



Hardening and Security for LiveCycle® ES

February 2008

Adobe® LiveCycle® ES
Version 8.0

© 2008 Adobe Systems Incorporated. All rights reserved.

Adobe® LiveCycle® ES (8.0) Hardening and Security for LiveCycle ES for Microsoft® Windows®, UNIX®, and Linux
Edition 1.1, February 2008

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe Systems Incorporated. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end-user license agreement.

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Incorporated. Adobe Systems Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Please remember that existing artwork or images that you may want to include in your project may be protected under copyright law. The unauthorized incorporation of such material into your new work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.

Any references to company names, company logos and user names in sample material or sample forms included in this documentation and/or software are for demonstration purposes only and are not intended to refer to any actual organization or persons.

Adobe, the Adobe logo, Acrobat, Flash, LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

BEA WebLogic Server is a registered trademark and BEA WebLogic Platform is a trademark of BEA Systems Inc.

IBM, AIX, DB2, and WebSphere are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle is a trademark of Oracle Corporation and may be registered in certain jurisdictions.

Red Hat and JBoss are registered trademarks of Red Hat, Inc. in the United States and other countries.

Sun, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

SUSE is a trademark of Novell, Inc.

UNIX is a registered trademark of The Open Group in the US and other countries.

All other trademarks are the property of their respective owners.

This product contains either BISAFE and/or TIPEM software by RSA Data Security, Inc.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes code licensed from RSA Data Security.

This product includes software developed by the JDOM Project (<http://www.jdom.org/>).

Macromedia Flash 8 video is powered by On2 TrueMotion video technology. © 1992-2005 On2 Technologies, Inc. All Rights Reserved.
<http://www.on2.com>.

This product includes software developed by the OpenSymphony Group (<http://www.opensymphony.com/>).

Portions of this code are licensed from Nellymoser(www.nellymoser.com)

MPEG Layer-3 audio compression technology licensed by Fraunhofer IIS and THOMSON Multimedia (<http://www.iis.fhg.de/amm/>).

This product includes software developed by L2FProd.com (<http://www.L2FProd.com/>)

The JBoss library is licensed under the GNU Library General Public License, a copy of which is included with this software.

The BeanShell library is licensed under the GNU Library General Public License, a copy of which is included with this software.

This product includes software developed by The Werken Company.

This product includes software developed by the IronSmith Project (<http://www.ironsmith.org/>).

The OpenOffice.org library is licensed under the GNU Library General Public License, a copy of which is included with this software.

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Notice to U.S. Government End Users. The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users

(a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA. For U.S. Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

Contents

About This Document.....	6
Who should read this document?	6
Conventions used in this document	6
Additional information.....	7
1 General Security Considerations	8
Vendor-specific security information.....	8
Operating system security information	8
Application server security information	9
Database security information.....	9
LiveCycle ES security considerations.....	10
Email credentials not encrypted in database	10
Sensitive content for LiveCycle Rights Management ES in the database	10
Password in clear text format in adobe-ds.xml.....	11
2 Hardening Your Environment	12
Preinstallation.....	12
Network layer security.....	13
Operating system security.....	14
Installation	14
Post-installation steps.....	15
LiveCycle ES server security.....	15
Application server security	18
Using JMX Console on JBoss.....	19
Database security.....	19
Configuring integrated security on Windows.....	19
Protecting access to sensitive content in the database.....	21
LDAP security.....	21
Auditing and logging	22
Configuring LiveCycle ES for access beyond the enterprise	22
Setting up a reverse proxy for web access.....	23
Secure network configuration.....	25
LiveCycle ES physical architecture.....	25
Network protocols used by LiveCycle ES	25
Ports for application servers.....	26
Configuring SSL	28
Configuring SSL redirect.....	28
Windows-specific security recommendations.....	28
JBoss Service accounts.....	28
File system security	29
JBoss-specific security recommendations	29
Disable JBoss Management Console and JMX Console.....	29
Ensure JBoss DeploymentFilRepository class vulnerability is patched	30
Disable directory browsing	30

2 Hardening Your Environment (Continued)

WebLogic-specific security recommendations	30
Disable directory browsing	30
Enable WebLogic SSL Port.....	30
WebSphere-specific security recommendations	31
Disable directory browsing	31
Enabling WebSphere administrative security	31
Enabling JMS bus security	31
To assign group privileges to the IDP_JMS Bus.....	32

3 Configuring Secure Administration Settings 33

Disabling non-essential remote access to services.....	33
Disabling non-essential anonymous access to services.....	34
Remove sample user and role assignments	35
Changing the default global time-out.....	35
Disabling LiveCycle 7.x backwards-compatibility API access.....	35

About This Document

This document contains information about how to maximize the security of the Adobe® LiveCycle® ES (Enterprise Suite) production environment.

Additional security information for LiveCycle ES is available at <http://www.adobe.com/devnet/livecycle/security.html>.

Security advisories and bulletins for LiveCycle ES are available at <http://www.adobe.com/support/security/index.html>.

Who should read this document?

This document is intended for consultants, security specialists, systems architects, and IT professionals responsible for planning application or infrastructure development and deployment of LiveCycle ES. These roles include the following common roles:

- IT and operations' engineers who must deploy secure web applications and servers in their own or customers' organizations
- Architects and planners who are responsible for planning the architectural efforts for the clients in their organizations
- IT security specialists who focus on providing security across the platforms within their organizations
- Consultants from Adobe and partners who require detailed resources for customers and partners

Conventions used in this document

This document uses the following naming conventions for common file paths.

Name	Default value	Description
<i>[LiveCycle ES root]</i>	C:\Adobe\LiveCycle8\	The installation directory that is used for all LiveCycle ES solution components. The installation directory contains subdirectories for LiveCycle Configuration Manager, the LiveCycle ES SDK, and each LiveCycle ES solution component installed.
<i>[JBoss_ES root]</i>	The home directory of the application server that runs LiveCycle ES	C:\Adobe\LiveCycle8\jboss

Additional information

The resources in this table can help you learn about LiveCycle ES.

For information about	See
LiveCycle ES, the solution components, and the development tools	LiveCycle ES Overview
Preparing your environment for installing or upgrading to LiveCycle ES	Preparing to Install LiveCycle ES Preparing to Upgrade to LiveCycle ES
Installing LiveCycle ES	Installing and Deploying LiveCycle ES for JBoss Installing and Deploying LiveCycle ES WebSphere Installing and Deploying LiveCycle ES for WebLogic
Upgrading to LiveCycle ES using the non-turnkey method	Upgrading to LiveCycle ES for JBoss Upgrading to LiveCycle ES for WebSphere Upgrading to LiveCycle ES for WebLogic
Installing LiveCycle Workbench ES	Installing Your Development Environment
Performing general administrative tasks for LiveCycle ES	Administering LiveCycle ES
Other services and products that integrate with LiveCycle ES	www.adobe.com/products/livecycle
Patch updates, technical notes, and additional information about this product version	www.adobe.com/support/products/enterprise/index.html
LiveCycle ES terminology	LiveCycle ES Glossary

1

General Security Considerations

This section provides introductory information that helps you prepare for hardening your LiveCycle ES environment. It includes prerequisite information about LiveCycle ES, operating system, application server, and database security. You should review this information before you continue to lock down your environment.

Vendor-specific security information

This section contains security-related information about operating systems, application servers, and databases that are incorporated into your LiveCycle ES enterprise solution.

Use the links in this section to find vendor-specific security information for your operating system, database, and application server.

