



# BEA WebLogic Network Gatekeeper™

## Application Test Environment User's Guide

# Copyright

Copyright © 2005 BEA Systems, Inc. All Rights Reserved.

## Restricted Rights Legend

This software and documentation is subject to and made available only pursuant to the terms of the BEA Systems License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the software except as specifically allowed in the agreement. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from BEA Systems, Inc.

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the BEA Systems License Agreement and in subparagraph (c)(1) of the Commercial Computer Software-Restricted Rights Clause at FAR 52.227-19; subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, subparagraph (d) of the Commercial Computer Software--Licensing clause at NASA FAR supplement 16-52.227-86; or their equivalent.

Information in this document is subject to change without notice and does not represent a commitment on the part of BEA Systems. THE SOFTWARE AND DOCUMENTATION ARE 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 SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

## Trademarks or Service Marks

BEA, Jolt, Tuxedo, and WebLogic are registered trademarks of BEA Systems, Inc. BEA Builder, BEA Campaign Manager for WebLogic, BEA eLink, BEA Liquid Data for WebLogic, BEA Manager, BEA WebLogic Commerce Server, BEA WebLogic Enterprise, BEA WebLogic Enterprise Platform, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic Personalization Server, BEA WebLogic Platform, BEA WebLogic Portal, BEA WebLogic Server, BEA WebLogic Workshop and How Business Becomes E-Business are trademarks of BEA Systems, Inc.

All other trademarks are the property of their respective companies.

# Contents

## 1. Introduction and Roadmap

Document Scope and Audience . . . . .	1-2
Guide to this Document . . . . .	1-2
Terminology . . . . .	1-3
Related Documentation . . . . .	1-3
Network Gatekeeper Application Test Environment documentation . . . . .	1-3
Other Documentation . . . . .	1-4

## 2. Introduction to Network Gatekeeper Application Test Environment

Capabilities of Network Gatekeeper Application Test Environment . . . . .	2-2
Network triggered events . . . . .	2-2
Application triggered requests . . . . .	2-2
Simulation . . . . .	2-3
Supported message types . . . . .	2-3
Starting Network Gatekeeper Application Test Environment . . . . .	2-3
Network Gatekeeper Application Test Environment Description . . . . .	2-3
Network Gatekeeper Application Test Environment GUI . . . . .	2-5
Network Gatekeeper Management Tool GUI . . . . .	2-6
Network Gatekeeper Application Test Environment SLEE . . . . .	2-6
Supported functions in Network Gatekeeper Application Test Environment GUI . . . . .	2-7
Utilities . . . . .	2-7

Phones . . . . .	2-7
Map . . . . .	2-8
Test flow . . . . .	2-8
Resources to use by the application developer . . . . .	2-10

### 3. Network Gatekeeper Management Tool

About the Network Gatekeeper Management Tool . . . . .	3-2
Graphical Network Gatekeeper Management Tool interface . . . . .	3-2
Main window . . . . .	3-2
File menu . . . . .	3-4
Actions menu . . . . .	3-4
Applications menu . . . . .	3-4
Scripts menu . . . . .	3-5
Help menu . . . . .	3-5
Network Gatekeeper Management Tool window . . . . .	3-6
SLEE pane . . . . .	3-6
Services pane . . . . .	3-6
Messages pane . . . . .	3-7
Invoke method window . . . . .	3-7
Starting a Network Gatekeeper Management Tool and adding a SLEE . . . . .	3-7
Working with the Network Gatekeeper Management Tool . . . . .	3-9

### 4. Using the Network Gatekeeper Application Test Environment GUI

Open the Network Gatekeeper Application Test Environment GUI . . . . .	4-2
Add a new map . . . . .	4-2
Open a map . . . . .	4-3
Add a mobile phone . . . . .	4-3

Remove a mobile phone . . . . .	4-3
Set the location of a mobile phone . . . . .	4-3
Send an MMS . . . . .	4-4
Open an MMS . . . . .	4-4
Send an SMS . . . . .	4-5
Open an SMS . . . . .	4-5

## 5. Using Network Gatekeeper Application Test Environment SLEE services

Open the Network Gatekeeper Application Test Environment GUI . . . . .	5-1
Close the Network Gatekeeper Application Test Environment GUI . . . . .	5-2
Empty a mailbox . . . . .	5-2
List mailboxes . . . . .	5-2
Add a mobile phone . . . . .	5-2
Remove a mobile phone . . . . .	5-3
Set the location of a mobile phone . . . . .	5-3
Get the location of a mobile phone . . . . .	5-4
Send an SMS . . . . .	5-4
Send an MMS . . . . .	5-5

## 6. System Upgrade

About license validity . . . . .	6-2
About system upgrade . . . . .	6-2

## 7. Installation and Configuration

Installation . . . . .	7-2
Software installation . . . . .	7-2
Java SDK installation . . . . .	7-2
Setting Java environment variables . . . . .	7-2

..... Database installation	7-3
Network Gatekeeper Application Test Environment installation.....	7-3
Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.4.2 installation.....	7-4
Start Network Gatekeeper Application Test Environment process.....	7-5
Starting a Network Gatekeeper Management Tool and creating initial users.....	7-5
Configuring notification end-points for Parlay X Web Services applications.....	7-8
Enable incoming message notification for Parlay X SMS and MMS.....	7-8
List incoming message notification for Parlay X SMS and MMS.....	7-10
Getting details about a notification listener.....	7-10
Disable incoming message notification for Parlay X SMS and MMS.....	7-10
Configuring database disk space alarm levels.....	7-11
Configuring alarm list filtering level.....	7-12
Configuring event log filtering level.....	7-12
Configuring trace buffer size and maximum trace log file size.....	7-13
Installing the documentation on intranet or file server.....	7-14
Alarms.....	7-14
Severity.....	7-14
Description.....	7-15
What to do.....	7-15
Severity.....	7-15
Description.....	7-15
What to do.....	7-15
Severity.....	7-15
Description.....	7-16
What to do.....	7-16
Troubleshooting the installation.....	7-16
Database access denied.....	7-16

SLEE start-up failure ..... 7-16

## A. Directory Structure and Contents

Structure ..... A-2

Contents ..... A-2

## B. References





# Introduction and Roadmap

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

- [“Document Scope and Audience”](#) on page 1-2
- [“Guide to this Document”](#) on page 1-2
- [“Terminology”](#) on page 1-3
- [“Related Documentation”](#) on page 1-3

## Document Scope and Audience

The purpose of this guide is to describe the operation and maintenance related to a single Windows 2000/XP BEA Network Gatekeeper Application Test Environment installation, including the following:

- information on the functions
- start up and configuration
- operation

Intended audience is developers and test engineers working with BEA Network Gatekeeper Application Test Environment and BEA WebLogic Network Gatekeeper.

## Guide to this Document

This guide contains the following chapters:

- [Chapter 1, “Introduction and Roadmap”](#) describes the structure and contents of this document, the used writing conventions, and related documentation.
- [Chapter 2, “Introduction to Network Gatekeeper Application Test Environment”](#) gives an overview of the main areas in BEA Network Gatekeeper Application Test Environment capabilities, architecture and scenarios of usage.
- [Chapter 3, “Network Gatekeeper Management Tool”](#) describes WebLogic Network Gatekeeper management application, the WebLogic Network Gatekeeper Management Tool used for some of the Network Gatekeeper Application Test Environment OAM tasks.
- [Chapter 4, “Using the Network Gatekeeper Application Test Environment GUI”](#) describes the operations possible to perform in the Network Gatekeeper Application Test Environment GUI
- [Chapter 5, “Using Network Gatekeeper Application Test Environment SLEE services”](#) describes the operations possible to perform in the Network Gatekeeper Application Test Environment SLEE services.
- [Chapter 6, “System Upgrade”](#) describes how system upgrades and patches are handled.
- [Chapter 7, “Installation and Configuration”](#) describes how to install the software and start up Network Gatekeeper Application Test Environment. It also tell you how to perform the configuration needed before Network Gatekeeper Application Test Environment can be taken into use.

- [Appendix A, “Directory Structure and Contents”](#) describes the directory structure created when installing Network Gatekeeper Application Test Environment.

