oracle Utilities Distributed Grid Management has the following predefined modes:

- *Manual*: All functionality is enabled, but device actions require user permission to be executed. This is the default mode.

```
<Mode2>
  <name>Manual</name>
  <description>Require manual approval before performing
   device actions.</description>
  <DeviceActions>
    <requireUserPermission>true</requireUserPermission>
    <restrictions />
  </DeviceActions>
  <optimizationsNotRun />
</Mode2>
```

- *Full Functionality*: This is a fully automatic mode where all functionality is enabled and device actions are executed automatically without need for user intervention.

```
<Mode1>
  <name>Full Functionality</name>
  <description>Perform device actions automatically</description>
  <DeviceActions>
    <requireUserPermission>false</requireUserPermission>
    <restrictions />
  </DeviceActions>
  <optimizationsNotRunoptimization />
</Mode1>
```

- *No Optimization:* All optimization functions are disabled.

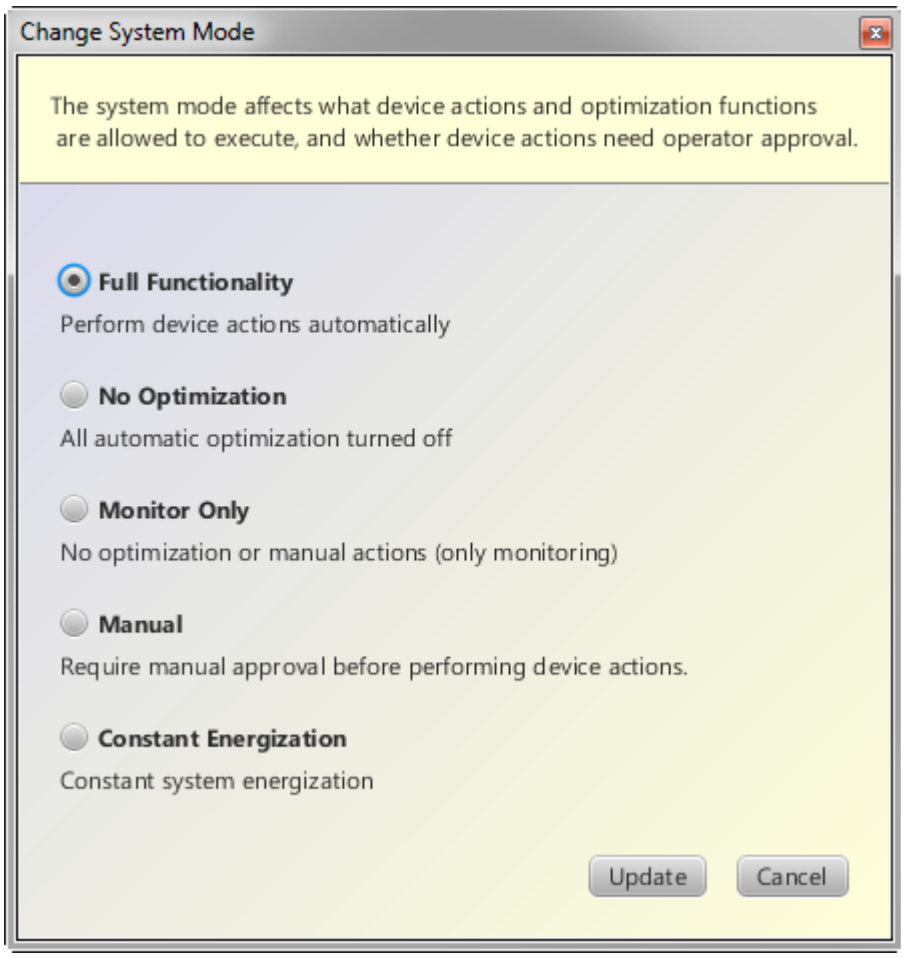
```
<Mode3>
  <name>No Optimization</name>
  <description>All automatic optimization turned off</description>
  <DeviceActions>
    <requireUserPermission>true</requireUserPermission>
    <restrictions />
  </DeviceActions>
  <optimizationsNotRun>
       OPT_VOLTVAR, OPT_SWITCHING, OPT_SCHEDULING, OPT_DISPATCH
  </optimizationsNotRun>
</Mode3>
```

- *Constant Energization*: Device actions are not allowed.

```
<Mode4>
  <name>Constant Energization</name>
  <description>Constant system energization</description>
  <DeviceActions />
  <optimizationsNotRunoptimization />
</Mode4>
```

