BEA WebLogic Network Gatekeeper™

SDK User Guide

Version 3.0™
Document Revised: 14 September 2007

Copyright

Copyright © 1995-2007 BEA Systems, Inc. All Rights Reserved.

Restricted Rights Legend

This software is protected by copyright, and may be protected by patent laws. No copying or other use of this software is permitted unless you have entered into a license agreement with BEA authorizing such use. This document is protected by copyright and may not be copied photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form, in whole or in part, without prior consent, in writing, from BEA Systems, Inc.

Information in this document is subject to change without notice and does not represent a commitment on the part of BEA Systems. THE DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, BEA SYSTEMS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE DOCUMENT IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Trademarks and Service Marks

Copyright © 1995-2007 BEA Systems, Inc. All Rights Reserved. BEA, BEA JRockit, BEA WebLogic Portal, BEA WebLogic Server, BEA WebLogic Workshop, Built on BEA, Jolt, JoltBeans, SteelThread, Top End, Tuxedo, and WebLogic are registered trademarks of BEA Systems, Inc. BEA AquaLogic, BEA AquaLogic Data Services Platform, BEA AquaLogic Enterprise Security, BEA AquaLogic Interaction, BEA AquaLogic Interaction Analytics, BEA AquaLogic Interaction Collaboration, BEA AquaLogic Interaction Content Services, BEA AquaLogic Interaction Data Services, BEA AquaLogic Interaction Integration Services, BEA AquaLogic Interaction Process, BEA AquaLogic Interaction Publisher, BEA AquaLogic Interaction Studio, BEA AquaLogic Service Bus, BEA AquaLogic Service Registry, BEA Builder, BEA Campaign Manager for WebLogic, BEA eLink, BEA Kodo, BEA Liquid Data for WebLogic, BEA Manager, BEA MessageQ, BEA SALT, BEA Service Architecture Leveraging Tuxedo, BEA WebLogic Commerce Server, BEA WebLogic Communications Platform, BEA WebLogic Enterprise, BEA WebLogic Enterprise Platform, BEA WebLogic Enterprise Security, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic Java Adapter for Mainframe, BEA WebLogic JDriver, BEA WebLogic Log Central, BEA WebLogic Mobility Server, BEA WebLogic Network Gatekeeper, BEA WebLogic Personalization Server, BEA WebLogic Personal Messaging API, BEA WebLogic Platform, BEA WebLogic Portlets for Groupware Integration, BEA WebLogic Real Time, BEA WebLogic RFID Compliance Express, BEA WebLogic RFID Edge Server, BEA WebLogic RFID Enterprise Server, BEA WebLogic Server Process Edition, BEA WebLogic SIP Server, BEA WebLogic WorkGroup Edition, BEA Workshop for WebLogic Platform, BEA Workshop JSP, BEA Workshop JSP Editor, BEA Workshop Struts, BEA Workshop Studio, Dev2Dev, Liquid Computing, and Think Liquid are trademarks of BEA Systems, Inc. Accelerated Knowledge Transfer, AKT, BEA Mission Critical Support, BEA Mission Critical Support Continuum, and BEA SOA Self Assessment are service marks of BEA Systems, Inc.

All other names and marks are property of their respective owners.

Contents

Document Roadmap

Network Gatekeeper SDK

Using the Network Gatekeeper SDK

Installing and configuring Network Gatekeeper SDK

CHAPTER 1

Document Roadmap

The following sections describe the audience for, and organization of, this document:

Document Scope and Audience

This guide describes the operation of the Network Gatekeeper SDK, including:

- Supported functionality
- Installation, start up and configuration
- General operation

The intended audience consists of developers and test engineers developing applications that will interact with WebLogic Network Gatekeeper.

Guide to This Document

This document contains the following chapters:

- Chapter 1, “Document Roadmap”: This chapter
- Chapter 2, “Network Gatekeeper SDK”: Introduction to the Network Gatekeeper Simulator
- Chapter 3, “Using the Network Gatekeeper SDK”: How to use the Network Gatekeeper Simulator
- Chapter 4, “Installing and configuring Network Gatekeeper SDK”: Installing the Network Gatekeeper Simulator

New Features in This Release

Previous versions of WebLogic Network Gatekeeper supported an Application Testing Environment (ATE) that required a fully installed version of Network Gatekeeper to run. Version 3.0 includes an SDK and Network Gatekeeper Simulator that runs in WebLogic Server without the need for any Network Gatekeeper installation. The Simulator also includes a customizable GUI for testing SMS, MMS, PAP, and Terminal Location. And because all application-facing interfaces are based on Web Services interfaces, application developers can use the tools of their choice for creating their applications.