## Terminology

The following terms and acronyms are used this document:

API —Application Programming Interface

ATE —Application Test Environment

ESPA —High level web services APIs

IP —Internet Protocol

MMS —Multimedia Message Service

NS —Name Service

ORB —Object Request Broker

SLEE —Service Logic Execution Environment

SLEE Service —A software module that is designed to execute in the SLEE.

SMIL —Synchronized Multimedia Integration Language

SMS —Short Message Service

URL —Universal Resource Locator

WESPA —Web Services ESPA. Web Services interface to ESPA.

## Related Documentation

### Network Gatekeeper Application Test Environment documentation

This user’s guide is a part of the Network Gatekeeper Application Test Environment documentation set. The following documents contain other types of product information:

- *Application Developer’s Guide - Parlay X for WebLogic Network Gatekeeper*

The application developer’s guides describe how to design and implement WebLogic Network Gatekeeper applications.

-

The API descriptions describe the APIs available for developers and applications.

## Other Documentation

The third party documentation needed to operate and maintain Network Gatekeeper Application Test Environment is listed in the Chapter [“References”](#) on page B-1.

# Introduction to Network Gatekeeper Application Test Environment

BEA Network Gatekeeper Application Test Environment is an interactive, graphical test environment where applications to be integrated through WebLogic Network Gatekeeper, can be tested. The current version of the Network Gatekeeper Application Test Environment supports generic messaging and user location for the Extended Web Services APIs and Parlay X.

It supports applications of the following types:

- WebLogic Network Gatekeeper Extended Web Services
- Parlay X Web Services

Network Gatekeeper Application Test Environment is used for functional tests. It simulates an WebLogic Network Gatekeeper. By using Network Gatekeeper Application Test Environment, there is no need for a WebLogic Network Gatekeeper when developing and performing functional tests of applications.

The following sections provide an overview of the Application Test Environment:

- [“Capabilities of Network Gatekeeper Application Test Environment” on page 2-2](#)
- [“Starting Network Gatekeeper Application Test Environment” on page 2-3](#)
- [“Network Gatekeeper Application Test Environment Description” on page 2-3](#)
- [“Supported functions in Network Gatekeeper Application Test Environment GUI” on page 2-7](#)
- [“Test flow” on page 2-8](#)

- “Resources to use by the application developer” on page 2-10

## Capabilities of Network Gatekeeper Application Test Environment

Network Gatekeeper Application Test Environment offers the following capabilities:

- Network Gatekeeper Application Test Environment gives support for the following APIs:
  - Access
  - Parlay X SMS
  - Parlay X Multimedia Messaging
  - Parlay X Terminal Location
  - Web Services ESPA Messaging, including MMS
  - Web Services ESPA User Location
- It supports the charging, alarms, and events functions in WebLogic Network Gatekeeper.
- Simulation of network related events, such as messages sent from the network to applications
- Simulation of network response to application triggered requests, such as messages sent from the application to a mobile phone in the network
- It also supports administration in a similar manner as for the WebLogic Network Gatekeeper

### Network triggered events

Network triggered events, such as messages sent from a mobile phone can be simulated, either using Management Tool or the Network Gatekeeper Application Test Environment GUI.

The following events are supported:

- Receive SMSes
- Receive MMSes

### Application triggered requests

- All ESPA request functionality is supported from the application to ESPA.

- All ESPA call back functionality is supported from ESPA to the application.

## Simulation

The following simulation is supported:

- Adding and deleting mobile phones
- Setting the geographical position of a mobile phone
- Send and receive SMSes and MMSes

## Supported message types

SMS and MMS.

The following MMS message types are supported:

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

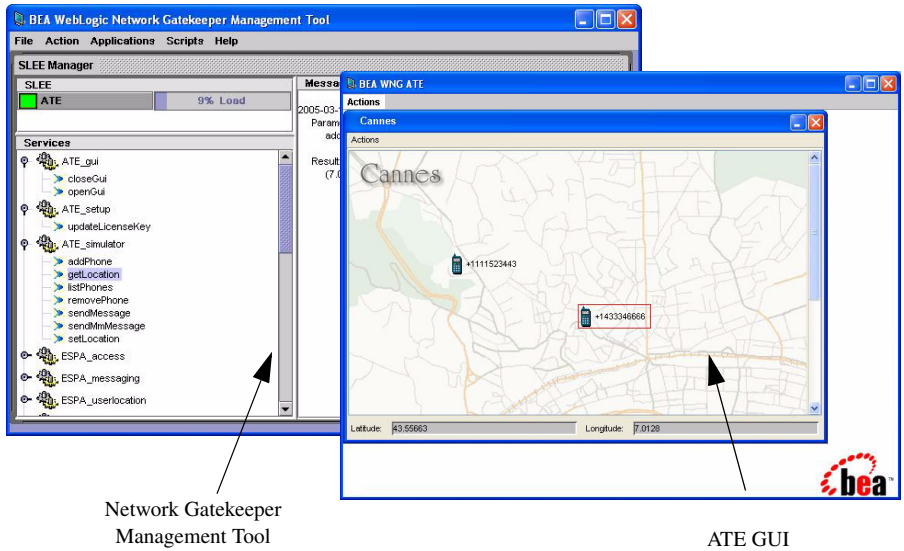
## Starting Network Gatekeeper Application Test Environment

See [“Start Network Gatekeeper Application Test Environment process”](#) on page 7-5.

## Network Gatekeeper Application Test Environment Description

The Network Gatekeeper Application Test Environment is built up of three main parts, the Network Gatekeeper Application Test Environment GUI, the Network Gatekeeper Application Test Environment SLEE, and the Management Tool.

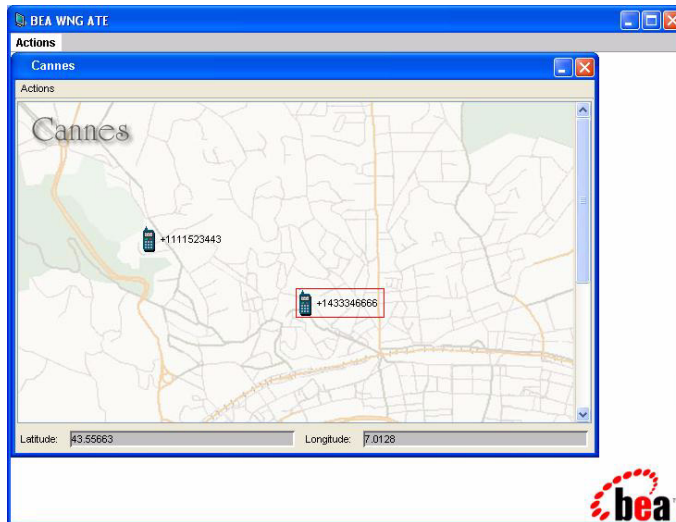
# Introduction to Network Gatekeeper Application Test Environment



**Figure 2-1 Network Gatekeeper Management Tool and Application Test Environment GUI**

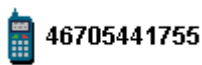


## Network Gatekeeper Application Test Environment GUI



**Figure 2-2 Network Gatekeeper Application Test Environment GUI**

The Network Gatekeeper Application Test Environment interface is based on a GUI where a map is displayed. The map can be changed to fit different locations. Through the GUI it is possible to add mobile telephony terminals. These terminals are given a subscription number. When the terminal has been defined, it can be moved to different locations on the map.



**Figure 2-3 Telephone symbol**

It is possible to send and receive messages through the terminals in the GUI. When a message has arrived to the telephone, an envelope is displayed beside the telephone. This message can be viewed.