- *Monitor Only*: Device actions are not allowed; optimization is disabled.

```
<Mode5>
  <name>Monitor Only</name>
  <description>No optimization or manual actions (only
   monitoring)</description>
  <DeviceActions>
    <requireUserPermission>false</requireUserPermission>
   <restrictions>SWITCH_STATUS, SWITCH_MODE_AUTO, DER_ON, DER_OFF,
    DER_POWER, DER_LOAD_FOLLOW, DER_MODE_AUTO, CAP_STEP,
    CAP_MODE_AUTO, TRANS_TAP, TRANS_MODE_AUTO, REG_TAP,
    REG_MODE_AUTO</restrictions>
  </DeviceActions>
  <optimizationsNotRun>
       OPT_VOLTVAR, OPT_SWITCHING, OPT_SCHEDULING, OPT_DISPATCH
  </optimizationsNotRun>
</Mode5>
```



Persistence

Settings for persistence of log and load flow result data to a database.

Key	Default	Values	Description
`enablePersistance`	false	true / false	True if database persistence should be enabled. False disables all persistence
`enableLFPersistance`	false	true / false	True enables load flow result persistence if enablePersistance is also true
`lfStoreInterval`	300	30-1800	Number of seconds between database persistance storage of load flow result data

Optimization

Optimization analysis settings.

Key	Default	Values	Description
`start`	1800	0-3600	Number of seconds in the future to start optimization. Optimization will not be run on time slots earlier than this.
`VoltageLimit`	General voltage settings for optimization		
`min`	90	80-99	Minimum voltage limit to allow for optimization purposes
`max`	110	101-120	Maximum voltage limit to allow for optimization purposes
`Reconfiguration`	Settings for switch reconfiguration optimization		
`kwSaving`	50	0.1 -1000	Minimum required kW savings from a switching action to allow change
`voltDiff`	0.01	0 – 1.0	Minimum p.u. voltage difference across an open switch required to allow optimization to consider a switching action
`VoltVar`	Volt/VAr optimization settings.		
`kwSaving`	2	0.1-1000	Minimum required kW savings from a VV analysis to allow changes

Key	Default	Values	Description
Dispatch			
startSeconds	300		Minimum time (seconds) from now for which to start short-term dispatch optimization
endSeconds	3600		Maximum time (seconds) from now for which to run short-term dispatch optimization
GenerationScheduling	Settings for DER scheduling optimization		
cycleTime	30	5, 10, 15, 20, 30, or 60	Periodicity at which the generation scheduling is executed.(in minutes)
TimeInterval	Time settings for DER scheduling		
length	60	15, 30, 60	Duration of the optimization time interval in minutes
number	24	2-48	Number of intervals to run scheduling
leadtime	30	15 - 60	Minimum time in minutes between execution time and start
EnergyStorage	Parameters related to energy storage optimization.		
costMultiplier	10		Cost multiplier for energy storage. Must be greater than 1.0.
Algorithm	Algorithm tuning options for DER scheduling. Incorrect settings may make the algorithm slow or fail to solve		
population	20	10-40	Number of particles to use for PSO
velocitylimit	300	0+	Particle velocity limit
inertia	0.9	0+	Particle inertia
interialowlimit	0.4	0+	Minimum interia value
learningconst1	1.9	0+	Learning constant 1
learningconst2	1.7	0+	Learning constant 2
iterations	30000	100+	PSO iterations
initpenfactor	100	10+	Penalty factor
mutmdtpenalty	10000	0+	Additional penalty factor
heuristicsStepSize	5.0	0.5+	Heuristics step size
hueristicsMaxI-terations	1000	10+	Heuristic iterations

Alerts

Configurable limits for alerts. Most alerts have two levels: one level for warning and another for more serious violations.

