SYBASE®

Installation Guide

Enterprise Portal – Information Edition

6.1

[Linux]

DOCUMENT ID: DC00085-01-0610-01

LAST REVISED: September 2004

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

About This Book

Audience

This guide is for Sybase® system administrators and other qualified professionals who are familiar with their system's environment, networks, disk resources, and media devices.

How to use this book

This book contains the following chapters:

- Chapter 1, "Overview," is the overview of the Enterprise Portal – Information Edition (EP) installation.
- Chapter 2, "Installation Procedures," describes system requirements, how to install EP on your system, how to perform special installation procedures, how to uninstall EP, and how to upgrade from an earlier version.
- Chapter 3, "Getting Started," describes how to get started using the Portal Interface and the Web Studio.
- Appendix A, "Installing EP in EAServer 5.0" describes how to deploy EP to EAServer.
- Appendix B, "Setting Up Authentication and Authorization" describes how to set up authentication and authorization using either Tomcat or EAServer, and either the portal database or a Lightweight Directory Access Protocol (LDAP) server.
- Appendix C, "Troubleshooting" provides troubleshooting information for common installation problems.

Related documents

Enterprise Portal – Information Edition documentation The following Enterprise Portal documents are available on the Getting Started with Enterprise Portal CD:

- The Enterprise Portal – Information Edition release bulletin for your platform contains last-minute information not documented elsewhere.
- The Enterprise Portal – Information Edition installation guide (this book) for your platform contains installation instructions.

Enterprise Portal online documentation The following Enterprise Portal documents are available in PDF format on the Enterprise Portal 6.1 Technical Library CD:

- The *Enterprise Portal Developer's Guide* includes developer-related topics for Enterprise Portal components, Portal Interface portlets, and Java Template Framework pages.
- The *Portal Interface User's Guide* describes the Portal Interface user interface and how to use Portal Interface to build and manage your enterprise's portal.
- The *Enterprise Portal – Information Edition Feature Guide* describes the features available in 6.1.

jConnect™ for JDBC™ documents Enterprise Portal 6.1 includes the jConnect for JDBC driver to allow JDBC access to Sybase database servers and gateways. The *Programmer's Reference jConnect for JDBC* is included on the Enterprise Portal Technical Library CD.

Other sources of information

Use the Sybase Getting Started CD, the Sybase Technical Library CD, and the Technical Library Product Manuals Web site to learn more about your product:

- The Getting Started CD contains release bulletins and installation guides in PDF format, and may also contain other documents or updated information. It is included with your software. To read or print documents on the Getting Started CD, you need Adobe Acrobat Reader (downloadable at no charge from the Adobe Web site, using a link provided on the CD).
- The Technical Library CD contains product manuals and is included with your software.
- The Technical Library Product Manuals Web site is an HTML version of the documents that you can access using a standard Web browser. In addition to product manuals, you will find links to EBFs/Maintenance, Technical Documents, Case Management, Solved Cases, newsgroups, and the Sybase Developer Network.

  To access the Technical Library Product Manuals Web site, go to Product Manuals at http://www.sybase.com/support/manuals/.

Sybase certifications on the Web

Technical documentation at the Sybase Web site is updated frequently.

❖ **Finding the latest information on product certifications**

1 Point your Web browser to Technical Documents at http://www.sybase.com/support/techdocs/.

2 Select Products from the navigation bar on the left.

3 Select a product name from the product list and click Go.

4 Select the Certification Report filter, specify a time frame, and click Go.

5 Click a Certification Report title to display the report.

❖ **Creating a personalized view of the Sybase Web site (including support pages)**

Set up a MySybase profile. MySybase is a free service that allows you to create a personalized view of Sybase Web pages.

1 Point your Web browser to Technical Documents at http://www.sybase.com/support/techdocs/.

2 Click MySybase and create a MySybase profile.

Sybase EBFs and software maintenance

❖ **Finding the latest information on EBFs and software maintenance**

1 Point your Web browser to the Sybase Support Page at http://www.sybase.com/support.

2 Select EBFs/Maintenance. Enter user name and password information, if prompted (for existing Web accounts) or create a new account (a free service).

3 Select a product.

4 Specify a time frame and click Go.

5 Click the Info icon to display the EBF/Maintenance report, or click the product description to download the software.

Conventions

The syntax conventions used in this manual are:

Key	Definition
commands and methods	Command names, command option names, utility names, utility flags, Java methods/classes/packages, and other keywords are in lowercase Arial font.
variable	Italic font indicates: • Program variables, such as *myServer* • Parts of input text that must be substituted, for example: *Server*.log • File names
$SYBASE	Variable used to represent the Sybase Enterprise Portal installation directory on UNIX systems.
File | Save	Menu names and menu items are displayed in plain text. The vertical bar shows you how to navigate menu selections. For example, File | Save indicates "select Save from the File menu."
`package 1`	Monospace font indicates: • Information that you enter in a GUI interface, a command line, or as program text • Sample program fragments • Sample output fragments

Note The installation and post-installation instructions frequently refer to the $SYBASE, $JAGUAR, and $JAVA_HOME variables.

$SYBASE refers to the EP installation directory; for example, */opt/sybase*.

$JAGUAR refers to the EAServer installation directory (if you are running Enterprise Portal – Information Edition in EAServer 5.0). This document assumes EAServer is installed in the same root directory as Adaptive Server Anywhere and Tomcat, so $JAGUAR is equivalent to *$SYBASE/EAServer*.

$JAVA_HOME refers to a valid JVM directory.

If you need help

Each Sybase installation that has purchased a support contract has one or more designated people who are authorized to contact Sybase Technical Support. If you cannot resolve a problem using the manuals or online help, please have the designated person contact Sybase Technical Support or the Sybase subsidiary in your area.

CHAPTER 1

Overview

This guide explains how to install Enterprise Portal – Information Edition (EP) version 6.1. Topics covered in this chapter are:

Product summary

This version is for Sybase Enterprise Portal – Information Edition 6.1, which is compatible with the following platform and operating system configuration:

- Red Hat Enterprise Linux Advanced Server 2.1

Sybase EP 6.1 is a ready-to-deploy solution that easily consolidates Web-accessible information sources and aggregates existing applications into a personalized view. This provides your employees, partners, and customers immediate access to the information and services they need to perform their jobs. EP combines ease-of-use and an intuitive user interface with advanced administration for enterprise application integration. With a completely browser-based management component, the portal translates the simplicity of the end-user experience to the developer and administrator, leading to a reduction in the time and cost of portal projects.

The Information Edition is the entry-level edition of the Sybase Enterprise Portal family and is the perfect solution for small projects and proof-of-concepts. It is designed for rapid deployment of information or content. You can install the product in a few minutes and quickly create portlets from JavaServer Pages (JSP) applications, Web accessible information sources, eXtensible Markup Language (XML) feeds, HyperText Markup Language (HTML) fragments, and databases.

CHAPTER 2

Installation Procedures

This chapter describes how to install Enterprise Portal – Information Edition (EP) on Linux.

The application database is supported on Adaptive Server® Anywhere (ASA). A Web browser provides access to Web Studio and Portal Interface.

System requirements

Table 2-1 lists system requirements.

Note Go to the Technical Library Product Manuals Web site at http://www.sybase.com/support/manuals, or see the release bulletin for your platform for components that require operating system patches.

Table 2-1: System requirements

Platform and OS	Release level	RAM	Disk space	Network protocol	Web browser
Red Hat Enterprise Linux	Advanced Server 2.1	512MB recommended	500MB minimum, 1G recommended	TCP	To access Portal Interface, use Internet Explorer 5.5 + or Netscape Navigator 7.01+. To access Web Studio, use Internet Explorer version 5.5 or 6.0.

Sybase EP installed on Red Hat Enterprise Linux Advanced Server is designed to act as the "server" while using Windows client browsers to access both the Portal Interface and Web Studio applications, so a PC running Windows is required.

Enterprise Portal default values

Table 2-2 lists the default values for the user names, passwords, and port numbers for Enterprise Portal.