Terminology

The following terms and acronyms are used in this document:

- Account—A registered application or service provider, associated with an SLA
- Account group—Multiple registered service providers or services which share a common SLA
- API—Application Programming Interface
- Application—A TCP/IP based, telecom-enabled program accessed from either a telephony terminal or a computer
- Application-facing Interface—The Application Services Provider facing interface
- Application Service Provider—An organization offering application services to end users through a telephony network
- Application User—An Application Service Provider from the perspective of internal Network Gatekeeper administration. An Application User has a user name and password

- End User—The ultimate consumer of the services that an application provides. An end user can be the same as the network subscriber, as in the case of a prepaid service or they can be a non-subscriber, as in the case of an automated mail-ordering application where the subscriber is the mail-order company and the end user is a customer to this company
- SMS—Short Message Service
- Subscriber—A person or organization that signs up for access to an application. The subscriber is charged for the application service usage. See End User
- WSDL —Web Services Definition Language
- XML—Extended Markup Language

Related Documentation

This SDK user guide is a part of the WebLogic Network Gatekeeper documentation set. The other documents include:

- *Architectural Overview*
- *System Administrator's Guide*
- *Handling Alarms*
- *Installation Guide*
- *Integration Guidelines for Partner Relationship Management*
- *Managing Service Providers and Applications*
- *Statement of Compliance*
- *Application Development Guide*
- *Extension Toolkit - Developer's Guide*
- *System Backup and Restoration Guide*
- *Licensing*
- *Traffic Path Reference*

Additionally, many documents in the WebLogic Server 9.2 documentation set are of interest, including:

- *Introduction to BEA WebLogic Service and BEA WebLogic Express™*
- *Programming Web Services for WebLogic Server*
- *Securing WebLogic Server*

CHAPTER 2

Network Gatekeeper SDK

Introduction to the Network Gatekeeper SDK

The BEA WebLogic Network Gatekeeper SDK provides a simulator for Network Gatekeeper and an interactive, graphical test environment for developers who are creating applications to interact with WebLogic Network Gatekeeper. The current version of the Network Gatekeeper Simulator supports the Parlay X 2.1 Short Messaging, Multimedia Messaging, Terminal Location interfaces, and the Extended Web Services WAP Push interfaces.

The Network Gatekeeper SDK is used for functional testing. Because it simulates a WebLogic Network Gatekeeper, it is not necessary to have an active instance of a WebLogic Network Gatekeeper when developing and performing functional tests of applications.

The following sections provide an overview of the Network Gatekeeper SDK:

What the Network Gatekeeper Simulator Provides

The Network Gatekeeper Simulator offers the following capabilities:

Supported interfaces

- Extended Web Services Access
- Extended Web Services Session Manager
- Parlay X 2.1 Short Messaging
- Parlay X 2.1 Multimedia Messaging
- Parlay X 2.1 Terminal Location
- Extended Web Services WAP Push

Supported message types

- SMS
- MMS
  - Text: plain text, HTML, and WML text only messages.
  - Graphics: gif, wbmp, tiff, png, and jpeg graphic files.
  - Applications: multipart, multipart-mixed, and SMIL.
- WAP Push

Supported Network Simulation

Network triggered events

Network triggered events, such as messages sent from a mobile phone to an application, can be simulated, using the Network Gatekeeper Simulator GUI.

The following events are supported:

- Receive SMSes
- Receive MMSes
- Periodic Terminal Location notifications

Application triggered requests

Application triggered requests, such as messages sent from the application to a mobile phone in the network, can be simulated, including:

- All request functionality from the application to WebLogic Network Gatekeeper.
- All call back functionality from WebLogic Network Gatekeeper to the application.

Other tasks

- Adding and deleting mobile phones
- Setting the geographical position of a mobile phone
- Adding application accounts for application login
- Provisioning of off-line notifications

What the Network Gatekeeper SDK Comprises

The Network Gatekeeper SDK is built up of these main parts:

- A simulator, including application-facing telecom interfaces
- A simulator GUI

The Network Gatekeeper Simulator

The Network Gatekeeper Simulator simulates a subset of the functionality of Network Gatekeeper. From an application point-of-view, the Simulator acts as a Network Gatekeeper that has connectivity to the telecom network. The Simulator provides an abstracted high-level simulation of the underlying network, with mobile terminals that can send and receive messages.