Operating system security information

When securing your operating system, carefully consider implementing the measures described by your operating system vendor, including these:

- Defining and controlling users, roles, and privileges
- Monitoring logs and audit trails
- Removing unnecessary services and applications
- Backing up files

For security information about operating systems that LiveCycle ES supports, see the resources in the this table.

Operating System	Security Resource
IBM AIX® 5L 5.3	http://www.ibm.com/servers/aix/overview/security.html
Microsoft® Windows® XP SP 2 (for LiveCycle Workbench ES only)	http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx
Microsoft Windows Server® 2003 Enterprise or Standard Edition	http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sqch00.mspx
Red Hat® Linux® Advanced Server 4.0	http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/
Sun™ Solaris™ 9	http://docs.sun.com/app/docs/doc/817-0365
Sun Solaris 10	http://docs.sun.com/app/docs/doc/816-4557
SUSE Linux Enterprise Server 9.0 i386	http://www.novell.com/linux/security/

Application server security information

When securing your application server, you should carefully consider implementing the measures described by your server vendor, including these:

- Using non-obvious administrator user name
- Disabling unnecessary services
- Securing the console manager
- Enabling secure cookies
- Closing unneeded ports
- Limiting clients by IP addresses or domains
- Using the Java™ SecurityManager to programmatically restrict privileges

For security information about application servers that LiveCycle ES supports, see the resources in this table.

Application Server	Security Resource
BEA Weblogic 9.2	http://e-docs.bea.com/wls/docs92/security.html
IBM WebSphere 6.1	ftp://ftp.software.ibm.com/software/webserver/appserv/library/v60/wasv600nd_security.pdf
Red Hat JBoss 4.0.3 Service Pack 1	http://wiki.jboss.org/wiki/Wiki.jsp?page=SecureJBoss

Database security information

When securing your database, you should consider implementing the measures described by your database vendor, including these:

- Restricting operations with access control lists (ACLs)
- Using non-standard ports
- Hiding the database behind a firewall
- Using input validation to prevent insertion attacks
- Encrypting sensitive data before writing it to the database

For security information about databases that LiveCycle ES supports, see the resources in this table.

Database	Security Resource
IBM DB2® 8.2 (Version 8.1 Fix Pack 7)	http://www-306.ibm.com/software/data/db2/index.html
Microsoft SQL Server 2005 SP1	http://www.microsoft.com/sql/technologies/security/default.aspx
MySQL 5	http://dev.mysql.com/doc/refman/5.0/en/security.html
Oracle® 10g	http://download-east.oracle.com/docs/cd/B19306_01/network.102/b14266/part1.htm

This table describes the default ports that are required to be open during your LiveCycle ES configuration process. If you are connecting over https, you must adjust your port information and IP addresses accordingly.

Product or service	Port number
JBoss	8080
WebLogic	7001
WebLogic Managed Server	Set by administrator during configuration
WebSphere	9060, if Global Security is enabled the default SSL port value is 9043. 9080
BAM Server	7001
SOAP	8880
MySQL	3306
Oracle	1521
DB2	50000
SQL Server	1433
LDAP	The port on which the LDAP server is running. The default port is typically 389. However, if you select the SSL option, the default port is typically 636. You must confirm with your LDAP administrator which port to specify.

LiveCycle ES security considerations

This section describes some LiveCycle ES-specific security issues that you should know about.

Email credentials not encrypted in database

The email credentials stored by LiveCycle ES applications are not encrypted before they are stored in the LiveCycle ES database. When you configure a service endpoint to use email, any password information used as part of that endpoint configuration is not encrypted when it is stored in the database.

Sensitive content for LiveCycle Rights Management ES in the database

LiveCycle ES uses the LiveCycle ES database to store sensitive document key information as well as other cryptographic material used for policy documents. Securing the database against intrusion helps to protect this sensitive information.

Password in clear text format in adobe-ds.xml

The application server used to run LiveCycle ES requires its own configuration for access to your database through a data source configured on the application server. You should ensure that your application server does not expose your database password in clear text in its data source configuration file.

The adobe-ds.xml file contains passwords in clear text format. Consult with your application server vendor on how to encrypt these passwords for your application server. For example, you can find the JBoss® instructions at <http://wiki.jboss.org/wiki/Wiki.jsp?page=EncryptingDataSourcePasswords>.

IBM® WebSphere® Application Server and BEA WebLogic Server® may encrypt data source passwords by default. However, you should confirm with your application server documentation to ensure that this is happening.

2

Hardening Your Environment

This section describes recommendations and best practices for securing servers that run LiveCycle ES. This is not a comprehensive host-hardening document for your operating system and application server. Instead, this section describes a variety of security-hardening settings that you should implement to enhance the security of LiveCycle ES that is running within a corporate intranet. To ensure that the LiveCycle ES application servers stay secure, however, you should also implement security monitoring, detection, and response procedures.

This section describes hardening techniques that should be applied during the following stages during the installation and configuration life cycle:

Preinstallation: Use these techniques before you install the LiveCycle ES software.

Installation: Use these techniques during the LiveCycle ES software installation process.

Post-installation: Use these techniques after installation and periodically thereafter.

LiveCycle ES is highly customizable and can work in many different environments. Some of the recommendations may not fit your organization's needs.

Preinstallation

Before installing LiveCycle ES, you can apply security solutions to the network layer and operating system. This section describes some issues and makes recommendations for reducing security vulnerabilities in these areas.

Installation and configuration on UNIX and Linux

You should not install or configure LiveCycle ES using a root shell. By default, files are installed under the /opt directory, and the user performing the install needs all file permissions under /opt. Alternatively, an installation can be performed under an individual user's /user directory where they already have all file permissions.

Installation and Configuration on Windows

You should perform the installation on Windows as an administrator if you are installing LiveCycle ES on JBoss using the turnkey method or if you are installing LiveCycle PDF Generator ES. Furthermore, when installing PDF Generator ES on Windows with native application support, you must run the installation as the same Windows user who installed Microsoft Office.

Network layer security

Network security vulnerabilities are among the first threats to any Internet- or intranet-facing application server. This section describes the process of hardening hosts on the network against these vulnerabilities. It addresses network segmentation, Transmission Control Protocol/Internet Protocol (TCP/IP) stack hardening, and the use of firewalls for host protection.

The following table describes common processes that reduce network security vulnerabilities.

Issue	Description
Demilitarized zones (DMZs)	Deploy LiveCycle ES servers within a demilitarized zone (DMZ). Segmentation should exist in at least two levels with the application server used to run LiveCycle ES placed behind the inner firewall. Separate the external network from the DMZ that contains the web servers, which in turn must be separated from the internal network. Use firewalls to implement the layers of separation. Categorize and control the traffic that passes through each network layer to ensure that only the absolute minimum of required data is allowed.
Private IP addresses	Use Network Address Translation (NAT) with RFC 1918 private IP addresses on LiveCycle ES application servers. Assign private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) to make it more difficult for an attacker to route traffic to and from a NAT'd internal host through the Internet.
Firewalls	Use the following criteria to select a firewall solution: <ul style="list-style-type: none">● Implement firewalls that support proxy servers and/or “stateful inspection” instead of simple packet-filtering solutions.● Use a firewall that supports a “deny all services except those explicitly permitted” security paradigm.● Implement a firewall solution that is dual-homed or multihomed. This architecture provides the greatest level of security and helps to prevent unauthorized users from bypassing the firewall security.
Database ports	Do not use default listening ports for databases (MySQL - 3306, Oracle - 1521, MS SQL - 1433). For information about changing database ports, see your database documentation. Caution: Using a different database port affects the overall LiveCycle ES configuration. If you change default ports, you must make corresponding modifications in other areas of configuration, such as the data sources for LiveCycle ES. For information about configuring data sources in LiveCycle ES, see <i>Installing and Deploying LiveCycle ES</i> or <i>Upgrading to LiveCycle ES</i> for your application server, at www.adobe.com/go/learn_lc_documentation .

