SYBASE®

Installation Guide

Unwired Accelerator™

8.0

Linux on POWER

DOCUMENT ID: DC00457-01-0800-01

LAST REVISED: January 2007

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

Contents

About This Book

Audience

This guide is for Sybase® system administrators and other 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 Unwired Accelerator installation.
- Chapter 2, "Installation Procedures," describes how to install Unwired Accelerator on your system, how to perform special installation and upgrade procedures, how to stop and start system components, and how to uninstall Unwired Accelerator.
- Chapter 3, "Troubleshooting," provides information for some common installation problems.
- Appendix A, "Setting Up Authentication and Authorization," describes how to set up authentication and authorization using Tomcat, and either the portal database or a Lightweight Directory Access Protocol (LDAP) server.

Related documents

Unwired Accelerator documentation The following Unwired Accelerator documents are available on the Getting Started with Unwired Accelerator CD:

- The Unwired Accelerator release bulletin for your platform contains up-to-date information not documented elsewhere.

  A more recent version of the release bulletin may be available on the World Wide Web. To check for critical product or document information that was added after the release of the product CD, use the Sybase Products Manuals Web site.
- The Unwired Accelerator installation guide (this document) contains installation instructions.
- The *Unwired Accelerator Quick Start Guide* shows how to deploy a database application to either a PDA or BlackBerry device.

- The *Unwired Accelerator Mobile Application Development Tutorial* provides tutorials that show how you can use Mobile Web Studio to develop and deploy mobile applications.
- *Unwired Accelerator .NET API Cookbook* – describes how to use the .NET API.
- *Adaptive Server Enterprise documents* – Unwired Accelerator 8.0 includes the Adaptive Server® Enterprise database to store system information including security authentication and authorization information.
- The *SyBooks Installation Guide* describes how to install SyBooks™.
- *jConnect for JDBC documents* – Unwired Accelerator 8.0 includes the jConnect™ for JDBC™ driver to allow JDBC access to Sybase database servers and gateways. The release bulletin and installation guide are included on the Getting Started CD.

Unwired Accelerator online documentation The following Unwired Accelerator documents are available on the SyBooks CD:

- The *Unwired Accelerator Developer's Guide* includes developer-related topics for Unwired Accelerator components, Portal Interface applications, and Java Template Framework pages.
- The *Unwired Accelerator Administration Guide* provides administration topics for Unwired Accelerator and its components.
- 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.
- *jConnect for JDBC documents* – Unwired Accelerator 8.0 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 SyBooks CD.

Other sources of information

Use the Sybase Getting Started CD, the SyBooks CD, and the Sybase 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 not included on the SyBooks CD. It is included with your software. To read or print documents on the Getting Started CD, you need Adobe Acrobat Reader, which you can download at no charge from the Adobe Web site using a link provided on the CD.

- The SyBooks CD contains product manuals and is included with your software. The Eclipse-based SyBooks browser allows you to access the manuals in an easy-to-use, HTML-based format.

  Some documentation may be provided in PDF format, which you can access through the PDF directory on the SyBooks CD. To read or print the PDF files, you need Adobe Acrobat Reader.

  Refer to the *SyBooks Installation Guide* on the Getting Started CD, or the *README.txt* file on the SyBooks CD for instructions on installing and starting SyBooks.

- The Sybase Product Manuals Web site is an online version of the SyBooks CD 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 Sybase 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 Click Certification Report.

3 In the Certification Report filter select a product, platform, and timeframe and then click Go.

4 Click a Certification Report title to display the report.

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

1 Point your Web browser to Availability and Certification Reports at http://certification.sybase.com/.

2 Either select the product family and product under Search by Base Product; or select the platform and product under Search by Platform.

3 Select Search to display the availability and certification report for the selection.

❖ **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. If prompted, enter your MySybase user name and password.

3 Select a product.

4 Specify a time frame and click Go. A list of EBF/Maintenance releases is displayed.

Padlock icons indicate that you do not have download authorization for certain EBF/Maintenance releases because you are not registered as a Technical Support Contact. If you have not registered, but have valid information provided by your Sybase representative or through your support contract, click Edit Roles to add the "Technical Support Contact" role to your MySybase profile.

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

Key	Definition
$SYBASE	Variable used to represent the Sybase Unwired Accelerator installation directory on UNIX/LINUX systems.
%SYBASE%	Variable used to represent the Sybase Unwired Accelerator MobiLink installation directory on Windows 2003 or XP 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 these variables:

$SYBASE refers to the Unwired Accelerator installation directory; for example, */opt/sybase/UA80*. In this document, $SYBASE/ASE indicates the location where Adaptive Server Enterprise is installed.

%SYBASE% refers to the Unwired Accelerator MobiLink installation on Windows 2003 or XP.

$CATALINA_HOME refers to the Apache Tomcat application server installation directory. Unwired Accelerator integrates the Tomcat application server in its installation directory, so $CATALINA_HOME is equivalent to *$SYBASE/UA80/tomcat*).

$JAVA_HOME refers to a valid JVM directory.

%RIM% refers to the Research in Motion installation directory; for example, *C:\Program Files\Research In Motion* or *C:\RIM*.

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, and configure Sybase Unwired Accelerator running in Tomcat.

Product summary

Unwired Accelerator (UA) mobilizes enterprise applications and data, which allows users to be productive and effective inside or outside the office. They can access the same applications and tools anytime, anywhere on a mobile device.

Unwired Accelerator enables users to rapidly mobilize existing enterprise Web applications and data sources, such as databases and Web services for both online and offline Web access. Users need not rewrite or modify existing applications or infrastructure.

Sybase Unwired Accelerator is compatible with these platform and operating system configurations:

- Red Hat Enterprise Linux Advanced Server 4.0
- SuSE Linux Enterprise Server (SLES) 9.0
- Mobile device, online access:
  - PocketPC 2003 (Windows CE)
  - Motorola MPx200 (Windows Mobile OS)
  - Sony Ericsson P900
  - RIM BlackBerry (including Proximus and Vodafone)
  - Palm
- Mobile device, offline access:

- PocketPC (Windows CE)
- RIM BlackBerry (including Proximus and Vodafone)

CHAPTER 2

Installation Procedures

This chapter describes how to install Unwired Accelerator with Linux on POWER.

System requirements

Go to the Sybooks 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 on page 3 lists system requirements for both Red Hat Linux, and SuSE Linux.

Table 2-1: System requirements

Platform and OS	Release level	RAM	Disk space	Network protocol	Web browser
Red Hat Enterprise Linux	Advanced Server 4.0	1.1MB minimum, 2GB recommended	1.1MB minimum, 2GB recommended	TCP	To access Portal Interface, use Internet Explorer 5.5+ or Netscape Navigator 7.01+. To access Mobile Web Studio, use Internet Explorer versions 5.5 and 6.0.