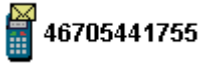


Figure 2-4 New message has arrived

## Network Gatekeeper Management Tool GUI

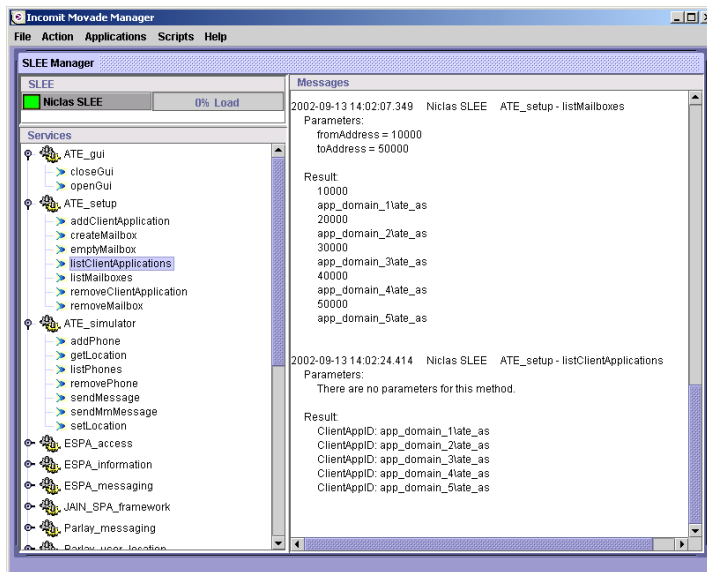


Figure 2-5 Network Gatekeeper Management Tool GUI

In addition to the Network Gatekeeper Application Test Environment GUI, three SLEE services; **ATE\_GUI**, **ATE\_setup**, and **ATE\_simulator** are included in the Network Gatekeeper Management Tool part of the Network Gatekeeper Application Test Environment. For information on general operation of Network Gatekeeper Management Tool, see [Chapter 3, “Network Gatekeeper Management Tool”](#).

## Network Gatekeeper Application Test Environment SLEE

The Network Gatekeeper Application Test Environment SLEE is a Service Logic Execution Environment that executes all the services offered by the Network Gatekeeper Application Test

Environment. It is a server process, and all OAM is performed using the Network Gatekeeper Management Tool.

## Supported functions in Network Gatekeeper Application Test Environment GUI

### Utilities

The utility in the Network Gatekeeper Application Test Environment GUI supports the following functions

- Save a configuration, that is the map including coordinates of the map, to file.
- Load a configuration from file.

### Phones

The phones in the Network Gatekeeper Application Test Environment GUI can

- show the ID of the phone.
- indicate when messages have arrived.
- be moved using click and drag functions.
- receive and display SMS:es.
- receive and display MMS:es 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.
- Send SMS:es.
- send MMS:es 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.

## Map

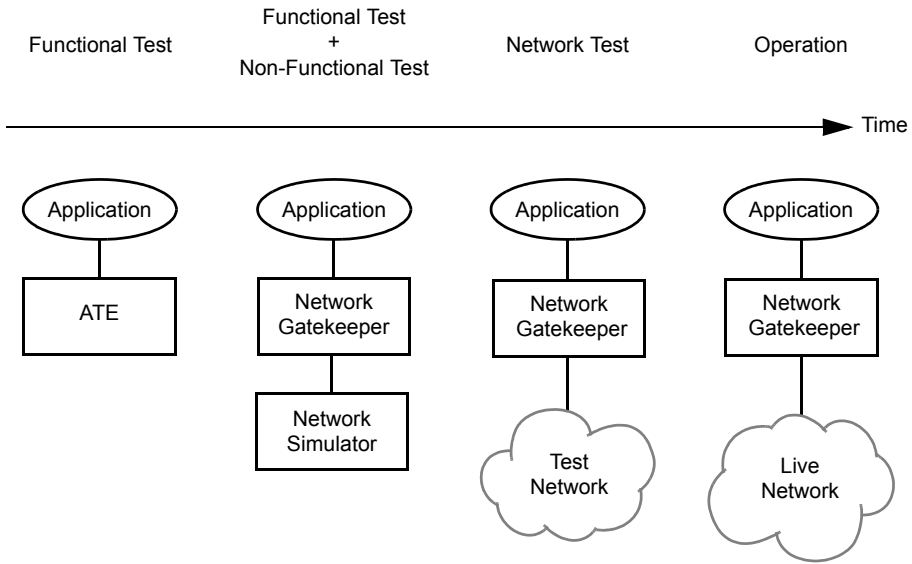
The map in the Network Gatekeeper Application Test Environment GUI supports the following:

- 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.

Several maps can be displayed simultaneously.

## Test flow

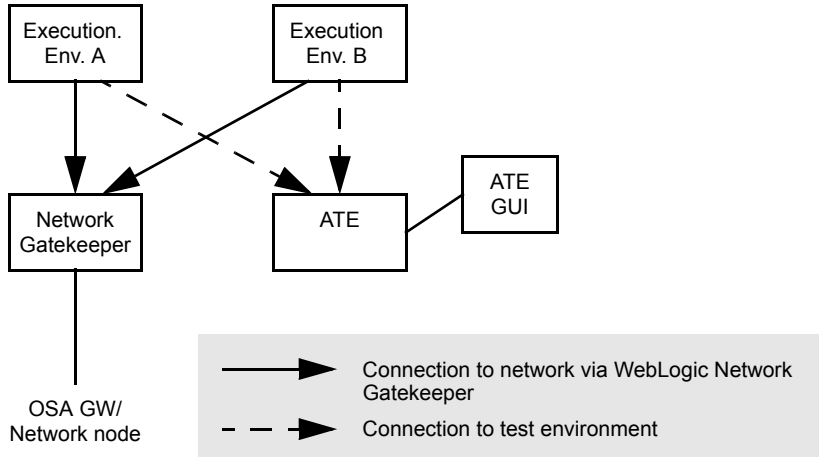
[Figure 2-6, “Application test flow,” on page 2-9](#) shows the complete WebLogic Network Gatekeeper application test flow, from the application developers’ functional test to deployment in a live network. An application developer can perform functional tests using Network Gatekeeper Application Test Environment. The other tests in the flow are performed in cooperation between the application provider and the service provider.



**Figure 2-6 Application test flow**

When an application shall be tested using the Network Gatekeeper Application Test Environment, the application is connected to Network Gatekeeper Application Test Environment, which emulates the WebLogic Network Gatekeeper. Before testing in a test telephony network, a network simulator can be used.

An overview of the relation between Network Gatekeeper Application Test Environment and WebLogic Network Gatekeeper is shown in [Figure 2-7, “Network Gatekeeper Application Test Environment in relation to the WebLogic Network Gatekeeper,”](#) on page 2-10.



**Figure 2-7 Network Gatekeeper Application Test Environment in relation to the WebLogic Network Gatekeeper**

For a applications based on Web Services, the applications uses the endpoints provided by Network Gatekeeper Application Test Environment during test. After successful verification, the application uses endpoints provided by the WebLogic Network Gatekeeper.

## Resources to use by the application developer

Network Gatekeeper Application Test Environment offers the following resources, which are configured during installation

Service Provider: default\_provider

Resource	Number	Name(s)/ID(s)
Application instance Groups	5 (one for each application account)	User name: domain_user Password: domain_user
Application account	5	app_domain_1 app_domain_2

Resources to use by the application developer

<b>Resource</b>	<b>Number</b>	<b>Name(s)/ID(s)</b>
		app_domain_3
		app_domain_4
		app_domain_5
Mailbox	5	For app_domain_1: 10000
		For app_domain_2: 20000
		For app_domain_3: 30000
		For app_domain_4: 40000
		For app_domain_5: 50000

## Introduction to Network Gatekeeper Application Test Environment



# Network Gatekeeper Management Tool

The following sections describe the Network Gatekeeper Management Tool:

- “About the Network Gatekeeper Management Tool” on page 3-2
- “Graphical Network Gatekeeper Management Tool interface” on page 3-2
- “Main window” on page 3-2
- “Network Gatekeeper Management Tool window” on page 3-6
- “Invoke method window” on page 3-7
- “Starting a Network Gatekeeper Management Tool and adding a SLEE” on page 3-7
- “Working with the Network Gatekeeper Management Tool” on page 3-9

## About the Network Gatekeeper Management Tool

The SLEEs and the SLEE services are managed through the Network Gatekeeper Management Tool. It provides a graphical and a text based interface, and connects to one or more SLEEs.

Both the graphical and the text based Network Gatekeeper Management Tool can access the SLEEs through a CORBA connection and support execution of OAM batch files. The text based manager may also be used through a remote connection as telnet.

