

Mr. Websphere Guy Presents – Ooops, I've Got a Flaming Hole in My Security!!!

By Gregg Larkin

E1 Editor's Note: Well, the title certainly tells the tale of what's to come. Gregg Larkin, fka "Mr. Solution Explorer Guy" switches gears this issue to share a relatively unknown "gotcha" he recently encountered with Websphere's security and the tips he learned overcome it. If you're a CNC or tasked with any sort of JD Edwards® security and use Websphere 5 or 6, this is a MUST READ.

Wanna look like a hero to your IT auditors? This is the article for you. Our beloved JD Edwards is moving beyond the GUI world and heading full steam into the wonderful world of Websphere. And with that, well, come a few surprises of the not-so-pleasant kind when it comes to security loop holes. This will be the first of a series of Websphere tips and tricks. We'll focus the attention on Websphere 6 since Websphere 5 is a month away from retirement.

If you see a screen like the example in Figure 1, you've got some work to do.

The documentation and training for installing the JDE Web client illustrates a basic installation of Websphere and then moves on to the

process of installing and configuring the JDE Web server. That's all well and good, but that leaves Websphere sitting in an unprotected, unsecured mode. Try this science experiment: Open your local browser and type in: `http://yourservername:9060/ibm/console` (Websphere 6.x) or `http://yourservername:9090/admin` (Websphere 5.0.2.x). If you see a screen like the example in Figure 1, you've got some work to do.

Recognize that screen? Yep, it's the login screen for the Websphere Admin console. Websphere, in its default mode, has security disabled. You can type in any name you want on the screen and you're in. At that point, what can someone do, you ask? Take a look at Figure 2. As you can see, you can stop services, start services, change configurations, delete configurations, that's all. Nothing to lose sleep over, right?



Figure 1—Local Browser Login Screen

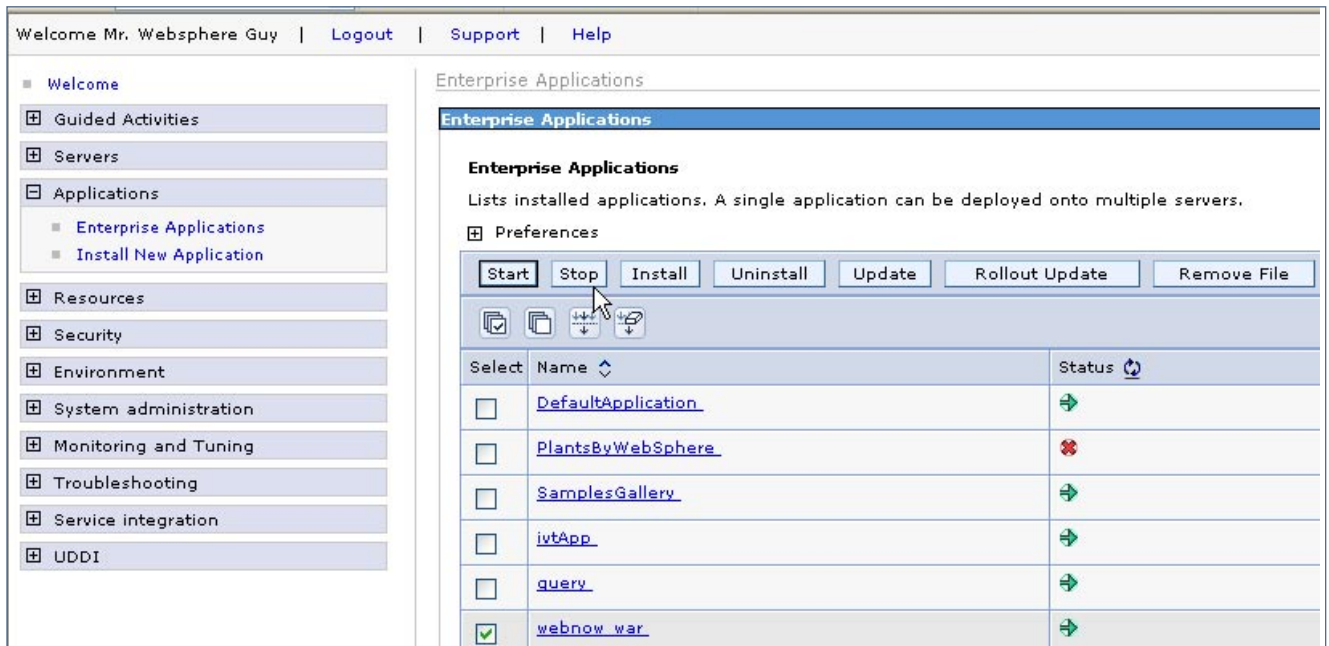


Figure 2 – WebSphere Admin Console Wide Open

To fix this problem, you will need to enable WebSphere Global Security. This article demonstrates how to do this using screen shots from WebSphere 6.0 application server running on a Windows 2003 server. If you are running on a different platform or running WebSphere 5.x, the basic theory is the same. For WebSphere 6, start by downloading the following two redbooks from IBM: 1) WebSphere Application Server V6: System Management and Configuration Handbook and 2) WebSphere Application Server V6 Security Handbook. You can purchase hard cover editions of these books for around \$110 and \$55 respectively, or just grab the PDFs for free at <http://ibm.com/redbooks>.

IBM provides three different methodologies for authenticating users once you have Global Security enabled. You can use Lightweight Directory Access Protocol (LDAP), Local Operating System security, or a custom registry, like a database. Some of you may have an LDAP server already set up in your infrastructure. We all have Operating

System security. I won't cover the third and most difficult choice. If you're a glutton for punishment, take a look at the Security Handbook for details on that.

Simple LDAP Procedure

To configure WebSphere using LDAP, perform the following steps:

- 1) The first step is to backup and rename the "security.xml" file. On my server it is found on this path:
 C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\YOURSERVERNAME1Node01Cell. I would rename the file to security_orig.xml. When you are done with the procedure of securing your server, I would make one more safe copy of that file, possibly storing that copy in an alternate location. If your WebSphere security gets screwed up or you lock yourself out, simply swap out the bad security.xml file for your safe copy.
- 2) Open the Administrative console, select Global Security (see Figure 3).
- 3) In the User registry section, select LDAP (see Figure 4).
- 4) Provide the details for the configuration panel:



Figure 3 – Global Security Menu

- 3) In the User registry section, select LDAP (see Figure 4).
- 4) Provide the details for the configuration panel:



Figure 4 – User Registries, LDAP

This Article Continues...

Subscribers, log in from our main search page to access the full article:

www.JDEtips.com/MyAccess.html

Not a Subscriber? Gain access to our full library of JDE topics:

www.JDEtips.com/JD-Edwards-Library

Visit www.JDEtips.com for information on the JDEtips University schedule, private training and consulting, and our Knowledge Express Document Library.

License Information: The use of JDE is granted to JDEtips, Inc. by permission from J.D. Edwards World Source Company. The information on this website and in our publications is the copyrighted work of JDEtips, Inc. and is owned by JDEtips, Inc.

NO WARRANTY: This documentation is delivered as is, and JDEtips, Inc. makes no warranty as to its accuracy or use. Any use of this documentation is at the risk of the user. Although we make every good faith effort to ensure accuracy, this document may include technical or other inaccuracies or typographical errors. JDEtips, Inc. reserves the right to make changes without prior notice.

Oracle and J.D. Edwards EnterpriseOne and World are trademarks or registered trademarks of Oracle Corporation. All other trademarks and product names are the property of their respective owners.

Copyright © by JDEtips, Inc.