# BEA AquaLogic Enterprise Security™

## Release Notes

Version: 3.0
Revised: December 2007

# Contents

# BEA AquaLogic Enterprise Security Version 3.0 Release Notes

The following topics are covered is this section:



## AquaLogic Enterprise Security 3.0 Features and Changes

BEA AquaLogic Enterprise Security (ALES) is a fine-grained entitlements product that was designed to enable centralized management of access to both application resources and application objects. ALES uses a centrally administered, distributed security services architecture that supports hierarchical policies across heterogeneous application environments. It also provides a unified and adaptable security infrastructure that enables a service-oriented approach to securing distributed applications. It allows shared security infrastructure and services to be leveraged and re-used across the heterogeneous enterprise—improving security and increasing IT efficiency.

ALES includes the Administration Application and a set of Security Services Modules (SSM).

The ALES Administration Application provides centralized management of application entitlements, letting you control all of your security policies and configuration data from a single web-based console. Configuration, security policy, and user metadata for ALES-distributed Security Services Modules are managed and provisioned by the Administration Application. All

administrative functions, including delegation, are fully configurable through administrative policies.

BEA AquaLogic Enterprise Security supports a variety of Security Service Modules (SSMs) that reside in the application environments protected by ALES. They provide the runtime enforcement of entitlements and integrate with the underlying security framework to provide services for authentication, authorization, auditing, role mapping, and credential mapping. The security framework also provides a simple application programming interface (API) that can be used by security and application developers to define security policies and services. SSMs are provided for the WebLogic Platform, Java applications, Web Server applications, Oracle application, WebSphere applications, and non-Java applications through a generic Web Services SSM.

This section covers the following topics:



# What's New in BEA AquaLogic Enterprise Security 3.0

This section describes new and changed features for this release of AquaLogic Enterprise Security.

This release of AquaLogic Enterprise Security has several new and changed features:



These features are described in the sections that follow.

# New Documentation Content and Design

The ALES 3.0 documentation set has been completely redesigned to make required tasks easier to understand and more accessible. The new organizational model includes *Securing Applications with ALES 3.0* documents and *How To* sections, which make it easier to find the information you need.

# New Entitlements UI Capabilities

In ALES 3.0 the Entitlements UI includes comprehensive administrative support, including the following management operations:

- Resource management (including resource attributes)
- Access policy authoring
- Role policy authoring
- Extended reporting capabilities
- Attributes and constants
- SSM bindings

The Entitlements UI also now includes support for all attribute types.

# API Runtime Enhancements

## Bulk Authorization

In ALES 3.0, bulk authorization APIs are exposed in both the Java API and the Web Service API. The APIs accept two kinds of input parameters and return a list of access decision as well as response attributes:

- A flat list of resource action-pairs for which authorization results will be returned.
- A single resource action-pair for which authorization results will be returned for all child resources.

## New Cache and Statistics Methods in AuthorizationService

The Java API `AuthorizationService` includes new `getStatistics`, `flushCache` and `flushCacheByUser` methods.

### User Entitlements Returned in API

ALES 3.0 includes the ability to return the following information through the API:

- The set of allowed actions, given a user and resource
- For a given resource and user, returns allowed and denied actions for this resource and all children of the resource.

## Additional Administration Features

### New Configuration Tool

ALES 3.0 includes a new SSM configuration tool that greatly simplifies the task of creating an SSM instance.

You need only make some simple edits to a properties file and the config tool creates the SSM, including providers and a default policy, and binds everything together in the console. If any information is missing in the properties file, the tool prompts for the data.

The config tool has check (validate) and process options.

The config tool is located in *BEA_HOME*/ales30-ssm/ssm-type/adm/ConfigTool.bat/sh.

### SSL Key Management is Simplified

In ALES 3.0 the keystores usage has been greatly simplified. ALES creates a single set of keys to represent a host where ALES components are installed. All ALES components located under a BEA_HOME installation directory use the same shared set of keys, located in BEA_HOME/ales30-shared/keys.

A new enroll tool uses these shared keys and you need only run it once once for any given BEA_HOME. This means you do not have to enroll every SSM that you might create.

### Attribute Retrievers Created and Managed in Console

This release of ALES provides out-of-the-box attribute retrievers that you can configure directly in the WebLogic Server Administration Console for the WLS 9.x/10.0 SSM, and in the ALES Administration Console for all other SSMs.