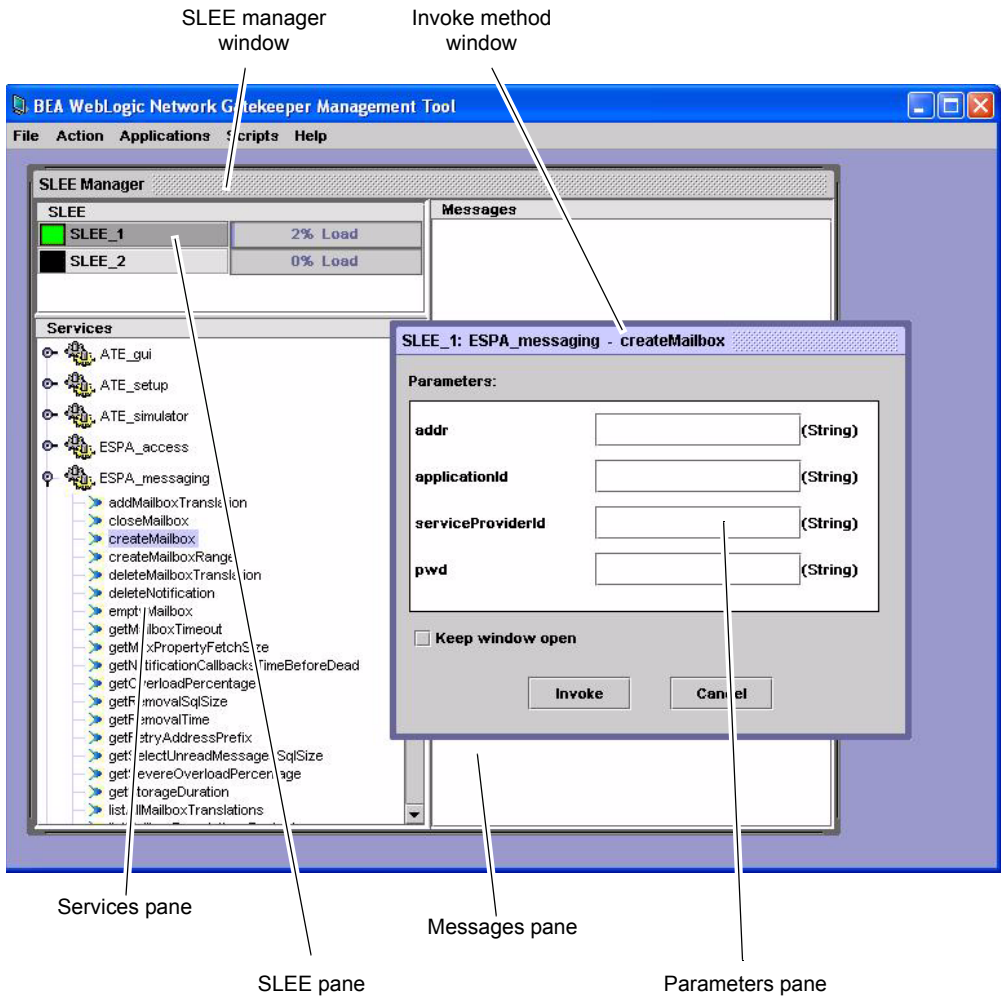
## Graphical Network Gatekeeper Management Tool interface

All installed SLEE services are displayed in the Network Gatekeeper Management Tool. When selecting one of the SLEE services, the administrative methods available for that service are displayed. Depending on the logged in user's authority level, different types of methods are displayed. A user has one of the following authority levels:

- Read only user
- Standard read and write user
- Administrator user

## Main window

All management can be performed through the Network Gatekeeper Management Tool's main window. The window and its components are shown in [Figure 3-1, "Network Gatekeeper Management Tool Main window,"](#) on page 3-3.



**Figure 3-1 Network Gatekeeper Management Tool Main window**

From the menu bar in the Main window you can initiate a number of actions related to the Network Gatekeeper Management Tool itself and to connecting and disconnecting SLEEs to the Management Tool.



Figure 3-2 Network Gatekeeper Management Tool menu bar

## File menu

File - Auto saving configurations

If the check box is selected, the SLEEs you have added to the SLEE manager window and the installed management plug-ins will automatically appear in the Network Gatekeeper Management Tool the next time you log on.

File - Exit

Exits and logs off the Network Gatekeeper Management Tool.

## Actions menu

Actions - Add SLEE...

Opens a dialog box where you can add a SLEE to the SLEEs pane.

Actions - Remove SLEE...

Opens a dialog box where you can remove a SLEE from the SLEEs pane.

Actions - Reload SLEE...

Opens a dialog box where you can reload a SLEE's services and methods.

Actions - Add as alarm listener

Adds the SLEE Management Tool as an alarm listener for the SLEEs in the SLEE pane. The alarms are displayed in the Messages pane.

Actions - Set alarm severity...

Opens a dialog box where you can set the lowest severity of the alarms to be displayed.

## Applications menu

Applications - SLEE manager - View SLEE manager

Clear the check box if you do not want to view the SLEE manager window.

Applications - SLEE manager - Login...

Opens a dialog box where you can log on to the Network Gatekeeper Management Tool.

Applications - SLEE manager - Logout

Logs off a user without exiting the Network Gatekeeper Management Tool.

Applications - Plug-in - Add plug-in...

Opens a dialog box where you can add a management plug-in. Added plug-ins appear in the menu.

Applications - Plug-in - Remove plug-in...

Opens a dialog box where you can remove a management plug-in.

## Scripts menu

Scripts - Run script...

Opens a dialog box where you can select and run an OAM batch file. The file could be a recorded OAM session or written from scratch. The result is presented in a separate window in the Network Gatekeeper Management Tool.

Scripts - Recording a test case - Set file name...

Opens a dialog box where you can specify a file name for file where the recorded OAM session will stored.

Scripts - Recording a test case - Start recording

Starts recording the OAM activities performed through the Network Gatekeeper Management Tool. The output file can be run as an OAM batch file.

Scripts - Recording a test case - Stop recording

Stops recording the OAM activities performed through the Network Gatekeeper Management Tool.

## Help menu

Help - User's Guide...

Opens a user's guide describing the Network Gatekeeper Management Tool and the tasks you can perform with it.

Help - About...

Opens the About dialog box.

## Network Gatekeeper Management Tool window






### SLEE pane

This pane contains a list displaying the status, name and load of the SLEEs connected to the Network Gatekeeper Management Tool. Clicking on a SLEE displays the SLEE’s services in the Services pane.

Right-clicking on a SLEE in the list displays a menu where the SLEE’s process can be started or stopped, and the SLEE’s state can be changed.

A SLEE’s status is indicated by an icon, see Table 3-1 on page 6.

**Table 3-1 SLEE status icons**

Icon	SLEE Status
	SLEE state <b>Running</b>
	SLEE state <b>Shutdown</b>
	The SLEE process is not responding
	The SLEE process and the SLEE agent process are not responding
	The SLEE user is not logged in

### Services pane

When a SLEE is selected in the SLEEs pane, this pane contains a list of all the SLEE’s services. Double-clicking on a service displays all administrative methods related to the service.

Double-clicking on a method displays the method and its parameters in the invoke method window.

Right-clicking on a method displays a menu where you can select Help to display a short help text in the Messages pane. The help text describes the purpose of the method and the parameters used by the method.

## Messages pane

This pane displays the results of method invocations and the alarms raised from the SLEE. Also, the Messages pane is used for displaying the method help texts.

## Invoke method window

All methods are invoked from the invoke method window. For the methods that uses parameters, the parameter values are set in this window before the method is invoked.

## Starting a Network Gatekeeper Management Tool and adding a SLEE

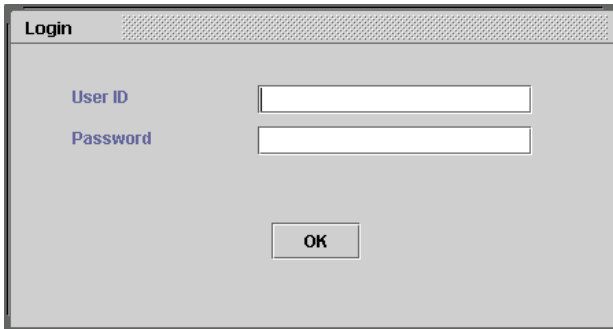
The following instructions tells you how to start a Network Gatekeeper Management Tool and connect it to a SLEE.

Starting the Network Gatekeeper Management Tool

1. Start the Network Gatekeeper Management Tool. Open the **Start** menu and select **Programs - BEA WebLogic Network Gatekeeper 1.0 - Management Tool**.