The Network Gatekeeper Simulator application-facing telecom Interfaces

The Network Gatekeeper Simulator exposes a subset of the interfaces and methods that Network Gatekeeper exposes:

- Parlay X 2.1 Interface SendSms:
  - sendSms

  - sendSmsLogo (only a binary representation of the logo is sent.)
  - sendSmsRingtone (only a binary representation of the ringtone is sent.)
  - getSmsDeliveryStatus
- Parlay X 2.1 Interface SmsNotification:
  - notifySmsReception
  - notifySmsDeliveryReceipt
- Parlay X 2.1 Interface ReceiveSms:
  - getReceivedSms
- Parlay X 2.1 Interface SmsNotificationManager:
  - startSmsNotification
  - stopSmsNotification
- Parlay X 2.1 Interface SendMessage:
  - sendMessage
  - getMessageDeliveryStatus
- Parlay X 2.1 Interface ReceiveMessage:
  - getReceivedMessages
  - getMessage
- Parlay X 2.1 Interface MessageNotification:
  - notifyMessageReception
  - notifyMessageDeliveryReceipt
- Parlay X 2.1 Interface MessageNotificationManager:
  - startMessageNotification
  - stopMessageNotification
- Parlay X 2.1 Interface TerminalLocation:
  - getLocation
  - getTerminalDistance

  - getLocationForGroup
- Parlay X 2.1 Interface TerminalLocationNotificationManager:
  - startPeriodicNotification
  - endNotification
- Parlay X 2.1 Interface TerminalLocationNotification:
  - locationNotification
  - locationError
  - locationEnd
- Extended Web Services WAP Push Interface PushMessage:
  - sendPushMessage
- Extended Web Services WAP Push Interface PushMessageNotification:
  - resultNotificationMessage
- Session Manager Service, Interface Session Manager
  - getSession
  - destroySession
  - refreshSession
  - getSessionRemainingLifeTime
  - changeApplicationPassword
- Access Service, Interface Access:

  Deprecated interface. Network Gatekeeper Simulator 3.0 is backward compatible with Network Gatekeeper 2.2 Access service for authentication and session management. New applications should use the Session Manager Service instead.

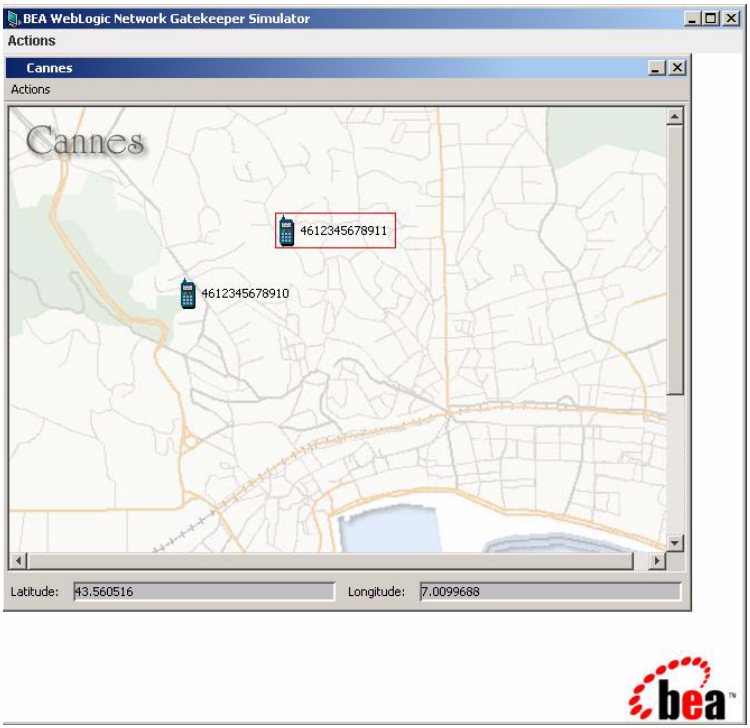
  - applicationLogin
  - applicationLogout
  - changeApplicationPassword
  - getLoginTicketRemainingLifeTime
  - refreshLoginTicket

When an application uses these interfaces, the simulator provides the same behavior as a Network Gatekeeper.

The Network Gatekeeper Simulator GUI

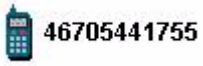
The Network Gatekeeper Simulator GUI is based on a map. The map can be changed to fit different locations. The GUI is used to add mobile telephony terminals (mobile telephones).

Figure 2-1 Network Gatekeeper Simulator GUI



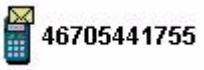
These terminals are given a subscription number. Once the terminal is defined, it can be moved to different locations on the map.

Figure 2-2 Telephone (terminal) icon



The terminals on the GUI can send and receive messages. When a message has arrived at the telephone, an envelope is displayed beside the telephone icon.

Figure 2-3 Telephone (terminal) icon with message



Using mobile terminals

The mobile terminals created in the Network Gatekeeper Simulator GUI can:

- Show the ID of the phone
- Indicate when messages have arrived
- Be moved using click and drag
- Receive and display SMSes.
- Receive and display PAP messages.
- Receive and display MMSes of the following types:
  - Text: plain text, HTML, and WML text only messages.
  - Graphics: gif, wbmp, tiff, png, and jpeg graphic files.
  - Applications: multipart, multipart-mixed.
- Send SMSes.
- Send MMSes of the following types:
  - Text: plain text, HTML, and WML text only messages.
  - Graphics: gif, wbmp, tiff, png, and jpeg graphic files.
  - Applications: multipart, multipart-mixed, and SMIL.

