# BEA WebLogic Platform™

## Introducing WebLogic Platform 7.0 Security

Release 7.0 Service Pack 2
Document Date: February 2003

## Copyright

## Restricted Rights Legend

## Trademarks or Service Marks

***Introducing WebLogic Platform 7.0 Security***

| Part Number | Date | Software Version |
|---|---|---|
| N/A | February 2003 | 7.0 Service Pack 2 |

# Contents

# Introducing WebLogic Platform Security

This document introduces security in the WebLogic Platform 7.0 environment, explaining how you can leverage the security options provided in WebLogic Platform for your solutions. In particular, this document describes the assumptions used by the different Platform components for their default security configurations. This document also provides references to key security topics in the WebLogic Platform documentation set, which is available on the documentation CD provided with this release. This document is intended for administrators who want to deploy secure WebLogic Platform applications.

This topic includes the following sections:

- WebLogic Server Security Configuration
- WebLogic Portal Security Configuration
- WebLogic Integration Security Configuration
- Configuring WebLogic Portal and WebLogic Integration on the Same Server
- Configuring Your WebLogic Server, Portal, and Integration Applications on Different Servers
- Migrating from Previous Releases
- Using an External LDAP Realm
- Where to Find More Information

# WebLogic Server Security Configuration

The *Introduction to WebLogic Security* provides an overview of the new and changed capabilities in the WebLogic Server security subsystem. If you are planning to use only the WebLogic Server component of WebLogic Platform, be sure to read this document. Also see *Securing WebLogic Resources* for details about how to use the WebLogic Server Administration Console to configure security for specific resources, such as users, groups, application resources, JDBC resources, and so on.

A typical WebLogic Server domain created using the BEA Configuration Wizard uses the default security settings. (For more information about the Configuration Wizard, see *Using the Configuration Wizard*.) These settings allow you to define authentication and authorization rules for your application. In particular, the new WebLogic Server security subsystem includes an embedded LDAP server that serves as the registry, or store, for the authentication and authorization information needed by your application. Note that this is an important change from previous releases, in which WebLogic Server used the File realm as the default realm. If you are already a WebLogic Server user, see the security sections in the following documents for more details about the impact of this change:

- *Frequently Asked Questions*
- "*Upgrading WebLogic Server 6.x to Version 7.0*" in *WebLogic Server 7.0 Upgrade Guide*

WebLogic Server now supports the use of the nCipher JCE provider. JCE providers, such as nCipher, offload SSL processing from Web servers, freeing the servers to process more transactions. JCE providers also provide strong encryption and cryptographic process to preserve the integrity and secrecy of keys.

For more information, see "Using the nCipher JCE Provider with WebLogic Server" in *Managing WebLogic Security* at the following URL:

`http://e-docs.bea.com/wls/docs70/secmanage/ssl.html`

In addition to the new security features, WebLogic Server 7.0 also supports the realm-based security mechanisms available in WebLogic Server versions 5.1, 6.0, and 6.1. If you want to use your existing realm-based security environment, you need to configure your application domain appropriately using compatibility mode, which is described in "Using Compatibility Security" in *Managing WebLogic Security*. This setting applies to all servers in the domain. WebLogic Server 7.0 allows a mixed-mode configuration that permits you to configure realm-based authentication with some of the new security functions. In particular, you can use the new authorization subsystem with your realm-based authentication.

The following table summarizes the authorization configurations supported with WebLogic 7.0 and a 6.x authentication realm.

| **Authorization** | **Comments** |
|---|---|
| 7.0 default provider | This configuration is fully supported. |
| 7.0 with a 3rd party provider | There is limited support for this configuration – third parties must use WebLogic Server interfaces for group resolution (in particular, `weblogic.security.SubjectUtils.isUserInGroup())` |
| 6.x (file realm) | This configuration is fully supported, but EJB and servlets authorization will be performed via the WebLogic Server 7.0 authorization provider. |

If you are planning to use WebLogic Server in conjunction with the WebLogic Portal and WebLogic Integration components, note that WebLogic Portal and WebLogic Integration still require the use of WebLogic Server 6.x security realms and must run in compatibility mode. The default for WebLogic Platform, if you use WebLogic Portal, is the WebLogic Portal RDBMS realm. Note that you can also use the new authorization functions provided by WebLogic Server 7.0 for your WebLogic Portal and WebLogic Integration applications.