Table 2-2: Enterprise Portal default installation values

Component	Default values	Description
Local Host Machine		
Local host machine name		The machine name; for example, "lab2".
Enterprise Portal port	4040	
Enterprise Portal https port	4443	
Adaptive Server Anywhere		
ASA port number	4747	
ASA administrator user name	dba	The user name used to log in to Adaptive Server Anywhere.
ASA administrator password	SQL	The password used to log in to Adaptive Server Anywhere.
Web Studio		

Component	Default values	Description
User name	opsuper	The user name used to log in to Web Studio. The account is created automatically during installation.
Password	0psuper (the first character is a zero)	The password used to log in to Web Studio.

Note If you are using Netscape 7.0.*x* and using HTTPS to protect passwords during login, you must run EP using ports 80 (HTTP) and 443 (HTTPS).

Pre-installation tasks

Before you install EP, you must:

- Verify that there is a "." (dot) in the PATH environment variable.
- Verify that you have write permission on your login home directory, the directory where you install the software, and the */tmp/logs* directory.
- Verify that you have 500MB free space in your temporary directory, otherwise, the installation fails.
- Know the domain name of the machine where you are installing EP. To find your domain name, contact your system administrator, or at a command prompt, enter:

  ```
  domainname
  ```

  Your domain displays; for example, `sybase.com`.

  Note If you do not have a domain, you can install only the demo version of EP.

Installation tasks

Typically, you install EP in a network environment. EP also includes a demo version of the product that you can install on a local machine.

The demo system is useful when you need system access for demonstrations or training sessions, or when your environment does not have a domain name. If you do have a domain, but want to use the demo system, you can access Web Studio via Internet Explorer. If you do not have a domain, the demo system is limited to Portal Interface access via Netscape, since Web Studio access requires Internet Explorer.

This section discusses installing EP in a network environment, but also includes special instructions for installing the demo system.

Installation takes five to ten minutes, depending on the speed of your machine.

Note If you are performing an upgrade from EP version 6.0 to 6.1, see "Special upgrade instructions" on page 13. If you are installing EP 6.1 in EAServer, see Appendix A, "Installing EP in EAServer 5.0."

❖ Installing EP in Tomcat

Typically you can use any account to install EP in Tomcat. However, if you plan to use ports 80 (HTTP) and 443 (HTTPS), you must log in as root to install EP.

1 If you plan to use ports 80 (HTTP) and 443 (HTTPS), log in as root. Otherwise skip this step.

2 Open a terminal window and create an installation directory in which to install EP; for example, */opt/sybase*. The installation directory is referred to as $SYBASE in this guide.

3 Copy the *IE610.tar.gz* file from the CD into the installation directory.

4 Using a zip utility, extract the *IE610.tar.gz* file into the installation directory. The command for extracting the file depends on the utility you are using.

   Note Make sure the zip utility allows the archive to create new folders in the location where you unzip it.

   Use one of the following commands to unzip:

   ```
   tar -zxvf IE610.tar.gz

   gunzip -c IE610.tar.gz | tar xvf -
   ```

5 Using a text editor, check the *hosts* file, located in */etc*, and verify you have the following entry:

```
127.0.0.1 localhost.localdomain localhost
```

For the demo system (described in the introduction to "Installation tasks" on page 5):

```
127.0.0.1 localhost demo.sybase.com
```

See "Changing the host, domain, and port of the portal" on page 11 for information.

6 Save the *hosts* file and exit the text editor.

7 If you are installing the demo system, go to step 8.

Otherwise, navigate to:

$SYBASE/infoedition

Enter `config.sh`. This modifies:

- Host name values in the *global.properties.xml* to the machine's name. The *global properties.xml* file is located in *$SYBASE/infoedition/tomcat/webapps/onepage/config* and contains many system settings.
- Host name and other values in the *portalexplorer.properties* file, which is located in *$SYBASE/infoedition/tomcat/webapps/portalexplorer/WEB-INF/classes*.

8 By default, the domain name in the *global.properties.xml* file is "sybase.com." To change the domain for your environment, modify *global.properties.xml* to use the domain name of the network on which your machine resides. See "Changing the host, domain, and port of the portal" on page 11.

9 From *$SYBASE/infoedition*, enter `startdb.sh`.

This starts the Adaptive Server Anywhere database. You may see several "Ping server failed – Database server not found" messages. You can disregard these messages.

When the database starts, you see "Ping server successful."

10 Enter `starttomcat.sh`.

When Tomcat starts, you see:

```
Using CATALINA_BASE:   /$SYBASE/infoedition/tomcat
Using CATALINA_HOME:   /$SYBASE/infoedition/tomcat
Using CATALINA_TMPDIR: /$SYBASE/infoedition/tomcat
```

```
                                /temp
    Using JAVA_HOME:            ./jdk1.4
```

11 The EP installation is complete. See “Verifying the installation” on page 8 to make sure the network installation works correctly.

If you cannot connect to the Portal Interface or Web Studio, go to *$SYBASE/infoedition/tomcat/logs* and check the *catalina.out* file for errors.

Post-installation tasks

This section describes post-installation steps.

- Verifying the installation
- Configuring for a proxy server
- Updating digital certificates
- Changing the host, domain, and port of the portal
- Configuring agentbuilder.jsp for alerts

Note In this section, the Tomcat version of path names is used, such as *$SYBASE/infoedition/tomcat/webapps/onepage*. If you are using EAServer, the comparable path name is *$JAGUAR/Repository/WebApplication/onepage*.

Verifying the installation

Verify that your EP installation is operating correctly by checking the following installations:

- Portal Interface
- Web Studio

❖ **Checking the installations**

1 Verify the Portal Interface installation by opening a browser window and entering:

```
http://HOSTNAME.PORTALDOMAIN:port/onepage/
```

```
index.jsp
```

where:

- *HOSTNAME* – the name of the machine where you installed Enterprise Portal – Information Edition 6.1; for example, "lab2k."
- *PORTALDOMAIN* – the domain name where the installation is located; for example, "sybase.com."
- *port* – the port number (the default is 4040).

For example:

```
http://lab2k.sybase.com:4040/onepage/index.jsp
```

Or, if you are using the demo system, enter:

```
http://demo.sybase.com:4040/onepage/index.jsp
```

2 Click Join Now to set up a new user profile. See "Getting started with Portal Interface" on page 19 for more information about setting up a user profile and using Portal Interface.

3 Verify the Web Studio installation by opening a browser window and navigating to:

```
http://HOSTNAME.PORTALDOMAIN:port/onepage/
index.html
```

For example, if your machine's name is "lab2k," your portal domain is "sybase.com," and your HTTP port number is "4040," enter:

```
http://lab2k.sybase.com:4040/onepage/index.html
```

Or, if you are using the demo system, enter:

```
http://demo.sybase.com:4040/onepage/index.html
```

Note Web Studio is accessible only through Microsoft Internet Explorer 5.5 and 6.0.

4 Log in using `opsuper` as the user name, and `0psuper` (the first character is a zero) as the password. See "Getting started with Web Studio" on page 22 for more information.

Configuring for a proxy server

If you are using a proxy server, you must configure EP with the appropriate proxy settings.

❖ **Using EP behind a proxy server**

1. Go to *$SYBASE/infoedition/tomcat/webapps/onepage/config*.
2. Using a text editor, open *global.properties.xml* and change the proxy value to "on." For example:

```
Property name="proxy" value="on"
description="(on/off). on ONLY if a squid type http
proxy is installed/available" menugroup="10"/
```

3. Change the proxy.host value to the IP address or host name of the proxy server. For example, if your proxy server host name is "proxy.hostname.com," the line looks like this:

```
Property name="proxy.host"
value="proxy.hostname.com"
description="(127.0.0.1). configure only if
proxy=on. IP of the squid server" menugroup="100"/
```

4. Change the proxy.port value to the port number on which the proxy server is running. For example, if the port is 1234, the line looks like this:

```
Property name ="proxy.port" value="1234"
description= "(3128). configure only if proxy=on.
port where squid cache is running" menugroup="100"/
```

5. To the proxy.bypass_list value, add the IP addresses or host names that should bypass the proxy server. You must keep the loopback address and local host in the bypass list. For example, if you want requests for URLs that end with "sybase.com" or start with "syberspace" to bypass the proxy server, enter:

```
Property name="proxy.bypass_list" value
="127.0.0.1|localhost|sybase.com|syberspace"
description="(host1|host2). please read
HTTPConnection javadocs for info on dontProxyFor()
method for more info" menugroup="100"/
```

Updating digital certificates

User authentication for the portal uses HTTPS, which uses Secure Sockets Layer (SSL) for posting the user names and passwords that users enter in an encrypted form over a secure channel. SSL and HTTPS rely on the usage of digital certificates, which are typically verified and signed by third-party trust authorities.