Note: SMSes and MMSes cannot be sent directly from a terminal to another. When sending a message, the message can be received by an application, but it cannot be sent directly to another phone.

Using the map

The Network Gatekeeper Simulator GUI can:

- Load new images as maps from any URL, stored locally or on the Internet.

- Set the geographical coordinates of the map.
- Display the coordinates of a selected phone.
- Display several maps simultaneously.

Using utilities

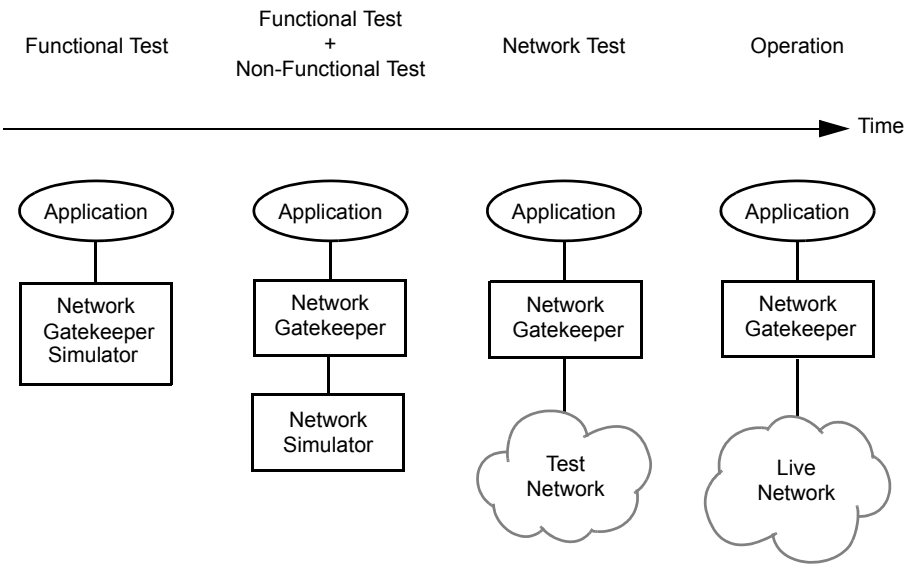
The Network Gatekeeper Simulator GUI can:

- Save a configuration - the map including coordinates - to file.
- Load a configuration from file.

Test Flow

Figure 2-4 shows the complete WebLogic Network Gatekeeper application test flow, from the application developers' functional test to deployment in a live network. An application developer can perform functional tests using Network Gatekeeper Simulator. The other tests in the flow must be performed in cooperation with a network operator.

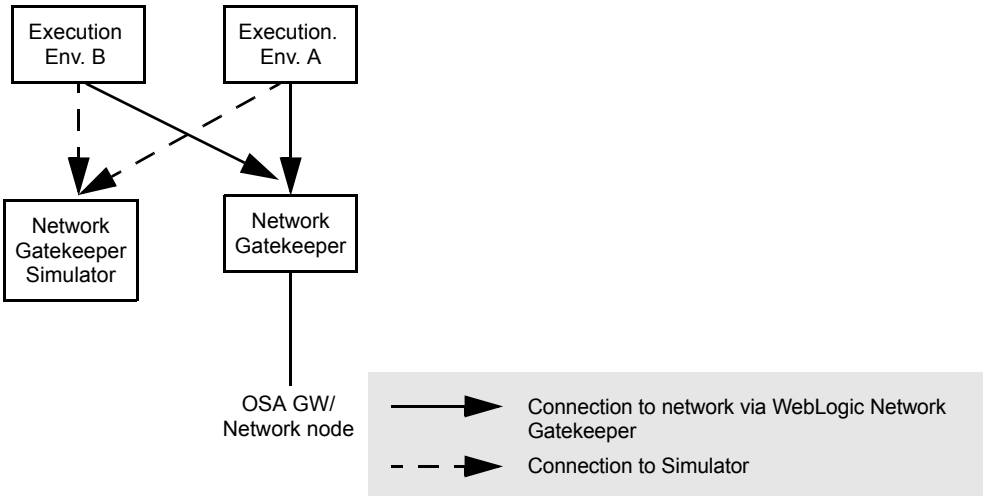
Figure 2-4 Application test flow



An overview of the relationship between Network Gatekeeper Simulator and WebLogic Network Gatekeeper is shown in Figure 2-5.

.