Platform and OS	Release level	RAM	Disk space	Network protocol	Web browser
SuSE Linux Enterprise Server (SLES)	SLES 9.0	1.1MB minimum, 2GB recommended	1.1MB minimum, 2GB recommended	TCP	To access Portal Interface, use Internet Explorer 5.5+ or Netscape Navigator 7.01+. To access Mobile Web Studio, use Internet Explorer versions 5.5 and 6.0.

Sybase Unwired Accelerator installed on Red Hat Enterprise Linux Advanced Server is designed to act as the "server." Windows client browsers are used to access both the Portal Interface and Mobile Web Studio applications, so a PC running Windows is required. Optionally, a PC running Windows is required for the MobiLink server.

Unwired Accelerator default values

Table 2-2 lists the default values for the user names, passwords, and port numbers for Unwired Accelerator (UA).

Table 2-2: Unwired Accelerator default installation values

Component	Default values	Description
Local host machine		
Local host machine name	(demo)	The machine name; for example, "labxp."
Unwired Accelerator port	4040	
Unwired Accelerator HTTPS port	4443	
Adaptive Server Enterprise 15.0.1, Enterprise Edition		
ASE database port number	5000	
ASE administrator user name	sa	This is the user name used to log in to Adaptive Server Enterprise.
ASE administrator password	" " (no password)	This is the password used to log in to Adaptive Server Enterprise.
Mobile Web Studio 8.0		

Component	Default values	Description
User name/password (uses mobile application terms)	masuper/m8super	Created automatically during installation. If you are installing Unwired Accelerator, use this user account to see mobile application terminology.
User name/password (uses Enterprise Portal terms)	opsuper/0psuper (the first character is a zero)	Created automatically during installation. If you are upgrading from Enterprise Portal to Unwired Accelerator, use this user account to see EP terminology; for example, “portlets” instead of “applications.”
MobiLink (optional, Windows only)		
Notification port	8777	
Database port	5000	Same as ASE value.
Database user name	sa	Same as ASE value.
Password	“ ” (no password)	Same as ASE value.

Preinstallation tasks

Before you install Unwired Accelerator, you must:

- Install Adaptive Server Enterprise, Enterprise Edition. Keep in mind the following:
  - Page size – when you create the Adaptive Server, it is imperative to set the page size to 8K or larger, otherwise the Unwired Accelerator installer stops and will not proceed. Once you set the page size to 8K or larger, you can restart the installation. A page size of 8K or larger avoids data truncation problems later when running Unwired Accelerator.
  - Localization with UTF-8 – to support non-English data, be sure to configure Adaptive Server with character set UTF-8. To do so, follow the Adaptive Server Enterprise installation/configuration menus, or run /$SYBASE/ASE-15_0/bin/asecfg to localize an existing server with the UTF-8 character set.

  See the Adaptive Server Enterprise 15.0.1 installation guide and release bulletin for installation procedures. The Adaptive Server Enterprise guides are located on the Getting Started CD.

- Create an Adaptive Server Enterprise data device and log device to act as a data store for Unwired Accelerator. You can use any method you like to create the devices, including using your own scripts, but you must use these exact device names and minimum sizes:
  - portalData – name for the data device (minimum size 250MB).
  - portalLog – name for the log device (minimum size 75MB).
  - uamlData – name for the MobiLink data device (minimum size 150MB).
  - uamlLog – name for the MobiLink log device (minimum size 75MB).

  See the *Adaptive Server Enterprise Administration Guide* and the *Adaptive Server Enterprise Performance and Tuning Guide* for additional information.

  Note You can select to have the Unwired Accelerator installer create the devices, although Sybase does not recommend this option. File-based devices do not take full advantage of Adaptive Server Enterprise data store features.

- Start Adaptive Server Enterprise before you start the Unwired Accelerator installation.
- Verify that there is a "." (dot) in the PATH environment variable.
- Verify that the $JAVA_HOME environment variable points to a valid JVM directory.
- Add $JAVA_HOME/bin to PATH.
- Verify that you have write permission on your login home directory, and the directory where you install the software.

  Note You must have a home directory, such as */usr/u/username*, on the IBM Linux POWER machine, otherwise the Unwired Accelerator installer cannot find the location for UA 8.0 and reports errors.

  If you are uninstalling Unwired Accelerator, verify you have write permission on the temporary directory, typically */tmp*. Uninstallation logs are written to */tmp*.
- Verify that you have 100MB free space in your temporary directory, typically */tmp*; otherwise, the installation fails.

If you do not have enough space in your */tmp* directory, redirect the installer to use a different directory for temporary space.

Note The temporary directory to which you are redirecting must exist before you set the environment variable.

To redirect your temporary directory, enter:

```
./setupLinux.bin -is:tempdir /work/tmp
```

where */work/tmp* is the directory of your choice.

- Know the domain name of the machine where you are installing Unwired Accelerator. To find your domain name, contact your system administrator, or at a command prompt, enter:

  ```
  hostname --fqdn
  ```

  Your host and domain displays, for example, `lapxp.sybase.com`, where `sybase.com` is the domain name.

- Install any Sybase EBFs listed in the release bulletin.
- If you plan to use MobiLink server to deploy mobile applications, identify a suitable Windows 2003 or XP machine on the network. The machine requirements include:
  - Disk Space: 75MB minimum; 100MB recommended
  - RAM: 512MB minimum; 700MB recommended

  You install the MobiLink server on the Windows machine as a post-installation task (described in “Installing MobiLink server on Windows (optional)” on page 16).

  You also need to install an Adaptive Server Enterprise EBF to obtain the correct ODBC driver (15.00.00.140 or higher) needed to communicate between Adaptive Server Enterprise, and MobiLink.

Installation tasks

This section discusses installing Unwired Accelerator in a network environment. Installation takes five to ten minutes, depending on the speed of your machine.

You can install Unwired Accelerator using the installer, or from the console. Both procedures are provided.

❖ **Installing Unwired Accelerator (installer)**

Typically you can use any account to install Unwired Accelerator in Tomcat.

1 Insert the Installation CD.

2 Launch the installer by running setupLinux.bin. This may take a few moments. The Sybase splash screen displays, followed by the Welcome window.

3 Click Next. The End-User License window displays.

4 Select the license agreement appropriate for the country or region where you are installing the software. The license displays.

Read the license agreement and select "I do agree to the terms of the Sybase license, for the install location specified." Click Next.

5 In the next window, accept the default installation directory, or enter the directory in which to install Unwired Accelerator. For example, enter */opt/sybase/UA80*. The installation directory is referred to as *$SYBASE* in this guide.

6 The installer checks for available disk space. If there is not enough disk space, the installer reports the problem and closes. You must free up disk space and start again.

The installer also verifies you have sufficient permission to create the directory. If there is not, the installer reports the problem and closes. You must fix the permissions and start again.