EP uses a certificate that is created using the keytool utility that ships with Java Development Kit (JDK) 1.4. This certificate is not signed by any trusted authority; therefore, you see the Security Alert pop-up when you sign in with your user name and password. Replace the *.keystore* file in the product folder with your certificate file of the same name.

Changing the host, domain, and port of the portal

By default, EP uses demo.sybase.com:4040 for the host, domain, and port.

To run the demo system on localhost, make the following entry in the *hosts* file:

```
127.0.0.1 localhost demo.sybase.com
```

To run EP in your network environment, change the host name and domain name for your environment; you may want to change the port if the port number is already used in your system.

For example, for EP to use `epdemo.example.com:5050` ("epdemo" is the host, "example.com" is the domain, and 5050 is the port), follow these steps:

1 Using a text editor, edit the *hosts* file located in */etc* by inserting the following entry on the last line:

```
127.0.0.1 localhost epdemo.example.com
```

2 Save the *hosts* file and close it.

Note To change other ports, such as the redirect port, make corresponding changes to the *global.properties.xml* and *server.xml* files, as described in Accessing EP from your network, next.

❖ **Accessing EP from your network**

When you run *config.sh*, the default host name"demo" is automatically changed to the machine name on which you installed Enterprise Portal 6.1. To complete the configuration process:

1 Using a text editor, open the *global.properties.xml* file, located in *$SYBASE/infoedition/tomcat/webapps/onepage/config*, and:

   a Search for all instances of *host_name*, where *host_name* is the name of the machine where you installed EP, and replace each instance with the new host name.

   b Search for all instances of `sybase.com`, and replace each instance with your domain name.

   c Search for all instances of `4040`, and replace each instance with the new port number.

   d Save *global.properties.xml* and close it.

2 Using a text editor, open the *server.xml* file, located in *$SYBASE/infoedition/tomcat/conf*, and:

   a Search for all instances of `4040`, and replace each instance with the new port number.

   b Save *server.xml* and close it.

3 Stop and restart the Tomcat application server as described in "Starting and stopping the Tomcat application server" on page 26.

Configuring *agentbuilder.jsp* for alerts

Modify the *agentbuilder.jsp* file to enable the Alert feature to work on resource identifiers (RIDs) other than 1.

❖ **Modifying *agentbuilder.jsp***

1 In a terminal window, navigate to *$SYBASE/infoedition/tomcat/webapps/onepage/home/docapps/agentbuilder*.

2 Copy *agentbuilder.jsp* to *agentbuilder.jsp-orig* as a backup.

3 Make sure you have write permission on *agentbuilder.jsp*.

4 With a text editor, open *agentbuilder.jsp*.

5 In *agentbuilder.jsp*, search for the following:

```
<%if ( _apps.equals("pi") && _pi_cmd.equals
("addSchedule") ) { %>
```

```
var IDsNode1 = requestDoc.selectSingleNode
("//RequestDef/RequestType/IDs");
```

6 Remove "`&& _pi_cmd.equals("addSchedule")`" from the line.

Original:

```
<%if ( _apps.equals("pi") && _pi_cmd.equals
("addSchedule") ) { %>
```

After modification:

```
<%if ( _apps.equals("pi")) { %>
```

7 Save the file and close it.

Configuring Tomcat for LDAP

Tomcat comes preconfigured with Common Security Infrastructure (CSI) and PortalDB provider. To configure Tomcat to use Lightweight Directory Access Protocol (LDAP), see Appendix B, "Setting Up Authentication and Authorization." The instructions are the same as EAServer instructions used to configure the CSI files to use LDAP. Check the Release Bulletin for additional information needed to run Web Studio successfully (CR #359766).

Special upgrade instructions

You can upgrade from EP 6.0 to EP 6.1 using an upgrade script to save certain files in the current installation and unpack the latest EP files on top of the 6.0 installation. Everything is replaced, including ASA, Tomcat, and JDK.

Before performing the upgrade:

- Create a backup of the $SYBASE directory, in which EP 6.0 Tomcat and ASA are installed.
- Verify that ASA and Tomcat are running.
- Verify that the $SYBASE environment variable is set to the Sybase installation directory where ASA and Tomcat are installed.

  To verify this variable, open a terminal window, and enter:

```
echo $variable
```

where $variable is the name of the variable you want to verify.

- Verify that the $TEMP and $TMP environment variables are set correctly; for example:

```
echo $TEMP
/tmp
echo $TMP
/tmp
```

❖ **Upgrading EP 6.0 to 6.1**

The script for performing the upgrade is located in the *IE610-UPDT-linux.tar.gz* file in the root directory of the EP 6.1 CD.

1 Navigate to the root directory of the EP 6.1 CD.

2 Using a zip utility, expand the *IE610-UPDT-linux.tar.gz* file to a temporary directory.

Note Make sure the zip utility allows the archive to create new folders in the location where you unzip it.

Use one of the following commands to unzip:

```
tar -zxvf IE610-UPDT-linux.tar.gz
```

```
gunzip -c IE610-UPDT-linux.tar.gz | tar xvf -
```

3 Navigate to the temporary directory and enter:

```
update-ie6_1.sh
```

You see “Welcome to the Enterprise Portal Info Edition 6.1 upgrade” and an overview of the upgrade procedure.

4 Respond to the prompts that display. Each prompt appears on a command line followed by a value in square brackets [ ]. The value in brackets is the default, based on the values set for $SYBASE.

Press Enter to accept the default value, or enter a new value and press Enter.

Upgrade script prompt	Default entry or example
Tomcat Host Name	The name of the machine where Tomcat is installed; for example: `lab2k` **Warning!** Do not enter "localhost." You must enter or accept the machine name.
Tomcat Port Number	The port number used to connect to Tomcat. `4040`
ASA Host Name	The name of the machine where Adaptive Server Anywhere is installed. The script displays the machine name you entered for the Tomcat host name as the default; for example: `lab2k`
ASA Port Number	The port number used to connect to Adaptive Server Anywhere. `4747`
ASA Admin User Name	The administrator user name used to log in to Adaptive Server Anywhere. `dba`
ASA Admin Password	The password the administrator uses to log in to Adaptive Server Anywhere. `SQL`

The input parameters are validated. You see:

```
Validating host mysysname:4747....

Validating database server mysysname:4747
dba/SQL....

Validating host mysysname:4040....
```

5 Any errors resulting from the validation display, as well as a summary of your input. You are then given a final opportunity to accept the input and proceed with the update.

```
Current environment is:
APASSWORD = SQL
APORT = 4747
AUSER = dba
TPORT = 4040
AHOST = mysysname
THOST = mysysname

Use this (yes|no) [yes]:
```

Press Enter if the entries are correct and you want to proceed.

If any of the entries are incorrect, enter `no` and press Enter. The script prompts you again for the upgrade information. You can correct any of the entries you made.

When you answer yes to the final prompt, the upgrade proceeds. When the upgrade process starts the new Tomcat server, a new terminal window is created.

6 You see the following output:

```
....Verify that database is running
....Check current version
....Stopping servers
....Wait for Tomcat to stop
....Wait some more
..............................
....Check disk space
....Back up the current installation
....Checksum the current installation
....Removing old tomcat and jdk
....Deploy update
....Determine changes
....Determine user only changes
....Update global.properties.xml
....Restore some things
....Update oem.xml
....Restore user apps
....Starting ASA
....Give ASA time to start
...................
....Update database data
....Update database stored procs
....Restore user added files
....Execute unjar script
....Starting Tomcat
....Give it time to get going
...................
....Verify that Tomcat is running
Upgrade complete
```

7 When the process finishes, you may see a message listing files that were modified by both you and Sybase. If you see the message, you must manually merge these files to update your installation, as described in “Merging changed files” on page 17.