Operating system security

The following table describes some potential approaches to minimizing security vulnerabilities found in the operating system.

Issue	Description
Security patches	<p>There is an increased risk that an unauthorized user may gain access to the application server if vendor security patches and upgrades are not applied in a timely fashion. Test security patches before you apply them to production servers.</p> <p>Also, create policies and procedures to check for and install patches on a regular basis.</p>
Virus protection software	<p>Virus scanners can identify infected files by scanning for a signature or watching for unusual behavior. Scanners keep their virus signatures in a file, which is usually stored on the local hard drive. Because new viruses are discovered often, you should frequently update this file for the virus scanner to identify all current viruses.</p>
Network Time Protocol (NTP)	<p>For forensic analysis, keep accurate time on LiveCycle ES servers. Use NTP to synchronize the time on all systems that are connected directly to the Internet.</p>

For additional security information for your operating system, see [“Operating system security” on page 14](#).

Installation

This section describes techniques you can use during the LiveCycle ES installation process to reduce security vulnerabilities. In some cases, these techniques use options that are part of the installation process. The following table describes these techniques.

Issue	Description
Privileges	<p>Use the least amount of privileges necessary to install the software. Log in to your computer using an account that is not in the Administrators group. On Windows, you can use the Run As command to run the LiveCycle ES installer as a non-administrative user. On UNIX and Linux systems, use a command such as <code>sudo</code> to install the software.</p>
Software source	<p>Do not download or run LiveCycle ES from untrusted sources.</p> <p>Malicious programs can contain code to violate security in several ways, including data theft, modification and deletion, and denial of service. Install LiveCycle ES from the Adobe DVD or only from a trusted source.</p>
Disk partitions	<p>Place LiveCycle ES on a dedicated disk partition. Disk segmentation is a process that keeps specific data on your server on separate physical disks for added security. Arranging data in this way reduces the risk of directory traversal attacks. Plan to create a partition that is separate from the system partition on which you can install the LiveCycle ES content directory. (On Windows, the system partition contains the system32 directory, or boot partition.)</p>

Issue	Description
Components	<p>Evaluate existing services and disable or uninstall any that are not required. Do not install unnecessary components and services.</p> <p>The default installation of an application server might include services that are not necessary for your use. You should disable all unnecessary services prior to deployment to minimize points of entry for an attack. For example, on JBoss, you can comment out unnecessary services in the META-INF/jboss-service.xml descriptor file.</p>
Backward compatibility	Do not enable LiveCycle 7.x backward compatibility if it is not required for your deployment.

Post-installation steps

After you have successfully installed LiveCycle ES, it is important to periodically maintain the environment from a security perspective.

The following section describes in detail the different tasks recommended to secure the deployed LiveCycle ES server.

LiveCycle ES server security

The following recommended settings apply to the LiveCycle ES server outside of the administrative web application (cfide\administrator). To reduce the security risks to the server, apply these setting immediately after installing LiveCycle ES.

Security patches

There is an increased risk that an unauthorized user might gain access to the application server if vendor security patches and upgrades are not applied in a timely fashion. Test security patches before you apply them to production servers to ensure compatibility and availability of LiveCycle ES applications. In addition, create policies and procedures to check for and install patches on a regular basis. LiveCycle ES updates are at http://www.adobe.com/support/products/enterprise/support_downloads.html.

Service accounts (Windows only)

LiveCycle ES installs a service account by default using the LocalSystem account. The built-in LocalSystem user account has a high level of accessibility; it is part of the Administrators group. If a worker-process identity runs as the LocalSystem user account, that worker process has full access to the entire system.

To run the application server on which LiveCycle ES is deployed, using a specific non-administrative account, follow these instructions:

1. In the Microsoft Management Console (MMC), create a local user for the LiveCycle ES service to log in as:
 - Select the **User cannot change password** option.
 - On the **Member Of** tab, ensure that the **Users** group is listed.
2. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
3. Double-click the LiveCycle 8 Application Server service and stop the service.

4. On the **Log On** tab, select **This Account** and browse for the user account you created. Enter the password for the account you created.
5. In the MMC, open Local Security Settings and select Local Policies > User Rights Assignment.
6. Assign the following rights to the user account that LiveCycle ES server is running under:
 - Deny log on through Terminal Services.
 - Deny log on locally.
 - Log on as Service (should be already set).
7. Give the new user account the Read & Execute, List Folder Contents, and Read permissions for the LiveCycle ES web content directories item.
8. Start the LiveCycle 8 Application Server service.

Disabling the LiveCycle Configuration Manager bootstrap servlet

LiveCycle Configuration Manager made use of a servlet deployed on your application server to perform bootstrapping of the LiveCycle ES database. Because LiveCycle Configuration Manager accesses this servlet before configuration is complete, access to it has not been secured for authorized users, and it should be disabled after you have successfully used LiveCycle Configuration Manager to configure LiveCycle ES.

1. Unzip the adobe-livecycle-[appserver].ear file.
2. Open the META-INF/application.xml file.
3. Search for the adobe-bootstrapper.war section:

```
<!-- bootstrapper start -->
<module id="WebApp_adobe_bootstrapper">
  <web>
    <web-uri>adobe-bootstrapper.war</web-uri>
    <context-root>/adobe-bootstrapper</context-root>
  </web>
</module>
<module id="WebApp_adobe_lcm_bootstrapper_redirector">
  <web>
    <web-uri>adobe-lcm-bootstrapper-redirector.war</web-uri>
    <context-root>/adobe-lcm-bootstrapper</context-root>
  </web>
</module>
<!-- bootstrapper end-->
```

4. Comment out the adobe-bootstrapper.war and the adobe-lcm-bootstrapper-redirectory.war modules as follows:

```
<!-- bootstrapper start -->
<!--
<module id="WebApp_adobe_bootstrapper">
  <web>
    <web-uri>adobe-bootstrapper.war</web-uri>
    <context-root>/adobe-bootstrapper</context-root>
  </web>
</module>
```

```
<module id="WebApp_adobe_lcm_bootstrapper_redirector">
  <web>
    <web-uri>adobe-lcm-bootstrapper-redirector.war</web-uri>
    <context-root>/adobe-lcm-bootstrapper</context-root>
  </web>
</module>
-->
<!-- bootstrapper end-->
```

5. Save and close the META-INF/application.xml file.
6. Zip the EAR file and redeploy it to the application server.
7. Test the change typing the URL in a browser and ensure that it no longer works.

Lockdown remote access to the Trust Store

LiveCycle Configuration Manager lets you upload a LiveCycle Rights Management ES Rights credential to the LiveCycle ES trust store. This means that access to the Trust Store Credential Service over remote protocols (SOAP and EJB) has been enabled by default. This access is no longer necessary after you have uploaded the Rights credential using LiveCycle Configuration Manager or if you decide to use LiveCycle Administration Console later to manage credentials.

You can disable remote access to all of the Trust Store services by following the steps in the section [“Disabling non-essential remote access to services” on page 33](#).

Disable all non-essential anonymous access

Some LiveCycle ES services have operations that may be invoked by an anonymous caller. If anonymous access to these services is not required, disable it by following the steps in [“Disabling non-essential anonymous access to services” on page 34](#).