Key	Default	Values	Description
Voltage	Alerts for voltage conditions.		
Violation.minLimit	80	60-99	Lower violation limit for a node voltage (%)
Warning.maxLimit	110	101-140	Upper warning limit for a node voltage (%)
Warning.minLimit	90	60-99	Lower warning limit for a node voltage (%)
Switch	Alerts for switch conditions.		
Current	Alerts for current violations and warnings.		
Violation.maxLimit	100	50-200	Violation limit for switch current loading (% of rating)
Warning.maxLimit	90	50-200	Warning limit for switch current loading (% of rating)
Transformer	Alerts for transformer conditions.		
Current	Alerts for current violations and warnings.		
Violation.maxLimit	120	50-200	Violation limit for transformer current loading (% of rating)
Warning.maxLimit	90	50-200	Warning limit for transformer current loading (% of rating)
Conductor	Alerts for conductor conditions.		
Current	Alerts for current violations and warnings.		
Violation.maxLimit	100	50-200	Violation limit for conductor current loading (% of rating)
Warning.maxLimit	80	50-200	Warning limit for conductor current loading (% of rating)
Regulator	Alerts for regulator conditions.		
Current	Alerts for current violations and warnings.		
Violation.maxLimit	130	50-200	Violation limit for regulator current loading (% of rating)
Warning.maxLimit	120	50-200	Warning limit for regulator current loading (% of rating)
VoltageUnbalance	Alerts for voltage unbalance conditions.		
Warning	3	1-50	Warning limit for 3-phase node voltage unbalance (%)

Adapters

See the *Oracle Utilities Distributed Grid Management Interface Guide* for information on adapter configuration.

Defining User Roles

User roles and permissions are defined in the user-roles file (`$MICROGRID_HOME/config/manager/user-roles.xml`).

The file defines user roles (*`role`*) and then associates each type with permission sets (*`perm-set`*) that define what actions are available. The file has the following structure:

- **`role:`** the containing element for the user role definition. It define user roles for groups as configured in an LDAP environment.
  - **`guid:`** name of the user role.
  - **`member:`** group id (simple).
  - **`member:`** group id (fully qualified name).
- **`perm-set:`** the containing element for permission sets that define privileges associated with a role. There is one <perm-set> element for every <role> element.
  - **`role:`** maps the privileges being defined to a role.
  - **`privilege:`** defines privileges with services.
    - **`service:`** defines a service/action that is available to the user. Multiple services are may be listed.

Information Services	Command Services
getMicrogridModel	addCommand
getDynamicModelData	deleteCommand
getCmdSeqQueue	modifySysOpMode
getDeviceCmdSeqQueue	updateDeviceInfo
getSystemMode	receiveMeasVals
getCurLFModelLastLoadFlowDate	addCommandSeq
getLastCommandProcessDate	deleteCommandSeq
getVoltageLimits	setSystemMode
getGeneratorSchedule	approveCmdSeq
	setGeneratorSchdule
	unapproveCmdSeq
	setVoltageLimits
	getConfiguredSystemModes

    - **`extend:`** defines inheritance of permissions from another permission set.

Example User Role File

In the following example, the **viewer** user role has a minimum set of privileges, the **operator** inherits (*extends*) the **viewer** privileges and has additional privileges granted, and the **admin** user extends the operator.

```
<roles-ds>
    <role>
        <guid>viewer</guid>
        <member><!-- simple --></member>
        <member><!-- fully qualified --></member>
    </role>
    <role>
        <guid>operator</guid>
        <member><!-- simple --></member>
        <member><!-- fully qualified --></member>
    </role>
    <role>
        <guid>admin</guid>
        <member><!-- simple --></member>
        <member><!-- fully qualified --></member>
    </role>

    <perm-set>
        <role>viewer</role>
        <privilege>
            <service>getMicrogridModel</service>
            <service>getDynamicModelData</service>
            <service>getCmdSeqQueue</service>
            <service>getDeviceCmdSeqQueue</service>
            <service>getSystemMode</service>
            <service>getCurLFModelLastLoadFlowDate</service>
            <service>getLastCommandProcessDate</service>
            <service>getVoltageLimits</service>
            <service>getGeneratorSchedule</service>
        </privilege>
    </perm-set>

    <perm-set>
        <role>operator</role>
        <privilege>
            <service>addCommand</service>
            <service>deleteCommand</service>
            <service>modifySysOpMode</service>
            <service>updateDeviceInfo</service>
            <service>receiveMeasVals</service>
            <service>addCommandSeq</service>
            <service>deleteCommandSeq</service>
            <service>setSystemMode</service>
            <service>approveCmdSeq</service>
            <service>setGeneratorSchdule</service>
            <service>unapproveCmdSeq</service>
            <service>setVoltageLimits</service>
            <service>getConfiguredSystemModes</service>
        </privilege>
        <extend>viewer</extend>
    </perm-set>

    <perm-set>
        <role>admin</role>
        <extend>operator</extend>
    </perm-set>
</roles-ds>
```