Attribute retrievers are used by ASI Authorization and ASI Role Mapping providers to retrieve attributes for use by AquaLogic Enterprise Security authorization and role mapping.

There is no longer any need to write code to create an attribute retriever.

The following attribute retrievers types are provided. You can cache attributes for RDBMS, LDAP, and Custom attribute retrievers.

- RDBMSAttribute Retriever
- LDAPAttribute Retriever
- SDOAttribute Retriever
- ALESIdentity Attribute Retriever
- Custom Attribute Retriever

# New SSMs

## SSM for WebSphere

ALES 3.0 includes a new SSM for the WebSphere Application Server. The WebSphere SSM is a Java SSM in WebSphere container, and it allows Java applications deployed in WebSphere to be protected by ALES.

The *BEA_HOME*\ales30-ssm\websphere-ssm\examples\PolicyQueryWebApp example shows how to configure and set up the WebSphere SSM. It also contains a simple Policy Query Web Application that shows how to retrieve basic security services, and use them to do authentication and authorization.

## SSM for Oracle RDBMS 9.x and 10.x

ALES 3.0 includes an SSM for Oracle. The SSM allows ALES policy to be used to limit access and secure data in one or more Oracle database tables.

The ALES Oracle SSM makes use of a feature in Oracle 10g called Fine Grained Access Control (FGAC). You control user access to Oracle tables by using the ALES Administration Console to specify access policies.

# New Integration Features

## New ALES Control for WebLogic Workshop 9.2 and 10.0

The ALES Control for WebLogic Workshop allows you to drag and drop methods from the ALES control onto a WLP page flow, or a WLI process, and then use the data returned by a selected method (access decision, roles, entitlements, etc.) to drive a downstream node in the page

flow or process. For example, the result of an IsAccessAllowed method call (grant/deny or set of responses) could drive a downstream decision or switch node in a WLI process.

The ALES control supports a standard set of methods, such as `IsAccessAllowed`, `GetRoles`, and so forth.

A sample showing the use of the ALES control in WLI process definition is included in *`BEA_HOME`*`\ales30-ssm\wls-ssm\examples\ALESControlForWLW`.

## Integration with WLI 9.2 MP2

ALES 3.0 includes WebLogic Integration 9.2 MP2 runtime resources protection. This allows you to create ALES policies to control access to resources in a WLI process integration, such as WLI processes, nodes, channels, task plans, and worklists Consider the following uses:

- Universal Security Configuration

  You can use one ALES Admin Console to manage users/groups/roles and configure policies for several WLI domains.

- User/Group based policies

  You can create user/group based policies for WLI in addition to role-based policies.

- Use fine grained policies with conditions

  You can create policies with conditions for WLI, such as when a user is allowed to perform a task.

- Use fine grained policies with attributes

  You can create policies with attributes for WLI.

- Use ALES runtime APIs to do security

  You can use ALES runtime APIs in WLI applications to do security, such as authenticate, authorization and so forth.

A sample showing the use of the ALES control in WLI process definition is included in *`BEA_HOME`*`\ales30-ssm\wls-ssm\examples\WLI92Domain`.

## Integration with ALBPM 6.0

ALES 3.0 integration with ALBPM 6.0 provides a set of APIs that an ALBPM process designer can call from inside of activities and transitions to get an authorization decision or to return responses. The information could then be stored in a BPM instance variable that could be used

anywhere else in the process. Similarly, you could use a BPM instance variable to set the context for an ALES call, such as the loan amount.

The data returned by the ALES policy decision can be used in a conditional transition (routing to the next task), or to set a work item for a user.

# New Platform Support

ALES 3.0 includes the following new platform support. "Supported Configurations" on page 7 describes all of the supported configurations.

- Support for WLS/WLP 10.0 MP1 for Admin Server and SSM
- Support for MS-SQL 2005 as ALES Database and authentication source
- Support for DB2 9.1 as ALES Database and authentication source
- Sybase 15 as ALES Database and authentication source
- Suse Linux 9.2 & 10.0 (32-bit & 64-bit) for Administration Server and SSMs.

# Supported Configurations

Table 1 lists the platform on which each AquaLogic Enterprise Security core component is supported.