WebLogic Workshop, which is bundled with WebLogic Server, can work with either the WebLogic Server default security or with the compatibility mode that is required by the other WebLogic Platform components. However, the samples included with WebLogic Workshop use the default LDAP-embedded server. If you are planning to use the Application Integration control, note that this control is from WebLogic Integration and therefore requires that you run your server in compatibility mode.

# WebLogic Portal Security Configuration

The following topics explain how to add security to Portal applications and how to administer users in groups in a WebLogic Portal-based domain:

- "Adding Security to a Portal" in the WebLogic Portal *Developer Guide*
- "Administering Users and Groups" in the WebLogic Portal *Administration Guide*

Refer to these two documents if you want to use the WebLogic Portal component of WebLogic Platform, or if you are upgrading from a previous version of WebLogic Portal.

A typical installation of WebLogic Portal includes the WebLogic Server and WebLogic Workshop components of WebLogic Platform, along with several sample servers and their preconfigured domains. By default, preconfigured sample servers use the custom security RDBMS realm provided with WebLogic Portal. This realm provides a store for users and groups. For more details about how you can set up or customize this realm, see "Adding Security to a Portal" in the WebLogic Portal *Developer Guide*. Note that the WebLogic Portal RDBMS realm is a WebLogic Server 6.x realm and requires the server that is running WebLogic Portal applications to run in compatibility mode. The samples delivered with the WebLogic Server and WebLogic Workshop components may not work with the WebLogic Portal default realm—these samples use the default WebLogic Server security (that is, the embedded LDAP server).

If you are creating a WebLogic Portal application domain, you can use the Configuration Wizard to assist you. By default, the Configuration Wizard configures WebLogic Portal security to use compatibility mode and the RDBMS realm. If you configure a multimachine application that uses other WebLogic Platform components (for example, WebLogic Portal and WebLogic Integration), and you are planning to use WebLogic Portal RDBMS for authentication, you should install WebLogic Portal on all the machines on which the application runs.

To add new users and groups to a WebLogic Portal application, use the WebLogic Portal User Management tools. See "Administering Users and Groups" in the WebLogic Portal *Administration Guide*. Using these tools ensure that your user profiles work properly with your WebLogic Portal application.

Please note that users added via the WebLogic Server Administration Console will not automatically be WebLogic Portal users. This caveat also applies to users or groups that you may have added via the WebLogic Integration user management tools, as described in the following section. We recommend that you use the Portal User Management tools to adjust the profiles of these users. This tool automatically attaches a WebLogic Portal profile to users that do not have such a profile – these users may have been defined with other tools, such as the WebLogic Server Administrative Console. Once a user has a WebLogic Portal profile, this user becomes a WebLogic Portal user.

# WebLogic Integration Security Configuration

The topic "Using WebLogic Integration Security" in *Deploying WebLogic Integration Solutions* explains how to configure the security of your WebLogic Integration applications. Refer to this document if you plan to use the WebLogic Integration component of WebLogic Platform.

A typical installation of WebLogic Integration includes the WebLogic Server and WebLogic Workshop components. If you are creating a WebLogic Integration application domain, the Configuration Wizard can assist you. By default, the Configuration Wizard configures the WebLogic Integration security to use compatibility mode and the WebLogic Server 6.x File realm for storing users and groups. All the WebLogic Integration samples use the File realm, and the samples delivered with WebLogic Server and WebLogic Workshop may not work in this configuration – these samples assume the default Server security (that is, the embedded LDAP server).

You should use the WebLogic Integration administration tools (see the WebLogic Integration administration topic) to configure users and groups. In particular, you can use the following administration tools:

- The Business Process Management (BPM) security subsystem uses the WebLogic Integration Studio tool to define users, organizations, and roles, and to map roles to groups in the security realm. Note that users defined via the WebLogic Administration Console or other user management tools are not necessarily BPM users. If you have added users via other tools, such as the WebLogic Server Administration Console, you need to explicitly assign these users to the `wlpiUsers` group and then use the Studio to add each user to a role and an organization. You can do this by right clicking on the `Users` node in the tree view and then selecting the `Add User` command. You can also use the Studio to assign other security attributes needed within BPM. In general, use the Studio to control the security of your workflows. For more information, see "Administering Data" in *Using the WebLogic Integration Studio*.