Configuring WebLogic Server

Configuring the WebLogic Server for Oracle Utilities Distributed Grid Management requires the following steps:

- **Create JDBC Data Source**
- **Configure WebLogic Server Arguments**
- **Create a Foreign JNDI Provider**
- **Create Foreign JNDI Object Links**
- **Configure Keystores**
- **Set Up SSL**
- **Configure Listen Ports**
- **Configure Logging**
- **Installing and Deploying the Manager in WebLogic**

Create JDBC Data Source

In WebLogic Server, you configure database connectivity by adding data sources to your WebLogic domain. WebLogic JDBC data sources provide database access and database connection management. To create a JDBC data source in your domain, you can use the Administration Console.

1. Access the WebLogic Server Administration Console by entering the following URL:

   `http://hostname:port/console`

   Here *hostname* represents the DNS name or IP address of the Administration Server, and *port* represents the number of the port on which the Administration Server is listening for requests (port 7001 by default).

2. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.

3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.

4. On the **Summary of Data Sources** page, click **New** and select **Generic Data Source**.

5. On the **JDBC Data Sources Properties** page, enter or select the following information:

   Name - Enter a name for this JDBC data source. This name is used throughout the Administration Console whenever referring to this data source. For example: JDBC Data Source – Oracle Utilities Distributed Grid Management.

   JNDI Name - Enter the JNDI path to where this JDBC data source will be bound. Applications look up the data source on the JNDI tree by this name when reserving a connection. Use **jdbc/DGM_POOL** for the JNDI path.

   Database Type - Select the DBMS of the database that you want to connect to. If your DBMS is not listed, select **Other**.

   Click **Next** to continue.

6. Select the database driver:

   Database Driver - Select the JDBC driver you want to use to connect to the database. The list includes common JDBC drivers for the selected DBMS.

7. On the **Transaction Options** page, follow these steps. Depending on the driver you selected on the JDBC Data Source Properties page, you may not need to specify any of these options.

   Supports Global Transactions - Select this check box (the default) to enable global transaction support in this data source.

   If you selected **Supports Global Transactions**, select an option for transaction processing: (available options vary depending on whether you select an XA driver or a non-XA driver)

   - **Two-Phase Commit** - Select this option to enable standard XA processing.

     This option is only available when you select an XA JDBC driver to make database connections.

   Click **Next** to continue.

8. On the **Connection Properties** page, enter values for the following properties:

   Service Name - This field is available only if you selected one of the available Oracle RAC Service-Instance connections drivers. Specify the service name of the database to which you want to connect. This must be the same for each data source in a given multi-data source.

   Database Name - Enter the name of the database that you want to connect to. Exact database name requirements vary by JDBC driver and by DBMS.

   Host Name - Enter the DNS name or IP address of the server that hosts the database.

   Port - Enter the port on which the database server listens for connections requests.

   Database User Name - Enter the database user account name that you want to use for each connection in the data source.

   Password/Confirm Password - Enter the password for the database user account.

   Click **Next** to continue.

9. On the **Test Database Connection** page, review the connection parameters and click **Test Configuration**.

   WebLogic attempts to create a connection from the Administration Server to the database. Results from the connection test are displayed at the top of the page. If the test is unsuccessful, you should correct any configuration errors and retry the test.

   Click **Next** to continue.

10. On the **Select Targets** page, select the server on which you want to deploy the data source.

11. Click **Finish** to save the JDBC data source configuration and deploy the data source to the target that you selected.

12. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

    If the server is running, you must restart the server for these changes to take effect.

Configure WebLogic Server Arguments

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
2. In the left pane of the Console, expand Environment and select **Servers**.
3. In the **Servers** table, click the name of the Managed Server you want to configure.
4. Select the **Configuration > Server Star**t.
5. On the Server Start page, add the following to the Arguments field:

   ```
   -DMICROGRID_HOME=/path/to/dgm -DDATA_SOURCE=jdbc/DGM_POOL
   -XX:MaxPermSize=256m
   ```

6. Click **Save**.
7. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

   If the server is running, you must restart the server for these changes to take effect.

Create a Foreign JNDI Provider

A foreign JNDI provider represents a JNDI tree that can reside outside of a WebLogic Server. This could be a JNDI tree in a different server environment or within an external Java program. By setting up a foreign JNDI provider you can lookup and use an object that exists outside of the WebLogic Server environment with the same ease that you would use an object bound in your WebLogic Server instance.