You can also start the Network Gatekeeper Management Tool by double-clicking on the `runSleeManager.bat` file in the installation directory. But, if you start the Network Gatekeeper Management Tool through the `runSleeManager.bat` file you will have to add the SLEEs to the Network Gatekeeper Management Tool every time you log in. If you start through the start menu, the SLEEs you have added will automatically be displayed at log in.

This displays the Network Gatekeeper Management Tool's **Login** window.



2. In the **User ID** field, enter your user ID.
3. In the **Password** field, enter your password.
4. Click **OK**.

You are now logged on to the Network Gatekeeper Management Tool. The SLEEs connected to the SLEE manger are displayed in the **SLEEs** pane. If there are no SLEE in the SLEEs pane or if you want to add more SLEEs to the manager, continue with Step 5. below.

#### Adding a SLEE to the Network Gatekeeper Management Tool

5. In the **SLEEs** pane, right-click on the background and select **Add SLEE...** from menu, or open the **Actions** menu and select **Add SLEE...**

This displays the **Add SLEE** dialog box.

6. Enter data according to the table below:

<b>Parameter</b>	<b>Description</b>
SLEE Name	The SLEE name you want to appear in the SLEE pane.
User ID	Your SLEE user ID.
Password	Your SLEE password.

7. Select if the SLEE connection shall be made using IP address and port numbers, or name service references files.



**Note:** If bi-directional CORBA is used on the Network Gatekeeper Application Test Environment the SLEE belongs to, the connection has to be made using name service reference files.

8. Enter IP address and port number, *or* name service references file data according to the table below:

Parameter	Description
IP Address	The SLEE host's IP address.
NS Port	The SLEE name service's port number. Default is 10007.
Agent Port	The SLEE agent's port number. Default is 6214.
SLEE reference file	The path to the SLEE's name service reference file.
Agent reference file	The path to the SLEE agent's name service reference file.

9. Click **OK**.

This displays the SLEE in the **SLEEs** pane.

## Working with the Network Gatekeeper Management Tool

The following instruction describes a general workflow on how to work with SLEE Services.

1. Start a Network Gatekeeper Management Tool, see [“Starting a Network Gatekeeper Management Tool and adding a SLEE” on page 3-7](#).
2. Select the SLEE you want to work with. Click on the desired SLEE in the **SLEEs** pane.

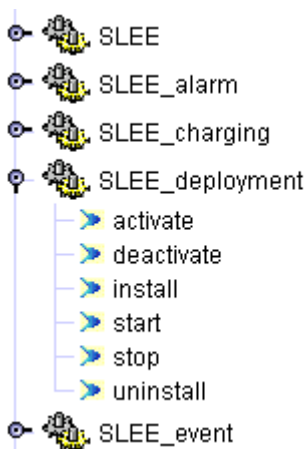
This displays all services available in the SLEE in the **Services** pane.



If the SLEE you want to work with is not displayed in the SLEEs pane, right-click in the background of the SLEEs pane and select **Add SLEE...** in the displayed menu.

3. Select the service you want to work with. Double-click on the desired service in the **Services** pane.

This displays all administrative methods related to the service below the service.



If you want a short description of what the method does, right-click on the method and select **Help** in the menu.

4. Display the parameters related to the method. Double-click on the method.

This opens the **Invoke Method** window and displays the method's parameters in it.

5. Enter the parameters values, if any, in the input fields and click **Invoke**.

The result of the invocation is displayed in the **Messages** pane.

## Network Gatekeeper Management Tool

# Using the Network Gatekeeper Application Test Environment GUI

The following sections describe how to use the GUI for the Network Gatekeeper Application Test Environment:

- [“Open the Network Gatekeeper Application Test Environment GUI” on page 4-2](#)
- [“Add a new map” on page 4-2](#)
- [“Open a map” on page 4-3](#)
- [“Add a mobile phone” on page 4-3](#)
- [“Remove a mobile phone” on page 4-3](#)
- [“Set the location of a mobile phone” on page 4-3](#)
- [“Send an MMS” on page 4-4](#)
- [“Open an MMS” on page 4-4](#)
- [“Send an SMS” on page 4-5](#)
- [“Open an SMS” on page 4-5](#)

## Open the Network Gatekeeper Application Test Environment GUI

See “Open the Network Gatekeeper Application Test Environment GUI” on page 5-1.

### Add a new map

Starting in the ATE GUI 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**.
7. Now the map and its’ meta information is stored under the name **<Map name>.map** in the directory **<ATE installation path>\bin\maps**. This file can be transferred to any other Network Gatekeeper Application Test Environment.

## Open a map

Starting in the ATEG UI 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 ATE GUI. Repeat this procedure for every map you want to display.

## Add a mobile phone

Starting in the <Map name> window:

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

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

2. In the **Phone number** field, enter the phone number of the telephone.

3. Click **OK**.

A telephone symbol and the telephone number associated with it is displayed on the map.

## Remove a mobile phone

Starting in the <Map name> window:

1. Right click on the telephone to be removed.

A menu is displayed.

2. From the menu, choose **Remove**.

The telephone is removed.

## Set the location of a mobile phone

Starting in the <Map name> window:

1. Click and hold down the left mouse button on the telephone.
2. Move the telephone on the map.  
The coordinates of it is displayed as the telephone is moved.

## Send an MMS

Starting in the <Map name> window:

1. Right click on the telephone to send the MMS from.  
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 mailbox to send the MMS to.
4. Click **Add content**.  
In the **Message** group, a row is opened for editing.
5. In the **Type** column, choose type of content from the selection list.
6. In the URL column, enter the URL to the content of the message, or choose a file located on the file system by clicking **Browse** and selecting a file.
7. Repeat Step 4. to Step 6. for each part of the MMS.
8. If a part of the content is to be removed, select the row containing the part and click **Remove content**.
9. Click **Send**.  
The MMS is sent.

## Open an MMS

When an MMS has arrived to a phone it is indicated by a letter symbol beside the telephone. Follow the instructions below to open an MMS.

Starting in the <Map name> window:

1. Right click on the telephone that has a new, unread, MMS in its INBOX.  
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

Starting in the <Map name> window:

1. Right click on the telephone to send the SMS from.

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 mailbox 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

When an SMS has arrived to a phone it is indicated by a letter symbol beside the telephone. Follow the instructions below to open an SMS.

Starting in the <Map name> window:

1. Right click on the telephone that has a new, unread, SMS in its INBOX.

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.

## Using the Network Gatekeeper Application Test Environment GUI

# Using Network Gatekeeper Application Test Environment SLEE services

The following sections describe how to use Application Test Environment SLEE services:

- “Open the Network Gatekeeper Application Test Environment GUI” on page 5-1
- “Close the Network Gatekeeper Application Test Environment GUI” on page 5-2 “Empty a mailbox” on page 5-2
- “List mailboxes” on page 5-2
- “Add a mobile phone” on page 5-2
- “Remove a mobile phone” on page 5-3
- “Set the location of a mobile phone” on page 5-3
- “Get the location of a mobile phone” on page 5-4
- “Send an SMS” on page 5-4
- “Send an MMS” on page 5-5

## Open the Network Gatekeeper Application Test Environment GUI

Starting in the SLEE service `ATE_gui` in Network Gatekeeper Management Tool:

1. Double click `openGUI`.

The Network Gatekeeper Application Test Environment GUI is opened.

## Close the Network Gatekeeper Application Test Environment GUI

Starting in the SLEE service **ATE\_gui** in Network Gatekeeper Management Tool:

1. Double click **closeGUI**.

The Network Gatekeeper Application Test Environment GUI is closed.

## Empty a mailbox

Starting in the SLEE service **ESPA\_messaging** in Network Gatekeeper Management Tool:

1. Double click **emptyMailbox**.
2. In the **addr** field, enter the ID of the mailbox to be deleted.
3. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane.

## List mailboxes

Starting in the SLEE service **ESPA\_messaging** in Network Gatekeeper Management Tool:

1. Double click **listMailboxes**.
2. In the **fromAddress** field, enter the mailbox ID of the starting point of the range of mailboxes to be listed.
3. In the **toAddress** field, enter the mailbox ID of the end point of the range of mailboxes to be listed.
4. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane.

