Oracle® Communication Services Gatekeeper

Release Notes

Release 4.0

June 2008

ORACLE®

Oracle Communication Services Gatekeeper Release Notes, Release 4.0

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

1. New Features

2. Backwards Compatibility

3. Gatekeeper 4.0 Known and Resolved Issues

CHAPTER 1

New Features

Welcome to Oracle Communications Services Gatekeeper™ 4.0. As the leading Telecom Service Access Gateway, Gatekeeper integrates telecom network technologies with Web Services to provide a reliable framework for developing and deploying highly available, scalable, and secure telecommunications applications and features. Gatekeeper's seamless integration of disparate, heterogeneous platforms and applications enables your network to leverage existing software investments and share the carrier-class services and data that are crucial to building next-generation telecommunication applications.

For version 4.0, Gatekeeper’s development has been driven by two main concerns:

- Evolve the Platform
- Respond to Customer Feedback

This chapter describes at a high level what new features in Gatekeeper have been created to support these goals. In addition the following topics are covered:

- Supported Interfaces
- Changed Behavior and Naming Conventions

Evolve the Platform

Version 3.0 marked a substantial change to the basic architecture of Gatekeeper. Version 4.0 builds on that change, preparing the way for future developments.

WebLogic Server 10.0 MP1

In version 4.0, Gatekeeper has been moved to WebLogic Server 10.0, MP1. This has multiple benefits for the Gatekeeper platform, including:

- Support for Java Enterprise Edition v5
- Unicast for cluster communication. Unicast is easier to configure and uses fewer network resources than multicast
- Support for Oracle Fast Connection Failover
- Cluster-wide timers
- Upgrades of Web Services Security Standards
  - WS-SecureConversations 1.0 -> 1.3
  - WS-Security 1.0 -> 1.1
  - WS-SecurityPolicy 1.2
  - WS-Trust 1.0 -> 1.3

Enhanced Deployment Model

In version 3.0, Gatekeeper was deployed as a single large EAR file. Making changes required editing the EAR, which was cumbersome. In addition, platform-wide services were stored in the same EAR as the components that implemented network integration logic (Communication Services), tying them to the Gatekeeper classloader and lifecycle. This has been changed in version 4.0

- Platform-wide services (Container Services) are integrated into WebLogic Server itself as Server Services. Their lifecycle is now tied to the lifecycle of the container, and they belong to the container’s classloader. The container itself is hardened and tuned for the needs of telecom usage.
- Each Communication Service is packaged in its own EAR, making it much simpler to deploy and un-deploy individual services, aligning the system more closely with the standard JEE application deployment model.

Production Upgrade

Gatekeeper 4.0 supports a fully automated upgrade model, supporting hitless (zero down time) upgrades

- Most Communication Services can be upgraded dynamically, with the older network translation component (the plugin) keeping track of in-flight traffic and retiring gracefully only after that traffic has been processed, while new traffic is sent to the updated version.
  - Supported for HTTP-based, Parlay, SMPP, SIP, and LDAP plug-ins
  - Not supported for INAP
- Platform-based Container Services can be upgraded using the WLS rolling upgrade method.
- Components are now versioned, and versioning information is now propagated through management interfaces, accounting records, logs, and so forth.
- All upgrades can be managed through the Administration Server.

Subscriber-Centric Policy

Previous versions of Gatekeeper supported fine-tuned policy control for service providers and applications. Version 4.0 introduces the capability of creating a similar system for an operator’s subscribers

- Provides a mechanism for highly granular subscriber personalization and protection.
- Adds subscriber SLAs, which can be enforced on a per subscriber level.
- Allows subscriber-centric throttling, based on the cluster-wide budget service.

CORBA Removal

Previous versions of Gatekeeper required the use of the ORB as a basic infrastructure component. This is not the case in version 4.0

- All OAM methods are now pure JMX-based MBeans
- Gatekeeper can be run in a completely ORB-free mode
- CORBA only used at the Communication Services level, for Parlay Gateway connectivity

New Account Module

Version 4.0 represents a major update in the handling of partner account information.