8 If you encounter problems during the upgrade process, check the *update-ie6_1.log* in the $SYBASE directory. Use the information to correct the problem, then retry the update using these steps:

   a After correcting the problem, remove the contents of the $SYBASE directory.

   b Restore the contents of the $SYBASE directory from the backup that you made as part of the pre-upgrade tasks listed in "Special upgrade instructions" on page 13.

   c Reexecute the upgrade tasks described in "Upgrading EP 6.0 to 6.1" on page 14.

Merging changed files

You must perform this procedure only to preserve settings or customizations from an earlier EP installation. After the upgrade completes successfully, you may see a list of files that you must merge manually.

The files that must be manually merged are located in *$SYBASE/backup/onepage-both-chgs_XX.1st*.

Note The generated files have a timestamp in their names for tracking purposes (indicated above by *XX*, where *XX* is a date/timestamp in the format "YYYYMMDDhhmm").

❖ **Merging changed files**

1 Expand the backed up WAR file into a temporary directory.

   a Open a terminal window and navigate to an existing temporary folder—for example, */work/tmp*—or create a new temporary folder.

   b Ensure the path is set properly to the *$SYBASE/infoedition/jdk1.4/bin* folder where the *jar* utility is located.

   Because *jar* expands the file to the directory in which you are located, change to the temporary directory and expand the WAR file. In a terminal window, enter:

```
cd /work/temp/
jar -xvf $SYBASE/backup/onepage.war_XX
```

XX is a date/timestamp in the format "YYYYMMDDhhmm" that indicates when you can the upgrade or when the file was generated. If you run the upgrade more than once, there are multiple copies of these files—use the earliest version for your changes.

2 For each file in the *onepage-both-chgs_XX.lst* file, use a file merge utility to reintegrate your 6.0 portal changes into your new 6.1 portal.

Note If you do not own a file merge utility, perform an Internet search for "file merge utility." The search results let you access dozens of file merge utilities, many of which are shareware.

Uninstalling EP from Tomcat

If necessary, you can easily uninstall EP. If you are uninstalling EP from EAServer, use the instructions in "Uninstalling EP from EAServer" on page 32.

❖ **Removing EP**

1 Shut down the Tomcat server and the Adaptive Server Anywhere database.

To shut down Tomcat, open a terminal window, navigate to *$SYBASE/infoedition*, and enter `stoptomcat.sh`.

To shut down ASA, open a terminal window, navigate to *%SYBASE/infoedition*, and enter `stopdatabase.sh`.

2 Delete the *$SYBASE/infoedition* directory.

3 Delete the directory used for log files (for example, */tmp/logs*).

CHAPTER 3

Getting Started

This chapter describes how to start using the Portal Interface and Web Studio.

Getting started with Portal Interface

This section provides a quick tutorial for using Portal Interface. In this tutorial, create a basic portlet using an existing Web portlet. For detailed information, see the *Portal Interface User's Guide*.

❖ Logging in to Portal Interface

1 Open a browser window, and enter:

```
http://HOSTNAME.PORTALDOMAIN:port/onepage/
index.jsp
```

where:

- *HOSTNAME* – name of the machine where you installed Enterprise Portal – Information Edition (EP) 6.1.
- *PORTALDOMAIN* – domain name where the installation is located.
- *port* – port number (the default is 4040).

For example, enter:

```
http://lab2k.sybase.com:4040/onepage/index.jsp
```

For the demo system, enter:

```
http://demo.sybase.com:4040/onepage/index.jsp
```

2 Click Join Now.

❖ **Entering your profile information**

1 Enter your first name.

2 Enter your last name.

3 Enter your e-mail address.

4 Enter your telephone number.

5 Choose a member name.

6 Choose a password.

7 Confirm your password.

8 Select the PortalUser role.

9 Read the terms and conditions. If you agree, select the "I agree to the terms and conditions" box and click Done.

You see the Portal Interface default page group. To add pages and portlets, you must first add a new page group.

❖ **Creating new page groups**

1 Click Manage Pages.

2 In the Manage Pages window, click Add Page Group.

3 In the Add Page Group window, enter `myTest` as the name for the page group.

4 Optionally, you can select additional devices from available navigation styles. The navigation style allows you to specify how you navigate pages based on your operating system and browser.

When you create a page group, select the navigation style from the Available list, then click the right arrow to move it to the Assigned list.

Note To remove a navigation style from the Assigned list, select the style and click the left arrow to move it back to the Available list.

5 Click Done.

You see the first page of the page group you just created. The first page of the new group is automatically assigned the same name as the page group.

The new page group now appears in the page group as a tab and as a selection in the toolbar drop-down list.

❖ **Creating new pages**

1. Select the page group where you want your page to appear. Click Add Page at the top of the window.
2. Select "Add new page," and enter `myTest2` as the page name. The page name must be unique; if the page name already exists within that page group, you cannot create the new page.
3. Select the Page Layout 30/70, and click Done.

   Your new page name appears in the page tabs, at the far right. You can change the order of the page tabs using the Manage Pages option at the top of the window and editing the page group.

❖ **Adding a portlet**

1. Click Add Portlet.
2. In the Add Portlet window, click the Search branch.
3. Click the Google Search portlet.
4. Click Done to close the Add Portlet pop-up. The Google search portlet appears on the page. You can use the portlet to perform a Web search.

❖ **Creating a portlet**

1. Click Create Portlet.
2. In the Create Portlet wizard URL field, enter:

   ```
   www.sybase.com
   ```

3. Click Go.
4. In the right pane, click Press (use the vertical scroll bar to scroll up and down if necessary to locate Press).
5. Click Next in the upper-right corner.
6. After the preview refreshes, click the first press release (the first bulleted link) under Press in the middle pane. The cursor flag gives instructions.
7. After the preview refreshes, click the second Add button. The Sybase press release list is added to your page. Click a link to access the press release.

8 Either log out, or minimize the window. If the browser session expires, you must log in again when prompted.

Getting started with Web Studio

This section provides a quick tutorial for using the Web Studio. In this tutorial, create an interactive portlet using an existing Web portlet. For detailed information, see the *Enterprise Portal – Information Edition Feature Guide* and the *Enterprise Portal Development Guide*.

Note You must use Internet Explorer 5.5 or 6.0 to access Web Studio.

❖ **Logging in to Web Studio**

1 Open a new browser window, and enter:

```
http://HOSTNAME.PORTALDOMAIN:port/onepage/
index.html
```

where:

- *HOSTNAME* – the name of the machine where you installed EP 6.1.
- *PORTALDOMAIN* – the domain name where the installation is located.
- *port* – the port number (the default is 4040).

For example, enter:

```
http://lab2k.sybase.com:4040/onepage/index.html
```

For the demo system, enter:

```
http://demo.sybase.com:4040/onepage/index.html
```

2 In the User Name field, enter:

```
opsuper
```

3 In the Password field, enter:

```
0psuper
```

The first character is zero. The Web Studio window displays.

❖ **Creating an interactive Web element (stock quote)**

1 Select Portlets in the left pane.

2 Select New from the Portlet Manager toolbar, and click the New button to open Portlet Builder.

3 Click the down arrow next to Add, and select Web Element from the drop-down list, or click Add, which opens the Web Element wizard.

4 In the Location field, enter `cbs.marketwatch.com`, and click Find.

5 If prompted, click the "Direct to cbs.marketwatch.com" link.

6 In the Enter Symbols field in the left pane, enter `SY`, and click the Quote/News arrow.

Click Next in the upper-right corner.

7 After the preview refreshes, click the word "Last" in the quote table. The cursor flag provides instructions.

8 After the preview refreshes, click Select next to the option that displays the entire quote table. You can scroll up and down to view other formats.

Click Next in the upper-right corner.

9 After the preview refreshes, click the Variable box, which is next to the "symb" parameter.

10 In the Display Name field, enter `Symbol`, and in the Default Value field, enter `SY`.

Click Next in the upper-right corner.

11 After the preview refreshes, enter `Quote` in the Element Name field.

Click Next.

12 In the Continuous Capture window, click Finish to close the Portlet Builder wizard.

13 Test the portlet by entering `IBM` in the Symbol field, and clicking Update.

❖ **Saving the portlet**

1 Click Save in the upper-left corner.

2 In the Finish window:

Content tab Enter `Stock Quote` in the Name field, and click In Context.

