Oracle® Communications Services Gatekeeper

Release Notes

Release 5.1

E37528-01

June 2013

These release notes list the new and enhanced features, resolved and known issues, documentation notes, as well as documentation updates, in this release of Services Gatekeeper.

This document contains the following sections:

New and Changed Features

This section describes new features and feature enhancements in this release of Services Gatekeeper.

OneAPI 3.0 Anonymous Customer References

A new RESTful interface supporting the use of Anonymous Customer Reference (ACR) subscriber identifiers in applications. See *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide* for more information.

New Portals for Partner Managers and Partners

Two new and interconnected applications, Partner Manager Portal and Partner Portal, provide an easy-to-use environment in which network operators and service providers can develop applications.

Partner Manager Portal with Support for Analytics

Partner Manager Portal provides a simple process by which network operators can set up APIs, SLAs, and other elements necessary for creating applications. These elements are displayed as menu selections and input fields in Partner Portal.

Additionally, network operators use Partner Manager Portal to register service providers as partners with access to Partner Portal. The network operators then review and manage the applications created in Partner Portal.

Network operators can use the Oracle Business Intelligence Support for Analytics in Partner Manager Portal to monitor the usage of the services in their applications and make the necessary adjustments for optimizing their products.

For more information see *Oracle Communications Services Gatekeeper Partner Manager Portal Online Help*.

Partner Portal

Partner Portal enables service providers to quickly and easily create applications and maintain their contact information. All applications created or updated in Partner Portal are instantly displayed in Partner Manager Portal for review and approval.

For more information see *Oracle Communications Services Gatekeeper Partner Portal Online Help*.

OAuth 2.0 Enhancements

In order to support new and evolving standards such as SAML-based grant flows, Client Credential-based grant flows and others, the Services Gatekeeper authorization framework must be extensible while leaving the basic OAuth2 protocol framework—endpoints and token types—intact. A new Platform Development Studio Eclipse wizard supports the creation of OAuth2 extension plug-ins, creating a Java project with skeletal validators, handlers and listeners.

Another new OAuth2 feature is Resource Parameter Rules Customization. Services Gatekeeper extends the token authentication mechanism, adding support for additional query string parameters that can further customize the OAuth2 policy handling, in conjunction with customized interceptors.

New Eclipse Wizards

The following new Eclipse wizards have been added to streamline Services Gatekeeper extension development:

- A Communication Service Wizard that can take WSDL files as input and create a communication service with both SOAP and RESTful facades.
- An OAuth 2.0 Extension Handler wizard.
- A RESTful Communication Service wizard that can accept WADL files as input.

For more information, see *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*.

EDR Enhancements

Additional informational fields have been added to Services Gatekeeper, existing EDR fields have been enhanced, new AspectJ pointcuts have been added, and an EdrServiceMBean has been added to filter the types of EDRs reported by the EDRService. For more information, see the following documents:

- *Oracle Communications Services Gatekeeper Communication Service Guide*
- *Oracle Communications Services Gatekeeper System Administrator's Guide*
- *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*

Upgraded Databases

Services Gatekeeper is now certified to be deployed with the following databases:

- Oracle 11g RAC
- Oracle 11g
- MySQL 5.6

Updated SOA Facades

The Services Gatekeeper SOA facades are now based on the OSB version 11g R1, 11.1.1.6.0. They also support the new Services Gatekeeper communication services introduced in this release.

IPV6

Services Gatekeeper supports Internet Protocol version 6 (IPV6) in the following communication services: Parlay X 2.1 SMS/SMPP, Native SMPP, Parlay X 2.1 MMS, and Parlay X2.1 Terminal Location.

New Communication Services

Services Gatekeeper provides the new communication services listed below.

See the appropriate chapters in the following guides for details about these services:

- *Oracle Communications Services Gatekeeper System Administrator's Guide*
- *Oracle Communications Services Gatekeeper Communication Service Guide*
- *Oracle Communications Services Gatekeeper Application Developer's Guide*
- *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*

Application Subscription Management Communication Service

Services Gatekeeper provides an Open Mobile Alliance (OMA) General Service Subscription Management (GSSM) compatible Application Subscription Management communication service for managing subscriber application subscriptions.

Email Communication Service

Services Gatekeeper provides an email communication service which uses MMS in the northbound interface and a plug-in that enables the sending of email through SMTP and receiving email through POP3 and IMAP protocols. See "Parlay X 2.1 Multimedia Messaging/SMTP, POP3, and IMAP" in *Oracle Communications Services Gatekeeper Communication Service Guide*. A RESTful interface is also available. For more details, see the *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*.