To create a foreign JNDI provider to access naming/directory services via the JNDI:

1. If you have not already done so, in the Change Center of the Administration Console, click Lock & Edit.
2. In the Administration Console, expand Services > Foreign JNDI Providers.
3. On the Summary of Foreign JNDI Providers page, click New.

   Note: Once you create a foreign provider you cannot rename it. Instead, you must delete it and create another one that uses the same name.
4. On the Create a Foreign JNDI Providers page:
   - In Name, enter a name for the foreign provider.
   - Click Next to select targets for the provider or click Finish to target all servers in the domain.
   - Optionally, select servers or clusters as targets for the foreign provider.
   - Click Finish to add the new provider to the Summary page.
5. From the Summary page, click the new provider to open it.
6. On the Configuration: General page:
   - In Initial Context Factory, enter the name of the class that must be instantiated to access the JNDI provider. This class name depends on the JNDI provider and the vendor that are being used. The value corresponds to the standard JNDI property,

java.naming.factory.initial. For Oracle's LDAP provider, use com.sun.jndi.ldap.LdapCtxFactory.

- In Provider URL, enter the URL that WebLogic Server will use to contact the JNDI provider. This value corresponds to the standard JNDI property, java.naming.provider.url.
- In User, enter the name of a user authorized to access the foreign JNDI.
- In Password, enter the user password.
- In Properties specify any additional properties that must be set for the JNDI provider. These properties will be passed directly to the constructor for the JNDI provider's InitialContext class.

  Note: The Properties may be a name=value list of properties, separated by commas. For example:

- com.sun.jndi.ldap.connect.pool=true
- com.sun.jndi.ldap.connect.pool.maxsize=16
- com.sun.jndi.ldap.connect.pool.prefsize=10
- com.sun.jndi.ldap.connect.pool.timeout=600000
- java.naming.referral=follow
- java.naming.security.authentication=simple

7. Click Save.
8. To activate these changes, in the Change Center of the Administration Console, click Activate Changes.

   Note: Not all changes take effect immediately—some require a restart.

After You Finish

Continue by adding Foreign JNDI Links that set up a relationship between a name in your local JNDI tree and the object in the remote tree.

Create Foreign JNDI Object Links

Before You Begin

If you haven't done so already, create a Foreign JNDI Provider.

A Foreign JNDI Object Link represents a local link to an object in a foreign (remote) JNDI tree. After you create a foreign JNDI provider you can add foreign JNDI links that set up a relationship between a name in your local JNDI tree and the object in the remote tree.

To create object links to a foreign JNDI provider:

1. If you have not already done so, in the Change Center of the Administration Console, click Lock & Edit.
2. In the Administration Console, expand Services > Foreign JNDI Providers.
3. On the Foreign JNDI Providers Summary page, click the provider to which you want to add object links.
4. On the Settings page for the provider, expand Configuration > Links and click New.
5. On the Foreign JNDI Links Properties page:
   - In Name, enter a name for the foreign JNDI link.
   - In Local JNDI Name, specify the name that the remote JNDI object will be bound to in the local server's JNDI tree and used to look up the object on the local server.
   - In Remote JNDI Name, specify the name of the remote object that will be looked up in the foreign JNDI directory.
6. Click OK.

   The name is added to the list of foreign links. You can access the properties by clicking the name in this list.
7. To add more links repeat steps 3-5.

   Note: To activate these changes, in the Change Center of the Administration Console, click Activate Changes.

   Not all changes take effect immediately—some require a restart.

After you Finish

You can access the linked objects from your WebLogic Server clients.

Configure Keystores

- **Before you Begin**
  - Obtain private keys and digital certificates from a reputable certificate authority such as Verisign, Inc. or Entrust.net.
  - Create identity and trust keystores.
  - Load the private keys and trusted CAs into the keystores.

After you have created the identity and trust keystores that you intend to use in a production environment, you must configure them with WebLogic Server.