7 In the next window, enter host and domain information, or accept the default values:

- Domain Name – the installer inserts the name of the domain (and subdomain if used) of the machine on which you are installing Unwired Accelerator; for example, *sybase.com*.
- Host Name – the installer inserts the name of the machine on which you are installing Unwired Accelerator; for example, `labxp`.

Click Next.

8 In the next window, enter Adaptive Server Enterprise database parameters, or accept the defaults:

- ASE Database Host – the machine name on which the Adaptive Server Enterprise database is installed; for example, `myASE`.
- ASE Database Port – by default, the installer inserts `5000` for the Adaptive Server Enterprise database (see Table 2-2 on page 4).
- ASE Database Username – the Adaptive Server Enterprise user name; for example, the default is `sa`.
- ASE Database Password – the Adaptive Server Enterprise user password; for example, the default for `sa` is blank (no password).

9 In the same window, indicate how to handle database and log devices:

- If the Create Default File-Based Data and Log Devices check box is not selected, the installer verifies the devices for portalData, portalLog, uamlData, and uamlLog exist.

  If they do not exist, an error message displays, and the installation does not proceed until these devices are created or the check box is selected.
- If the check box is marked, the installer creates four files in the specified directory to be used as ASE data devices: portalData, portalLog, uamlData, and uamlLog.

  If insufficient disk space is available for the given directory, an error message displays and the installation does not continue.

Note The databases (portaldatabase, uaml) that will use these devices are created and populated during the configuration phase later in the installation process.

Click Next.

The installer uses the values to connect to the database. If the connection fails, or the database version is not as expected, an error message displays and the installation process stops until a successful connection can be made.

10 In the next window, enter Unwired Accelerator server port numbers, or accept the defaults:

- HTTP Port – by default, the installer inserts `4040` for the Unwired Accelerator HTTP port (see Table 2-2 on page 4). Accept the default or provide another valid value. Note that UA configuration files use `4040` as the default Unwired Accelerator HTTP port.

- HTTPS Port – by default, the installer inserts `4443` for the Unwired Accelerator HTTPS port (see Table 2-2 on page 4). Accept the default or provide another valid value.

Note If you change the server or port value, and are using the Pocket PC client developed by the .NET API, you will need to update the MobiLink database with the new value (as described in the postinstallation procedure, "Updating MobiLink database with new server/port settings (optional)" on page 19). [CR #447165]

Click Next.

11 The Installation Progress window displays. During installation, these files are updated with the configuration information you supplied:

- *global.properties.xml* – changes the default host name and domain name to the machine name and domain name that you provided. The *global.properties.xml* file is located in:

  $SYBASE/tomcat/webapps/onepage

- *domain.js* – changes the default domain name to the name you provided. The *domain.js* file is located in:

  $SYBASE/tomcat/webapps/onepage/javascript

- *server.xml* – changes the default port number to the number you provided. The *server.xml* file is located in:

  $SYBASE/tomcat/conf/

The Installation Summary window displays and reports success or failure of the installation.

12 Click Finish.

13 In the terminal window, from *$SYBASE*, enter `starttomcat.sh` or `startua.sh`. This starts the Tomcat application server and Unwired Accelerator (if Adaptive Server Enterprise is running).

Note If you are using port 80 (HTTP) and port 443 (HTTPS), you must log in as root to start Tomcat.

When Tomcat starts, you see a series of messages in the Tomcat window, including the following:

```
Using CATALINA_BASE:   $SYBASE/tomcat
```

```
Using CATALINA_HOME:   $SYBASE/tomcat
Using CATALINA_TMPDIR: $SYBASE/tomcat/temp
Using JAVA_HOME:       ./JDK1.5.0_05
```

14 The Unwired Accelerator installation is complete. See "Verifying the installation" on page 12 to verify the network installation works correctly

If you cannot connect to the application, go to *$SYBASE/tomcat/logs* and check the *catalina.out* file for Tomcat errors, or go to *$SYBASE/logs* for Unwired Accelerator and installer logs.

❖ **Installing Unwired Accelerator (from the console)**

You can install Unwired Accelerator using a script from the console, instead of the GUI installer. Sybase recommends installing as root from the console.

1 Log in as root.

2 Insert the Installation CD.

3 Launch the installer by running setupLinux.bin -console. The installer panels appear in the same order as in the GUI installer.

4 Enter a value for each item in order. For an item with a choice, select the option using numbers (such as `1/2/3`) and press Enter.

You can navigate on each panel using `back/next/cancel`, and refresh the panel using `redisplay`.

5 Once the installer script finishes:

- If you installed UA as root, you can either restart the machine to start the Tomcat application server automatically as a service, or you can use `starttomcat.sh` or `startua.sh` to start Tomcat application server and Unwired Accelerator manually without restarting the machine.
- If you did not install as root, you can use either `starttomcat.sh` or `startua.sh` to start the Tomcat application server and Unwired Accelerator.

Post-installation tasks

This section describes post-installation tasks. Only perform the procedures for the features needed in your installation. Topics include:

- Verifying the installation
- Configuring for a proxy server
- Updating digital certificates
- Installing MobiLink server on Windows (optional)
- Installing the UA offline client
- Installing BlackBerry server
- Installing the UA .NET container client on Windows (optional)
- Setting up a SAP connection
- Configuring Tomcat for LDAP

Note In this section, the Tomcat version of path names is used, such as *$SYBASE/tomcat/webapps/onepage*.

Verifying the installation

Verify your Unwired Accelerator installation by checking the Portal Interface and Mobile Web Studio installations.

❖ **Checking the Portal Interface installation**

1 Open an Internet Explorer browser window, and enter the Unwired Accelerator address in the following format:

```
http://hostname.domain:port/onepage/mpindex.jsp
```

where:

- *hostname* – is the name of the machine where you installed Unwired Accelerator; for example, “labxp.”
- *domain* – is the domain name where the installation is located; for example, “sybase.com.”
- *port* – is the Unwired Accelerator port number (the default is 4040 for Tomcat).

For example:

```
http://labxp.sybase.com:4040/onepage/mpindex.jsp
```

The Portal Interface Welcome window displays.

2 Click Join Now to set up a new user profile.

3 Set up a new user profile:

a Enter your first name.

b Enter your last name.

c Enter your e-mail address.

d Enter your telephone number.

e Choose a member name.

f Choose a password.

g Confirm your password.

h Select the PortalUser role.

i 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 Welcome window. This initial window is the Default Page Group. See the *Portal Interface User's Guide* for more information.

Note Once you set up a user profile, you receive registration confirmation at the e-mail address you provided when setting up the profile.

❖ **Checking the Mobile Web Studio installation**

1 Open another browser window and navigate to:

`http://`*`hostname`*`.`*`domain`*`:`*`port`*`/onepage/loader.html`

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

```
http://labxp.sybase.com:4040/onepage/loader.html
```

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

The Mobile Web Studio window opens. (If a window with a Close button opens, minimize the window, but do not close it).