- Completely re-written partner on-boarding account management

- SLA management (including editing) from the Adminstrative Console
- CORBA removed
- Aligned with CSS and the Java security model
- The on-boarding account structure documented in the security contex of the thread
- Database access no longer necessary from the Access Tier, increases firewall security

PRM

- WS-Security support
- No sessions required for 4.0 clients
- Stateless WS to JMX bridge
- Multiple deployment options
- Version 2.2 and 3.0 backwards compatible

Respond to Customer Feedback

The updated design of Gatekeeper version 4.0 also includes multiple features requested by customers, in both the area of usability and extensibility.

Usability

The task of managing a service access gateway is inherently complex, but version 4.0 has a number of features designed to ease the process.

Plugin Instantiation

- New Plugin hierarchy
  - New Plugin Service module contains the plugin definition, including a mapping to a specific protocol. It is also responsible for aspects of the instance’s lifecycle
  - New Plugin Instance is a single runtime instance of a Plugin Service
- Instances can be added and provisioned at runtime, without redeployment
- Each plugin instance can have a separate configuration

- Out of the box installation creates no instances by default, saving on resources
- Extension APIs to cover this new hierarchy

Sessions Optional

- System-wide setting to enable clients to authenticate with the Gatekeeper using only WS-Security.
- Sessions can be used to hold client identity when WS-Security is disabled
- Sessions are necessary in the context of Geo-Redundancy

SMPP

- Support for multiple SMPP BINDs
  - Dynamically configurable pool of connections for each plugin instance
  - Supported for Transmitter, Receiver, and Transceiver
  - Distinct pool sizes can be set up
  - Optional per connection window size
- Support for concatenation of segmented messages (network-triggered) in the plugin.

OAM

- Based on standard MBeans, available through JMX. No CORBA
- Verbose description of every method argument
- Published, JavaDoc'ed API
- ObjectName Conventions

Customization and Extensibility

Because all networks are different, being able to customize and extend Gatekeeper to tune its behavior is crucial.

Service Interceptors

Previous versions of Gatekeeper relied on a Policy Engine to make enforcement decisions. This release introduces an entirely new mechanism designed to be both very powerful and easily extensible.

- Interceptors have full control over all traffic flow: application-initiated and network-triggered
- The Interceptor Stack represents all out of the box traffic processing: validation, policy enforcement, and routing
- The Policy Engine is still available via the Interceptor Stack if desired
- The order of processing in the Stack can be easily changed
- There is a rich SPI for creating new interceptors
- Interceptors are deployed in their own EAR

Platform Development Studio

The Extension Toolkit that was shipped with version 3.0 has been extended and enlarged, and is now called the Platform Development Studio.

- The Eclipse Wizard has been updated to reflect the new architecture
- A full range of scripts, ANT tasks, and code samples has been added
- The Unit Test Framework has been brought forward
- The Platform Test Environment, formerly known as GTool, and offered only through Dev2Dev, has been substantially upgraded and extended. It is now a part of the product. It includes tools for accessing all aspects of Gatekeeper, including an MBean browser, JMS listeners, database table browsers, and much more, as well as a rich testing enviroment, including test clients and network simulators. It also easily extensible.

Proxy Communication Service

The SOAP-to-SOAP Communication Services function allows operators to expose SOAP-based Web Services requests of any kind to the rigorous monitoring, routing, and resource protection facilities of Gatekeeper, even if the data itself is not being transported by Gatekeeper’s standard Communication Services.

- Generated and deployed from WSDLs using the Eclipse Wizard. No development effort is needed.
- Exposes existing operator SOAP resources without having to code a line
- Can supports both application-initiated and network-triggered traffic.
- Provides:
  - Resource protection
  - Resource monitoring
  - Routing
  - Health monitoring
  - Load balancing

Subscriber Data Access

In addition to the Subscriber-Centric Policy mechanism mentioned above, Gatekeeper offers a new Subscriber Profile Communication Service that provides LDAP access

- Applications can access subscriber data, within bounds defined by operator constructed filters
- Uses an efficient connection pool to manage access