**Table 1 ALES Core Components**

| Component | Platform | Operating System |
|---|---|---|
| Admin Console & E-UI Browser | MS IE 6.0, 7.0 | Windows 2000 SP4, 2003 R2, XP SP2 |
| Admin Server Platform: | WebLogic Server 8.1 SP5, SP6<br>WebLogic Server [1]9.2 MP2, 10.0 MP1<br>Tomcat 5.5.23 | Sun Solaris 8, 9, 10 (32-bit)<br>Windows 2000 SP4, 2003 R2, XP SP2<br>Red Hat Adv. Server 3.0, 4.0<br>Suse Linux [2]9.2 & 10.0 |

**Table 1 ALES Core Components**

| Component | Platform | Operating System |
|---|---|---|
| ALES Policy Store | Oracle 9.2.0.5, 10.1.2, 10.2.0.2 | |
| | Sybase 12.5.3, 15 | |
| | MS-SQL 2000 & 2005 | |
| | PointBase 5.1 | |
| | DB2 Universal DB Enterprise Server 9.1 | |
| ALES Policy Export | AquaLogic Enterprise Repository 2.6 & 3.0 | |
| User Directory | Microsoft Windows NT Domain | |
| | Microsoft Active Directory | |
| | SunONE Directory Server v5.2 | |
| | Novell eDirectory v8.7.31 | |
| | Open LDAP v2.2.24 | |
| | Oracle 9.2.0.5, 10.1.2, 10.2.0.2 | |
| | Sybase 12.5.3, 15 | |
| | DB2 Enterprise Server Edition 9.1 | |
| | MS-SQL 2000 & 2005 | |
| | PointBase 5.1 | |
| IDEs | WebLogic Workshop 9.0 & 10.0 | |
| | Studio 3.0 | |

1. Works with WLS configured to use either the Sun JVM or the JRockit JVM that ships with the 9.x or 10.x version of the server. JRockit JVM supported on Intel hardware only.
2. Suse Linux is supported on both 32-bit and 64-bit hardware.

Table 2 lists the AquaLogic Enterprise Security SSMs, the platforms on which they run, and operating systems under which they are supported.

**Note:** ALES does not include the JDBC driver for MS SQL and PointBase. If you want to use MS SQL or PointBase for your database, you must download the appropriate JDBC driver. You must use the latest MS SQL 2005 JDBC driver with all versions of MS SQL.

**Table 2 System Requirements**

| SSM | Platform Version(s) | Windows 2000, 2003[1] | Solaris 8, 9, 10 | RHAS[2] 3.0, 4.0 | Suse[3] 9.2, 10.0 | AIX[4] 5.3 |
|---|---|---|---|---|---|---|
| Web Services | MS .NET 1.1 and 2.0[5]<br>WebLogic Workshop 9.0, 10.0<br>Studio 3.0 | Yes | Yes | Yes | Yes | Yes |
| BEA WebLogic Platform | WLS/P 8.1 SP5, SP6<br>WLS/P[6] 9.2 MP2, 10.0 MP1<br>WLI 9.2 MP2 | Yes | Yes | Yes | Yes | No |
| BEA AquaLogic Products | ALDSP 2.5, 3.0[7]<br>ALSB 2.6, 3.0[8]<br>ALBPM 6.0 | Yes | Yes | Yes | Yes | No |
| IBM WebSphere | WebSphere 6.1 | Yes | Yes | Yes | Yes | Yes |
| Java | Sun JVM 1.4.2, 5.0, 6.0<br>JRockit 1.4.2, 5.0, 6.0<br>IBM JDK 1.4.2, 5.0, 6.0 | Yes | Yes | Yes | Yes | Yes |
| Web Servers | Apache | Yes | Yes | Yes | Yes | No |
| | IIS Web Server | Yes | No | No | No | No |

1. Windows 2000 SP4 and higher, Windows 2003 R2 and higher.
2. RedHat Advanced Server.
3. Suse Linux is supported on both 32-bit and 64-bit hardware.
4. AIX SSM support will be delivered post-GA as a CP to ALES 3.0.
5. NET Web Services client on Windows 2000 and 2003 only.
6. Works with WLS configured to use either the Sun JVM or the JRockit JVM that ship with the 9.x or 10.x version of the server. JRockit JVM supported on Intel hardware only.
7. ALDSP 2.5 running on WLS 8.1.x, ALDSP 3.0 running on WLS 10.0 MP1.
8. ALSB 2.6 running on WLS 9.2, ALSB 3.0 running on WLS 9.2 MP1 and WLS 10.0 MP1.