Roles tab Click Add All to select all roles.

Administration tab From the Category and Subcategory drop-down lists, select Business and Investing.

3 Click Finish in the upper-right corner.

4 In the confirmation pop-up, click OK.

5 Click Close in the upper-right corner to close the Portlet Builder.

❖ **Approving the portlet**

1 Click Portlet in the left pane, and click New in Portlet Manager Status menu. The new portlet loads in the detail pane.

2 Right-click the Stock Quote portlet in the detail pane, and select Approval Status | Approved.

3 From the Approval Status submenu, and select Approved.

4 In the confirmation pop-up, click OK. The portlet is now listed under the Approved Status menu.

❖ **Updating the portlet catalog**

1 In the left pane, click Catalogs.

2 From the Catalog Manager menu, click the Approved branch in the Status tree.

3 Double-click the Default Catalog with version 1.0.

4 In the Catalog Builder window, select the Search branch.

Click Add in the Catalog Builder toolbar.

5 From the Find Portlet pop-up, click Search.

6 From the Find Portlet result list, select the Stock Quote portlet, and click Add. The Find Portlet window closes.

7 In the Catalog Builder toolbar, click Save.

8 In the confirmation pop-up window, click OK.

9 Click Close in the upper-right corner. The Catalog Builder closes.

❖ **Approving the updated portlet catalog**

1 From the Catalog Manager, under the Status tree, click the New branch.

2 In the Catalog Manager detail view, right-click Default Catalog version 1.1.

3 Scroll down to the Approval Status selection. From the Approval Status submenu, select Approved.

4 In the confirmation pop-up, click OK.

❖ **Making the updated portlet catalog active**

1 From the Catalog Manager menu, under the Status tree, click the Approved branch.

2 In the Catalog Manager detail view, right-click the Default Catalog version 2.0.

3 Scroll down to the Active selection, and from the Active submenu, select Yes.

4 In the warning pop-up window, click OK.

5 In the confirmation pop-up window, click OK.

❖ **Updating the Portal Interface**

1 Select Update from the Catalog Manager toolbar.

2 Click OK in the confirmation pop-up.

❖ **Adding the stock quote portlet to the demo page**

1 Log in to the Portal Interface using the same account you used in "Getting started with Portal Interface" on page 19.

2 Select the `myTest` page.

3 Click Add Portlet.

4 Click the Search branch.

5 Click the Stock Quote portlet.

6 Click Done to close the Add Portlet pop-up.

7 Use the vertical scroll bar to scroll down to view the Stock Quote portlet.

8 In the Stock Quote portlet, enter `IBM` in the Symbol input field.

9 Click OK to display IBM quote information.

For information about creating advanced interactive portlets from Web, XML, database, and JSP sources, see the *Enterprise Portal Developer's Guide*, and the *Enterprise Portal – Information Edition Feature Guide*.

Starting and stopping the system

This section describes how to start and stop the Adaptive Server Anywhere database and the Tomcat application server.

Stop the applications in this order:

1 Tomcat

2 ASA database

Start the applications in this order:

1 ASA database

2 Tomcat

Starting and stopping the database

This section describes how to start and stop the Adaptive Server Anywhere database.

❖ **Starting the ASA database**

1 From a terminal window, navigate to *$SYBASE/infoedition*.

2 Enter `startdb.sh`.

This starts the Adaptive Server Anywhere database. You may see several "Ping server failed – Database server not found" messages. You can disregard these messages.

When the database starts, you see "Ping server successful," and the icon for the Sybase ASA database appears in your taskbar.

❖ **Shutting down the ASA database**

1 From a terminal window, navigate to *$SYBASE/infoedition*.

2 Enter `stopdatabase.sh`.

Starting and stopping the Tomcat application server

This section describes how to start and stop the Tomcat application server. If you are running EP in EAServer, see the EAServer documentation for procedures to start and stop the application.

❖ **Starting the Tomcat application server**

1 From a terminal window, navigate to *$SYBASE/infoedition*.

2 Enter `starttomcat.sh`.

When Tomcat starts, you see:

```
Using CATALINA_BASE:   /$SYBASE/infoedition/tomcat
Using CATALINA_HOME:   /$SYBASE/infoedition/tomcat
Using CATALINA_TMPDIR: /$SYBASE/infoedition/tomcat
                       /temp
Using JAVA_HOME:       ./jdk1.4
```

❖ **Shutting down the Tomcat application server**

1 From a terminal window, navigate to *$SYBASE/infoedition*.

2 Enter `stoptomcat.sh`.

APPENDIX A

Installing EP in EAServer 5.0

This appendix provides information for installing and configuring Enterprise Portal – Information Edition (EP) in an EAServer 5.0 environment.

Overview

This appendix describes how to install EP 6.1 in an EAServer environment instead of a Tomcat environment, and how to uninstall EP 6.1 from EAServer if necessary.

In this section, $JAGUAR is defined as $SYBASE/EAServer, and $JAVA_HOME points to a valid JVM directory.

Installing EP in EAServer

You must install EP with EAServer 5.0. Install EAServer 5.0 before you install EP. If you already have EAServer 4.*x* installed, upgrade to EAServer 5.0, and then install EP.

To install EAServer, use the EAServer automated Install Shield package and follow the EAServer installation documentation. If you have problems or questions, see the EAServer installation documentation.

Before you start:

- Verify that EAServer 5.0 is installed.

- Install EAServer patches or EBFs. See the *Enterprise Portal – Information Edition Release Bulletin* for information.
- Make sure JDK 1.4 is installed, as EP requires JDK 1.4.

❖ Installing EP in EAServer

Typically you can use any account to install EP in EAServer. However, if you plan to use port 80 (HTTP) and port 443 (HTTPS), you must log in as root to install EP.

1. If you plan to use ports 80 (HTTP) and 443 (HTTPS), log in as root. Otherwise, skip this step.
2. Make sure EAServer is up and running before you proceed. Note the following assumptions
   - Server name – must be "Jaguar"
   - Default HTTP port – 8080
   - Default HTTPS port – 8081

   Note Currently, these port numbers are required.
3. Make sure that EAserver has been started with the correct JDK version (`$JAGUAR/bin/serverstart.sh -jdk14`), by checking the *Jaguar.log* for the following:

   ```
   Jul 20 13:27:58 2004: 180389-Java virtual machine
   initialized: javaversion 1.4.
   2_03

   Jul 20 13:27:58 2004: 180389-Java virtual machine
   initialized: Java HotSpot(TM)
   Client VM (version 1.4.2_03-b02, mixed mode)
   ```
4. Make sure no other Adaptive Server Anywhere instance is using port 4747.
5. From a terminal window, make sure the $SYBASE, $JAGUAR, and $JAVA_HOME environment variables are set. If not, set them; for example:

   ```
   setenv SYBASE /opt/sybase
   setenv JAGUAR $SYBASE/EAServer
   ```

```
setenv JAVA_HOME $SYBASE/shared/jdk1.4.0
```

Note The $SYBASE environment variable is set to the parent directory of $JAGUAR if $SYBASE is not set. You can also set $SYBASE to a JDK 1.4 installation, otherwise it is set to the JDK 1.4 version that is used by EAServer.

6 Using a zip utility, locate *ep61EAS.tar.gz* on the installation CD, and unzip its contents to $SYBASE.

7 Optionally, you can set the $JAGTOOL and $JAGTOOLARGS environment variables, which are supported by the *setup.sh* file. For example, if you are using a non-default IIOP port in EAServer, you can set the environment to:

```
setenv JAGTOOL $JAGUAR/bin/jagtool
setenv JAGTOOLARGS "-n 9100"
```

8 Go to *$SYBASE/EP/scripts* and execute:

```
setup.sh sybase.com csi
```

Note The csi argument is required.

This installs and configures EP, including:

- Web components:
  - onepage
  - DiscussionForum
  - InstantMessaging
  - PortalExplorer
  - CustView
- EAServer package:
  - csi-easerver

When the installation is complete, EAServer restarts, and Sybase ASA starts on port 4747.