Quality of Service (QoS)

The Services Gatekeeper QoS feature provides applications with a RESTful interface that allows them to control the quality of a subscriber connection. Among the connection quality aspects that the QoS feature can control include limiting and boosting subscriber connection bandwidth, as well as tuning connection latency. Available operations include: Applying, modifying and removing QoS policies, querying QoS policies and registering and unregistering for QoS events. For more information, see *Oracle Communications Services Gatekeeper Communication Service Guide* and *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*.

ParlayX 3.0 Address List Management

The Services Gatekeeper Address List Management plug-in interface is used to create and manage groups of resource owners and to associate them with group Uniform Resource Identifiers (URIs). Group URIs can be used to authenticate requests on behalf of group members. For more information, see *Oracle Communications Services Gatekeeper Communication Service Guide*.

ParlayX 2.1 SMS/MMS/EWS PAP Split and Submit Messaging

The Split and Submit Messaging Feature splits application SMS/MMS/EWS PAP requests with multiple addresses into multiple individual requests sent separately to the network with no effort on the part of the application developer, and independent of the capabilities of the SMSC. The Split and Submit Messaging feature also supports customized message content for each address included in the submission when the PluginManager MBean attribute **supportBulkRequest** is set to **true**, and an xparam, **DifferentContentForSingleAddressInBulk**, is set to **true** and added to the request. For more information, see *Oracle Communications Services Gatekeeper System Administrator's Guide* and *Oracle Communications Services Gatekeeper Application Developer's Guide*.

Enhancements to Previously Existing Communication Services

The following Services Gatekeeper communication services have been enhanced.

See the appropriate chapters in the following guides for details about these services:

- *Oracle Communications Services Gatekeeper System Administrator's Guide*
- *Oracle Communications Services Gatekeeper Communication Service Guide*
- *Oracle Communications Services Gatekeeper Application Developer's Guide*
- *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*

ParlayX 3.0 Payment Volume Charging

The Payment Volume charging feature fleshes out the existing Parlay X 3.0 Part 6 Payment interface. In addition to charging fixed currency costs to a subscriber account, Services Gatekeeper now supports charging a volume measured in time (seconds), storage size (bytes) or a user-defined metric. For more information, see *Oracle Communications Services Gatekeeper Communication Service Guide* and *Oracle Communications Services Gatekeeper Application Developer's Guide*.

New Alarms, CDRs and EDRs

For information on new alarms, CDRs and EDRs, see "Upgrading Oracle Communications Services Gatekeeper" in *Oracle Communications Services Gatekeeper Installation Guide*.

WebLogic Server Upgrade

This release of Services Gatekeeper is built on WebLogic Server 11g R1 (10.3.6).

OCCAS Upgrade

This release of Services Gatekeeper is integrated with Oracle Communications Converged Application Server (OCCAS) version 5.1 to provide support for SIP functionality.

Resolved Issues

Table 1 describes known issues from the previous release that have been resolved in this release.

Table 1 Issues Resolved in This Release

Bug ID SR ID	Description
13929611 3-5521749101	The Plugin_px21_short_messaging_smpp has been updated to prevent extraneous characters from displaying in some text fields in the Service Gatekeeper's Administration console.
13983876 3-5609301131	The stopWeblogic.cmd stops the WebLogic server correctly.
14221484 3-5831531241	To enable the SNMP trap client to identify the application instance that caused the alarm, the ADDITIONAL_INFO column in the SLEE_ALARM table for SNMP traps now contains ApplicationID entry.
14643295 3-6199319091	A new MBean attribute, connectDelayValue, now specifies the delay to use between connection attempts when a connection to the SMSC is lost. The default value is 5 seconds.
13427226 3-4471023581	The following enhancements were made to the **submitReq** operation in all supported MM7 schema versions: ■ The optional element ExpiryDate is now supported by the ExpiryDate xparameter. ■ The optional element EarliestDeliveryTime is now supported by the EarliestDeliverytime xparameter.
13526755 3-5081620071	The Extended Web Services Binary SMS service now correctly handles mobile-terminated binary SMS messages where the user data header or the message content is empty.
13514854 3-5056667411	When you use ParlayX sendMessage to send MMS messages, the message delivery status (deliveryStatus) field in the notifyMessageDeliveryReceipt uses the following mapping: ■ Expired (MM7) maps to DeliveryImpossible (ParlayX ■ Retrieved (MM7) maps to DeliveryToTerminal (ParlayX ■ Rejected (MM7) maps to DeliveryImpossible (ParlayX ■ Indeterminate (MM7) maps to DeliveryUncertain (ParlayX ■ Forwarded (MM7) maps to DeliveryToNetwork (ParlayX ■ Unrecognized (MM7) maps to DeliveryUncertain (ParlayX ■ Deferred (MM7) maps to DeliveryNotificationNotSupported (ParlayX
14112113 3-5740979701	Issues in schema upgrades from Services Gatekeeper version 4.1 to Services Gatekeeper 5.0.0.1 were fixed.
14784088 3-6331697421	The logs generated for Multimedia messaging with ParlayX2.1 now correctly handle Simple Object Access Protocol (SOAP) fault messages.