If the Mobile Web Studio window does not display, see Table 3-2 on page 36 for information.

2 In Mobile Web Studio, log in using `masuper` as the user name, and `m8super` as the password. See the *Quick Start Guide* and *Mobile Application Development Tutorial* for information.

Setting the mail.host property

When you create a new user in Mobile Web Studio, a verification e-mail message with the user's password is sent to you. Change the mail.host property in the *global.properties.xml* file to your SMTP host.

1 Navigate to *$SYBASE/tomcat/webapps/onepage/config*, and open the *global.properties.xml* file with a text editor.

2 Locate the `Property name="mail.host" value="xx.xx.xx.xxx"` line and change the value to the IP address of the SMTP host of your mail server.

Configuring for a proxy server

If you are using a proxy server, configure Unwired Accelerator with the appropriate proxy settings. Make changes in the *global.properties.xml* file, located in *$SYBASE/tomcat/webapps/onepage/config*. The settings include:

- proxy – enables a proxy server, if a squid type HTTP proxy is available.
- proxy.host – identifies the proxy server name or IP address.
- proxy.port – identifies the proxy server port number.
- proxy.bypass_list – identifies a list of IP addresses or host names that should bypass the proxy server.

Note See the *Unwired Accelerator Administration Guide* for more information about the *global.properties.xml* file and setting up a proxy server.

❖ **Configuring UA to access the Internet through a proxy server**

Use this approach when UA needs to use a proxy to access Web sites on the Internet.

1 Navigate to *$SYBASE/tomcat/webapps/onepage/config*.

2 In 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 http proxy
server 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 http proxy 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 3128, the line looks like this:

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

5 To the proxy.bypass_list value, add the IP addresses or host names to bypass the proxy server. 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" description="(host1|host2).
please read HTTPConnection javadocs for info on
dontProxyFor() method for more info"
menugroup="100"/
```

❖ **Configuring end user access to UA (via a firewall and reverse proxy)**

Use this approach when an end-user is trying to access UA, but must go through a firewall and reverse proxy to access it.

1 Modify the *global.properties.xml* file:

   a Navigate to *$SYBASE/tomcat/webapps/onepage/config*.

   b In a text editor, open *global.properties.xml* and change the proxy value to "on."

   c Set the proxy.host and proxy.port values to the host and port values where the reverse proxy is running.

d Save the changes and close the file.

2 Modify the *server.xml* file, by adding the proxyName and proxyPort attributes to the `<Connector>` element.

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 trusted authorities.

Unwired Accelerator uses a certificate that is created using the keytool utility that ships with Java Development Kit (JDK) 1.4.*x*. 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.

Installing MobiLink server on Windows (optional)

This section describes how to install MobiLink server on Windows, if you want to use MobiLink to deploy mobile applications to devices. Basically you:

- Install the Adaptive Server Enterprise ODBC driver (15.00.00.140 or higher), needed to communicate between Adaptive Server Enterprise and MobiLink, onto the Windows machine.
- Unzip the MobiLink software onto the same Windows machine.
- Run scripts to configure MobiLink to communicate with Unwired Accelerator running on Linux on POWER.

Before you install the MobiLink server on the Windows machine, you must:

- Make sure you have the correct MSXML Service Pack installed on the Windows machine (as described in “Installing MSXML 4.0 SP2” on page 17).
- Create a log file directory on the Windows machine, typically *X:\tmp\logs*. The MobiLink log file (*ml.Log*) will be written to this directory.

Note You must have Internet access to install MobiLink.

❖ **Installing MSXML 4.0 SP2**

Before you start installing MobiLink server, make sure MSXML 4.0 Service Pack 2 is installed. MobilLink requires this version of MSXML, which includes the *ulxml.exe* file, to generate schema files for clients.

1 On the Windows 2003 or Windows XP machine, make sure MSXML 4.0 Service Pack 2 (SP2) is installed.

To check the version:

a Locate the *msxml4.dll* file, typically found in *x:\WINDOWS\system32*.

Note You will find multiple *msxml* files; be sure to find *msxml4.dll*.

b Right-click *msxml4.dll*, and select Properties | Version to display the version.

2 If you do not have MSXML 4.0 SP2 installed, you can download it from the Microsoft download site at http://www.microsoft.com/downloads/. Search for "MSXML 4.0" to find the MSXML 4.0 Service Pack 2 download.

Note If you choose the MSI file option, you need Windows Installer 2.0 on the Windows machine. You may have an older version of Windows Installer installer on the Windows machine; if it is not sufficient, you are prompted to download a more current version.

3 Follow the instructions on the Microsoft Web site to download the software. See the *MSXML 4.0 SP2 Release Notes* for additional information.

You can start the installation immediately, or copy the download to your Windows machine and install the software at a later time.

Note If you chose to install MSXML using the MSI file option, and have an older version of Windows Installer on the Windows machine, you may be prompted to download a more current version.

❖ **Installing MobiLink server**

Install MobiLink server on a Windows 2003 or Windows XP machine with network and Internet access.

1 Install the Adaptive Server Enterprise ODBC driver (15.00.00.140 or higher), which is needed to communicate between MobiLink and Adaptive Server Enterprise. To do so:

   a Obtain the ODBC driver:

      1 On the Windows machine, go to the Sybase download site at http://downloads.sybase.com.

      2 Log in using your account.

      3 Select "Software Development Kit."

      4 Scroll down to Windows x86.

      5 Download "Software Development Kit – EBF 13955: 15.0 ESD #6 (16 Oct 2006)."

   b Install the ODBC driver on the Windows machine.

   c Create the ODBC connection by configuring DSN so that the Adaptive Server Enterprise ODBC driver points to the Adaptive Server Enterprise installed on Linux on POWER.

2 Make sure JAVA_HOME is set, and the executable is in the PATH.

3 On the Installation CD, locate *mlForWindowsPPC.zip*.

4 Unzip *mlForWindowsPPC.zip* onto the Windows 2003 or Windows XP machine. You can unzip the file into any directory, as long as the directory path uses contiguous characters, and includes no spaces (spaces in the path name causes problems); for example, *C:\Sybase\MobiLink* or *C:\MobiLink*. This creates a directory *mlForPPC* and includes some *.bat* script files and the */asa* directory.

Note In this document, %SYBASE% is used to indicate the Unwired Accelerator MobiLink installation directory on Windows 2003 or XP.

5 Edit the *%SYBASE%\setenv.bat* script:

   a Modify the `DB_DSN` name to be the ODBC DSN name you just created.

   b Set `INSTALL_FOR_PPC` to `true`.

6 Edit the *%SYBASE%\configML.sql* script to change database URL's, user names, and passwords for the UASMS and UAUSM gateway entries:

   a Open the file in a text editor.

b Make the following changes:

- Check the UASMS URL value; it should contain `...:5000/portaldatabase` so that gateway ends up in the portaldatabase where the tables it needs are.
- Check the UAUSM value; it should change to `...:5000/uaml` to use the consolidated database.
- Check `db_user` and `db_pwd`, and change the default values if you changed them.

  Your entries should look similar to:

```
exec ml_add_property 'SIS',
'com.sybase.ua.gateway.USMGateway(UAUSM)',
'database_url', 'jdbc:sybase:Tds:powerplay2.sybase.com:4101/uaml' ;
...
exec ml_add_property 'SIS',
'com.sybase.ua.gateway.USMGateway(UAUSM)',
'db_user', 'sa' ;
exec ml_add_property 'SIS',
'com.sybase.ua.gateway.USMGateway(UAUSM)',
'db_pwd', '' ;
```

- Edit other properties if you made additional configuration changes to set up your environment.

c Save the file.

7 Run the *%SYBASE%\setAsaRegistry.bat* script to set the values in the registry.

8 Run the *%SYBASE%\configml.bat* script to define the MobiLink values in the portaldatabase.

9 Run the *%SYBASE%\startmlsrv.bat* script to start MobiLink.

If you encounter any problems, see the MobiLink error log in *X:\tmp\logs\ml.log* for information.

❖ **Updating MobiLink database with new server/port settings (optional)**

This step is only necessary if you changed the HTTP server or port values during installation, and are using the Pocket PC client developed by the .NET API. This step updates the MobiLink database with the new server or port value, so you can synchronize mobile applications successfully. [CR #447165]

1 Log in to Mobile Web Studio.

2 Click the MobiLink menu item. This automatically updates all the appropriate database entries with the new server/port settings.

❖ **Uninstalling MobiLink server**

Do the following to uninstall the Unwired Accelerator MobiLink server from the Windows 2003 or XP machine:

1 Run the *%SYBASE%\delAsaRegistry.bat* script to remove the ASA registry entries

2 Remove the directory *%SYBASE%\mlForPPC*.

3 Uninstall the Adaptive Server Enterprise PC Client software using the uninstaller software.

Installing the UA offline client

This section shows how to install the Unwired Accelerator offline client application on a BlackBerry device via the BlackBerry Desktop Manager or over the air (OTA), and on a simulator. The offline client enables you to use the applications you create through Unwired Accelerator on your BlackBerry device in offline mode.

- The UA offline client is available in:

  $SYBASE/tomcat/webapps/onepage/ota/bb/direct

- The OTA version of the UA client is available in:

  $*SYBASE/tomcat/webapps/onepage/ota/bb*

Develop a process for making the offline client available for BlackBerry users.

❖ **Installing an offline client on a BlackBerry device using BlackBerry Desktop Manager**

The offline client enables you to use the applications you create through Unwired Accelerator on your BlackBerry device in offline mode.

1 Connect the BlackBerry device to the computer that contains your UA offline client files.

2 Run the BlackBerry Desktop Manager using the RIM documentation.

3 Click Application Loader to start the wizard, then click Next. The Application Loader wizard displays.

4 Click Add, navigate to *$SYBASE/UA80/tomcat/webapps/onepage/ota/bb/direct*, and select the *UAclient.alx*, *Uaframework.alx*, and *Ualistener.alx* files.

5 Click Open. The application is listed on the Application Loader wizard.

6 Click Next to continue. The application is installed on your BlackBerry device.

7 Access your BlackBerry device. You see the Unwired Accelerator (UA) icon.

8 To run the Unwired Accelerator offline client, use the trackwheel to highlight the Unwired Accelerator (UA) icon, and open it. The Unwired Accelerator screen displays. The message starting with `Currently there are no synchronized applications available` displays.

9 Set up a user on the BlackBerry device as described in "Setting up a UA user on BlackBerry" on page 21.

❖ **Obtaining the offline client OTA**

1 On the BlackBerry device, use the BlackBerry browser to navigate to `http://hostname.domain:port/onepage/ota/`.

2 Click on UA Framework, to down load *Uaframework.jad*. This downloads and installs the UA framework, needed for push synchronization.

3 Click on UA Listener, and then on Standard Client to down load *Ualistener.jad* and *Uaclient.jad*. This downloads and installs the UA listener and UA client, also needed for push synchronization.

❖ **Setting up a UA user on BlackBerry**

1 Make sure the BlackBerry offline client is running on the device. You should see the Unwired Accelerator icon in the application menu.

2 Select the Profiles option on the trackwheel menu.

3 From Connection Profiles, select the New Profile option from the trackwheel menu.

4 On the New Profile window, enter:

- Profile Name – the profile name for the account, such as `mwsAdmin`.
- Username – the account user name, such as `masuper`.
- Password – the account password, such as `m8super`.

- Resource ID – the default resource identifier (RID) for the account, such as `21` for Unwired Accelerator.
- Server name – the server and domain on which Unwired Accelerator is running, such as `machinename.sybase.com`.
- Port number – the port used to access Unwired Accelerator, such as `4040`.

5 Select Save from the trackwheel menu, and save the settings.

6 Highlight the new profile, and select Set as Active from the trackwheel menu.

7 Select Close from the trackwheel menu to return to Unwired Accelerator.

Once you use Mobile Web Studio to create mobile applications, and synchronize, you see the applications on the mobile device. To create mobile applications, see these Unwired Accelerator documents:

- *Quick Start Guide*
- *Mobile Application Development Tutorial*

Downloading the BlackBerry simulator

If you do not have a BlackBerry device, a simulator is available for download from the RIM BlackBerry Web site at http://www.blackberry.net/developers.

1 On the Developers page, under the Downloads link, select BlackBerry Simulators.

2 On the BlackBerry Simulators page, click Download a Device Simulator.

3 In the next window, select BlackBerry Handheld Simulator v4.1 from the drop-down list.

4 Select BlackBerry Handheld Simulator v4.1.0.292.

For simulator documentation, access the Developer's window; select the Developer Documentation link under "Development Questions;" and scroll down to the Simulator section.

❖ Installing an offline client on a BlackBerry simulator

A BlackBerry simulator, installed on the desktop, can be a useful tool for testing and troubleshooting mobile applications during development.

1 Navigate to *$SYBASE/tomcat/webapps/onepage/ota/bb/direct*.

2 Copy the *Uaclient.**, *Uaframework.**, and *Ualistener.** files into your BlackBerry simulator installation directory:

$RIM/Research In Motion/BlackBerry JDE 4.x/simulator

3 Optionally, select Start | Programs | Research In Motion | BlackBerry Java Development Environment 4.1.*x* | MDS Simulator to start the BES simulator. You can minimize the Java.exe window.

4 Select Start | Programs | Research In Motion | BlackBerry Java Development Environment 4.1.*x* | Device Simulator to start the BlackBerry device simulator. You can minimize the Device Simulator window.

5 Access the BlackBerry Handheld Simulator window. You see the Unwired Accelerator (UA) icon.

6 To run the UA offline client, highlight the Unwired Accelerator icon, and open it. The Unwired Accelerator window displays. The message starting with `Currently there are no synchronized applications available` displays.

7 Set up a user on the BlackBerry simulator as described in "Setting up a UA user on BlackBerry" on page 21.

Installing RIM BlackBerry server

This section provides information for setting up a Research In Motion (RIM) BlackBerry server.

Installing BlackBerry server

The RIM BlackBerry Enterprise Server (BES) serves as a centralized link between a company's enterprise infrastructure and messaging platform with the company's mobile wireless users.

To use BES to deploy applications to BlackBerry devices, make sure of the following before you install the offline client on the BlackBerry device:

- The RIM BES software is installed and configured correctly, using the RIM installation documentation.
- The RIM BlackBerry Desktop Manager software is installed and configured correctly. The minimum requirement for the BlackBerry Desktop Manager software is version 4.0.

- The BlackBerry device has connectivity with BES, and that you can synchronize between BES and the BlackBerry device.

Configuring BES to maintain cookies

Configure the BlackBerry BES to maintain cookies on behalf of BlackBerry devices. Without cookies, the JSESSIONID cookie cannot be maintained, BlackBerry users receive `Permission denied` errors, and transactions do not make it to the portaldatabase. [CR #445712]

See your RIM documentation for information about configuring how the Mobile Data Service manages web requests from handhelds. To summarize the official documentation:

1 In BlackBerry Manager, right-click a server, and click Mobile Data Service Properties.

2 Select the HTTP tab.

3 Select the “Allow the Mobile Data Service to handle HTTP Cookie Storage” check box.

4 Click OK. This setting caches cookies on behalf of the handheld and permits the MDS to add cookie information to HTTP request from handhelds.

Setting up BlackBerry users

See your RIM documentation for information about setting up BlackBerry users on the BES server:

Installing the UA .NET container client on Windows (optional)

You can also install the 8.0 .NET container client on a Windows mobile PDA. The .NET container client enables you to deploy and synchronize mobile applications between Unwired Accelerator and Windows-based mobile devices.

See the *Unwired Accelerator Developer's Guide* for information about installing and using the .NET container client. Keep in mind that Unwired Accelerator pathnames are different for Linux on POWER, typically:

$SYBASE/UA80/tomcat/webapps/onepage/ota

Setting up a SAP connection

This section describes how to set up a SAP connection, if you plan to develop mobile applications using the SAP framework.

To set up the SAP connection you must:

- Configure the SAP connection using the SAP Java Connector (SAP JCo). SAP JCo is a toolkit that allows a Java application to communicate with any SAP system. The SAP Java Connector can be downloaded from the SAP Service Marketplace Web site by a registered SAP customer.
- Modify the *global.properties.xml* file to enable SAP and identify ConnectionPools.
- Create a property file for each ConnectionPool, and configure connection properties.

Details for each of these steps are provided in the procedures that follow. Once you have set up the SAP connections, you can create SAP elements in the Mobile Web Studio Application Builder. See the *Unwired Accelerator Developer's Guide* for information about using the SAP element.

❖ **Configuring the SAP Java connector**

1 Open a Web browser window and enter the SAP Marketplace URL, which currently is:

```
https://websmp204.sap-ag.de/swdc
```

The Client Authentication window displays.

2 Select the certificate to use when connecting, and click OK. The Enter Network Password window displays.

3 Enter your registered SAP customer user name and password in the User Name and Password fields, and click OK. The SAP Software Distribution Center window displays.

4 In the You Are Here navigation bar on the left side of the page, navigate to Download | SAP Connectors | SAP Java Connector | Tools and Services. Click the link for SAP JCo Release 2.0.12 to download the SAP Java Connector.

5 Follow the installation instructions provided by SAP. When prompted, copy the *.jar* and *.so* files to these locations:

- Copy *sapjco.jar* to:

  Tomcat

$SYBASE/tomcat/webapps/onepage/WEB-INF/lib

- Copy *librfccm.so* and *libsapjcorfc.so* to:

  Tomcat

  $SYBASE/jdk1.5.0_05/jre/bin

6 Close the Web browser.

7 Change to the following directory:

Tomcat

$SYBASE/tomcat/webapps/onepage
/WEB-INF/classes

8 As a backup, save a copy of the *sapjco.properties* file to a name such as *template.sapjco.properties*.

9 Using a text editor, open the *sapjco.properties* file and edit it for your environment. The SAP wizard uses information in the *sapjco.properties* file to connect to your SAP system.

Check the documentation that comes with the JCO package for information about the 30-40 properties you can set to define a SAP connection. Specifically see the Javadocs for the JCO.createClient (java.util.Properties) method. The six most commonly used properties are included in the file as a sample (for example, jco.client.client=400).

10 Save the file and close it.

11 Restart the Tomcat application server, using information in "Starting and stopping the Tomcat application server" on page 29.

❖ **Modifying the *global.properties.xml* file for SAP**

Modify the SAP-related properties in *global.properties.xml*.

- SAP.Enabled – enables SAP in Mobile Web Studio.
- ConnectionPools – a comma-separated list of connection pool names. Each connection pool must have a *poolname.properties* file defined as described in "Creating ConnectionPool property files" on page 27.
- DefaultConnectionPoolName – identifies the connection pool to use for the default SAP connection.

1 In a text editor, open *global.properties.xml*, located in *$SYBASE/tomcat/webapps/onepage/config* if you are using Tomcat.

2 Search the file for `SAPGroup`.

3 Look for SAP.Enabled. By default, SAP.Enabled is set to “false.” Change the entry to “true.”

4 Look for: `<Property name="ConnectionPools"`. By default, ConnectionPools is set to “sapjco.”

```
<Property name="ConnectionPools" value="sapjco"
    description="Comma separated list of connectionpool
    names." menugroup="100" />
</PropertyGroup>
```

The default ConnectionPool “sapjco” has a corresponding property file *sapjco.properties* in which SAP connection properties are defined. Each ConnectionPool name in the list must have its own property file, as described in “Creating ConnectionPool property files” on page 27.

Identify the ConnectionPools you need for SAP connection, using SAP documentation, and change the value as necessary.

5 Look for: `<Property name="DefaultConnection PoolName".`

By default, DefaultConnectionPoolName is set to “sapjco.”

```
<Property name="DefaultConnectionPoolName"
value="sapjco"
    description="connection pool name for the default
    SAP connection" menugroup="100" />
</PropertyGroup>
```

Determine which ConnectionPool to use as the default SAP connection from the list, and change the value as necessary.

6 Save the file and close it.

❖ **Creating ConnectionPool property files**

For each ConnectionPool listed in the *global.properties.xml* file, there should be a *poolname.properties* file in *$SYBASE/tomcat/onepage/WEB-INF/classes*. Use the *sapjco.properties* file (or *template.sapjco.properties* file) as a base, and modify the ConnectionPool connection properties, using information in the JCO package Javadocs as a guide.

1 In a text editor, open *sapjco.properties* (located in *$SYBASE/tomcat/webapps/onepage/config*).

2 Save the file in the same directory, using the following naming format:

poolname.properties

Substitute one of the ConnectionPool names you established in the *global.properties.xml* file for *poolname*.

3 Modify the file by setting up the connection properties for the SAP connection. The following properties are included in the file as an example. Check the Javadocs for information about these properties, and many more.

