



BEA WebLogic Portal™

Security

Copyright

Copyright © 2004-2005 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, BEA WebLogic Server, 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 Enterprise Security, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic JRockit, BEA WebLogic Personalization Server, BEA WebLogic Platform, BEA WebLogic Portal, BEA WebLogic Server Process Edition, 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

WebLogic Portal Security

Overview	1
Preventing Direct Access to Portlet Resources	1

WebLogic Portal Security

Overview

This document covers various security issues related to portal application development.

For an overview of portal security and information on core security concepts, see [Securing Portal Applications](#) in the WebLogic Workshop help system.

Preventing Direct Access to Portlet Resources

When you develop portlets that use JSPs and other resources, you can control access to those portlets using visitor entitlements in the WebLogic Administration Portal.

However, if you fail to use J2EE security to also restrict access to those JSPs and other resources, a user can access those resources directly by typing the exact URL to those resources. For example:

```
http://avitek/avitekPortal/portlets/hr/vpSalaries.jsp
```

To prevent direct access to portal resources, add a security entry in your portal Web project's /WEB-INF/web.xml file. For example:

```
<!-- Use declarative security to block direct address to portlets -->
<security-constraint>
  <display-name>Default Portlet Security Constraints</display-name>
  <web-resource-collection>
    <web-resource-name>Portlet Directory</web-resource-name>
    <url-pattern>/portlets/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>Admin</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>NONE</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

This security entry in `web.xml` protects all files in the portal Web project's `/portlet` directory and subdirectories from being directly accessed by a request URL.

Entitled portlets will still display these protected resources, but only users entitled to access those portlets will see them.

Note: A `<url-pattern>` of `/portlets/*.jsp` is not legal syntax and does not protect subdirectories.

This approach, however, means that resources such as images that do not require security restrictions be stored in unsecured directories (for example, outside of the `/portlets` directory).