Change the administrator password

When LiveCycle ES is installed, a single default user account is configured for user Super Administrator/login-id Administrator with a default password of *password*. You should immediately change this password using the LiveCycle Configuration Manager.

► To change the default administrator password:

1. Type the following URL in a web browser:

```
http:// [host name] : [port] /adminui
```

The default port number is one of these:

JBoss: 8080

WebLogic Server: 7001

WebSphere: 9080.

2. In the **User Name** field, type administrator and, in the **Password** field, type password.
3. Click **Settings > User Management > Users and Groups > Edit User**.
4. Change the password on the Edit User page.

Application server security

The following table describes some techniques for securing your application server after the LiveCycle ES application has been installed.

Issue	Description
Application server administrative console	After you have installed, configured, and deployed LiveCycle ES on your application server, you should disable access to the application server administrative consoles. Consult your application server documentation for details.
Application server cookie settings	Application cookies are controlled by the application server. When deploying the application, the application server administrator can specify cookie preferences on a server-wide or application-specific basis. By default, the server settings take preference. You can restrict cookies to be sent using HTTPS-only. As a result, they are not sent unencrypted over HTTP. Application server administrators should enable secure cookies for the server on a global basis. For example, when using the JBoss Application Server, you can modify the connector element to <code>secure=true</code> in the <code>server.xml</code> file. Consult your application server documentation for further details.
Directory browsing	<p>When someone requests a page that does not exist or requests the name of a director (the request string ends with a forward slash (/)), the application server should not return the contents of that directory. To prevent this, you can disable directory browsing on your application server. You should do this for the LiveCycle Administration Console application as well as other applications running on your server.</p> <p>For JBoss, set the value of the <code>listings</code> initialization parameter of the <code>DefaultServlet</code> property to <code>false</code> in the <code>web.xml</code> file, as shown by this example:</p> <pre data-bbox="722 1297 1449 1640"> <servlet> <servlet-name>default</servlet-name> <servlet-class> org.apache.catalina.servlets.DefaultServlet </servlet-class> <init-param> <param-name>listings</param-name> <param-value>>false</param-value> </init-param> <load-on-startup>1</load-on-startup> </servlet> </pre> <p>For WebSphere, set the <code>directoryBrowsingEnabled</code> property in the <code>ibm-web-ext.xmi</code> file to <code>false</code>.</p> <p>For WebLogic, set the <code>index-directories</code> properties in the <code>weblogic.xml</code> file to <code>false</code>, as shown by this example:</p> <pre data-bbox="722 1818 1222 1938"> <container-descriptor> <index-directory-enabled>>false </index-directory-enabled> </container-descriptor> </pre>

Using JMX Console on JBoss

When the Java Management Extensions (JMX) console is installed with JBoss, URLs can be constructed for use as cross-site scripting (XSS) exploits that can reveal sensitive information about your system.

If you installed LiveCycle ES using the turnkey method and are using the version of JBoss that was included with the turnkey installation, the JBoss JMX Console is removed by default to ensure that security risks are minimized. However, if you need to use the JBoss JMX Console, reinstall it by following these steps.

► To enable JBoss JMX Console:

1. Download a copy of JBoss 4.0.3SP1 (or later) from this site:
http://sourceforge.net/project/showfiles.php?group_id=22866&package_id=16942&release_id=365509
2. Stop the JBoss Application Server.
3. From the zipped archive file you downloaded, extract the files from `jboss-4.0.3SP1/server/all/deploy/jmx-console.war/`.
4. Place the `jmx-console.war/...` files in the `[LiveCycleES root]/jboss/server/all/deploy` directory.
5. Restart JBoss.
6. Go to the following URL to ensure that the JBoss JMX Console is available:
`http://localhost:8080/jmx-console`.

Database security

When securing your database, you should implement the measures described by your database vendor. You should allocate a database user with the minimum required database permissions granted for use by LiveCycle ES. For example, do not use an account with database administrator privileges.

On Oracle, the database account that you use needs only the CONNECT, RESOURCE, and CREATE VIEW privileges. For similar requirements on other databases see [Preparing to Install LiveCycle ES](#).

Configuring integrated security on Windows

This section applies to SQL Server database and LiveCycle ES running on a Windows Server.

On WebSphere, you can configure integrated security only when you use an external SQL Server JDBC driver, not the SQL Server JDBC driver that is embedded with WebSphere.

► To use integrated security to make a trusted connection with SQL Server:

1. Modify `[JBoss_HOME]\server\all\deploy\adobe-ds.xml` to add `integratedSecurity=true` to the connection URL, as shown in this example:

```
jdbc:sqlserver://<serverhost>:<port>;databaseName=<dbname>;integratedSecurity=true
```

2. Add the `sqljdbc_auth.dll` file to the Windows systems path on the computer that is running the application server. The `sqljdbc_auth.dll` file is located with the Microsoft SQL JDBC 1.1 driver installation (the default is `<InstallDir>/sqljdbc_1.1/enu/auth/x86`).

3. Modify JBoss Windows service (JBoss for Adobe LiveCycle ES v8.0) property for Log On As from Local System to a good login account. If you are running JBoss from the command line instead of as a Windows service, you do not need to perform this step.
 4. Set Security for SQL Server from **Mixed** mode to **Windows Authentication only**.
- **To use integrated security to make a trusted connection with SQL Server from WebLogic:**
1. Start the WebLogic Server Administration Console by typing `http://[hostname]:7001/console` in the URL line of a web browser.
 2. Under Change Center, click **Lock & Edit**.
 3. Under Domain Structure, click **[base_domain] > Services > JDBC > Data Sources** and, in the right pane, click **IDP_DS**.
 4. On the next screen, on the **Configuration** tab, click the **Connection Pool** tab and, in the **Properties** box, type `integratedSecurity=true`.
 5. Under Domain Structure, click **[base_domain] > Services > JDBC > Data Sources** and, in the right pane, click **RM_DS**.
 6. On the next screen, on the **Configuration** tab, click the **Connection Pool** tab and, in the **Properties** box, type `integratedSecurity=true`.
 7. Add the `sqljdbc_auth.dll` file to the Windows systems path on the computer that is running the application server. The `sqljdbc_auth.dll` file is located with the Microsoft SQL JDBC 1.1 driver installation (the default is `<InstallDir>/sqljdbc_1.1/enu/auth/x86`).
 8. Set Security for SQL Server from **Mixed** mode to **Windows Authentication only**.
- **To use integrated security to make a trusted connection with SQL Server from WebSphere:**
1. Log in to the WebSphere Administrative Console.
 2. In the navigation tree, click **Resources > JDBC > Data Sources** and, in the right pane, click **IDP_DS**.
 3. In the right pane, under Additional Properties, click **Custom Properties**, and then click **New**.
 4. In the **Name** box, type `integratedSecurity` and, in the **Value** box, type `true`.
 5. In the navigation tree, click **Resources > JDBC > Data Sources** and, in the right pane, click **RM_DS**.
 6. In the right pane, under Additional Properties, click **Custom Properties**, and then click **New**.
 7. In the **Name** box, type `integratedSecurity` and, in the **Value** box, type `true`.
 8. On the computer where WebSphere is installed, add the `sqljdbc_auth.dll` file to the Windows systems path (C:\Windows). The `sqljdbc_auth.dll` file is in the same location as the Microsoft SQL JDBC 1.1 driver installation (default is `[InstallDir]/sqljdbc_1.1/enu/auth/x86`).
 9. Select **Start > Control Panel > Services**, right-click the Windows service for WebSphere (IBM WebSphere Application Server V6.1 - <node>) and select **Properties**.