# Known Issues in BEA AquaLogic Enterprise Security 3.0

This section describes known limitations in BEA AquaLogic Enterprise Security, Version 3.0 and may include a possible workaround or fix, where applicable. If an entry includes a CR (Change Request) number, a possible solution may be provided in a future BEA AquaLogic Enterprise Security release where BEA will provide vendor specific code to fix the problem. Refer to the CR number to conveniently track the solution as problems are resolved.

Please contact your BEA Technical Support for assistance in tracking any unresolved problems. For contact information, see the section "Contacting BEA Customer Support" on page 14.

Table 3 lists the known issues in this release of AquaLogic Enterprise Security 3.0.

**Table 3 Known Issues in This Release**

| CR | Description |
|---|---|
| CR352922 | There is a current limitation that you cannot configure an SDO Attribute Retriever when the Admin Console is hosted on Tomcat. |
| CR349150 | Currently the SDO Attribute retriever is supported for the WLS SSM only when configured via an Admin Console that is also hosted on WLS. |
| CR352399 | When using ALES Admin console and/or EUI on Tomcat with JRocket 1.4.x, the following file needs to be updated as follows:<br>Open or edit /ales30-admin/config/WLESTomcat.conf and either remove or comment out the following line:<br>wrapper.java.additional.28=-XX:MaxPermSize=256m<br>Make sure to add the line back if you switch your Tomcat to use the SUN JDK 1.4.x. |

**Table 3 Known Issues in This Release**

| CR | Description |
|---|---|
| CR351924 | If you need to run the ConfigureSSL tool, you need to be aware of the following two scenarios.<br>1. If the Admin Server and SSM are installed on the same system, there will be 2 ConfigureSSL tools. One will be in 'ales30-shared/bin' and the other is in 'ales30-admin/bin'. The first one is for SSM components and the second one is for Admin components. Either can be used to disable or enable SSL connections for both the SSM and Admin.<br>2. If the Admin Server and SSM are **not** installed on the same system, please run 'ales30-admin/bin/configureSSL.bat\|sh' for Admin component and run 'ales30-shared/bin/configureSSL.bat\|sh' for SSM component.<br>**Note:** For both cases, the 'install_home' keyword in ales30-shared/bin/ConfigureSSL.bat\|sh needs to be updated correctly before running it. |
| CR249585 | If you intend to load a large set of policy using the Policy Loader tool, then it is advisable not to do so in a single transaction (which is the default). You can turn off Transaction across an entire policy set by setting "disableTransaction" to true for the Policy Loader. |
| CR347420 | The perfDB Audit provider does not currently record Authentication Statistics. |
| CR246828 | The default JDK for Tomcat is 1.5. If you intend to use JDk 1.4 then you need to make the following 2two changes in the 'ales30-admin/config/WLESTomcat.config' file:<br>1. Replace the first classpath with the actual JDK1.4 file path<br>For example, replace:<br>wrapper.java.classpath.1=/bea/jrockit150_06/lib/tools.jar<br>with:<br>wrapper.java.classpath.1=/bea/jrockit142_08/lib/tools.jar<br>2. Update the 24th java parameter as follows:<br>Replace:<br>`wrapper.java.additional.24=-Djavax.xml.transform.TransformerFactory=com.sun.org.apache.xalan.internal.xsltc.trax.TransformerFactoryImpl`<br>With<br>`wrapper.java.additional.24=` |