Supported Interfaces

Gatekeeper 4.0 has support for a number of application-facing interfaces. The following communication services (application-facing interfaces with related network plugins) are included in this release, including three call control services built on the Parlay X 3.0 standards, which allow multiple functionalities to interact within the same call session. All of these services take advantage of the enhanced version 3 architecture. They include:

- Parlay X 3.0 Audio Call connecting to Parlay 3.3
- Parlay X 3.0 Third Party Call connecting to Parlay 3.3
- Parlay X 3.0 Call Notification connecting to Parlay 3.3
- Parlay X 2.1 Third Party Call connecting to INAP and SIP
- Parlay X 2.1 Call Notification connecting to SIP

- Parlay X 2.1 SMS connecting to SMPP 3.4
- Extended Web Services Binary SMS connecting to SMPP 3.4
- Parlay X 2.1 MMS connecting to MM7
- Parlay X 2.1 Terminal Location connecting to MLP3.0/3.2
- Parlay X 2.1 Presence connecting to SIP
- Extended Web Services WAP Push connecting to PAP
- Extended Web Services Subscriber Profile connecting to LDAP

Changed Behavior and Naming Conventions

The changes in version 4.0 mean that some features and naming conventions from earlier versions have changed in significant ways.

- The components previously called “traffic paths” are now called “communication services”.

  Note: These components were also call “exposure services” in the version 4.0 Technical Preview.

- The “Extension Toolkit” has become the “Platform Development Studio”.
- Parlay Gateway connectivity is not supported, except in the three Parlay X 3.0 call control services.
- What used to be called the “Application Instance Group” is now called the “Application Instance” and functions essentially as an authentication username. It must be unique.
- Some database tables have been changed. There are migration scripts provided as part of the post-installation phase of setting up Gatekeeper to bring installed databases up to current status.

Supported Configurations

The supported configurations have not changed since the writing of the *Architectural Overview*. For a complete listing, see the Technical Specifications chapter.

Backwards Compatibility

This section covers backwards compatibility between Weblogic Network Gatekeeper 3.0 and Oracle Communication Services Gateway 4.0. The following areas are discussed:

- Platform Upgrades
- Communication Services
- Extensions
- Partner Relationship Management
- Operations and Management
- Database
- EDR Generation
- Service Level Agreements

Platform Upgrades

Upgrade from Network Gatekeeper 3.0 to Gatekeeper 4.0 are supported. The upgrade process requires a full cluster restart and will need to be scheduled during a maintenance window. WebLogic Server does not support hitless upgrades across major releases, so this is a result of the fact that the base platform used by Gatekeeper has been upgraded from WebLogic Server 9.2 to WebLogic Server10 MP1.

Scripts and tools to facilitate upgrade and migration of data are provided.

Upgrades from Network Gatekeeper 2.2 are *not* supported. They are considered new installations.

Communication Services

There are some changes in out-of the box communication services.

OSA/Parlay connectivity has been removed from the standard platform, except for the Parlay X 3.0 call control related services, which based directly on customer-driven requirements. As a result, the following communication services have been removed from the standard platform:

- Parlay X 2.1 Third Party Call/Parlay 3.3 MultiParty Call Control
- Parlay X 2.1 Call Notification/Parlay 3.3 MultiParty Call Control
- Parlay X 2.1 Short Messaging/Parlay 5.0 Multimedia Messaging
- Parlay X 2.1 Multimedia Messaging/Parlay 5.0 Multimedia Messaging
- Parlay X 2.1 Payment/Parlay 3.3 Charging
- Parlay X 2.1 Terminal Status/Parlay 3.3 Mobility, User Status
- Parlay X 2.1 Terminal Location/Parlay 3.3 Mobility, User Location
- Parlay X 2.1 Call Handling/Parlay 3.3 MultiParty Call Control and User Interaction
- Parlay X 2.1 Audio Call/Parlay 3.3 User Interaction and MultiParty Call Control

Backwards compatible communication services based on the deprecated Network Gatekeeper 2.2 and earlier CORBA based architecture are no longer supported. That is, the architecture that relied on the SESPA and ESPA modules is no longer supported. All OOTB communication services in this release, including the ones in 3.0 that were built on the older architecture, use the new architecture.