10. In the Properties dialog box, click the **Log On** tab.
11. Select **This Account** and provide the information required to set the login account you want to use.
12. Set Security on SQL Server from **Mixed** mode to **Windows Authentication only**.

Protecting access to sensitive content in the database

The LiveCycle ES database schema contains sensitive information about system configuration and business processes. The database needs to be considered within the same trust boundary as the LiveCycle ES server. To guard against information disclosure and theft of business data, the database must be configured by the DBA to allow access by authorized administrators.

As an added precaution, you should consider using database vendor-specific tools to encrypt columns in tables containing the following data: Rights Management ES Document Keys, Trust Store HSM PIN encryption key and Local User Password Hashes.

For information about vendor-specific tools, see [“Database security information” on page 9](#).

LDAP security

A Lightweight Directory Access Protocol (LDAP) directory is typically used by LiveCycle ES as a source for enterprise user and group information, and a means to perform password authentication. You should ensure that your LDAP directory is configured to use Secure Socket Layer (SSL) and that LiveCycle ES is configured to access your LDAP directory using its SSL port.

LDAP denial of service

A common attack using LDAP involves an attacker deliberately failing to authenticate multiple times. This forces the LDAP Directory Server to lock out a user from all LDAP-reliant services.

You can set the number of failure attempts and subsequent lock-out time that LiveCycle ES implements when a users repeatedly fails to authenticate to LiveCycle ES. In the LiveCycle Administration Console, choose low values; for example, if you set the LiveCycle ES value to three authentication failures, LiveCycle ES locks out the user before the LDAP Directory Server does.

► To set automatic account locking settings:

1. Log in to LiveCycle Administration Console.
2. Click **Settings > User Management > Domain Management**.
3. Under Automatic Account Locking Settings, set **Maximum Consecutive Authentication Failures** to a low number, such as 3.
4. Click **Save**.

Auditing and logging

The proper and secure use of application auditing and logging can help ensure that security and other anomalous events are tracked and detected as quickly as possible. Effective use of auditing and logging within an application includes such items as tracking successful and failed logins, as well as key application events such as the creation or deletion of key records.

You can use auditing to detect many types of attacks, including these:

- Brute force password attacks
- Denial of service attacks
- Injection of hostile input and related classes of scripting attacks

This table describes auditing and logging techniques you can use to reduce your server's vulnerabilities.

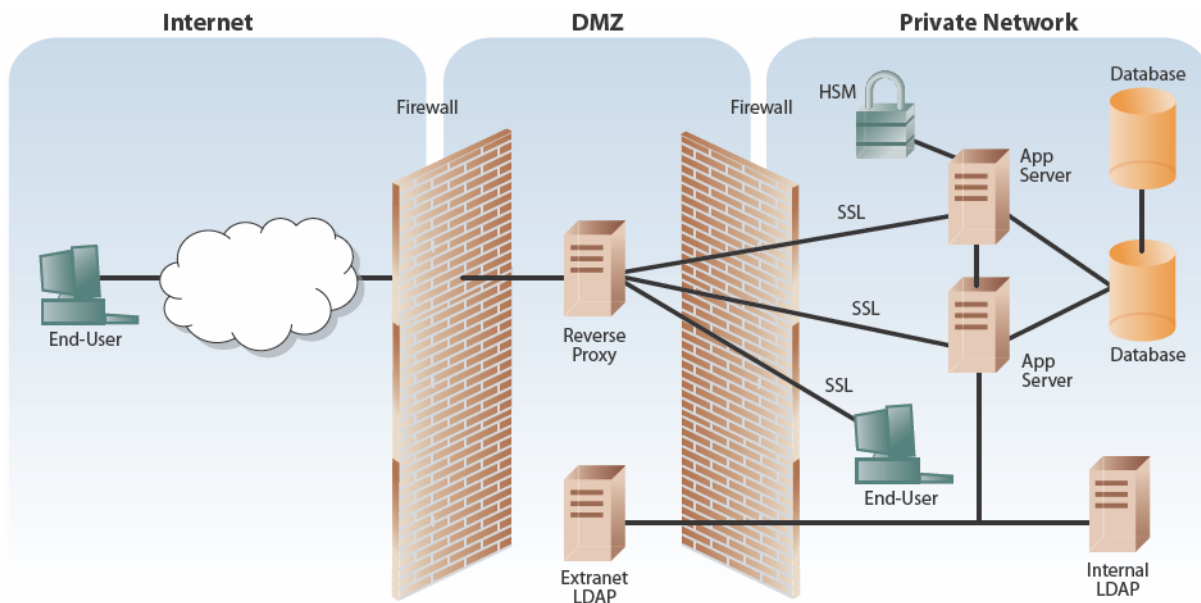
Issue	Description
Logging events	<p>Create logging event sources during deployment, not programmatically through application code.</p> <p>Creating an event source requires administrative privileges. Do not grant these privileges to a running application process. Instead, in the deployment procedure of an application, document a stand-alone script that is necessary to create the new event sources. An administrator executes this script once. When the event source is created, the script is no longer necessary; remove it from the system.</p>
Log file ACLs	<p>Set appropriate LiveCycle ES log file access control lists (ACLs).</p> <p>Setting the appropriate credentials helps prevent attackers from deleting the files.</p> <p>The security permissions on the log file directory should be Full Control for Administrators and SYSTEM groups. The LiveCycle ES user account should have Read and Write permissions only.</p>
Log file redundancy	<p>If resources permit, send logs to another server in real time that is not accessible by the attacker (write only) by using Syslog, Tivoli, Microsoft Operations Manager (MOM) Server, or some other mechanism.</p> <p>Protecting logs this way helps prevent tampering. In addition, storing logs in a central repository aids in correlation and monitoring (for example, if multiple LiveCycle ES servers are in use and a password-guessing attack is taking place across multiple computers where each computer is queried for a password).</p>

Configuring LiveCycle ES for access beyond the enterprise

After you have successfully installed LiveCycle ES, it is important to periodically maintain the security of your environment. This section describes the tasks recommended to maintain the security of your LiveCycle ES production server.

Setting up a reverse proxy for web access

A *reverse proxy* can be used to ensure that one set of URLs for LiveCycle ES web applications are available to both external and internal users. This configuration is more secure than allowing users to connect directly to the application server on which LiveCycle ES is running. The reverse proxy performs all HTTP requests for the application server running LiveCycle ES. Users only have network access to the reverse proxy and can only attempt URL connections that are supported by the reverse proxy.



LiveCycle ES root URLs for use with reverse proxy server

The following application root URLs for each LiveCycle ES web application. You should configure your reverse proxy only to expose URLs for web application functionality that you want to provide to end users.

Certain URLs are highlighted as end-user-facing web applications. You should avoid exposing other URLs for LiveCycle Configuration Manager for access to external users through the reverse proxy.