9 Verify that EAserver restarted with the correct JDK version, by checking the *Jaguar.log* for the following:

```
Jul 20 13:27:58 2004: 180389-Java virtual machine
initialized: javaversion 1.4.
```

```
2_03

Jul 20 13:27:58 2004: 180389-Java virtual machine
initialized: Java HotSpot(TM)
Client VM (version 1.4.2_03-b02, mixed mode)
```

If not, stop EAServer using standard procedures, and restart it by using `$JAGUAR/bin/serverstart.sh -jdk14`.

10 Verify that Adaptive Server Anywhere started correctly.

Note Start and stop scripts for Sybase ASA are in *$SYBASE/EP*:

- `startdb.sh` – starts the ASA portaldatabase on port 4747
- `stopdatabase.sh` – stops the ASA portaldatabase

11 Verify the EP installation by accessing Web Studio from a browser window and entering:

`http://`*HOSTNAME.PORTALDOMAIN*`:`*port*`/onepage/index.html`

For example:

```
http://lab2k.syabse.com:8080/onepage/index.html
```

See “Getting started with Portal Interface” on page 19 and “Getting started with Web Studio” on page 22 for information. Be sure to use port 8080 when running Enterprise Portal – Information Edition from EAServer.

Configuring LDAP for EAServer

Tomcat comes preconfigured with CSI and PortalDB provider. To configure LDAP for EAServer, see Appendix B, “Setting Up Authentication and Authorization.” The instructions are the same as EAServer instructions used to configure the CSI files to use LDAP.

Uninstalling EP from EAServer

If necessary, you can easily uninstall EP from EAServer.

❖ **Removing EP from EAServer**

1 Shut down the Sybase ASA database. In a terminal window, enter:

```
stopdatabase.sh
```

2 Optionally, set the $JAGTOOL and $JAGTOOLARGS environment variables, which are supported by the *uninstall.sh* file. For example, if you are using a non-default IIOP port in EAServer, you can set the environment to:

```
setenv JAGTOOLS JAGUAR/bin/jagtool
setenv JAGTOOLARGS "-n 9100"
```

Update the related command in the *uninstall.sh* file:

a Search for the line:

```
${JAGTOOL} delete WebApplications:onepage
```

b Change the line to:

```
${JAGTOOL} $JAGTOOLARGS delete
WebApplications:onepage
```

3 Execute the *uninstall.sh* file, located in *$SYBASE/EP/scripts*.

```
uninstall.sh
```

This removes the Web applications and EAServer package.

4 Manually delete the *$SYBASE/EP* installation directory.

5 Delete the */tmp/logs* directory used for log files.

6 Manually remove the Web Studio roles that were created by *setup.sh*. Use EAServer Manager to remove the following roles:

- PortalUser
- PortalAdmin
- PortalGuest
- StudioAdmin
- superuser
- manager

7 Manually remove these files from *$JAGUAR/EAServer/java/classes*:

- *csi-core.jar*
- *csi-ldap.jar*

- *csi-portaldb.jar*

APPENDIX B

Setting Up Authentication and Authorization

This chapter describes how to set up authentication and authorization for Enterprise Portal – Information Edition (EP) 6.1, using either Tomcat or EAServer, and either the portal database or a Lightweight Directory Access Protocol (LDAP) server.

Preconfigured for PortalDB This version of EP is preconfigured to support authentication and authorization using the PortalDB security provider. If you plan to use Tomcat and PortalDB, you need not perform any of the configuration steps described in this chapter.

Overview

In this version of EP, a Common Security Infrastructure (CSI) realm works together with a security provider, either PortalDB or LDAP, to support authentication and authorization. The CSI realm is a component that plugs in to either a Tomcat 4.1.29 Web application container or an EAServer 5.0 application server. To support authentication and authorization, the PortalDB provider uses the Enterprise Portal database portaldatabase; the LDAP provider uses an LDAP server.

A CSI realm is an abstract interface to security information such as user names, passwords, and role membership. When a user logs in to Enterprise Portal, the user's name and password are verified against the data server, and if valid, role information is retrieved to provide Tomcat or EAServer with a list of the user's roles.

To use a combination of components other than Tomcat and the PortalDB security provider:

If your system components are	Perform these steps
Tomcat and the LDAP provider	• Configure the LDAP provider
EAServer and the PortalDB provider	• Configure the EAServer realm
EAServer and the LDAP provider	1 Configure the EAServer realm 2 Configure the LDAP provider

You can also use both security providers at the same time. If your system is configured to use both the LDAP provider and the PortalDB provider, a user's name and password are first passed to the LDAP provider for authentication, then they are passed to the PortalDB provider. If authentication succeeds with either provider, the user is authenticated. If the user cannot be authenticated with either the LDAP or PortalDB provider, the user is not authenticated. Similarly, when performing authorization role checks, both providers are queried to see whether either of them grants the specified role to the user.

Note For development, you may want to use the preconfigured PortalDB provider, as it can simplify debugging.

Configuring the CSI realm

Enterprise Portal supports authentication and authorization for both the Tomcat Web application container and the EAServer application server. This version of Enterprise Portal is preconfigured to use Tomcat. To use EAServer, see "Configure the EAServer realm" on page 37.

Configure the Tomcat realm

The Tomcat CSI realm plugs in to a Tomcat 4.1.29 Web application container. Its purpose is to delegate authentication and authorization checks to the security provider.

To enable debugging in the Tomcat CSI realm, create a file called *log4j.properties* in *$CATALINA_HOME/server/classes*, where $CATALINA_HOME represents the Tomcat root installation directory, and insert the following text:

```
# sample log4j.properties
# SecurityAppender for security packages only
log4j.appender.SecurityAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.SecurityAppender.DatePattern='.'yyyy-MM-dd
log4j.appender.SecurityAppender.File=/opt/sybase/infoedition/tomcat/logs/
   security_debug.log
log4j.appender.SecurityAppender.layout=org.apache.log4j.PatternLayout
log4j.appender.SecurityAppender.layout.ConversionPattern=%d{ISO8601}
   %-5p %-25c{1} %x - %m%n
log4j.category.com.sybase.security=DEBUG, SecurityAppender

# make sure security messages stay in the security log
log4j.additivity.com.sybase.security=false

# other packages go to the root appender
log4j.appender.RootAppender=org.apache.log4j.ConsoleAppender
log4j.appender.RootAppender.layout=org.apache.log4j.PatternLayout
log4j.appender.RootAppender.layout.ConversionPattern=%d{ISO8601}
   %-5p %-25c{1} %x - %m%n
log4j.rootCategory=INFO, RootAppender
```

The debugging output is written to the file whose name and location are specified by the log4j.appender.SecurityAppender.File property; in the example above, */opt/sybase/infoedition/tomcat/logs/security_debug.log*.

Initially, the Tomcat CSI realm is configured to use the PortalDB provider. To use the LDAP provider, see “Configure the LDAP provider” on page 39.

Configure the EAServer realm

The EAServer CSI realm plugs in to an EAServer application server. Its purpose is to delegate authentication and authorization checks to the security provider.

❖ **Setting up the EAServer realm**

1 To debug the CSI realm, create a file called *log4j.properties* in *$JAGUAR/java/classes*, where JAGUAR is the EAServer installation directory, and insert the following text, which causes debug and log messages to be written to *$JAGUAR/bin/Jaguar.log*:

```
log4j.appender.RootAppender=org.apache.log4j.ConsoleAppender
log4j.appender.RootAppender.layout=org.apache.log4j.PatternLayout
log4j.appender.RootAppender.layout.ConversionPattern=%d{ISO8601}
   %-5p %-25c{1} %x - %m%n
log4j.rootCategory=WARN, RootAppender
log4j.category.com.sybase.security=DEBUG
```

2 To use the PortalDB security provider only, skip to step 4.

If you are using the LDAP security provider, the EAServer CSI realm does not validate the LDAP provider's XML configuration file against the schema. To validate the XML configuration file:

a Verify that the JVM supports Java API for XML Processing (JAXP) 1.2 or higher.

b Configure the XML validation property:

1 In EAServer Manager, expand the Servers folder, highlight Jaguar, and select File | Properties. The Server Properties dialog box displays.