**Table 3 Known Issues in This Release**

| CR | Description |
|---|---|
| CR245536 | Currently ALES 3.0 supports upgrading both the Admin and the SSM simultaneously only if they both share the same BEA HOME. |
| CR344800 | When using Microsoft SQL Server 2000 you can only have attribute values no larger then 900 bytes. This is because of a known limitation of the Database and is documented on the Microsoft website:<br>http://msdn2.microsoft.com/en-us/library/aa224343 |
| CR344796 | The Admin log might contain intermittent messgeas as follows:<br>`java.net.ConnectException: Connection refused: connect`<br>This is part of the https connection establishment and currently does not negatively impact the working of the product in any way and can be ignored. |
| CR344150 | The new DBConfig tool does not currently support DB2 database. For that database you will need to follow the steps listed in the Admin install guide on how to set it up such that it can be used by ALES30 product. |
| CR343702 | On Windows 2000 you may encounter the following error if your BEA_HOME dir name is longer then 12 char.<br>"The input line is too long" when running install_ales_schema.bat.<br>In order to fix this issue you need to create an empty jar file with a manifest file that has the Class-Path attribute. Set this attribute to point to the relative path of jar files listed in the set-env.bat file. |
| CR343145 | ALES 3.0 does not currently support ALER26 for import and export of ALES policies. |
| CR334444 | It is advisable not to use directories with spaces in them with the ALES 3.0 product. If you do need to use such a dir that does have spaces then you will have to manually update the WLESWebLogic.conf or WLESTomcat.conf files such that they are correctly quoted for your particular platform. |

**Table 3 Known Issues in This Release**

| CR | Description |
|---|---|
| CR329699 | ALES does not support running any two SSM instances with the same name and config ID on the same host.<br>Assume that you have two SSM instances with the same name on the same host, using the same Config ID to connect to the ALES Admin system. The only difference is that they use different port numbers.<br>In this case, only the first SSM will be able to register with the policy distributor (PD). When the second SSM tries to register with the PD, it does not allow it since there is already a URL registered for that particular SSM instance and Config ID.<br>Note that this is not a problem if the SSM instances with the same name and config ID are running on different host machines. In that case, the instance name that is registered is uniquely scoped by the host name. |
| CR299209 | The help message of the ASISignal utility is incorrect. ASISignal supports the following actions only: ping, comtest, wait, waitready, and status. Actions restart, shutdown, and log are no longer supported. |
| CR300568 | SSM configuration names must not start with provider types or the configuration cannot be exported using PolicyIX.<br>Modify the name of the SSM configuration so it does not start with the following strings: "Adjudication","Auditing","Authentication","Authorization","CredentialMapping","RoleMapping". |
| CR303946 | If an SSM that does not use an SCM fails to start with a ConfigurationException, change the `wles.config.signer` property to upper case. The `wles.config.signer` property contains the host name of the admin server.<br>For a Java SSM, the property is set in the *`BEA_HOME`*`/ales30-ssm/java-ssm/instance/instancename/bin/set-env` script.<br>For a WLS 8.1 SSM, the property is set in the *`BEA_HOME`*`/ales30-ssm/wls8-ssm/instance/instancename/bin/set-wls-env` script.<br>For a Web Services SSM, the property is set in the *`BEA_HOME`*`/ales30-ssm/webservice-ssm/instance/instancename/config/security.properties` file.<br>In the file paths above, instancename is the name you assigned to the SSM instance when you created it. |

**Table 3 Known Issues in This Release**

| CR | Description |
|---|---|
| CR308526 | In BLM API, ruleManager's `modifyRule` method cannot be called more then once in one transaction |
| CR277538 | Default Java 1.4 Browser Plugin Doesn't Work with asiconsole hosted on 9.x WLS.<br>**WORKAROUND**: For that console to work correctly you need to install Java 1.5 Browser Plugin. |
| CR380213 | When you restart an Administration Server running in WebSphere and attempt to log in to the administration console (*https://<host>:7010/asi*), you receive an Access Denied response, regardless of the log in credentials<br>As a workaround, navigate to the log in screen of the Entitlements Administration Application (*https://<host>:7010/entitlementsadministration*) — you do not need to actually log in. Then return to the administration console and log in as usual. |

# Contacting BEA Customer Support

Your feedback on the product documentation is important to us. Send us e-mail at docsupport@bea.com if you have questions or comments. Your comments will be reviewed directly by the BEA professionals who create and update the product documentation.

In your e-mail message, please indicate that you are using the documentation for the BEA AquaLogic Enterprise Security Version 3.0 release.

If you have any questions about this version of the BEA AquaLogic Enterprise Security product, or if you have problems installing and running the product, contact BEA Customer Support through BEA Web Support at **http: //support.bea.com**. You can also contact Customer Support by using the contact information provided on the Customer Support Card, which is included in the product package.

When contacting Customer Support, be prepared to provide the following information:

- Your name, e-mail address, phone number, and fax number
- Your company name and company address
- Your machine type and authorization codes

- The name and version of the product you are using
- A description of the problem and the content of pertinent error messages