Root URL	Purpose and/or associated web application	Web-based interface	End-user access
/ReaderExtensions/*	LiveCycle Reader Extensions ES end-user web application for applying usage rights to PDF documents	Yes	Yes
/edc/*	LiveCycle Rights Management ES end-user web application	Yes	Yes
/pdfg-adminui/*	LiveCycle PDF Generator ES administration web application	Yes	Yes
/workspace/*	LiveCycle Workspace ES end-user web application	Yes	Yes
/workspace-server/*	LiveCycle Workspace ES servlets and data services that the Workspace ES client application requires	Yes	Yes

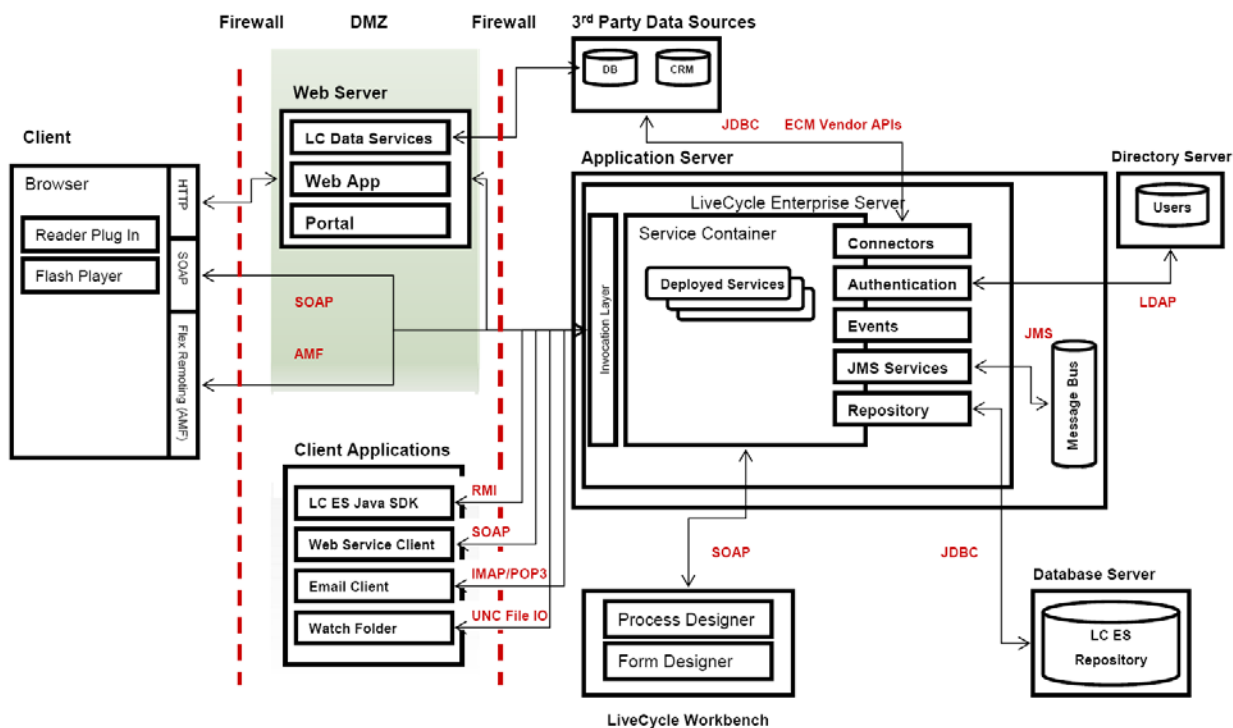
Root URL	Purpose and/or associated web application	Web-based interface	End-user access
/adobe-bootstrapper/*	Servlet for bootstrapping the LiveCycle ES repository	No	No
/adobe-lcm-bootstrapper/*	Redirect to bootstrap servlet/redirects LiveCycle 7.x style bootstrap requests to /adobebootstrapper/	No	No
/soap/*	Information page for LiveCycle ES web services	No	No
/soap/services/*	Web service URL for all LiveCycle ES services	No	No
/edc/admin/*	LiveCycle Rights Management ES administration web application	Yes	No
/adminui/*	LiveCycle Administration Console home page	Yes	No
/TruststoreComponent/secured/*	Trust Store Management administration pages	Yes	No
/FormsIVS/*	Forms IVS application for testing and debug of form rendering	Yes	No
/OutputIVS/adminui/secured/admin/*	Output ES IVS administration pages for fetching images in HTML	Yes	No
/OutputAdmin/*	LiveCycle Output ES administration pages	Yes	No
/FormServer/*	LiveCycle Forms ES web application files	Yes	No
/FormServer/GetImageServlet	Used for fetching JavaScript™ during HTML transformation	No	No
/FormServerAdmin/*	LiveCycle Forms ES administration pages	Yes	No
/repository/*	URL for WebDAV (debugging) access	Yes	No
/appstore/Forms/*	Compatibility: Redirect to repository WebDAV implementation for clients of LiveCycle Form Manager 7.x WebDAV	No	No
/AACComponent/*	Archive Administration user interface	Yes	No
/WorkspaceAdmin/*	LiveCycle Workspace ES administration pages	Yes	No
/WorkflowAdmin/*	LiveCycle Process Management ES administration pages	Yes	No
/CoreSystemConfig/*	LiveCycle ES Core Configuration settings page	Yes	No
/um/*	User Management administration interface	Yes	No

Secure network configuration

This section describes the protocols and ports required by LiveCycle ES and provides recommendations for deploying LiveCycle ES in a secure network configuration.

LiveCycle ES physical architecture

This illustration shows the components and protocols used in a typical LiveCycle ES deployment, including the appropriate firewall topology.



Network protocols used by LiveCycle ES

When you configure a secure network architecture as described in the previous section, the following network protocols are required for interaction between LiveCycle ES and other systems in your enterprise network.

Protocol	Use
HTTP	<ul style="list-style-type: none"> Browser displays LiveCycle Configuration Manager and end-user web applications All SOAP connections
SOAP	<ul style="list-style-type: none"> Web service client applications, such as .NET applications Adobe Reader® uses SOAP for LiveCycle ES web services Adobe Flash® applications uses SOAP for LiveCycle ES web services LiveCycle ES SDK calls when used in SOAP mode Workbench ES design environment

Protocol	Use
RMI	LiveCycle ES SDK calls when used in Enterprise JavaBeans™ (EJB) mode
IIOp	LiveCycle 7.x applications (PDF Manipulation Module APIs) calling LiveCycle ES services through the CORBA Backwards Compatibility Layer.
IMAP / POP3	<ul style="list-style-type: none"> • Email-based input to a service (Email endpoint) • User task notifications over email
UNC File IO	LiveCycle ES monitoring of watched folders for input to a service (watched folder endpoint)
JMS	Application server job system used by LiveCycle ES for asynchronous processing
LDAP	<ul style="list-style-type: none"> • Synchronizations of organizational user and group information in a directory • LDAP authentication for interactive users
JDBC	<ul style="list-style-type: none"> • Query and procedure calls made to an external database during execution of a process using the JDBC service • Internal access LiveCycle ES repository.
WebDAV	Enables remote browsing of the LiveCycle ES design-time repository (forms, fragments, and so on) by any WebDAV client
AMF	Flash applications, where LiveCycle ES services are configured with a Remoting endpoint
JMX	LiveCycle ES exposes MBeans for monitoring using JMX

Ports for application servers

This section describes the default ports (and alternate configuration ranges) for each type of application server supported. These ports must be enabled or disabled on the inner firewall, depending on the network functionality you want to allow for clients that connect to the application server running LiveCycle ES.

Note: By default, the server exposes several JMX MBeans under the adobe.com namespace. Only information useful for server health monitoring is exposed. However, to prevent information disclosure, you should prevent callers in an untrusted network from looking up JMX MBeans and accessing health metrics.