2 On the Advanced tab, click Add, then enter `com.sybase.security.core.XmlConfiguration.XmlValidation` as the property name and "true" as the property value.

Click OK.

3 Configure the security provider—see "Configuring the security provider" on page 38.

4 Restart EAServer. In EAServer Manager, highlight Jaguar, and select File | Shutdown and Start.

Configuring the security provider

Enterprise Portal includes two security providers, the PortalDB provider and the LDAP provider. Initially, Enterprise Portal is configured to use the PortalDB provider. You can use the LDAP provider instead of the PortalDB provider, or you can use both providers concurrently. To configure a security provider, see:

- "Configure the LDAP provider" below, or
- "Restore the PortalDB provider configuration" on page 46

Configure the LDAP provider

Enterprise Portal LDAP support includes authentication, attribution, and authorization services. The LDAP provider authenticates users when they log in using credentials that can be validated on the LDAP server.

1 To use both the LDAP provider and the PortalDB provider, go to step 2.

To use only the LDAP provider:

a Change to the location of the *global.properties.xml* file, either:

- Tomcat – *$SYBASE/infoedition/tomcat/webapps/onepage/config*, where SYBASE is the installation directory of your Sybase software, or
- EAServer – *$JAGUAR/Repository/WebApplication/onepage/config*, where JAGUAR is the EAServer installation directory.

b Using a text editor, open *global.propeties.xml*, and change the value of the AuthenticationUsing property to "CSI".

2 Change to the location of the *csi.xml* file, either:

- Tomcat – *$CATALINA_HOME/conf*, where $CATALINA_HOME represents the Tomcat root installation directory, or
- EAServer – *$JAGUAR/Repository/Component/csi-easerver*

3 Using a text editor, open *csi.xml*, and edit the values appropriate for your system.

The sample *csi.xml* file that is installed with Enterprise Portal contains the following LDAP provider definitions, which are commented out. Remove the comment delimiters:

```
<!--

<config:authenticationProvider
   name="com.sybase.security.ldap.LDAPLoginModule"
   controlFlag="optional">

   <config:options name="ServerType" value="sunone5" />
   <config:options name="ProviderURL" value="ldap://localhost:389" />
   <config:options name="DefaultSearchBase" value="dc=sybase,dc=com" />
</config:authenticationProvider>

-->
```

```
<!-- LDAP attributer - commented out
   <config:provider name="com.sybase.security.ldap.LDAPAttributer"
     type="attributer" />
-->
```

4 Comment out the following PortalDBAttributer definition. To comment out the definition, insert "<!--" at the beginning of the definition, and "-->" at the end of the definition.

```
<config:provider name="com.sybase.security.portaldb.PortalDBAttributer"
   type="attributer" />
```

Table B-1 on page 40 defines the complete list of options that you can use to configure the authentication provider. You can enable any of the options by adding the option name and value to *csi.xml*, using the same syntax as illustrated in step 3. You must add new option definitions within the authenticationProvider definition; that is, between the following two lines:

```
<config:authenticationProvider
   name="com.sybase.security.ldap.LDAPLoginModule">
...
</config:authenticationProvider>
```

Table B-1: LDAP configuration options

Configuration option	Default value	Definition
AuthenticationFilter	Most LDAP servers: (&(uid={uid}) (objectclass=personal) Microsoft ActiveDirectory: (&(userPrincipalName={uid}) (objectclass=user))	The filter to use when authenticating users. When performing a user name/password-based authentication, this filter is used to determine the LDAP entry that matches the supplied user name. The string "{uid}" in the filter is replaced with the user name.
AuthenticationMethod	simple	The authentication method to use for all LDAP authentication requests. The supported methods are: • "simple" – clear text authentication. • "DIGEST-MD5" – more secure, hashed password authentication. Passwords must be stored in plain text on your LDAP server, and you must use JRE 1.4 or higher.
AuthenticationScope	onelevel	Can be set to either "onelevel" or "subtree." If set to "onelevel," only the AuthenticationSearchBase is searched used to search for user records; if set to "subtree," the AuthenticationSearchBase and its subtree are searched.

Configuration option	Default value	Definition
AuthenticationSearchBase		The location of user records. If not specified, the DefaultSearchBase is used.
BindDN		The DN to bind to when creating the initial LDAP connection. This DN must identify a user who has read capability on all records that are accessed when users authenticate using the login module. This property also defines the credentials that are used to perform anonymous attribution operations when LDAP authentication has not occurred. If this property is not specified, anonymous binding is used, which works on most servers.
BindPassword		The password to bind to when creating the initial LDAP connection. You must specify this only when the BindDN property is specified.

DefaultSearchBase		The search base that is used if no other LDAP search base is specified for authentication, roles, or attribution. Use either of the following two syntax options, and verify that the syntax you choose matches what is configured on the LDAP server:
		dc=<*domain_name*>,dc=<*top_level_domain*>
		o=<*company_name*>,c=<*country_code*>
		For a machine in the Sybase organization, the previous two syntax options map to:
		`dc=sybase,dc=com`
		`o=Sybase,c=us`

InitialContextFactory	com.sun.jndi.ldap.LdapCtxFactory	Specifies the JNDI provider to use. If you are using a Sun Java VM version 1.3 or higher, the default value should work. If you are using an IBM or other third-party VM, adjust this value accordingly.
ProviderURL	ldap://localhost:389	The URL to connect to the LDAP server. The default value should work if the LDAP server is located on the same machine as the portal and listens on port 389.

Configuration option	Default value	Definition
RoleFilter	SunONE: (&(objectclass=ldapsubentry) (objectclass=nsroledefinition)) Netscape Directory Server: (|(objectclass=groupofnames) (objectclass=groupofuniquenames)) Microsoft ActiveDirectory: (|(objectclass=groupofnames) (objectclass=group))	The role filter, which when used with the RoleSearchBase and RoleScope, returns the complete list of roles from the LDAP server.
RoleMemberAttributes	Netscape Directory Server: member,uniquemember	A comma-delimited list of one or more role attributes that define the DNs for users who have the role. The DNs are used to determine which roles the user has. This property may be helpful if you use LDAP groups as placeholders for roles. **Note** The default value applies only to Netscape Directory Server; no default exists for other servers.
RoleNameAttribute	cn	The attribute that identifies the common names of roles. If a role name value is "dn," the role name is assumed to be the full DN of the role.
RoleScope	onelevel	Can be set to either "onelevel" or "subtree." If set to "onelevel," only the RoleSearchBase is used to search for roles; if set to "subtree," the RoleSearchBase and its subtree are searched.
RoleSearchBase		The search base used to retrieve a list of roles. If not specified, the DefaultSearchBase is used.

Configuration option	Default value	Definition
ServerType		The type of LDAP server you are connecting to; supported server types are: • "msad2k" – Microsoft ActiveDirectory Windows 2000—see "Caveats when using Microsoft ActiveDirectory LDAP servers" on page 45. • "nsds4" – Netscape Directory Server 4. • "sunone5" – SunONE Directory Server 5. This value is not required, but if provided, establishes default values for the following configuration properties: • AuthenticationFilter • RoleFilter • RoleMembershipAttributes • UserRoleMembershipAttributes
UserFreeformRole MembershipAttributes		The "free-form" role membership attribute list. Users who have attributes in this comma-delimited list are automatically granted access to roles whose names match the attribute value. For example, if the value of this property is "department" and the user's LDAP record has the values "sales" and "consulting" for the department attribute, then the user will be granted roles whose names are "sales" and "consulting." If you are using a SunONE Directory Server 5: 1 From the LDAP Administration console's Generic Editor, add a multivalue attribute called "department" for the user. 2 Highlight "department," click Add Value, and enter "sales." 3 Click Add Value again, and enter "consulting."
UserRoleMembership Attributes	SunONE: nsRoleDN Microsoft ActiveDirectory: memberOf	Defines a user attribute to store the list of role DNs for all the roles a user has been granted. These role DNs are cross-referenced against the roles retrieved using the RoleSearchBase and RoleFilter to get a complete list of a user's roles. **Note** For servers other than SunONE and Microsoft ActiveDirectory, there is no default value.