In addition. exceptions thrown by Extended Web Services interfaces are now aligned with Parlay X exceptions. That is, `ESVCxxx` is now `SVCxxx` and `EPOLxxx` is now `POLxxx`.

Extensions

Traffic paths and plug-ins built using Network Gatekeeper 3.0 Extension Toolkit must be adapted to the features of this release. Because there is a new deployment model for communication service and because the Extension Toolkit has been restructured and folded into the Platform Development Studio, extensions built in the 3.0 architecture are source compatible only and cannot be directly deployed. See section Converting Traffic Paths and Plug-ins to

Communication Services in *Platform Development Studio - Developer’s Guide* for more information.

Extension plug-ins that use the storage service need to be repackaged to deploy their schema configuration using the new storage service configuration deployment model.

Backwards compatible communication services based on the deprecated Network Gatekeeper 2.2 and earlier CORBA based architecture are no longer supported. They must be re-implemented using the new architecture.

Extension APIs that are deprecated:

- com.incomit.slee.*
- com.bea.wlcp.wlng.api.plugin.common.AbstractManagedPlugin
- com.bea.wlcp.wlng.api.edr.EdrManager
- com.bea.wlcp.wlng.api.plugin.ManagedPlugin

Partner Relationship Management

Support for provisioning of data specific to individual communication services has been removed from the PRM interfaces. The PRM interfaces are re-positioned to provide on-boarding, workflow management, monitoring and SLA provisioning for applications and service providers. Provisioning of individual communication services should be performed using JMX.

Operations and Management

All OAM MBean interfaces have been updated as a result of unified exception handling and support for MBean hierarchies.

All return types and exceptions for the MBean have been packaged in a JAR file, `$PDS_HOME/wlng_pds400/lib/wlng/oam.jar`, for easy of JMX integration.

All OAM interfaces based on IDL/CORBA have been removed and aligned with standard JMX.

The following OAM interfaces have been removed:

- com.incomit.espa.access
- com.incomit.espa.charging
- com.incomit.espa.messaging

- com.incomit.espa.userlocation
- com.incomit.policy
- com.incomit.resources.messaging.mm7
- com.incomit.resources.mm.ul
- com.incomit.sespa.access
- com.incomit.sespa.charging
- com.incomit.sespa.userlocation
- com.incomit.slee.alarm
- com.incomit.slee.charging
- com.incomit.slee.event
- com.incomit.slee.scsmgr
- com.incomit.slee.snmp

Of particular interest are the ESPA_Access and SESPA_Access MBeans which have been replaced with a set of MBeans under com.bea.wlcp.wlng.account.*

The interfaces have been removed either because of the overall MBean updates or because their functionality has been removed from the platform.

The text-based Management Tool has been discontinued and is replaced by WLST.

Unused Alarm IDs have been removed.

Database

Database schemas have been changed and migration scripts are provided for upgrades.

EDR Generation

The contents of cdr.xml, edr.xml, and alarm.xml have been consolidated into `$DOMAIN_HOME/config/custom/wlng-edr.xml`. This file should only be edited using the EDR configuration pane in the Administrative Console.

Service Level Agreements

SLA schemas are now controlled and managed in conjunction with the release cycle of the product. This means that extending SLA schemas is no longer supported.

SLA XSDs are split into:

- Service Provider Group
- Application Group
- Common for Service Provider group and Application Group.
- Service Provider Group Node
- Global Node
- Common for Global Node and Service Provider Node

The attribute serviceProviderGroupID in the Global Node SLA is deprecated and made optional in the XSD.