JBoss ports

Purpose	Port
Access to web applications	<p>[JBoss root]/server/all/deploy/jbossweb-tomcat50.sar/server.xml</p> <p>HTTP/1.1 Connector port 8080</p> <p>AJP 1.3 Connector port 8009</p> <p>SSL/TLS Connector port 8443</p>

Purpose	Port
Access to LiveCycle ES services	<p>[JBoss root]/server/all/conf/jboss-service.xml</p> <p>WebService port 8083</p> <p>NamingService Port 1099</p> <p>RMIport from 1098</p> <p>RMIObjectPort from 4444</p> <p>PooledInvoker ServerBindPort 4445</p>
J2EE cluster support	<p>[JBoss root]/server/all/deploy/cluster-service.xml</p> <p>ha.jndi.HANamingService port from 1100</p> <p>RmiPort 1101</p> <p>RMIObjectPort 4447</p> <p>(clusters only) ServerBindPort 4446</p>
Access to JMS queues	<p>[JBoss root]/server/all/deploy/jms\hajndi-jms-ds.xml</p> <p>java.naming.provider.url port 1100</p> <p>[JBoss root]/server/all/deploy-hasingleton/jms/ui2-service.xml</p> <p>ServerBindPort 8093</p>
CORBA support	<p>[JBoss root]/server/all/conf/jacorb.properties</p> <p>OAPort 3528</p> <p>OASSLPort 3529</p>
SNMP support	<p>[JBoss root]/server/all/deploy/snmp-adaptor.sar/META-INF/jbosservice.xml</p> <p>ports 1161, 1162</p> <p>[JBoss root]/server/all/deploy/snmp-adaptor.sar/managers.xml</p> <p>port 1162</p>

WebLogic 9.2 ports

Purpose	Port
Access to web applications	<ul style="list-style-type: none"> Admin Server listen port: default is 7001 Admin Server SSL listen port: default is 7002
WebLogic administration ports not required for access to LiveCycle ES	<ul style="list-style-type: none"> Managed Server listen port: Configurable from 1 to 65534 Managed Server SSL listen port: Configurable from 1 to 65534 Node Manager listen port: default is 5556

WebSphere 6.1 ports

For information about WebSphere ports required by LiveCycle ES, go to http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/rmig_portnumber.html.

Configuring SSL

Referring to the physical architecture described in the section [“LiveCycle ES physical architecture” on page 25](#), you should configure SSL for all of the connections that you plan to use. Specifically, all SOAP connections must be conducted over SSL to prevent exposure of user credentials on a network.

For instructions on how to configure SSL on JBoss, WebLogic, and WebSphere, see [Administering LiveCycle ES](#).

Configuring SSL redirect

After configuring your application server to support SSL, you must ensure that all HTTP traffic to LiveCycle ES applications and services are enforced to use the SSL port.

► To configure SSL redirect for JBoss:

1. Navigate to the adobe-livecycle-jboss.ear and unzip it.
2. Extract the adminui.war file and open the web.xml file for editing.
3. Add the following code to the web.xml file:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>app or resource name</web-resource-name>
    <url-pattern>/*</url-pattern>
    <!-- define all url patterns that need to be protected-->
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

► To configure SSL redirect for WebSphere:

See the documentation for the WebSphere Application Server.

► To configure SSL redirect for WebLogic:

See the documentation for the WebLogic Server.

Windows-specific security recommendations

JBoss Service accounts

The LiveCycle ES turnkey installation sets up a service account, by default, using the Local System account. The built-in Local System user account has a high level of accessibility; it is part of the Administrators group. If a worker process identity runs as the Local System user account, that worker process has full access to the entire system.

► **To run the LiveCycle ES application server using a specific non-administrative account:**

1. In the Microsoft Management Console (MMC), create a local user for the LiveCycle ES service to log in as:
 - Select **User cannot change password**.
 - On the **Member Of** tab, ensure that the Users group is listed.
2. Select **Settings > Control Panel > Administrative Tools > Services**.
3. Double-click the LiveCycle 8 Application Server service and stop the service.
4. On the **Log On** tab, select **This Account** and browse for the user account you created. Enter the password for the account you created.
5. In the Local Security Settings window, under User Rights Assignment, give the following rights to the user account that LiveCycle ES server is running under:
 - Deny log on through Terminal Services
 - Deny log on locally
 - Log on as Service (should be already set)
6. Give the new user account Read & Execute, List Folder Contents, and Read permissions to LiveCycle ESweb content directories.
7. Start the LiveCycle 8 Application Server service.

File system security

LiveCycle ES makes use of the file system in the following ways:

- Temporary files used while processing document input & output
- A global archive store with files used to support the solution components installed
- Watched folders (if configured) for dropping files used as input to a service from a file system folder location

When using watched folders as a way to send and receive documents with a LiveCycle ES service, you should take extra precautions with file system security. When a user drops content in the watched folder, that content is exposed through the watched folder. In this case, the service does not authenticate the actual end user. Instead, it relies ACL and Share level security to be set at the folder level to determine who can effectively invoke the service.

JBoss-specific security recommendations

This section contains application server configuration recommendations that are specific to JBoss 4.0 when used to run LiveCycle ES.

Disable JBoss Management Console and JMX Console

Access to the JBoss Management Console and JMX Console is already configured (JMX monitoring is disabled) when you install LiveCycle ES on JBoss using the turnkey installation method. If you are using your own JBoss Application Server, you should ensure that access to the JBoss Management Console and JMX monitoring console are secured. Access to the JMX monitoring console is set in the JBoss configuration file, `jmx-invoker-service.xml`.

Ensure JBoss DeploymentFileRepository class vulnerability is patched

A known security vulnerability exists in the `DeploymentFileRepository` class of the JBoss Application Server. A remote attacker who can access the Management Console could read or write to files with the permissions of the JBoss AS user, which could potentially lead to arbitrary code execution as the JBoss AS user.

The JBoss Application Server console manager should always be secured prior to deployment, as directed in the JBoss Application Server guide. By default, using the JBoss installer, users can password-protect the Management Console, limiting an attack that exploits this vulnerability to authorized users. These steps can also be performed manually. (See <http://wiki.jboss.org/wiki/Wiki.jsp?page=SecureJBoss>.)

This vulnerability affects all JBoss releases from version 3.2.4 to version 4.0.5. To fix this vulnerability, go to <http://jira.jboss.com/jira/browse/JBAS-3861>.

Disable directory browsing

Set the value of the listings initialization parameter of the `DefaultServlet` property to `false` in the `web.xml` file. For example:

```
<servlet>
  <servlet-name>default</servlet-name>
  <servlet-class>
    org.apache.catalina.servlets.DefaultServlet
  </servlet-class>
  <init-param>
    <param-name>listings</param-name>
    <param-value>false</param-value>
  </init-param>
  <load-on-startup>1</load-on-startup>
</servlet>]
```

WebLogic-specific security recommendations

This section contains application server configuration recommendations for securing WebLogic 9.1 when running LiveCycle ES.

Disable directory browsing

Set the `index-directories` properties in the `weblogic.xml` file to `false`, as shown by this example:

```
<container-descriptor>
  <index-directory-enabled>false
</index-directory-enabled>
</container-descriptor>
```

Enable WebLogic SSL Port

By default, WebLogic does not enable the default SSL Listen Port, 7002. Enable this port in the WebLogic Administration Console before configuring SSL.

WebSphere-specific security recommendations

This section contains application server configuration recommendations for securing WebSphere 6.1 running LiveCycle ES

Disable directory browsing

Set the `directoryBrowsingEnabled` property in the `ibm-web-ext.xml` file to `false`.

Enabling WebSphere administrative security

► **To enable WebSphere administrative security:**

1. Log in to the WebSphere Administrative Console.
2. In the navigation tree, click **Security > Secure administration, applications, and infrastructure**.
3. Select **Enable administrative security**.
4. Deselect both **Enable application security** and **Use Java 2 security**.
5. Click **OK** or **Apply**.
6. In the **Messages** box, click **Save directly to the master configuration**.