Table 1 (Cont.) Issues Resolved in This Release

Bug ID SR ID	Description
14801942 3-6331392411	When you use the ParlayX 2.1 short messaging (SMS) interface, Service Gatekeeper no longer sends duplicate SMS delivery notifications to the application endpoint.
16266476 3-6748413291	A new system property called **ocsg.terminal_location.use_subclient_element** (set by default to TRUE) now indicates the presence of <subclient> element tags in the Mobile Location Protocol (MLP) request header created by Services Gatekeeper. To disable the use of the <subclient> element, add the following Java system property in the startup script for Services Gatekeeper: `-Docsg.terminal_location.use_subclient_element=false`
12396257 3-3429942321	In the NT cluster environment, the Partner Relationship Management interface in Services Gatekeeper no longer fails when a node in the cluster goes down.
13769759	The following enhancements were made in the ParlayX 21 SMPP plug-in to enable the handling of latency statistics, plug-in reset and deactivation: ■ A new EDR attribute, SmscResponselatency, now tracks response latency introduced by an SMSC for submitSM, submitMultiSM or dataSM requests. ■ This plug-in resets all SMPP connections following a submitSM, submitMultiSM or dataSM request timeout. ResetSMPPConnectionsOnRequestTimeout, the new MBean attribute, specifies whether the connections must be reset. By default, this attribute is **disabled**. To enable the resetting of connections that timeout, enable ResetSMPPConnectionsOnRequestTimeout. The request timeout is specified in the existing MBean attribute RequestTimerValue. ■ The plug-in will unbind all SMPP connections when it receives a configurable command status in a submitSMresp, submitMultiSMResp or dataSMresp response from SMSC. The feature is enabled/disabled by the new MBean attribute, DeactivateOnCommandStatus. The commandstatus codes that should trigger this feature and the timeperiod the plug-in should wait before trying to auto-reconnect is set by new MBean operation ConfigureDeactivateOnCommandStatus. You can specify one single commandstatus value or a comma separated list of values. If the timeperiod is set to **0** the auto-reconnect feature is disabled and plug-in will stay disconnected until the existing MBean operation resetSMPPConnection is invoked. The current configuration can be checked by new MBean operation listDeactivateOnCommandStatusConfiguration.

Table 1 (Cont.) Issues Resolved in This Release

Bug ID SR ID	Description

13975834
3-5600784601
	When Services Gatekeeper receives the delivery report for a segmented message but information about the first segment is already deleted because it has expired, it now checks to see whether information for any other related segment is missing or was deleted because the message expired.
	If information for any other related segment is missing, Services Gatekeeper stops processing the delivery report and sends the configurable "permanent error" in its response to SMSC. It then deletes the information about the current processed segment from is internal storage.
	The system property, **ocsg.sms.decimal_smsc_permanent_error_code** can be used to specify the error code the SMPP plug-in sends in response to the SMSC to indicate the error is a permanent error:
	■ The default value is **8** to indicate ESME_RSYERR.
	You can set a different error code. Specify a decimal value. For example, the following entry sets the error code to indicate ESME_RX_P_APPN:
	`-Docsg.sms.decimal_smsc_permanent_error_code=101`
	By default, Services Gatekeeper sends CancelSM requests to SMSC when message information in its internal storage is considered too old.
	■ The new system property, **ocsg.sms.cancel_at_expiry** which controls this feature is enabled by default.
	■ To disable Services Gatekeeper from sending such CancelSM requests, set this property to false:
	`-DDocsg.sms.cancel_at_expiry=false`