- The B2B Integration security guide, *Implementing Security with B2B Integration*, provides more detail about how to use the B2B Console to configure business protocols, conversations, trading partners, and collaboration agreements. Typically, for B2B Integration, you can use the WebLogic Server Administration Console to configure most of the resources needed; for example, users, groups, policies, and the SSL stack. You then use the B2B Console to configure the security of your trading partners. In particular, you use the B2B Console to map a trading partner to a WebLogic Server user and to assign other security attributes. If you are planning to use the B2B component, note that the WebLogic Server SSL settings apply to the whole server. For example, mutual authentication also applies to a WebLogic Portal application if you are planning to run this application on a server configured with the B2B component to require mutual authentication. You also need to configure the WebLogic Keystore provider (with which you register the keystores for storing keys and certificates for authenticating your trading partners) by following the instructions in "Configuring the Keystore" in *Implementing Security with B2B Integration*. You need to configure the keystores via the WebLogic Server Administration Console before you deploy the server application in your B2B domain.

- An application using the Application Integration component to access an Enterprise Information System (EIS) might need to provide authentication credentials, such as a login name and password, to access that system. The topics "Defining an Application View" and "Using Application Views by Writing Custom Code" in *Using Application Integration* contain information about how to configure the security setting of deployed application views.

Note that if you are planning to add WebLogic Portal applications to a server already configured with a WebLogic Integration application, the WebLogic Portal RDBMS realm will become the primary realm. This realm can operate with the File realm, but we strongly recommend that you avoid having replicated users and groups in both realms.

# Configuring WebLogic Portal and WebLogic Integration on the Same Server

You can configure an application that uses all of the WebLogic Platform components on the same server. In this case, the WebLogic Portal RDBMS realm will be the default security realm, and the server will be configured in compatibility mode. The WebLogic Portal RDBMS realm comes enabled with all the predefined data required by WebLogic Integration. If you use the WebLogic Server Administration Console or the WebLogic Integration Studio to define new users, these users are stored in the RDBMS realm.

As a rule, you should use the user management tools provided by each WebLogic Platform component to properly enable the user profiles defined by these components. Also note that you may be requested to reauthenticate when switching from one management tool to another.

If you are planning to use the WebLogic Integration B2B component, note that B2B uses SSL with mutual authentication. This setting applies to the whole WebLogic Server. Therefore, this may also have an impact on other components of WebLogic Platform you may want to use conjointly.

# Configuring Your WebLogic Server, Portal, and Integration Applications on Different Servers

You may want to configure the applications based on the WebLogic Platform components on different servers. For example, you might want to manage your WebLogic Portal application independently from your WebLogic Integration, Workshop, and EJB applications. By configuring your WebLogic Portal application in its own server, you can adjust quickly to the needs of your customers and still communicate with your applications.

Note that a realm configuration is domain-wide and, therefore, this configuration applies to the entire set of servers that make up your application domain. If you are planning to use WebLogic Portal and its default RDBMS realm in the same application, we recommend that you install the WebLogic Portal software and configure the RDBMS realm on every machine used by the application.

You can also configure WebLogic Platform components in different domains. Configuring your applications in different domains would be probably the best choice if you want quickly to migrate your existing applications to WebLogic Platform. For example, your WebLogic Integration applications could continue to use the users, groups, and other data configured in the old File realm associated with your application. However, you need to be careful with this multidomain configuration because you may end up with different security stores (realms), depending on the Platform component that you might want to use.

When you configure the WebLogic Platform components in their own domains, you also need to consider if you want end-user single sign-on across the domains. WebLogic Platform supports propagation of user identity across WebLogic Server, Workshop, Portal, and Integration applications so that end-user sign-on can be achieved, provided that the user information is properly populated across these applications. In WebLogic Platform, a trust relationship (where principals from one domain will be accepted as principals in another domain) is set up when the `Credential` attribute of the `SecurityConfigurationMBean` (see the `config.xml` file) in one domain matches the `Credential` attribute on the `SecurityConfigurationMBean` in the other domain. If you boot an administration server for the first time, and the `Credential` attribute is not set, the administration server notices that this attribute is not set and generates a random credential that is then used to sign the principals created in that domain. Other servers in the domain retrieve the credential from the administration server and, therefore, will be able to establish the trust relationship within the domain. See the *Introduction to WebLogic Security* for more information about this topic.

# Migrating from Previous Releases

If you are migrating from a WebLogic Server 6.x to WebLogic Server 7.0 environment, read the security chapters from *Upgrading WebLogic Server 6.x to Version 7.0*. Basically you can either migrate all your users and groups to the new security (you will be able to use a tool provided at BEA dev2dev Online), or you can continue using your existing realm. If you adopt the latter option, your server needs to be configured in compatibility mode.