Figure 2-5 Network Gatekeeper SDK in relation to WebLogic Network Gatekeeper



In the first stage of testing, the Web Services endpoints are provided by Network Gatekeeper Simulator. In production, the application uses endpoints provided by the WebLogic Network Gatekeeper.

Supported Configurations

The Network Gatekeeper SDK and Simulator runs on Web Logic Server 9.2. It is supported on the following platforms:

Microsoft Windows XP SP2 on x86

Table 2-1 Requirements

Operating System Version and Patches	Windows XP Service Pack 2 and later Service Packs
Chip Architecture and Minimum Processor Speed	x86 and compatible chip architectures (1.3 GHz)
RAM	1 GB minimum, 2 GB recommended

Red Hat Enterprise Linux 4.0 on x86

Table 2-2 Requirements

Operating System Version and Patches	Red Hat Enterprise Linux 4.0-1 AS, ES, WS Kernel 2.6.9-11.ELsmp #1 SMP x86_32 GNU/Linux with glibc 2.3.4-2.9 and later updates and errata levels
Chip Architecture and Minimum Processor Speed	x86 (400 MHz)
RAM	1 GB minimum, 2 GB recommended
Additional	Must support X11

CHAPTER 3

Using the Network Gatekeeper SDK

The following sections describe how to use the Network Gatekeeper SDK:

- Start the Network Gatekeeper Simulator
- Add a new map
- Open a map
- Create user credentials for an application
- Remove a mobile phone/terminal
- Set the location of a mobile phone
- Send an MMS
- Open an MMS
- Send an SMS
- Open an SMS or PAP message
- Register an off-line notification for SMS
- Register an off-line notification for MMS

Start the Network Gatekeeper Simulator

To start the Network Gatekeeper Simulator from the Windows Start Menu:

Choose **Network Gatekeeper SDK 3.0.0**, and then **Start WebLogic Network Gatekeeper SDK**.

To start the Network Gatekeeper Simulator from the command line, enter:

- *BEA_Home*`\sdk300\samples\domains\sdk\startWebLogic` (Windows)
- *BEA_Home*`/sdk300/samples/domains/sdk/startWebLogic.sh` (UNIX)

where *BEA_Home* is the name of the directory in which you installed the Network Gatekeeper SDK.

The Network Gatekeeper SDK Simulator GUI is displayed.

The WebLogic Server Administration console can be used to configure the Network Gatekeeper SDK simulator and runtime environment. Use a supported web browser to go to `http://<server>:<port>/console` where the `<server>` and port correspond to your Network Gatekeeper installation. Default values are `localhost` and `7001`.

Add a new map

Starting in the **Network Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Add Map...**

   This opens the **Add Map** dialogue box.

2. In the **Map name** field, enter a description of the map.

3. In the **Map URL** field, enter the URL to the map, or choose a map located on the file system by clicking Browse and selecting a file.

   Supported map formats are GIF, JPEG, and BMP. The URL can be HTTP or File, for example http://some-map-hosting-company/london.jpg.

4. In the **Upper left corner coordinates** group:

   In the **Latitude field**, enter the latitude of the upper left coordinate of the map. North of the equator is a positive value between 0 and 90. South of the equator is a value between 0 and -90.

   In the **Longitude field**, enter the longitude of the upper left coordinate of the map. West of the Greenwich zero meridian is a negative value between 0 and -180. East of the Greenwich zero meridian is a positive value between 0 and 180.

5. In the **Lower right corner coordinates** group:

In the **Latitude** field, enter the latitude of the lower right coordinate of the map. North of the equator is a positive value between 0 and 90. South of the equator is a negative value between 0 and -90.

In the **Longitude** field, enter the longitude of the lower right coordinate of the map. West of the Greenwich zero meridian is a negative value between 0 and -180. East of the Greenwich zero meridian is a positive value between 0 and 180.

6. Click **OK**.

   Now the map and its meta information is stored under the name <Map name>.map in the directory `$DOMAIN_HOME\servers\<Servername>\maps`. This file can be transferred to any other Network Gatekeeper Simulator.

Open a map

Starting in the **Network Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Open Map...**

   This opens the **Open map** dialogue box.

2. From the **Map name** drop down list, choose a map to display.

   A preview of the map, together with data on the coordinates of the map, is displayed.

3. Click **OK**.

   This opens the map in the simulator GUI. Repeat this procedure for every map you want to display.

Create user credentials for an application

Starting in the **Network Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Create User...**

   This opens the **Create User** dialogue box.

2. In the **Application Instance Group Id** field, enter the user name the application should use when establishing a session (login). Must be unique.

3. In the **Service Provider Id** field, enter the service provider account ID for the application.

4. In the **Application Id** field, enter the application account ID for the application.

5. In the **Password** field, enter the password the application should use when establishing a session (login). The password must be at least 8 characters long.
6. Click **OK**.