14022537 3-5644334921	Improvements in Services Gatekeeper have greatly reduced the time needed to process the generated statistics used for calculating the busy hour transactions.
14251619 3-5824599731	Improvements were made in the service interceptor mechanism in Services Gatekeeper that is used to select what plug-in(s) shall handle a message with two or more target addresses. The improvements also correct how statistics are generated for such messages.
14294187 3-5824822231	In alignment with the ParlayX specifications, Services Gatekeeper converts any message criteria that is in upper case to lower case. This rule is bi-directional and applies to all messages, whether they are mobile originated or mobile terminated.
14634682 3-5777293991	The following enhancements to ParlayX 2.1 SMPP Plug-in enable custom EDR listeners to track segmented and non-segmented messages that reach SMSC: ■ A new MBean attribute, submitSmResponseDelayAlarmTreshold holds the threshold set in milliseconds. ■ An alarm is raised when the SMSC response to a SubmitSm or SubmitSmMulti request is delayed more than the value configured in submitSmResponseDelayAlarmTreshold. ■ Set the value in submitSmResponseDelayAlarmTreshold to zero or negative to indicate no threshold. If there is no threshold, alarms will not be fired when the SMSC response to a SubmitSm or SubmitSmMulti request is delayed.

Table 1 (Cont.) Issues Resolved in This Release

Bug ID SR ID	Description
15974927 3-6520176541	The following enhancements were made to enable Services Gatekeeper to handle delivery reports when different legacy SMPP plug-ins are connected to different ports on the same SMSC or when plug-ins are connected to a clustered SMSC with multiple network interfaces: ■ A new MBean attribute, SmscGroupIdEnabled (disabled by default). Enable this attribute when your Services Gatekeeper installation has multiple Legacy SMPP plug-in instances that connect to different SMSC ports on the same logical SMSC. ■ A new MBean attribute, SmscGroupId (blank by default) Set SmscGroupId to a string value that is common value in all plug-in instances connecting to the same logical SMSC.
16316294 3-6732418601	For Parlayx 2.1 SMPP Plug-in, if the tunnelled parameter (**com.bea.wlcp.wlng.plugin.sms.DestinationAddressType**) is present in the request but the type mapping is not present in the plug-in configuration, Services Gatekeeper now uses the following values as default: ■ The configured values for Enterprise Social Messaging Environment Type of Number (TON) (in the MBean attribute DestinationAddressTon) ■ Enterprise Social Messaging Environment Numbering Plan Indicator (NPI) (in the MBean attribute DestinationAddressNpi)
16517793 3-6952943391	Double forward slash characters ("//") are preserved by WebLogic web servers in the requests that the server forwards to Services Gatekeeper.

Known Issues

Table 2 lists the other known issues in this release.

Table 2 Known Issues

Bug ID	Description
16735392	During the upgrade to Services Gatekeeper, the database migration script could fail if high traffic (such as more than 300 transactions per second) occurs at the same time. This is because, during high traffic, the **pl_mt_sms_smpp** table is locked to prevent changes to the table's schema. migration script. If you encounter this error, rerun the appropriate database migration script: ■ runConfigurationMigration.sh (Linux) ■ runConfigurationMigration.bat(Windows)
16706623	When you install the API analytics, if there is an **edr** folder located in the Oracle instance location defined when OBIEE was installed, the installer will not replace the **edr** folder. You must delete the existing **edr** folder from this location before you install the API analytics. (The default location for the **edr** folder is: **`$OBIEE_Instance/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog/edr`**.)