To configure the WebLogic identity and trust keystores:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
2. In the left pane of the Console, expand Environment and select **Servers**.
3. Click the name of the server for which you want to configure the identity and trust keystores.
4. Select **Configuration > Keystores**.
5. In the **Keystores** field, select the method **Custom Identity and Custom Trust** for storing and managing private keys/digital certificate pairs and trusted CA certificates.
6. In the **Identity** section, define attributes for the identity keystore.
   - **Custom Identity Keystore**: The fully qualified path to the identity keystore.
   - **Custom Identity Keystore Type**: The type of the keystore. Generally, this attribute is Java KeyStore (JKS); if left blank, it defaults to JKS.
   - **Custom Identity Keystore Passphrase**: The password you will enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore.
7. In the **Trust** section, define properties for the trust keystore.
   - **Custom Trust Keystore**: The fully qualified path to the trust keystore.
   - **Custom Trust Keystore Type**: The type of the keystore. Generally, this attribute is JKS; if left blank, it defaults to JKS.
   - **Custom Trust Keystore Passphrase**: The password you will enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore.
8. Click **Save**.
9. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

   If the server is running, you must restart the server for these changes to take effect.

Set Up SSL

Secure Sockets Layer (SSL) provides secure connections by allowing two applications connecting over a network connection to authenticate the other's identity and by encrypting the data exchanged between the applications. Authentication allows a server and optionally a client to verify the identity of the application on the other end of a network connection. Encryption makes data transmitted over the network intelligible only to the intended recipient.

WebLogic Server supports SSL on a dedicated listen port which defaults to 7002. To establish an SSL connection, a Web browser connects to WebLogic Server by supplying the SSL listen port and the HTTPs protocol in the connection URL, for example, https://myserver:7002.

SSL can be configured one-way or two-way:

- With one-way SSL, the server is required to present a certificate to the client but the client is not required to present a certificate to the server.
- With two-way SSL, the server presents a certificate to the client and the client presents a certificate to the server. WebLogic Server can be configured to require clients to submit valid and trusted certificates before completing the SSL handshake.

To Configure SSL:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
2. In the left pane of the Console, expand **Environment** and select **Servers**.
3. Click the name of the server for which you want to configure SSL.
4. Select **Configuration > SSL** page, and choose the location of identity (certificate and private key) and trust (trusted CAs) for WebLogic Server.
5. Set SSL attributes for the private key alias and password.
6. At the bottom of the page, click **Advanced**.
    - Set the **Two Way Client Cert Behavior** attribute. The following options are available:
        - **Client Certs Not Requested**: The default (meaning one-way SSL).
        - **Client Certs Requested But Not Enforced**: Requires a client to present a certificate. If a certificate is not presented, the SSL connection continues.
        - **Client Certs Requested And Enforced:** Requires a client to present a certificate. If a certificate is not presented, the SSL connection is terminated.
7. Click **Save**.
8. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes.**

    If the server is running, you must restart the server for these changes to take effect.

Configure Listen Ports

To configure the listen ports for a server:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit.**
2. In the Administration Console, expand **Environment** and select **Servers**.
3. On the **Servers** page, click the name of the server.
4. Select **Configuration > General.**
5. If you want to disable the non-SSL listen port so that the server listens only on the SSL listen port, deselect **Listen Port Enabled**.
6. If you want to disable the SSL listen port so that the server listens only on the non-SSL listen port, deselect **SSL Listen Port Enabled**.

   Note: You cannot disable both the non-SSL listen port and the SSL listen port. At least one port must be active.
7. If you are using the non-SSL listen port and you want to modify the default port number, change the value in **Listen Port**.
8. If you want to modify the default SSL listen port number, change the value in S**SL Listen Port.**
9. Click **Save**.
10. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

If the server is running, you must restart the server for these changes to take effect.

Configure Logging

Setup file rotation for logging:

1. Log into Admin Server
2. In the left pane, expand Environment and select Servers.
3. In the Servers table, click the name of the server instance (for example, dgm_1, dgm_2, etc.) whose log files you want to configure for rotation.
4. Select Logging > General.
5. Setup the rotation settings (rotation type, rotation file size, etc)
6. Expand the Advanced setting
7. Check the Redirect stdout logging enabled check box
8. Change the Standard Out: Severity Level to Off

Installing and Deploying the Manager in WebLogic

Installing an **enterprise application** refers to making its physical file or directory known to WebLogic Server. An Enterprise application like Oracle Utilities Distributed Grid Management is installed as an archived EAR file. After you have installed Oracle Utilities Distributed Grid Management, you can start it so that users can begin using it.