   The user credentials are now registered and applications can use these to login.

Remove a mobile phone/terminal

Starting in the <Map name> window:

1. Right click on the telephone to be removed.
2. From the displayed menu, choose **Remove**.

   The telephone is removed.

Set the location of a mobile phone

Starting in the <Map name> window:

1. Click and hold the cursor on the telephone icon using the left mouse button.
2. Drag the telephone on the map.

   The terminal's coordinates are displayed as it is moved.

Send an MMS

This procedure is used for sending Multimedia Messages to an application. Sending messages from one terminal in the Gatekeeper to another is not supported.

Starting in the <Map name> window:

1. Right click on the icon of the telephone from which you wish to send the MMS.

   A menu is displayed.
2. From the menu, choose **Send multimedia message....**

   The **Send multimedia message** dialogue box is opened.
3. In the **To** field, enter the service number to which you wish to send the MMS.
4. Click **Add content**.

In the **Message** group, a row is opened for editing.

5. In the **Type** column, choose the type of content from the selection list.
6. In the **URL** column, enter the URL pointing to the content you wish to add to the message, or choose a file located on the file system by clicking **Browse** and selecting a file.
7. Repeat the above steps for each part of the MMS.
8. To remove any content, select the row containing the part and click **Remove content**
9. Click **Send**.

   The MMS is sent.

Open an MMS

When an MMS arrives at a phone, an envelope symbol appears beside the telephone icon. Follow the instructions below to open the MMS.

Starting in the <Map name> window:

1. Right click on the telephone that has received a new MMS.

   A menu is displayed.

2. From the menu, choose **Read multimedia message....**

   The **Read multimedia message** dialogue box is opened.

   In the left pane, a reference to the new message is displayed. Select the message reference and the content of the MMS is displayed in the right pane.

Send an SMS

This procedure is used for sending Short Messages to an application. Sending messages from one terminal in the Gatekeeper to another is not supported.

Starting in the <Map name> window:

1. Right click on the icon of the telephone from which you wish to send the SMS.

   A menu is displayed.

2. From the menu, choose **Send message....**

   The **Send message** dialogue box is opened.

3. In the **To** field, enter the service number to send the SMS to.
4. In the **Message** field, enter the text to send.
5. Click **Send**.

   The SMS is sent.

Open an SMS or PAP message

When an SMS or PAP message arrives at a phone, an envelope symbol appears beside the telephone. Follow the instructions below to open the SMS or PAP message.

Starting in the <Map name> window:

1. Right click on the telephone that has received a new SMS or PAP message.

   A menu is displayed.

2. From the menu, choose **Read message....**

   The **Read message** dialogue box is opened.

   In the **From** field, the mailbox ID is displayed.

   In the **Message** field, the message is displayed.

Register an off-line notification for SMS

When sending Short Messages from a terminal in the Network Gatekeeper Simulator, the message is sent to a service activation number. This registers an offline notification for applications that poll for mobile originated short messages. Mobile originating Short Messages sent to the service activation number that match a given criteria do not result in a notification callback to an application. Instead the message is stored in Network Gatekeeper Simulator.

Starting in the **Network Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **SMS Notifications...**

   This opens the **SMS Notifications** dialogue box.

2. Click **Add Notification.**
3. In the **Activation Number** field, enter the service activation number. In the **Criteria** field, enter a text to match against to determine if the application should receive the notification. This text is matched against the first word in the message. Leave empty to match all messages.

4. Click **OK**.

The notification is displayed with a registration identifier. The notification can be removed by selecting the notification and then clicking **Remove Notification**.

Register an off-line notification for MMS

When sending Multimedia Messages from a terminal in the Network Gatekeeper Simulator, the message is sent to a service activation number. This procedure registers an offline notification for applications that poll for mobile originated multimedia messages. Mobile originating Multimedia Messages sent to the service activation number do not result in a notification callback to an application. Instead the message is stored in Network Gatekeeper Simulator.

Starting in the **Network Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Enable Received MMS...**

   This opens the **Enable Receive MMS** dialogue box.

2. In the **Activation Number** field, enter the service activation number.
3. Click **OK**.

The notification is displayed with a registration identifier. The notification can be removed by selecting the notification and then clicking **Remove Notification**.

Define session lifetime

When an application establishes a session with Network Gatekeeper, the session has a lifetime (session ticket lifetime).The default lifetime can be changed.

Starting in the **Network Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Session Lifetime...**

   This opens the **Session Lifetime** dialogue box.