If you are migrating from WebLogic Portal 4.0 to WebLogic Portal 7.0, you can fully reuse users, groups, and entitlements already defined in your WebLogic Portal 4.0 RDBMS realm.  If you are using a custom realm, you can continue to use this realm. However, if you want to have this custom realm work with WebLogic Integration, complete the steps in the section "Security Realm Guidelines" in "Customizing WebLogic Integration" from *Starting, Stopping, and Customizing WebLogic Integration*.  You cannot use the new authentication facility in WebLogic Server 7.0 with the WebLogic Portal component included in WebLogic Platform. You can use only a WebLogic Server 6.x realm, and your domains should be configured in compatibility mode.

If you are migrating from WebLogic Integration 2.1 to WebLogic Integration 7.0, you can use your old File realm.  But you must configure WebLogic Server in compatibility mode. You need to be aware that if you are planning to use WebLogic Portal in the same application domain, the WebLogic Portal RDBMS realm will be the default realm.  You will need to migrate your users to the WebLogic Portal RDBMS realm (for example by adding the users with the WebLogic Integration Studio).  You could also configure your WebLogic Portal application in a different domain and continue to use your old File realm. You cannot use the new authentication facility in WebLogic Server 7.0 with WebLogic Integration included in WebLogic Platform. You can use only a WebLogic Server 6.x realm, and your domains should be configured in compatibility mode.

# Using an External LDAP Realm

You can use third-party LDAP products with WebLogic Platform.  To do this, configure your domain in compatibility mode with the WebLogic Server 6.x LDAP realm. The LDAP realm is read-only. Therefore, using the LDAP realm may require additional intervention using third-party tools, especially when performing user, group, and other administration or management tasks.

You can find more information about how to configure the LDAP realm in the following guides:

- The WebLogic Server document, *Managing WebLogic Security*, contains a chapter "Using Compatibility Security," which explains how to use compatibility security. See especially the topic "Configuring the LDAP Security Realm," which explains how to use an external LDAP product with WebLogic Server 7.0.

- The steps that you would need to complete to configure WebLogic Integration with an external LDAP product are available in the section "Understanding the BPM Security Model" in "Customizing WebLogic Integration" from *Starting, Stopping, and Customizing WebLogic Integration*. In particular, you need to configure certain users and groups needed by WebLogic Integration and the samples (defined in those documents). See especially the topic "Configuring a Custom Security Realm," which provide the basic steps you can use to add an external LDAP product to WebLogic Integration.

- The section "Adding Security to a Portal" in the WebLogic Portal *Developer Guide* provides more information about realms in WebLogic Portal. The section "Administering Users and Groups" in the WebLogic Portal *Administration Guide* provides information about groups required by a WebLogic Portal application. These groups should be defined in your LDAP realm.

You can also use custom realms with WebLogic Platform. The documentation in the preceding list provides you with more information about how to set up a custom realm.

# Where to Find More Information

You can obtain more information about how to configure the security attributes used by the different WebLogic Platform components in the following guides:

- WebLogic Platform, *Installing BEA WebLogic Platform*
- WebLogic Platform, *Using the Configuration Wizard*
- WebLogic Server, *Introduction to WebLogic Security*
- WebLogic Server, *Managing WebLogic Security*
- WebLogic Server, chapter "Using Compatibility Security" in *Managing WebLogic Security*
- WebLogic Server, *Frequently Asked Questions*
- WebLogic Server, chapter "Upgrading WebLogic Server 6.x to Version 7.0" in *WebLogic Server 7.0 Upgrade Guide*
- WebLogic Portal, chapter "Adding Security to a Portal" in the WebLogic Portal *Developer Guide*
- WebLogic Portal, chapter "Administering Users and Groups" in the WebLogic Portal *Administration Guide*
- WebLogic Integration, chapter "Using WebLogic Integration Security" in *Deploying WebLogic Integration Solutions*
- WebLogic Integration administration topics
- WebLogic Integration, *Implementing Security with B2B Integration*
- WebLogic Integration, *BEA WebLogic Integration Migration Guide*
- WebLogic Integration, chapter "Defining an Application View" in *Using Application Integration*
- WebLogic Integration, chapter "Using Application Views by Writing Custom Code" in *Using Application Integration*
- WebLogic Workshop, *Workshop Security Overview*