To Install the Manager:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
2. In the left pane of the Console, select **Deployments**.
3. In the right pane, click **Install**.
4. Using the **Install Application Assistant**, locate the **`dgm.ear`** file to install. This will be in the **`$MICROGRID_HOME/`** directory. Select the radio button to the left of the application.
5. Click **Next**.
6. Select **Install this deployment as an application**.
7. Click **Next**.

   If you previously selected the option to target the entire Enterprise application to the same server or cluster, the **Select Deployment Targets** window appears.

   > **Note**: If you have not created Managed Servers or clusters, other than the current Administration Server, you will not see this assistant page.

8. Follow these steps:
   - Select the Managed Server to which you want to deploy the entire Enterprise application.
   - Click **Next**.
9. Optionally update settings about the deployment. Typically, the default values are adequate.
10. Click **Finish**.
11. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

Chapter 3

Viewer Installation and Configuration

This chapter provides instructions for installing and configuring the Oracle Utilities Distributed Grid Management client component, the Viewer. This chapter includes the following topics:

- **Before You Begin**
- **Installing the Viewer**
- **Configuring the Viewer**

Before You Begin

The Viewer is installed and runs on Microsoft Windows and requires the Java Runtime Environment (JRE) and JavaFX. The Java Platform, Standard Edition (Java SE) lets you deploy Java applications on desktops and servers. JavaFX provides the runtime environment required for running JavaFX desktop applications and applets, such as the Viewer.

See the *Oracle Utilities Distributed Grid Management Quick Install Guide* "Certified and Supported Platforms" section to verify that you have installed the required versions for each prerequisite software component.

Installing the Viewer

Installing the Viewer contains the following topics:

- **Before You Begin**
- **Keystore File Installation**
- **Install Viewer Files**

Before You Begin

It is important to note the importance of choosing the correct user account to perform the installation. If you want the option to create an installation folder for the Viewer in the All Users folder, or in the Local User's Start menu folder, you must use an account that has administrator privileges when you log in to the target system.

Keystore File Installation

The Viewer can be configured to communicate with the Manager securely using two-way SSL. Previously during the **Manager Configure Keystores** steps (see **Configure Keystores** on page 2-23), the client credentials were created on the server. Now you need to copy the **`client-trust-store.jks`** and **`client-key-store.jks`** files to the client machine and store them in a user directory where the Viewer will have read access.

Install Viewer Files

Create a directory where you can unzip the distribution zip file. Oracle recommends installing the Viewer at **`C:\Oracle\DGM\viewer`**.

Define MICROGRID_HOME

In Microsoft Windows 7 System Properties, add a system environment variable:

- **Variable name:** `MICROGRID_HOME`
- **Variable value:** `C:\Oracle\DGM`

  (or applicable path based on your installation)

Configuring the Viewer

Configuring the Viewer contains the following topics:

- **Configuring Viewer Communication Parameters**
- **Configuring Viewer Language Settings**
- **Configuring Map and Electrical Symbols**
- **Start the Viewer to Configure the Keystore Password**

Configuring Viewer Communication Parameters

Before starting the Viewer, it must be configured correctly to communicate with the Manager. Edit the `ViewerConfig.xml` in the `MICROGRID_HOME\viewer\config` folder and set the following properties correctly:

- **General Configuration**
  - **applicationUserMode:** If the Viewer is being configured to communicate with the Manager over two way SSL, this needs to be set to "**`ADMIN`**" (all values quotes removed) initially and then change back to "**`DGM`**" once setup is complete.
  - **refreshPeriod:** Viewer refresh time, in seconds.
  - **communicationTimeout:** Maximum time (in seconds) to wait for a response from the Manager before reporting status as disconnected.
  - **applicationUserMode:** If the Viewer is being configured to communicate with the Manager over two way SSL, this needs to be set to "**`ADMIN`**" (all values quotes removed) initially and then change back to "**`DGM`**" once setup is complete.
- **Communication with Manager Settings**
  - **ManagerCommunication.managerServiceProtocol:** "**`https`**"
  - **ManagerCommunication.managerServiceHost:** fully qualified name of the Oracle Utilities Distributed Grid Management server
  - **ManagerCommunication.managerServicePort:** SSL port at which the WebLogic server is listening for requests.
  - **SslParam.trustStoreLocation:** Full path and file name of the trust store. USE FORWARD SLASHES in file path instead of backward slashes.
  - **SslParam.trustStorePassword:** Provide the trust store password.
  - **SslParam.keyStoreLocation:** Full path and file name of the key store. USE FORWARD SLASHES in file path instead of backward slashes.