## Add a mobile phone

This can also be done in the Network Gatekeeper Application Test Environment GUI, see [“Add a mobile phone” on page 4-3](#).

Starting in the SLEE service **ATE\_simulator** in Network Gatekeeper Management Tool:

1. Double click **addPhone**.
2. In the **address** field, enter the ID of the phone, that is the telephone number.
3. In the **longitude** field, enter the longitude for the of the phone's initial location. 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.
4. In the **latitude** field, enter the latitude for the of the phone's initial location. North of the equator is a positive number between 0 and 90. South of the equator is a negative value between 0 and -90.
5. In the **altitude** field, enter the altitude for the of the phone's initial location. Given in metres related to the sea level.
6. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane, and the phone is displayed in the interactive graphic interface if the phone's location is within the limits of the map displayed.

## Remove a mobile phone

This can also be done in the Network Gatekeeper Application Test Environment GUI, see [“Remove a mobile phone” on page 4-3](#).

Starting in the SLEE service **ATE\_simulator** in Network Gatekeeper Management Tool:

1. Double click **removePhone**.
2. In the **address** field, enter the ID of the phone, that is the telephone number.
3. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane, and the phone is removed from the Network Gatekeeper Application Test Environment GUI.

## Set the location of a mobile phone

This can also be done in the Network Gatekeeper Application Test Environment GUI, see [“Set the location of a mobile phone” on page 4-3](#).

Starting in the SLEE service **ATE\_simulator** in Network Gatekeeper Management Tool:

1. Double click **setLocation**.
2. In the **address** field, enter the ID of the phone, that is the telephone number.
3. In the **longitude** field, enter the longitude for the of the phone's initial location. 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.
4. In the **latitude** field, enter the latitude for the of the phone's initial location. North of the equator is a positive value between 0 and 90. South of the equator is a negative value between 0 and -90.
5. In the **altitude** field, enter the altitude for the of the phone's initial location. Given in metres related to the sea level.
6. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane, and the phone is moved in the Network Gatekeeper Application Test Environment GUI. If the phone's new location is within the limits of the map displayed it will be moved on the map. If outside, it will not appear but it is still possible to perform actions on the phone from Network Gatekeeper Management Tool.

## Get the location of a mobile phone

Starting in the SLEE service **ATE\_simulator** in Network Gatekeeper Management Tool:

1. Double click **getLocation**.
2. In the **address** field, enter the ID of the phone, that is the telephone number.
3. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane.

## Send an SMS

This can also be done in the Network Gatekeeper Application Test Environment GUI, see [“Send an SMS” on page 4-5](#).

Starting in the SLEE service **ATE\_simulator** in Network Gatekeeper Management Tool:

1. Double click **sendMessage**.

2. In the **from** field, enter the ID of the phone, that is the telephone number, of the phone the message is sent from.
3. In the **to** field, enter the Parlay mailbox the message will be sent to.
4. In the **message** field, enter the message to send. Maximum 255 characters.
5. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane.

## Send an MMS

This can also be done in the Network Gatekeeper Application Test Environment GUI, see [“Send an MMS” on page 4-4](#).

Starting in the SLEE service **ATE\_simulator** in Network Gatekeeper Management Tool:

1. Double click **sendMmMessage**.
2. In the **from** field, enter the ID of the phone, that is the telephone number, of the phone the message is sent from.
3. In the **to** field, enter the ID of the Parlay mailbox to send the message to.
4. If sending a normal text message:  
In the **messageContextText** field, enter the message to send. Use a plain text.
5. If sending a message in HTML:  
In the **messageContextHTML** field, enter the message to send. Use HTML formatting.
6. If sending a message in WML:  
In the **messageContextWML** field, enter the message to send. Use WML formatting.
7. Click **Invoke**.

The result of the operation is displayed in the Network Gatekeeper Management Tool message pane.

Using Network Gatekeeper Application Test Environment SLEE services



# System Upgrade

The following sections describe upgrading the Application Test Environment:

- [“About license validity” on page 6-2](#)
- [“About system upgrade” on page 6-2](#)

## About license validity

The Network Gatekeeper Application Test Environment has a license which allows it to be used during a certain time period. An alarm is displayed in the Network Gatekeeper Management Tool when the licence is about to expire, see alarm description [“1028 License about to expire”](#) on [page 7-14](#).

If the license period expires, an alarm, see alarm description [“1029 License expired”](#) on [page 7-15](#), is displayed and the Network Gatekeeper Application Test Environment will automatically shut down.

## About system upgrade

How to upgrade your current system to a new version is dependant on the version you are upgrading to. Version specific instructions are provided when ordering the new version.

Individual SLEE services can be upgraded in run-time. To upgrade a SLEE, the SLEE has to be shutdown.

If patches to the current version are provided, instructions on how to install the patch are provided with the patch.

# Installation and Configuration

This chapter describes the installation and configuration of an Network Gatekeeper Application Test Environment. For a complete and successful installation, all sections and steps below have to be performed in the order they are presented.

Before you start the installation it is recommended that you learn the basics about the Network Gatekeeper Application Test Environment by reading [Chapter 2, “Introduction to Network Gatekeeper Application Test Environment”](#).

This chapter contains the following sections:

- “Installation” on page 7-2
- “Starting a Network Gatekeeper Management Tool and creating initial users” on page 7-5
- “Configuring notification end-points for Parlay X Web Services applications” on page 7-8
- “Configuring database disk space alarm levels” on page 7-11
- “Configuring alarm list filtering level” on page 7-12
- “Configuring event log filtering level” on page 7-12
- “Configuring trace buffer size and maximum trace log file size” on page 7-13
- “Installing the documentation on intranet or file server” on page 7-14
- “Alarms” on page 7-14
- “1028 License about to expire” on page 7-14

- [“Troubleshooting the installation” on page 7-16](#)

## Installation

### Software installation

Follow the instruction below to install Network Gatekeeper Application Test Environment:

1. Log in as **administrator** on the computer where Network Gatekeeper Application Test Environment will be installed.
2. Copy from the CD or the download directory, the file `wng10_dev.zip` to the local file system.
3. Extract the installation binaries in `wng10_dev.zip`
4. The ATE installation files are extracted to the local file system in the subdirectory `wng_ate\windows`
5. Open Windows Explorer.
6. Go to the `<Path to installation files>\wng_ate\windows` directory.
7. Double-click the file `slee_setup.bat`

The Network Gatekeeper Application Test Environment installation script is started.

### Java SDK installation

8. When the question `Do you want to install Java Development Kit?` is displayed in the window running the Network Gatekeeper Application Test Environment installation script, enter `y` to install, or `n` to skip the installation of the Java Development Kit.
9. If you selected to install the JDK, the setup wizard for it is started. Follow the instructions in the wizard.

### Setting Java environment variables

It is necessary to manually set environment variables to include the Java SDK.

10. Define the environment variable **JAVA\_HOME** to the top-level directory of the Java installation, for example `C:\jdk1.4.2_04`  
This variable is defined in the **Control Panel**. Choose **System Properties, Advanced, Environment Variables**.
  11. Define the path to the Java installation. Define this path first in the **PATH** variable. Define the path to be `%JAVA_HOME%\bin`
- Note:** The **PATH** variable must contain the fully qualified path, for example  
`C:\java\java142\bin`

## Database installation

Follow the instruction below to install MySQL:

12. When the question  
`Do you want to install MySQL?`  
is displayed in the window running the Network Gatekeeper Application Test Environment installation script., enter `y` to install, or `n` to skip the installation of MySQL.
13. If you selected to install MySQL, the setup wizard for it is started. Follow the instructions in the wizard.  
  
**Note:** Default MySQL passwords should be changed after installation. See MySQL documentation.
14. In the console window, follow the instructions and press any key to proceed the installation after the database is installed.

## Network Gatekeeper Application Test Environment installation

Follow the instruction below to install the Network Gatekeeper Application Test Environment software:

15. When complete, the Network Gatekeeper Application Test Environment setup wizard is started. Follow the instructions in the wizard.
16. When asked for, enter the licence key. The key is obtained from the BEA eLicense system.
17. When asked for, enter the destination path. It is recommended to use the default path.
18. When asked for, enter the name of the program group and name. It is recommended to use the default name. Subgroups are separated by back slashes (`\`).

After the file copy process has finished (this may take a few minutes), the setup wizard prompts for installation data.