Role computation

Role computation techniques are used to list roles for both authenticated and unauthenticated users. The LDAP provider performs access control using roles, and supports three types of role constructs; each may be used independently, or all three may be used at the same time:

- User-level role attributes – this is the most efficient role definition format, and is supported by SunONE and ActiveDirectory. Using this technique, a user's roles are enumerated by a read-only attribute in the user's LDAP record, which is managed by a directory server. The advantages of this technique are the efficiency with which role memberships can be queried, and the ease with which they can be managed using the native LDAP server's management tools. To use this option, configure the following LDAP properties, which are described in Table B-1 on page 40:
  - RoleFilter
  - RoleNameAttribute
  - RoleSearchBase
  - RoleScope
  - UserRoleMembershipAttributes
- LDAP group role definitions – supported by almost all LDAP servers and a common construct in older LDAP servers. This technique may be useful if you want to use the same LDAP schema across multiple LDAP server types. Unlike the user-level role attributes, LDAP group memberships are stored and checked on a group-by-group basis. Each defined group has an attribute that lists all the members in the group. Groups are typically in one of two object classes, either groupofnames or groupofuniquenames.

  To use this option, configure the following properties in the *csi.xml* file:
  - RoleFilter
  - RoleMemberAttributes
  - RoleNameAttribute
  - RoleScope
  - RoleSearchBase

See Table B-1 on page 40 for more information. The value of RoleMemberAttributes is a comma-delimited list of attributes, each of which defines members of the group. An example value for this property is "uniquemember,member," which represents the membership attributes in the groupofnames and groupofuniquenames object classes.

- Free-form role definitions – unique in that the role itself does not have an entry in the LDAP data store. To create a free-form role definition, begin by defining one or more user-level attributes. When roles are calculated for a user, the collective values of the attributes—which can have multiple values—are added as roles of which the user is a member. This technique requires less administrative overhead than either of the two previously described techniques.

  As an example, assign a free-form role definition that is equivalent to the department number of a user. A role check performed on a specific department number is satisfied only by users who have the appropriate department number attribute value. To use free-form role definitions, configure the UserFreeformRoleMembershipAttributes property—see Table B-1 on page 40.

Caveats when using Microsoft ActiveDirectory LDAP servers

If you are using the Microsoft ActiveDirectory Windows 2000 server, the following restrictions apply:

- The DIGEST-MD5 authentication mode is not supported.
- The value of DefaultSearchBase must match exactly the value set for the directory server, including case.
- If you set the value of DefaultSearchBase to "DC=epstg,DC=com," you must set the values of both AuthenticationSearchBase and RoleSearchBase to "CN=Users,DC=epstg,DC=com."
- Anonymous binding is not permitted. You must specify a BindDN/BindPassword that identifies a user who can view all other users and groups; for example, specify "mtester@epstg.com" as the BindDN and "secure123" as the BindPassword.
- From the ActiveDirectory Users and Computers console, you must create users and groups, then add users to the groups so they are authorized to perform tasks in Enterprise Portal. Create the following groups, then add users to these groups:
  - everybody

- PortalAdmin
- PortalGuest
- PortalUser
- StudioAdmin
- superuser

Restore the PortalDB provider configuration

Initially, Enterprise Portal is configured to use the PortalDB security provider. If your system was changed to use the LDAP security provider, you can restore the PortalDB configuration using the following procedure.

1 Change to the location of the *global.properties.xml* file, either:

   - Tomcat – *$SYBASE/infoedition/tomcat/webapps/onepage/config*, where SYBASE is the root installation directory of your Sybase software, or
   - EAServer – *$JAGUAR/Repository/WebApplication/onepage/config*, where JAGUAR is the EAServer root installation directory.

2 Using a text editor, open *global.propeties.xml*, and set the value of the AuthenticationUsing property to "Database".

3 Change to the location of the *csi.xml* file, either:

   - Tomcat – *$CATALINA_HOME/conf*, where $CATALINA_HOME represents the Tomcat root installation directory, or
   - EAServer – *$JAGUAR/Repository/Component/csi-easerver*

4 Open *csi.xml*, and verify that the PortalDB provider definitions are not commented out. The sample *csi.xml* file that is installed with Enterprise Portal contains the following PortalDB provider definitions:

```
<config:authenticationProvider
   name="com.sybase.security.portaldb.PortalDBLoginModule"
   controlFlag="optional">

   <config:options name="DatasourceName"
      value="java:comp/env/jdbc/portaldb" />

</config:authenticationProvider>
```

```
<config:provider name="com.sybase.security.portaldb.PortalDBAttributer"
   type="attributer" />
```

The value of DatasourceName defines the name that is passed to the javax.naming.InitialContext().lookup(*datasourceName*) method to retrieve a connection to the portaldatabase. The default value is "java:comp/env/jdbc/portaldb," and Enterprise Portal creates this JNDI name automatically during deployment. If the DatasourceName configuration option is missing, the default value is used.

5 To use the PortalDB provider only, comment out the LDAP provider definition in *csi.xml*. To comment out the definition, insert "<!--" at the beginning of the definition, and "-->" at the end of the definition. In the following example, the LDAP provider definition is commented out:

```
<!--
<authenticationProvider
name="com.sybase.security.ldap.LDAPLoginModule">
   <options name="ServerType" value="sunone5"/>
   <options name="DefaultSearchBase" value=""/>
   <options name="ProviderURL" value="ldap://localhost:389"/>
   <options name="AuthenticationMethod" value="simple"/>
   <options name="AuthenticationScope" value="subtree"/>
   <options name="AuthenticationSearchBase" value=""/>
   <options name="RoleScope" value="subtree"/>
   <options name="RoleSearchBase" value=""/>
</authenticationProvider>
-->
```

To use both the PortalDB provider and the LDAP provider, verify that neither of the provider definitions is commented out.

APPENDIX C

Troubleshooting

This chapter describes how to troubleshoot Enterprise Portal – Information Edition (EP) installation and configuration problems.

Overview

Use the following resources to help troubleshoot installation and configuration problems:

- Viewing log files
- Viewing error messages
- Checking port numbers
- Checking configuration files
- Testing connections
- Running the Portal Interface and Web Studio

Troubleshooting EP configuration

Table C-1 identifies common EP configuration problems and provides useful troubleshooting information.

Table C-1: Troubleshooting EP problems

Problem	Try this
Cannot start ASA database: `Connection error: Unable to initialize requested communication links`	If you receive this error when trying to start the ASA database using `startdb.sh`: • Check the *global.properties.xml* and *server.xml* files to make sure you changed the ASA port number to the correct value. The default is 4747. • If you ran the upgrade script, to upgrade from EP 6.0 to 6.1, make sure you entered the correct ASA port number. The default is 4747.
Cannot start application server	This can happen if you are using ports 80 (HTTP) and 443 (HTTPS) with Netscape, and you did not install EP as root. Root is required to start these ports in the production system. • Check the *catalina.out* file, located in *$SYBASE/infoedition/tomcat/logs*, for errors. Try uninstalling and then reinstalling EP. Be sure to log in as root as described in "Installation tasks" on page 5 (Tomcat application server), or "Installing EP in EAServer" on page 29 (EAServer).
Cannot start the Portal Interface: File Not Found 404 error	If you receive this error when trying to start Portal Interface: • Check to make sure you ran `config.sh` to change *localhost* to your machine name (such as `lab2k`) and to set other values as described in "Installation tasks" on page 5 (or "Installing EP in EAServer" on page 29). • Check to make sure you changed the machine name and domain name for your network as described in "Changing the host, domain, and port of the portal" on page 11. • Check to make sure you entered the URL correctly to access Portal Interface as described in "Verifying the installation" on page 8. • Check to make sure you are using the correct port number; for example, 4040 when running in Tomcat, and 8080 (required) when running in EAServer. • Check the *catalina.out* file, located in *$SYBASE/infoedition/tomcat/logs*, for errors.
Cannot start Web Studio	If you cannot start Web Studio: • Verify that you are using Internet Explorer and not Netscape. • Verify that you are using the correct version of Internet Explorer as described in Table 2-1 on page 4. • Verify that you are using the correct port number, for example, 4040 when running in Tomcat, and 8080 (required) when running in EAServer.

Index

Symbols

A

B

C

D

E

G

I

J

L

M

O

P

R

S

T

U

W