Enabling JMS bus security

Before installing LiveCycle ES, you must enable Java Message Service (JMS) bus security in WebSphere.

► **To create a JAAS to J2C authentication for JMS:**

1. Access the WebSphere Administrative Console.
2. In the navigation tree, click **Security > Secure administration, applications and infrastructure**.
3. Under Authentication click **Java Authentication and Authorization Service > J2C authentication data**.
4. Click **New** to add a new J2C authentication data and, under General Properties, provide the required information:
 - A new alias (for example, `lc_jms`)
 - A user ID (for example, `lc_jms`)
 - A password for the user ID
5. Click **OK**.

► **To create a group:**

1. In the navigation tree, click **Users and Groups > Manage Groups**, and then click **Create**.
2. In the **Group Name** box, type `lc_jms_group`.
3. Click **Create**.

► **To create a user:**

1. In the navigation tree, click **Users and Groups > Manage Users**.
2. Click **Create**.
3. Click **Group Membership**.
4. Click **Search**, and then select the group name `lc_jms_group`.
5. Click **Close**.
6. In the **User ID** box, type the first name and last name for *[JAAS authentication name]*.
7. Type the password for the *[JAAS authentication name]*.
8. Click **Create**.

► **To associate security:**

1. In the navigation tree, click **Resources > JMS > Activation specification**.
2. Select one of the activation specifications.
3. Click **Additional > Authentication Alias**, and then select the JMS authentication alias created.
4. Click **Apply**, and then click **Save**.
5. Perform the steps 1 to 4 for all activation specifications.

To assign group privileges to the IDP_JMS Bus

1. In the navigation tree click **Service Integration > Buses**.
2. Select the *[Bus name]*, and then click **Security**.
3. Click **Additional Properties > Users and groups in the bus connector role**.
4. Click **New** and then select **Group**.
5. In the Group Name box, type `lc_jms_group`.
6. Click **OK**.
7. Restart the server and verify that no startup errors occur.

3

Configuring Secure Administration Settings

Typically, developers do not use the LiveCycle ES production environment to build and test their applications. Therefore, you must administer user accounts and services that, although required in a private development environment, are not required in a production environment.

This section describes methods for reducing the overall attack surface through administration options that LiveCycle ES provides.

Disabling non-essential remote access to services

After LiveCycle ES is installed and configured, many LiveCycle ES services are available for remote invocation over SOAP, Enterprise JavaBeans™ (EJB), and LiveCycle Remoting. The term *remote*, in this case, means any caller with network access to the SOAP, EJB, or Action Message Format (AMF) ports for the application server.

Although LiveCycle ES services require valid credentials to be passed for an authorized caller, you should only allow remote access to the services that you need to be remotely accessible. To achieve limited accessibility, you should reduce the set of remotely accessible services to the minimum possible for a functioning system and then enable remote invocation for the additional services that you need.

Some LiveCycle ES services always need at least SOAP access. These services are typically required for use by LiveCycle Workbench ES, but also include services that are called by the LiveCycle Workspace ES web application.

Follow these steps using the Archive Administration web page in LiveCycle Administration Console:

1. Log in to LiveCycle Administration Console by typing the following URL in a web browser:

```
http://[host name]:[port]/adminui
```

2. Click **Services > Archive Administration > Preferences**.
3. Set the Preferences to view up to 200 services and endpoints on the same page.
4. Click **Services > Archive Administration > Endpoint Management**.
5. To disable all endpoints, browse for and select the check box beside each one in the list that has **EJB** listed in the **Provider** column, and then click **Disable**.
6. With the exception of the SOAP endpoints for the following LiveCycle ES services, to delete endpoints, browse for and select the check box beside all other endpoints that have **SOAP** listed in the **Provider** column, and then click **Delete**.
 - AuthenticationManagerService
 - DirectoryManagerService
 - JobManager
 - event_management_service
 - event_configuration_service
 - ProcessManager

- TemplateManager
- RepositoryService
- TaskManagerService
- TaskQueueManager
- TaskManagerQueryService
- WorkspaceSingleSignOn
- EventGenerationandReceipt

Disabling non-essential anonymous access to services

Some LiveCycle ES services permit unauthenticated (anonymous) invocation for some operations. This means that one or more operations exposed by the service may be invoked as any authenticated user or as no authenticated user at all.

The following LiveCycle ES services permit unauthenticated (anonymous) invocation for some of their operations:

- AuthenticationManagerService
- EJB
- Email
- JobManager
- WatchedFolder
- UsermanagerUtilService
- Remoting
- RemoteEvents
- RepositoryProviderService
- EMCDocumentumRepositoryProvider
- IBMFilenetRepositoryProvider
- FormAugmenter
- TaskManagerService
- TaskManagerConnector
- TaskManagerQueryService
- TaskQueueManager
- TaskEndpointManager
- LCMTMInvoker
- UserService
- WorkspaceSearchTemplateService
- WorkspaceSingleSignOn
- WorkspacePropertyService
- OutputService
- FormsService

If you intend to expose any of these services for remote invocation, you should also consider disabling anonymous access for these services. Otherwise, any caller with network access to this service may invoke the service without passing valid credentials.

Anonymous access should be disabled for any services that are not needed. Many internal services require anonymous authentication to be enabled because they need to be invoked by potentially any user in the system without being preauthorized.

Remove sample user and role assignments

You may have included sample users and roles when you installed LiveCycle ES; for example “Kel Varsen” and the “Finance Corp” User Domain. Using the User Management administration pages, you should remove the sample user domain and sample roles.

Changing the default global time-out

End users can authenticate to LiveCycle ES through Workbench ES, LiveCycle ES web applications, or custom applications that invoke LiveCycle ES services. There is one global time-out setting used to specify how long such users can interact with LiveCycle ES (using a SAML-based Assertion) before they are forced to reauthenticate. The default setting is two hours. On a production environment, the amount of time should be reduced to the minimum number of minutes acceptable.

► **To minimize reauthentication time limit:**

1. Export the User Manager Configuration XML.
2. Locate the Assertion Validity property, currently set to 120 minutes.
3. Change the value to a lower amount (for example 30 minutes).
4. Reimport the new User Manager Configuration XML.

Disabling LiveCycle 7.x backwards-compatibility API access

Applications developed by using the LiveCycle 7.x SDK do not invoke LiveCycle ES services using an authenticated EJB or SOAP Request. Instead, they make an unsecured CORBA invocation to a CORBA service that is deployed on the application server.

If you choose the upgrade option in LiveCycle Configuration Manager during the installation and configuration process, a CORBA service is deployed that allows existing LiveCycle 7.x applications that use the LiveCycle 7.x SDK to run when deployed on your application server. If you did not choose Upgrade, this CORBA service is not installed.

► **To disable the LiveCycle 7.x backwards-compatibility CORBA service:**

1. Locate the `adobe-livecycle-[appserver].ear` file in the `[LiveCycleES root]/jboss/deploy` directory. Make a backup copy of this EAR file.
2. Within the `adobe-core-[appserver].ear` file, locate the `adobe-core-compat-7to8-[appserver].ear` file. This EAR file is present if you have already performed a LiveCycle ES configuration and deployment with the Upgrade option.
3. Within the `adobe-core-compat-7to8-[appserver].ear` file, locate the `application.xml` file.
4. Modify the `application.xml` file to comment out the following module:

```
<!-- adobe-PDFManipulation start -->
<module id ="WebApp_PDFManipulation">
  <web>
    < web-uri>adobe-PDFManipulation.war</ web-uri>
    < context-root>/adobe-PDFManipulation</ context-root>
  </web >
</module >
```