19. In the wizard, enter the following data:

- Name of the SLEE. This is an identifier for the SLEE. This identifier is used in, for example alarm and event records and trace files. Do not use whitespaces in the name.
- IP address of the computer.
- Home directory of MySQL, as defined when installed it. Default is `c:\mysql`
- MySQL User. Default is `root`.
- MySQL Password.
- Port number for the embedded Tomcat servlet engine.

The MySQL user must have full privileges from localhost. If the MySQL database is newly installed, the MySQL user is root and the password is an empty string (MySQL default values).

The suggested paths are default paths.

20. Click **Next**, and then **Finish** to exit the setup wizard.

## Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.4.2 installation

Due to import control restrictions for some countries, the Java Cryptography Extension (JCE) policy files shipped with the Java 2 SDK, Standard Edition and the Java 2 Runtime Environment allow strong but limited cryptography to be used.

An unlimited strength version of these files indicating no restrictions on cryptographic strengths is available on the Java 2 SDK web site for those living in eligible countries.

21. Download Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. The files can be found at the download page for the J2SE used under the heading **Other Downloads**.

**Note:** The version of the JCE Policy files must be correlated with the Java version installed.

22. Replace the `local_policy.jar` and `US_export_policy.jar` files in the directory `%JAVA_HOME%\jre\lib\security` with the files included in the downloaded zip file.

## Start Network Gatekeeper Application Test Environment process

23. Start the SLEE process through the SLEE agent.  
Starting in the directory `C:\bea\wng\ate<version>\bin\`, enter command:  
`runAgent.bat`  
or:  
Choose **ATE** from the **BEA WebLogic Network Gatekeeper** program group in the start menu.
24. In the command prompt window you can see how the SLEE agent is starting up the SLEE process. When the process has started, the SLEE will be in state SHUTDOWN.  
  
During operation, the SLEE agent is used for SLEE process supervision.  
  
**Note:** Do not close the command prompt window. If you do so, the SLEE process will terminate.

## Starting a Network Gatekeeper Management Tool and creating initial users

Follow the instruction below to start a Network Gatekeeper Management Tool and create an administrator user.

Start a Network Gatekeeper Management Tool and add the SLEE

1. See [“Starting a Network Gatekeeper Management Tool and adding a SLEE” on page 3-7](#).  
Use the following login data:  
**User:** install  
**Password:** install
2. In the **SLEEs** pane, right-click on the background and select **Add SLEE...** from menu, or open the **Actions** menu and select **Add SLEE...**  
  
This displays the **Add SLEE** dialog box.
3. Enter data according to the table below:

**Note:** For the SLEE name parameter, it is recommended use the SLEE name as defined when the SLEE was installed.

Parameter	Description
SLEE Name	The SLEE name you want to appear in the SLEE pane.
User ID	Your SLEE user ID. Default is install.
Password	Your SLEE password. Default is install.

4. Select if the SLEE connection shall be made using IP address and port numbers, or name service references files.

**Note:** If bi-directional CORBA is used on the Network Gatekeeper Application Test Environment the SLEE belongs to, the connection has to be made using name service reference files.

5. Enter IP address and port number, *or* name service references file data according to the table below:

Parameter	Description
IP Address	The SLEE host's IP address.
NS Port	The SLEE name service's port number. Default is 10007.
Agent Port	The SLEE agent's port number. Default is 6214.
SLEE reference file	The path to the SLEE's name service reference file.
Agent reference file	The path to the SLEE agent's name service reference file.

6. Click **OK**.

This displays the SLEE in the **SLEEs** pane.

Start the SLEE

7. Select the SLEE in the **SLEEs** pane.
8. Double-click the **SLEE** service in the **Services and Methods** pane.
9. Double-click the **start** method.



10. Click **Invoke** in the **Invoke Method** window.

The new SLEE state (RUNNING) is displayed in the **Messages** pane when the SLEE has started. The SLEE symbol also turns green. It may take a few minutes before the SLEE is running.

Create an administrator user

11. Double-click the **addUser** method in the **SLEE** service in the **Services and Methods** pane.

12. Enter a user name and password, and set **userLevel** to 3.

By setting the user level to 3 you will get administrator authority, that is, the highest authority level.

13. Click **Invoke**.

Your administrator user is now created and can be used for the configuration tasks performed through the Network Gatekeeper Management Tool.

Add new administrative user to service group

14. Double-click the **addUserToGroup** method in the **Services and Methods** pane.

15. Enter `ALL` in the **group** field and the user name in the **user** field.

The service group `ALL` contains the SLEE and all SLEE services.

16. Click **Invoke**.

The new administrative user can now administrate all services appearing in the Network Gatekeeper Management Tool's **Services** pane.

Delete the install user

**Note:** The **install** user is deleted for security reasons. The install user must not be deleted until the Network Gatekeeper Application Test Environment has been set up correctly by the Network Gatekeeper Application Test Environment services.

**Note:** If manually running the postconfig scripts, the **install** user is added automatically.

17. Double-click the **deleteUser** method in the **Services and Methods** pane.

18. Enter the user `install` in the **Invoke Method** window.

19. Click **Invoke**.

The install user is deleted.

20. Logout from the Network Gatekeeper Management Tool, select **Applications - SLEE Manager - Logout** in the menu.

**Note:** You have to logout from the Network Gatekeeper Management Tool since the install user is now deleted from the database. This means that as an install user, you have no authority to perform any administrative work through the Network Gatekeeper Management Tool. All further configuration work have to be performed using the administrative user created in Steps 11. to 19. above.

## Configuring notification end-points for Parlay X Web Services applications

### Enable incoming message notification for Parlay X SMS and MMS

Follow the instruction below to enable notifications on incoming SMSes and multimedia messages to a Parlay X application. Notifications have to be enabled for each mailbox registered for the application instance group.

1. Select a SLEE where the **SESPA\_messaging** service is installed.
2. Double-click the **SESPA\_messaging** service.
3. Double-click the **enableMessageNotification** method.

4. Enter the following data.

Parameter	Description
mailbox	The mailbox for which to enable notifications on incoming messages. Format is tel:<mailbox>, for example tel:10000
mailboxPassword	The password related to the mailbox.
smsEndPoint	URL to the end point of the callback/notification web service implementation for incoming SMSes. For example: http://<mysoapengine>/<mylistenerapplication>
mmsEndPoint	URL to the end point of the callback/notification web service implementation for incoming MMSes. For example: http://<mysoapengine>/<mylistenerapplication>
serviceProviderID	The service provider account ID.
applicationID	The application account ID.
applicationInstanceGroupID	The application instance group ID.
serviceCode	A string identifying the service (application) issuing the request. The information may be used for calculating charging related information. The format is unspecified.
requesterID	An ID for the requester of this service, could be a token received during log-in or the full address for the requester. If it's a full address the format shall adhere to the format as specified for the EndUserIdentifier. In other cases the format is unspecified. If the requester is unknown/unspecified an empty string shall be used.

5. Click **Invoke**.

The listener is registered and an ID for the listener is displayed.

## List incoming message notification for Parlay X SMS and MMS

Follow the instruction below to list notifications on incoming SMSes and multimedia messages to a Parlay X application.

1. Select a SLEE where the **SESPA\_messaging** service is installed.
2. Double-click the **SESPA\_messaging** service.
3. Double-click the **listMessagingNotifications** method.
4. Click **Invoke**.
5. A list of IDs of active messaging notifications is displayed in the SLEE pane.

## Getting details about a notification listener

Follow the instruction below to get details on individual notification listeners for incoming SMSes and multimedia messages to a Parlay X application.

1. Select a SLEE where the **SESPA\_messaging** service is installed.
2. Double-click the **SESPA\_messaging** service.
3. Double-click the **getMessagingNotification** method.
4. In the **Id** field, enter the ID of the notification listener and click **Invoke**.  
See [“List incoming message notification for Parlay X SMS and MMS” on page 7-10](#) for information on how to retrieve the ID.
5. A list of IDs of active messaging notifications is displayed in the SLEE pane.

## Disable incoming message notification for Parlay X SMS and MMS

Follow the instruction below to disable notifications on incoming SMSes and multimedia messages to a Parlay X application.