The following SLA elements are removed from the Global Node SLA XSD:

- serviceProviderGroupID
- overloadLimit
- severeOverLoadLimit
- maxSizeOfSendList
- reqWarningLimit
- serviceType

The following SLA elements are removed from the Service Provider Node SLA XSD:

- overloadLimit
- severeOverLoadLimit
- maxSizeOfSendList
- reqWarningLimit
- serviceType

The following SLA elements are removed from the Service Prover Group and Application Group SLA XSDs:

- maxNoOfActiveCalls
- maxNoOfCallLegsInCall
- allowedCharging
- allowedMmCharging
- maxMessageSize
- maxMmMessageSize
- permission
- serviceCode
- uiResourceType
- gmsEventCriteria
- allowedMpccEvents
- allowedGccEvents
- allowedContentTypes
- allowedEncodingTypes
- currencyRestriction
- applySubscriptionRule

Gatekeeper 4.0 Known and Resolved Issues

Known Issues in Gatekeeper 4.0

.

Change Request Number	Description and Workaround or Solution	Found In	Fixed In
CR372355	Non-ASCII values for sendName in SMS and Binary SMS sendSMS result in garbled data. Values for this parameter must be ASCII per the SMPP standard.	4.0	
CR372834	The MLP Simulator in Platfor Test Environment will parse longitude/latitude incorrectly when the locale is not English. Switch locale to English	4.0	
CR365666	Installing the Windows version using the installer does not work if the installer file is in the root directory of the disk. Remove the installer file from root and place in a sub-folder.	4.0	

Change Request Number	Description and Workaround or Solution	Found In	Fixed In
CR366737	Some Gatekeeper DB tables specify primary keys and/or indexes that exceed the maximum key length for MySQL with MyISAM table type and UTF-8 character type. Either: 1. If you are using the MyISAM engine, set the character type to latin1 or 2. Use the InnoDB engine with UTF-8 or latin1 character set	4.0	
CR370718	Return values from methods on the Store are not size limited. This can cause out-of-memory errors if the dataset is very large. Make sure your queries don't fetch the entire key/entry/value set from stores	4.0	
CR372233	Warnings are thrown even when the silent installer is run successfully. These warnings have no impact on functionality.	4.0	
CR372323	An IllegalArgumentException can be thrown when retrieving MMS message details in the Platform Test Environment. This usually does not affect the outcome of the operation.	4.0	
CR372242	Gatekeeper can create new connections to the database when all the connections in the pool are in use. This can cause lock contention. Make sure that the database is configured with an adequate value for `MaximumCapacity`.	4.0	
CR372847	The Statistics Service createWeeklyReport operation fails to retrieve a value which the report requires, which causes the operation to fail.	4.0	

Change Request Number	Description and Workaround or Solution	Found In	Fixed In
CR346962	If the address of the MLP server is changed using OAM, the plug-in does not try to connect to the new server immediately. Instead it waits for the heartbeat interval before trying to connect.	3.0MP1	
CR310647	During startup, there is a warning that no appenders can be found for loggers. The messages occur in the brief period of time when classes try to log messages before log4j has been initialized. They do not indicate a problem.	3.0	

Resolved Issues in Gatekeeper 4.0

CR341661	Installing WLNG defaults to a development mode installation instead of production mode.	3.0	4.0
CR330939	There is no OAM method to enable trace for Access Tier servers	3.0	4.0
CR329979	Changing buffer size property for Trace service erases the trace files content.	3.0	4.0
CR311065	If you make changes in WS-Security options using the Admin Console, the Console offers to let you store plan.xml in the directory of your choice. But WLS itself only looks for the plan.xml in the default location, so a file saved to other than the default location has no impact on WLS behavior. .	3.0	4.0