Table 2 (Cont.) Known Issues

Bug ID	Description
16677204	When you access Partner Manager Portal using Internet Explorer, and attempt to create a partner group service level agreement for an interface, the Interface selection does not display correctly in the **Contract Details** section of the **Create Partner Group Service Level Agreements** panel. This is a compatibility issue with respect to Internet Explorer. If you encounter this issue, please use Mozilla Firefox to access Partner manager Portal and Partner Portal.
16676196	An application name must not start with a blank character. The application approval process in Partner Manager Portal rejects any application that is named with an initial blank character such as " my app" with a message requesting the partner to contact the administrator. Ensure that all application names do not start with a blank character.
16633181	At times in Partner Manager Portal, when the partner manager clicks the **Reset Password** link in the **All Partners** panel to reset the password for a partner account, the cursor starts spinning continuously. If this occurs, please refresh the page using the refresh method appropriate for your Web browser.
16482973	The Up and Down scrolling arrows on the keyboard do not work correctly when you are in the **Services Level Agreements** panel. If this issue occurs, please use the mouse to select the table rows.
16346121	When you upgrade from OCSG 5.0.0.1 with the following command: `java weblogic.Deployer -adminurl @ t3://`*server*`:`*port* `-user weblogic -password weblogic123 -redeploy -name wlng_nt_oauth2 -source` the Open Authorization Protocol (OAuth) entry does not have a version number and the upgrade attempt fails. If the upgrade attempt fails: 1. Use the Weblogic Administration console to un-deploy the old oauth2 package. 2. Deploy the new oauth2 package manually.
16213288	In a Solaris 11 environment, if the network tier of a 1x1 cluster fails to boot up, use one of the following workarounds: ■ Configure a 2x2 cluster environment. At runtime, perform a startup of the appropriate 1x1 cluster. ■ Delete the `<server-name>WLNG_NT2</server-name>` entry from the **datatier.xml** file located at `$DomainHOME/config/customer/datatier.xml` Where, `$DomainHOME` is the Services gatekeeper domain. Save the file.
14178804	Service Gatekeeper is unable to reconnect automatically to a Diameter server that has been stopped and then restarted. If this issue occurs, connect to the service manually using the **PaymentMBean.connect** method. This MBean operation will disconnect Services Gatekeeper from the Diameter server and then connect to it.

Table 2 (Cont.) Known Issues

Bug ID	Description
13456099	In some instances, when you log into Service Gatekeeper Administration Console, it displays a login error. When you attempt to log in again, Service Gatekeeper logs you into the console. The login process of Service Gatekeeper Administration Console is controlled by the WebLogic server and beyond the scope of Service Gatekeeper. Please ignore this exception.

Documentation Notes

This section contains late-breaking documentation updates that were not able to be included in main documentation set.

Composite Service Contract SLA Policy Deny Codes

Table 3 describes the composite service contract service level agreement policy deny codes.

Table 3 Composite Service Contract SLA Policy Deny Codes

Deny Code	Alarm TagPolicy Value	Policy Exception Error Message
1	1001	Application instance does not exist
2	1001	Application instance is not active
3	1001	Application does not exist
4	1001	Service provider account does not exist
6	1002	Unable to get service provider and application information
7	2003	Application request limit exceeded, 3026
8	2003	Service provider request limit exceeded, 3026
9	2001	Application request limit exceeded for Service Type
10	2001	Service provider request limit exceeded for Service Type
11	1001	Service provider account is not active
12	1001	Application instance is not active
13	2002	Service provider quota limit exceeded
14	2002	Application quota limit exceeded
15	2008	Service provider quota limit exceeded for Service Type
16	2008	Application quota limit exceeded for Service Type
20	4001	All properties denied
21	3001	Value *$string* for parameter *$string* was denied by SLA

Table 3 (Cont.) Composite Service Contract SLA Policy Deny Codes

Deny Code	Alarm TagPolicy Value	Policy Exception Error Message
22	4002	Request info is empty
23	3002	Service method *$string* is not allowed to be accessed
24	3003	No service provider group SLA found for application instance *$string*
25	3003	No application group SLA found for application instance *$string*
26	4003	ExternalInvocator threw an Exception: *$string*
27	4004	Error validating the request: *$string*
28	2004	SP node request limit exceeded
29	2005	Global or SP node service contract is out of date
30	3004	No global or SP node found
31	3005	Application or Service Provider group Service Contract is out of date for type: *$string*
32	3006	Application or Service Provider group Service Type contract is out of date for type: *$string*
33	3003	No SLA found for type: *$string*
34	3007	No Service Contract found for type: *$string*
35	2006	Subscriber restrict all
36	2007	Subscriber quota limit reached for URI: *$string*
37	2007	Subscriber rate limit reached for URI: *$string*
38	2004	Global request limit exceeded
39	1003	Application *$string* is not logged in
40	3008	Application or Service Provider group Composed Service contract is out of date for type: *$string*
41	3009	Application request limit exceeded for Composed Service
42	3009	Service provider request limit exceeded for Composed Service
43	3010	Service provider quota limit exceeded for Composed Service
44	3010	Application quota limit exceeded for Composed Service

ParlayX 3.0 Payment Default Timeout

The maximum wait time for a response from a billing server is 30 seconds. After 30 seconds, Services Gatekeeper will throw an SVC0001 exception.

SMS/MMS Delivery Receipts Expiry Time

The default expiry time for SMS and MMS delivery receipts in Services Gatekeeper storage is one week.