1. Select a SLEE where the **SESPA\_messaging** service is installed.

2. Double-click the **SESPA\_messaging** service.
3. Double-click the **disableMessageNotifications** method.
4. In the **Id** field, enter the ID of the notification listener and click **Invoke**.  
See “[List incoming message notification for Parlay X SMS and MMS](#)” on page 7-10 for information on how to retrieve the ID.

## Configuring database disk space alarm levels

Follow the instruction below to specify at which threshold levels database disk space alarms should be raised. The threshold levels specify the amount of disk space left on the database partition disk at the time alarm is raised.

At the first threshold level only an alarm is raised. Default is 20MB.

At the second threshold level, the system shuts down the database and raises an alarm. Default is 10MB.

Also, the update interval for the system to check available disk space is set. Default is 60s.

1. Start a Network Gatekeeper Management Tool and log in.
2. Select the SLEE on the host where the database is installed.
3. Double-click the **SLEE** service.
4. Double-click the **setDbDiskFreeWarningThreshold** method.
5. Enter the threshold value (in MB).
6. Click **Invoke**.
7. Double-click the **setDbDiskFreeShutdownThreshold** method.
8. Enter the threshold value (in MB).
9. Click **Invoke**.
10. Double-click the **setDiskMonitorUpdateInterval** method.
11. Enter the update interval (in seconds).
12. Click **Invoke**.

The database alarm threshold levels are now configured.

## Configuring alarm list filtering level

Follow the instruction below to specify which type of alarms are written to the alarm list. As default, all alarms are written to the alarm list.

The task is performed through a Network Gatekeeper Management Tool.

1. Start a Network Gatekeeper Management Tool and log in.
2. Select the SLEE to work with.
3. Double-click the **SLEE\_alarm** service.
4. Double-click the **setFilterLevel** method.
5. From the drop-down menu, choose:

Menu item	To log:
Warning	Warnings, minor, major and critical alarms.
Minor	Minor, major and critical alarms.
Major	Major and critical alarms.
Critical	Critical alarms only.

6. Click **Invoke**.

The alarm filter level is now configured.

## Configuring event log filtering level

Follow the instruction below to specify which type of events are written to the event log. As default, all events are written to the event log.

The task is performed through the Network Gatekeeper Management Tool.

1. Start a Network Gatekeeper Management Tool and log in.
2. Select the SLEE to work with.
3. Double-click the **SLEE\_event** service.

4. Double-click the **setFilterLevel** method.
5. From the drop-down menu, choose:

Menu item	To log:
Low	Low, medium and high importance events.
Medium	Medium and high importance events.
High	High importance events only

6. Click **Invoke**.

The event filter level is now configured.

## Configuring trace buffer size and maximum trace log file size

Follow the instruction below to define the number of trace messages buffered in the memory before written to disk, and the maximum size of the trace files.

The smaller the trace message buffer is, the more disk accesses will be caused by the trace. That is, if the trace message buffer is too small, it has a negative influence on the system performance. As default, 100 messages are buffered and the maximum trace file size is 1000 kB.

The task is performed through the Network Gatekeeper Management Tool.

1. Start a Network Gatekeeper Management Tool and log in.
2. Select the SLEE to work with.
3. Double-click the **SLEE\_trace** service.  
Set trace buffer size
4. Double-click the **setBufferSize** method.
5. Enter the number of messages buffered in the memory before written to disk.  
Value range: 1-500 messages
6. Click **Invoke**.

The trace buffer size is now configured.

Set maximum trace file size

7. Double-click the **setMaxLogFileSize** method.

8. Enter the maximum size of the trace file.

Value range: 100-100000 kB

9. Click **Invoke**.

The trace file size is now configured

Turn off trace

The trace is active on all SLEE services at installation time so that any problems that may occur during installation should be detected. After the system installation has been verified the trace should be turned off for all SLEE services since excessive tracing has a negative influence on system performance.

10. Double-click the **deactivateTraceForAllServices** method.

11. Click **Invoke**.

The trace is now turned off for all current SLEE services.

When an application is installed, trace for that application is automatically turned on or off depending on a setting in the application's deployment descriptor.

## Installing the documentation on intranet or file server

The documentation for Network Gatekeeper Application Test Environment is available on the CD-ROM.

## Alarms

The following alarms are specific for Network Gatekeeper Application Test Environment.

### 1028 License about to expire

### Severity

Warning



## Description

The time-limited licence key for the Network Gatekeeper Application Test Environment will expire within the time indicated in the alarm text. The first alarm is raised 7 days before the licence expires. It is then raised periodically, on an hourly basis. When the licence has expired, the Network Gatekeeper Application Test Environment will shut down.

## What to do

1. Contact the supplier of the Network Gatekeeper Application Test Environment and request a new licence key.
2. Update the license key for the product. Use the **updateLicenseKey** method in the **ATE\_setup** SLEE service.

If the licence has expired, so the Network Gatekeeper Application Test Environment cannot be started, see [“1029 License expired” on page 7-15](#).

## 1029License expired

### Severity

Critical

### Description

The licence has expired and the Network Gatekeeper Application Test Environment will automatically shut down.

### What to do

1. Contact the supplier of the Network Gatekeeper Application Test Environment and request a new licence key.
2. Edit the file `<installation directory>ate\bin\.licence` with the new licence key.

## 9950Licence key not found

### Severity

Major

## Description

A valid licence can not be found. The file may be removed.

## What to do

1. Enter a valid license key in the file <installation directory>\ate\bin\license

# Troubleshooting the installation

## Database access denied

If database access is denied. Run the post config script. The script is found at:  
<installation directory>\bin\postconfig.bat

Execute the script with MySQL user name and password as arguments:  
postconfig.bat <mysql user name> <mysql password>

## SLEE start-up failure

If the SLEE during start-up reports:

Unable to use very strong encryption algorithms. Please verify that JCE Unlimited Strength Jurisdiction Policy files are installed.

- Verify that the JCE files have been replaced in directory  
%JAVA\_HOME%\jre\lib\security
- Check that the JCE version matches the Java version.
- Make sure that  
%JAVA\_HOME%\bin  
is located first in the **Path** environment variable.

# Directory Structure and Contents

The following sections describe the [Structure](#) and [Contents](#) of an Application Test Environment installation.

## Structure

At a standard Windows 2000/XP Network Gatekeeper Application Test Environment installation, the directory structure in Table 1 is created.

*Table 1: Network Gatekeeper Application Test Environment Windows 2000/XP Directory Structure*

C:\	bea\wng\    mysql\ j2sdk<version>\	ate<version>\	bin\   lib\ 	_autoslee\  autosrv\  services\  trace\ 
-----	---	---------------	--------------------------	---

## Contents

A brief introduction to the contents of each directory is given below.

- C:\bea\wng\ate<version>\
 

Contains all directories and files related to the Network Gatekeeper Application Test Environment SLEE.
- C:\bea\wng\ate<version>\bin\  
 Contains start up scripts and reference files for the name service, repository, and trading service.
- C:\bea\wng\ate<version>\bin\\_autoslee\  
 Contains the jar files of the SLEE utility services.
- C:\bea\wng\ate<version>\bin\autosrv\  
 Contains the jar files of the SLEE services (except the SLEE utility services) that will be automatically started when the SLEE is started or restarted.
- C:\bea\wng\ate<version>\bin\services\

The directory where SLEE services will be stored when they are installed in the SLEE. That is, the services working directory.

- C:\bea\wng\ate<version>\bin\trace\  
Contains the trace files generated by the trace service.
- C:\bea\wng\ate<version>\lib\  
Contains Network Gatekeeper Application Test Environment executables other than SLEE services. For example the SLEE itself.
- C:\mysql\  
Contains all directories and files related to the MySQL database.
- C:\j2sdk<version>  
Contains the Java Development kit.

## Directory Structure and Contents

# References

## Developer's Guides

Application Developer's Guide - Parlay X for WebLogic Network Gatekeeper

Application Developer's Guide - Extended Web Services for WebLogic Network Gatekeeper

API Descriptions - Parlay X for WebLogic Network Gatekeeper

API Descriptions - Extended Web Services for WebLogic Network Gatekeeper

## Database

MySQL Reference Manual

## Orb

ORBacus For C++ and Java

## OSA/Parlay

Parlay X specifications

## Servlet engine

Tomcat Servlet Engine Documentation

## References