2. Enter the default lifetime, given in minutes.
3. Click **OK**.

CHAPTER 4

Installing and configuring Network Gatekeeper SDK

This chapter describes setting up the WebLogic Network Gatekeeper SDK for use. The chapter includes information on:

Installation procedure

To install the WebLogic Network Gatekeeper SDK:

Note: The sample domain that is provided with the Network Gatekeeper SDK can be used directly. Separate domain configuration is unnecessary.

Launch the GUI Installer - Windows

If you are using the GUI-based installer on a Windows machine, do the following:

1. Log in to the Windows system.
2. Go to the directory where you have copied the installation program. You acquire this program either from a WebLogic Network Gatekeeper SDK CD or the Download Center.
3. If you are using Explorer to find the file, double-click the installation file, `wlng_sdk300_win32.exe`
4. If you are using the console window to find the file, enter the following command:

```
wlng_sdk300_win32
```

Note: You can also include the `-log=full_path_to_log_file` option in the command line to create a verbose installation log. For example:

```
wlng_sdk300_win32 -log=<full_path>install.log
```

5. Go on to "Respond to the Prompts" on page 4-2

Launch the GUI Installer - UNIX/Linux

If you are using the GUI-based installer on a UNIX/Linux machine, do the following:

1. Log into the target UNIX system
2. Go to the directory where you have copied the installation program. You acquire this program either from the WebLogic Network Gatekeeper SDK CD or the Download Center.
3. Launch the installation by entering the following commands:

```
chmod a+x wlng_sdk300_<appropriate-platform-filename>.bin


./wlng_sdk300_<appropriate-platform-filename>.bin
```

Note: You can also include the `-log=full_path_to_log_file` option in the command line to create a verbose installation log. For example:

```
wlng_sdk300_<appropriate-platform-filename>.bin
-log=<full_path>install.log
```

4. Go on to "Respond to the Prompts" on page 4-2

Respond to the Prompts

The installation program prompts you to enter specific information about your system and configuration. For instructions on responding to the prompts during installation, see the following table.

In this window...	Perform the following action...
Welcome	Click **Next** to proceed with the installation. You may cancel the installation at any time by clicking **Exit**.
BEA License Agreement	Read the BEA Software License Agreement and indicate your acceptance of the terms of the agreement by selecting **Yes**. To continue with the installation, you must accept the terms of the license agreement and then click **Next**.
Choose BEA Home Directory	Specify the BEA Home directory that will serve as the central support directory for all BEA products installed on the target system. If you already have a BEA Home directory on your system, you can select that directory (recommended) or create a new BEA Home directory. If you choose to create a new directory by typing a new directory name in the BEA Home Directory field, the installation program automatically creates one for you. You can also click **Browse** and select a directory from the **BEA Home Directory Selection** window.
Choose Product Installation Directory	Specify the directory in which you want to install the Network Gatekeeper software. This is the directory from which information will be copied during the domain configuration phase. Once you have chosen your directory, click **Next**. You can accept the default product directory (sdk300) or create a new product directory.
Choose Shortcut Location This window is displayed only under the following conditions: • You have Administrator privileges. • You are performing an initial installation. • You are installing on a Windows platform.	Specify the Start menu folder in which you want the Start menu shortcuts created. You can select from the following options: • **All Users Start menu folder** Selecting this option provides all users registered on the machine with access to the installed software. However, only users with Administrator privileges can create shortcuts in the All Users folder. Therefore, if a user without Administrator privileges uses the Configuration Wizard to create domains, Start menu shortcuts to the domains are not created. In this case, users can manually create shortcuts in their local Start menu folders, if desired. Press ALT+Y on the keyboard to select the All Users Start Menu. • **Local user's Start menu folder** Selecting this option ensures that other users registered on this machine will not have access to the Start menu entries for this installation. Press ALT+N on the keyboard to select the Local User's start menu.

In this window...	Perform the following action...
Status	Read the information displayed about BEA products and services. When the installation program has finished copying the specified files to your system, click **Next**.
Installation Complete	Specify whether you want to run the QuickStart application. QuickStart, designed to assist first-time users in evaluating, learning, and using the software, provides quick access to domain configuration wizard. Clear the check box for this option if you do not want to launch QuickStart. Unless you wish to make changes to the standard sample domain, a separate domain configuration is not necessary.

Note: When you install and configure WebLogic Network Gatekeeper SDK, a temporary 90 day evaluation license is generated for you automatically. You are responsible for acquiring a permanent license for your installation. Contact your Local BEA Sales Representative or Order Management Representative and they will assist you in acquiring the appropriate license.