CR327407	When SLAs are updated, only the server where the SLA is updated gets the current settings immediately. The budget service does not push budget configuration changes to slaves on update, so other Network Tier servers keep the old budget settings until the budget service polls for configuration changes.	3.0	4.0
CR326236/ CR328083/ CR328439/CR306501	In some cases of NT failover while running MMS, WAP Push with Delivery Notifications, or Terminal Location traffic, there may be a brief period during which throughput falls to zero and some messages are lost.	3.0	4.0
CR327200	If you are using the backwards compatible version of the SMS traffic path with SMPP, and you have multiple plug-ins, each of which is set to different limits in the Node SLA, node policy enforcement will not work correctly. **Note:** This communication service is no longer supported	3.0	4.0
CR319714	When there are multiple address fields in a StartCallNotification message, only the SIP URL in the first address field is checked for format.	3.0	4.0
CR319715	Trying to stop CallNotification with an invalid correlator produces an SVC001 exception instead of the correct SVC002.	3.0	4.0
CR317967	If an application calls StopSmsNotification with an invalid correlator, an incorrect error message is produced. An SVC0002 exception is thrown, but the variables field in the response message contains the value of the correlator, not the text "Correlator"	3.0	4.0
CR318556	If an application calls EndCall with an incorrectly formatted identifier, an incorrect error message is produced. An SVC0001 exception is thrown, with error code SIP000003 instead of an SVC002.	3.0	4.0

CR318555	If an application calls EndCall with an invalid identifier, no error message is produced. An SVC002 should be thrown.	3.0	4.0
CR318552	If an application calls MakeCall with a charging part defined and the ThirdPartyCall plug-in for SIP has ChargingAllowed set to false, no error message is produced. A POL0008 exception should be thrown.	3.0	4.0
CR319755	If an application calls StartCallDirectionNotification more than once for a single SIP address, an incorrect error message is produced. An SVC0001 exception is thrown with the error code CN-000001. The correct value would be an SVC0002 exception with a variable field that indicates the SIP address. **Note:** The decision was that the current implementation is more useful for end user. Marked Works as Designed.	3.0	4.0
CR327292	Both SP and Global node SLA contracts are enforced even if the use period falls outside of specified start and end dates.	3.0	4.0
CR329959	If there are overlapping <override> tags in the SLA, enforcement may choose either tag value.	3.0	4.0
CR327429	Node/Global policy enforcement throws service exceptions instead of policy exceptions	3.0	4.0
CR330699	In the Extension Toolkit the Turn On Plug-in Debug option cannot be selected.	3.0	4.0
CR305817	There is no mechanism for unregistering interfaces for a ManagedPlugin instance. New objects that are registered are simply appended to the existing list.	3.0	4.0

CR329497	The alarm page of the Management Console does not limit the number of alarms displayed. In a situation where many alarms are being emitted, this may cause significant lag times as the page is being rendered.	3.0	4.0
CR326557	The management operation PolicyArrow symbolreloadServiceProviderXmlDriver does not reload the XSD for the Service Provider SLAs.	3.0	4.0
CR305375	Management operation SLEEArrow symbolgetFreeDiskSpace does not return the correct value. A NumberFormatException Exception is thrown.	3.0	4.0
CR327896	Application sessions expire one minute early. If LoginTicket Lifetime (session) check is enabled, the time-out value expires one minute earlier than expected.	3.0	4.0
CR329465	In the SMPP plug-in for SMS, the methods getReceivedSms and getSmsDeliveryStatus produce events, but these are not described in the edr.xml file. This means that the event will not be classified, and will appear to listeners as "Unknown." As a result, it is impossible to have these events trigger CDRs.	3.0	4.0
CR326808	Network Gatekeeper cannot process MMSes without attachments, as, for example, an MMS that is sent with a subject but no content. If a SOAP attachment is NULL, SVC0001 is thrown to the application and NullPointerExceptions are logged in Network Gatekeeper	3.0	4.0

CR306833	If an application calls SendSms with no destination address specified, an incorrect error message is produced. An SVC0001 exception is thrown, but the variables field in the response message reads: "No plug-in available for type: interface com.bea.wlcp.wlng.px21.plugin.SendSmsPlugin".	3.0	4.0
CR311849	Service Level Agreements fail to load if there are space characters prior to the <?xml> tag.	3.0	4.0
CR327194/CR327314	Alarms are not generated in certain circumstances: for Node/Global policy enforcement, when Node SLA limit for application-initiated traffic is reached	3.0	4.0
CR318142	If you use the Eclipse plug-in to generate a communication serviceskeleton, the GUI does not give you the option of naming the Administration Server anything but AdminServer. Also using the plug-in GUI you cannot specify t3 as the protocol for the WLS administration URL.	3.0	4.0