Billing Inconsistencies when the Services Gatekeeper Storage Database is Unavailable

When the Services Gatekeeper storage database is unavailable, Services Gatekeeper can continue to handle traffic and send Charging Data Records (CDRs) via the Java Message Service (JMS) interface. However, since those CDRs cannot be stored in the Services Gatekeeper database, when the database is available again, if you calculate charges based upon the CDRs in the database, the result will be less than the actual value.

Oracle Business Intelligence Access Denied for User to Path Error

If you have installed Oracle Business Intelligence (OBI) to support Services Gatekeeper Reporting, you may encounter the following issue where, after logging in as the OBI administration user, and then trying to access **My Folders** or **My Dashboard**, you get the error:

```
Access denied for user to path /users/<Admin User Name>
```

To resolve this issue, do the following:

1. On the machine hosting the OBI installation, navigate to the directory

   ```
   OBI_Home\instances\instance1\bifoundation\OracleBIPresentationServicesComp
   onent\coreapplication_obips1\catalog\<Your Catalog Name>\root\users
   ```

2. Delete the <*Admin User Name*> folder and the file <*Admin User Name*>*.atr*.
3. Restart the OBI server.
4. Login as <*Admin User Name*>.

You should now have access to **My Folders** and **My Dashboard**.

Startup Customization for Solaris11 When User Credentials Fail

This customization is necessary if you use **`ocsg510_solaris_sparc.bin`**, the 32-bit JDK installer, to install Services Gatekeeper on a 64-bit Solaris machine.

In such a scenario, when you start a Weblogic Server, using **startWeblogic.sh** or **startManagedWeblogic.sh** script directly in the Solaris 11 environment, the server prompts for a user name and password.

A native library (`terminalio`) prevents passwords typed on the command line from being echoed to the terminal (a requirement for production modes).

The start process for the server exits with the following error:

```
Native Library(terminalio) to read the password securely from commandline is not
found
```

To resolve this issue, do the following:

1. Create a folder/directory called **security** under $*DOMAIN_HOME*/**servers/***x_server*

where

- *DOMAIN_HOME* is the root directory for the Service Gatekeeper domain.
- *x_server* is the appropriate server, such as *Admin, NT1, AT1*

2. Create a boot identity file called **boot.properties** as a text file.

   This file should contain the user name and password for starting and stopping the instance of WebLogic Server for the server.

   For more information on creating boot identity files, see the description of *Boot Identity Files* in *WebLogic Server Administration Console Online Help* documentation.

3. Store the **boot.properties** file under the **security** directory.

If you store the **boot.properties** file under **security** directory no further action is required. WebLogic Server will locate the file.

Pointing the Startup Script to a Custom boot.properties File Location

If you stored the **boot.properties** file in a different location (that is, not in the **security** directory), update your **setDomainEnv.sh** script with the information necessary to retrieve the encrypted user credentials from the **boot.properties** file.

To do so:

1. Using a text editor, open the $*DOMAIN_HOME*/**bin/setDomainEnv.sh** file for the WebLogic Server.
2. Add the following entry to the JAVA_OPTIONS property:

   `-Dweblogic.system.BootIdentityFile=`*filename*

   Where, *filename* is the fully qualified pathname of a valid boot identity file, **boot.properties**.

3. Save the **setDomainEnv.sh** file.

Restart the instance of the WebLogic Server.

Documentation Updates and Enhancements

The following enhancements and updates have been made to the Services Gatekeeper documentation.

OAuth Guide

Oracle Communications Services Gatekeeper OAuth Guide has been reorganized for clarity and updated with new release features.

Security Guide

A new book, *Oracle Communications Services Gatekeeper Security Guide*, has been added to this release. The guide explains how to install, configure and use Services Gatekeeper securely.

Installation Guide

Oracle Communications Services Gatekeeper Installation Guide has been revised and reorganized for clarity. Installation procedures for Oracle Express Edition Database as

well as for Portal and Reporting support and upgrade scenarios from earlier versions have been added as well.

JavaDocs and OAM JavaDocs

More than 650 Java source files have been reviewed and edited in order to improve the clarity of the *Oracle Communications Services Gatekeeper Java API Reference* and *Oracle Communications Services Gatekeeper OAM Java API Reference*.

Eclipse Wizard Documentation

All Eclipse wizard documentation has been combined into a single chapter, "Using the Eclipse Wizard," in the *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*. References to that chapter have been placed as required in the other documents.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle Communications Services Gatekeeper Release Notes, Release 5.1
E37528-01