Setting up WS-Policy

One of the first things you must do in setting up Network Gatekeeper SDK is to establish Web Services security. Web Services security controls Network Gatekeeper Simulator's interactions with Application Service Providers

Web Services Security

Web Services Security provides end-to-end message-level security for web services through an implementation of the WS-Security standard. WS-Security defines a mechanism for adding three levels of security to SOAP messages:

- Authentication tokens. WS-Security authentication tokens lets an application provide a user name and password or X509 certificate for the purpose of authentication headers.
- XML encryption. WS-Security's use of W3C's XML encryption standard enables the XML body or portion of it to be encrypted to ensure message confidentiality.
- XML digital signatures. WS-Security's use of W3C's XML digital signatures lets the message be digitally signed to ensure message integrity. The signature is based on the content of the message itself (by applying a hash function and public key), so if the message is altered en route, the signature becomes invalid.

Network Gatekeeper uses WebLogic Server mechanisms for Web Services security- see:

- *Programming Web Services for WebLogic Server*, http://e-docs.bea.com/wls/docs92/webserv/security.html
- *Understanding WebLogic Security*, http://edocs.beasys.com/wls/docs92/secintro/concepts.html
- *Web Services Security specifications,* http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Message level security for SOAP messages is achieved by applying WS-Security and WS-Security policy standards. Authentication is handled transparently by WS-Security and subsequently by the configured authentication providers and login modules of the WebLogic Security framework. WS-Security also supports signing and encrypting a message by providing a security token hierarchy associated with the keys used for signing and encryption (for message integrity and confidentiality).

The following steps outline the general WebLogic security configurations that have to be performed, either automatically using a script or manually from the Administration Console.

- Configure Policies for WS-Security as described below.
- If using SAML tokens, configure WebLogic SAML Identity Assertion Provider which authenticates users based on SAML assertions and SAML credential mapping provider. A SAML Identity Assertion Provider is required only if you are using SAML assertions.

Configuration workflow: Policies for WS-Security

This section outlines how to apply an existing WS-Policy and where to find more information about creating and using custom WS-Policies.

Apply a WS-Policy to a Web Service: Quick start

This section outlines how to apply a WSSE policy to a Web Service endpoint in the Network Gatekeeper Simulator.

Standard WebLogic Server mechanisms are used - see http://e-docs.bea.com/wls/docs92/ConsoleHelp/taskhelp/webservices/ConfigureWSPolicyFile.html for a full description.

The Network Gatekeeper Simulator must be started, see Start the Network Gatekeeper Simulator.

Starting in WebLogic Console:

1. In the **Domain Structure** pane, select **Deployments**.
2. In **Summary of Deployments** page, expand **simulator**.
3. Click on a Web Service to apply Web Services security to, for example **SendSmsService**. All Web Services are named according to the interface they implement.

   This shows the page **Settings for <Web Service>**
4. Click the **Configuration** tab.
5. Click **WS-Policy** sub-tab.
6. Click **Service endpoint <Web Service>**.
7. Choose which security policy to apply for the endpoint:
   a. Select the appropriate WS-Policy file in **Available Endpoint Policies**, see "Available default WS-Policies" on page 4-7.
   b. Move it to the list in **Chosen Endpoint Policies** by clicking on the arrow button.
   c. When the WS-Policy files have been chosen, click **OK**.
8. In the **Save Deployment Plan Assistant** you choose where to store the deployment plan.
9. Apply the changes.

Note: Applying a security policy to a Web Service establishes, by default, both inbound and outbound security policies. Because there is no way for Network Gatekeeper Simulator to know what security policies may be required by a client to which it is returning a notification, outbound security must be turned off. If you wish to secure the link by which Network Gatekeeper Simulator returns notifications, you should use SSL.

To turn off outbound security associated with a particular WS-Policy file, you must edit the plan.xml file that is created when you attach Policy to a Web Service, as in step 8 above. Make sure the <value> element is set to `inbound` as in the following stanza:

Listing 4-1 Plan.xml snippet to be edited

```
<variable>
      <name>WsPolicy_policy:Auth.xml_Direction_11745107731400</name>
      <value>inbound</value>
</variable>
```

Create and use custom a custom WS-Policy

Section *Creating and Using a Custom WS-Policy File* in http://e-docs.bea.com/wls/docs92/webserv/security.html describes how to create and use a custom WS-Policy file. Also see http://e-docs.bea.com/wls/docs92/ConsoleHelp/taskhelp/webservices/ConfigureWSPolicyFile.html.

Available default WS-Policies

WS-Policy files can be used to require applications clients to authenticate, digitally encrypt, or digitally sign SOAP messages. Out-of-the-box Network Gatekeeper supplies files to do those three things, respectively: auth.xml, encrypt.xml, and sign.xml. If the built-in WS-Policy files do not meet your security needs, you can build custom policies.

WS-Policy assertions are used to specify a Web Services' requirements for digital signatures and encryption, along with the security algorithms and authentication mechanisms that it requires, for example Policy for SAML.

See http://e-docs.bea.com/wls/docs92/webserv/security.htm for a description.