Configuring Viewer Language Settings

The Viewer supports two languages at present: English and Chinese. The language can be changed by modifying the language setting in the **`Country`** parameter, which has two attributes:

- `language`: language alias. Valid values are "en" for English and "zh" for Chinese.
- `countryAlias:` country alias, *e.g.*, "US" for English and "CN" for Chinese.

```
<Country>
 <language>en</language>
 <countryAlias>US</countryAlias>
</Country>
```

Configuring Map and Electrical Symbols

The Viewer configuration file (ViewerConfig.xml) defines network symbols (for example, generators, loads, and switches), which are drawn on the Map using SVG (Scalable Vector Graphics) paths. Each symbol has a 'path' (SVG path) and 'color' (display color) associated with it.

Symbol Definition. The Viewer symbols are configured by defining the SVG Path *path data* attribute with the following parameters:

- **M:** moveto
- **L:** lineto
- **C:** curve
- **A:** arc
- **Z:** closepath

> **Note:** The SVG Paths specification is available at: `http://www.w3.org/TR/SVG/paths.html`.

Color. Symbol color is defined with a color element that uses RGB color codes to fill the shape.

Compound Symbols. A compound symbol is created with multiple symbol definitions. Each subsequent symbol in the definition will be drawn over the preceding symbol.

Examples.

Modify a Symbol

Scenario: the compound generator symbol has a white second symbol that you need to change to black. The original symbol:

Steps

1. Open ViewerConfig.xml
2. Find the MapSymbol `<Generator>` definition:

```
<Generator> <!-- Symbol for generator -->
            <symbol1>
                <path>M 0,-10 A 10,10 0 0,0 0,10 A 10,10 0 0,0 0,-10</path>
                <color>255,165,0</color>
            </symbol1>
          <symbol2>
                <path>M -8,0 C-6,-6 -2,-6 0,0 S8,6 8,0 </path>
                 <linecolor>255,255,255</linecolor>
                 <width>2</width>
            </symbol2>
        </Generator>
```

3. Modify `symbol2 linecolor` to black (0, 0, 0)

```
<Generator> <!-- Symbol for generator -->
            <symbol1>
                <path>M 0,-10 A 10,10 0 0,0 0,10 A 10,10 0 0,0 0,-10</path>
                <color>255,165,0</color>
            </symbol1>
          <symbol2>
                <path>M -8,0 C-6,-6 -2,-6 0,0 S8,6 8,0 </path>
                 <linecolor>0,0,0</linecolor>
```

```
                <width>2</width>
            </symbol2>
        </Generator>
```

4. Save the file.
5. Restart the Viewer

The symbol will have changed to:  .

Example: Create a Compound Symbol

Scenario: define the following compound symbol for a generator:

Steps

1. Open ViewerConfig.xml
2. Edit the `<MapSymbol>` element by adding two symbols in the Generator tag:

```
<Generator> <!-- Symbol for generator -->
            <symbol1> <!-- triangle -->
                <path>M -10,10 L 10,10 L 0,-10 z</path>
                <color>139,137,137</color>
            </symbol1>
            <symbol2> <!-- square -->
                <path>M -5,-5 L 5,-5 L 5,5 L -5,5 z </path>
                <color>0,0,255</color>
            </symbol2>
    </Generator>
```

Start the Viewer to Configure the Keystore Password

Next, you will start the Viewer to configure the keystore password.

Note: This step is required for two way SSL communication only.

1. Ensure Ensure that the applicationUserMode is set to "ADMIN" in ViewerConfig.xml. Make sure that the ViewerConfig.xml file is closed.
2. In a browser, open:

   `https://<DGM Server Name:port>/ViewerVeb/viewerLaunch.html`
3. The Viewer launch web page will appear. (Accept the server certificate if prompted.)
4. Launch the Viewer by clicking the appropriate link on the web page. A dialog box will appear asking the key store password; follow the instructions.
5. After the message appears that the keystore password was successfully configured, click **Quit**.

   The Viewer does not validate the password; if the provided password is incorrect, communication with the Manager will fail.
6. Edit ViewerConfig.xml to set the `applicationUserMode` back to "`DGM`", save, and close the file.

The Viewer is configured and ready to be used. Create a shortcut for the **`ViewerLaunch.html`** URL at a convient location for operator's use, such as the Windows 7 Desktop.