```
jco.client.client=400
jco.client.user=sap
jco.client.passwd=1sap
jco.client.lang=EN
jco.client.ashost=sap.try.sybase.com
jco.client.sysnr=00
```

4 Save the file and close it.

Configuring Tomcat for LDAP

Tomcat comes preconfigured with Common Security Infrastructure (CSI) and PortalDB security provider. To configure Tomcat to use the Lightweight Directory Access Protocol (LDAP) security provider, see Appendix A, “Setting Up Authentication and Authorization.”

Currently, a user created in LDAP server must log in to the Portal Interface to activate their profile (see the release bulletin for information about CR #359766).

See the *Unwired Accelerator Administration Guide* for information about CSI and its security features.

Starting and stopping the system

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

Stop the applications in this order:

1 Application server (Tomcat)

2 Database (ASE)

Start the applications in this order:

1 Database (ASE)

2 Application server (Tomcat)

Starting and stopping Adaptive Server Enterprise

Typically Adaptive Server Enterprise is left running. If you need to stop and start Adaptive Server Enterprise, see the Adaptive Server Enterprise documentation for instructions.

Starting and stopping the Tomcat application server

This section describes how to start and stop the Tomcat application server.

❖ **Starting the Tomcat application server**

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

2 Enter `starttomcat.sh`, or `startua.sh` to start the Unwired Accelerator server.

When Tomcat starts, you see:

```
Using CATALINA_BASE:   $SYBASE/tomcat
Using CATALINA_HOME:   $SYBASE/tomcat
Using CATALINA_TMPDIR: $SYBASE//tomcat/temp
Using JAVA_HOME:       ./JDK1.5.0_05
```

❖ **Shutting down the Tomcat application server**

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

2 Enter `stoptomcat.sh`, or `stopua.sh` to stop the Unwired Accelerator server.

Starting and stopping MobiLink

This section describes how to start and stop MobiLink.

❖ **Starting MobiLink**

1 From a Command Prompt window, navigate to *%SYBASE%\UA80*.

2 Enter `startmlsrv`, or double-click the *startmlsrv.bat* file in Windows Explorer.

❖ **Shutting down MobiLink**

1 From a Command Prompt window, navigate to *%SYBASE%\UA80*.

2 Enter `stopmlsrv`, or double-click the *stopmlsrv.bat* file in Windows Explorer.

Uninstalling Unwired Accelerator

This section provides instructions for uninstalling Unwired Accelerator using the uninstaller. Two options are available – for one option, the installer removes files, databases, and devices automatically, for the other, you must manually remove some files.

Note Before you start, make sure you have a home directory, permissions set, $JAVA_HOME set properly, as described in "Preinstallation tasks" on page 5. The Unwired Accelerator installer requires these environmental settings, whether installing or uninstalling Unwired Accelerator.

❖ **Removing Unwired Accelerator**

In this option, the uninstaller removes the Unwired Accelerator files and the entire Tomcat application server, drops the appropriate databases, and drops the devices.

1 Shut down Tomcat, by opening a terminal window, navigating to *$SYBASE*, and entering `stoptomcat.sh`.

2 Navigate to *$SYBASE/Uninstaller*.

3 At the command line, use one of the following commands to launch the Unwired Accelerator uninstaller:

```
./uninstallUA80
```

or:

```
java -jar uninstallUA80.jar
```

4 Answer the uninstaller prompts. The uninstaller removes Unwired Accelerator and the Tomcat application server, and drops uaml and portaldatabase.

5 Remove the UA log directory, *UALogs<user_login>*, for example, */tmp/UALogsmarkusb*.

Note If you find that databases are not dropped, or devices are not deleted, this may indicate a lock. See the Adaptive Server Enterprise documentation for information about locating and removing the lock. You can manually drop the databases and devices.

CHAPTER 3

Troubleshooting

This chapter describes how to troubleshoot installation and configuration problems for Unwired Accelerator and various integrated products.

Overview

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

- Viewing error log device output
- Viewing log files, typically found in *$SYBASE/logs*
- Viewing error messages
- Checking port numbers
- Checking configuration files (especially *global.properties.xml*, *server.xml*)
- Testing connections
- Running the Portal Interface and Mobile Web Studio
- Running the .NET client
- Running the BlackBerry client
- Running mobile device applications

Installer/Uninstaller

Table 3-1 identifies common installation and uninstall problems, and provides troubleshooting information

Table 3-1: Troubleshooting installation problems

Problem	Try this
The Unwired Accelerator installer stops with errors.	The installer checks the following, and stops with errors if it encounters a problem. • Checks for available disk space for installing Unwired Accelerator. • Checks for sufficient permission to create the $SYBASE installation directory. • Verifies Unwired Accelerator can connect to Adaptive Server Enterprise. • Verifies the Adaptive Server Enterprise page-size is 8K or more. You must fix the problem, and then restart the installer from the beginning.
The Unwired Accelerator installer reports errors [CR #445501]	Make sure you have a home directory, such as */usr/u/username*, on the IBM POWER machine, otherwise Unwired Accelerator installer cannot find the location for UA 8.0 and reports errors.

Problem	Try this

Conflict with JIT compiler	The Tomcat JIT compiler may conflict with the IBM Linux POWER JIT compiler. Sybase recommends disabling the Tomcat JIT compiler:
	1 Navigate to:
	$SYBASE/jdk1.5.0_05
	2 Check to see whether the JIT compiler is enabled:
	`java -version`
	Information similar to the following displays:
	`java version "1.5.0"`
	`Java(TM) 2 Runtime Environment,`
	`Standard Edition (build pxp64dev-`
	`20061002a (SR3) )`
	`IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9`
	`2.3 Linux ppc64-64 j9vmxp6423-20061001`
	`(JIT enabled)`
	`J9VM - 20060915_08260_BHdSMr`
	`JIT - 20060908_1811_r8`
	`GC - 20060906_AA)`
	`JCL - 20061002`
	3 If you see `JIT enabled`, modify the Java command line in *catalina.sh* to include:
	`-Xnojit`
	This disables the Tomcat JIT compiler.

MobiLink cannot connect with Adaptive Server Enterprise, and reports errors	Check the MobiLink console and the *$SYBASE/logs/ml.log* file for error messages. Then correct the configuration, using information in "Installing MobiLink server on Windows (optional)" on page 16.
After uninstalling Unwired Accelerator, UA databases or devices remain	This could indicate that a lock is in place for the databases or devices. see the Adaptive Server Enterprise documentation for information about finding and removing the lock.

Unwired Accelerator setup

Table 3-2 identifies common Unwired Accelerator configuration problems and provides useful troubleshooting information.

Table 3-2: Troubleshooting Unwired Accelerator problems

Problem	Try this
Cannot start the application server	This can happen if you are using ports 80 (HTTP) and 443 (HTTPS) with Netscape, and you did not install Unwired Accelerator with root privileges, which are required to start these ports in the production system. • Check the *catalina.out* file, located in *$SYBASE/tomcat/logs*, for errors. Try uninstalling and then reinstalling Unwired Accelerator. Log in as root as described in "Installation tasks" on page 7 (Tomcat application server).
Cannot start the Portal Interface: File Not Found 404 error	If you receive this error when trying to start Portal Interface: • Check to make sure you entered the URL correctly to access Portal Interface as described in "Verifying the installation" on page 12. • Check to make sure you are using the correct port number; for example, 4040 when running in Tomcat. • Check the *catalina.out* file, located in *$SYBASE/tomcat/logs*, for errors.
Cannot start Mobile Web Studio	If you cannot start Mobile 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 3. • Verify that you are using the correct port number, for example, 4040 when running in Tomcat.

BlackBerry Enterprise Server setup

Table 3-3 identifies common BlackBerry Enterprise Server (BES) setup problems and provides useful troubleshooting information.

Table 3-3: Troubleshooting BES problems

Problem	Try this
The Unwired Accelerator client cannot be installed using BlackBerry Desktop Manager	Verify that the BlackBerry Desktop Manager and BlackBerry device versions match.

Problem	Try this
The BlackBerry device is unable to connect after switching to a different BES or user	1 From the BlackBerry device, select Option | Security, and click on Track Wheel 2 Select Wipe Handheld to clear the security data. 3 Repeat the Enterprise Activation setup, or pair up the BES.
Unwired Accelerator cannot connect to the BlackBerry Desktop Manager	Verify that the BlackBerry Desktop Manager is version 3.6 SP3a, the version required by Unwired Accelerator.
BlackBerry users receive Permission denied errors, and database transactions never make it to the portaldatabase.	This may indicate that cookies are not enabled for the BES. Cookies are needed to maintain the JSESSIONID; without it, access and transactions are denied. See "Configuring BES to maintain cookies" on page 24.

MobiLink setup

Table 3-4 identifies common MobiLink setup problems and provides troubleshooting information.

Table 3-4: Troubleshooting MobiLink problems

Problem	Try this
Deploying an application to MobiLink causes a `FileNotFoundException – missing...\tomcat\temp\<host.domain.rid>.usm` error.	Check the Registry entry and verify `HKLM\Software\Sybase\Adaptive Server Anywhere\9.0` exists and has the correct values for the `Location` and `Shared Location` values.
Starting MobiLink server shows an ODBC error.	Go to the ODBC Data Source Administrator and verify the uaml data source exists under the System DSN tab. Verify the properties for the uam1 data source are set correctly.
Starting MobiLink server shows this message: `Error: cannot open file \tmp\logs\ml.Log`	This indicates the *X:\tmp\logs* directory does not exist. Creating the directory was a pre-installation requirement, described in "Installing MobiLink server on Windows (optional)" on page 16. Create the directory to view the `ml.Log`.
MobiLink console shows that the SMSGateway connection is refused.	In the *configML.sql* script, modify the SMSGateway (UASMS) and UAMAIL sections with the correct values, then execute *configML.bat*. See "Installing MobiLink server" on page 17.
Push using UAMAIL does not work, or send e-mails to the clients.	In the *configML.sql* script, modify the SMSGateway (UASMS) section with the correct values, then execute *configML.bat*. See "Installing MobiLink server."

Problem	Try this
Cannot connect to MobiLink	If you changed any of the default MobiLink parameters in the *startmlsrv.bat* and *mlservice.bat* files, you must verify that the -x parameter is configured correctly and in sync in both files. You must then reinstall the Windows Service for MobiLink.
Cannot see any messages in the MobiLink log file after selecting Mobile users | List Subscriptions | Select apps, and right clicking Device | Synchronize in Mobile Web Studio	This typically indicates the *ulxml.exe* file is missing. You must install MSXML 4 Service Pack 2 as described in "Installing MobiLink server on Windows (optional)" on page 16. MSXML includes *ulxml.exe*, which is used to generate schema files for clients.

Mobile device and client setup

Table 3-5 identifies common mobile device and client configuration problems, and provides useful troubleshooting information.

Table 3-5: Troubleshooting mobile device and client problems

Problem	Try this
JVM error when attempting to load UA client on the BlackBerry device	This problem is typically seen on small memory devices (like the 7230) that only have 16MB of memory, especially when the device is loaded for Chinese language (or multiple European languages) support. To correct the problem: 1 Check the device memory to see whether less than 1.5MB of memory is available. Select Options | Status. 2 If less than 1.5MB of memory is available, remove components to free memory. Some of the components you can remove are unused Input Methods for Chinese (for devices running Chinese support), or unused European language support (for devices running support for multiple European languages).
The UA icon does not appear on the BlackBerry mobile device	Make sure that you installed the offline client on the BlackBerry device (or BlackBerry simulator), as described in "Installing the UA offline client" on page 20 (or "Downloading the BlackBerry simulator" on page 22).
The UA icon does not appear on the Windows mobile device	Make sure that you installed the .NET client on the Windows device, as described in the *Unwired Accelerator Developer's Guide*.

Problem	Try this
Mobile application does not appear on the mobile device	• For BlackBerry devices, verify the configuration is correct, as described in "Installing the UA offline client" on page 20. Also check Mobile Web Studio to make sure the Offline BlackBerry option is selected for the application, and that the application is in a grid/table format. • For .NET devices, verify the configuration is correct, as described in the *Unwired Accelerator Developer's Guide*.

SAP setup

Table 3-6 identifies common SAP connection problems and provides useful troubleshooting information.

Table 3-6: Troubleshooting SAP connection problems

Problem	Try this
Cannot download the SAP Java connector from SAP	You must be a registered SAP customer to download the SAP Java connector from the SAP Service Marketplace Web site.
Unwired Accelerator cannot connect with the SAP environment	Check the following configuration settings: • Verify that you configured the SAP Java connector correctly, using information in "Configuring the SAP Java connector" on page 25. Specifically, make sure the *sapjco.jar*, *librfc32.so*, and *sapjcorfc.so* files are in the correct location, and that the connection pools are defined in the *sapjco.properties* file. • Check the *global.properties.xml* file and make sure the connection pools are defined as described in "Modifying the global.properties.xml file for SAP" on page 26. • Verify that a properties file is defined for each connection pool entry in the *global.properties.xml* file, as described in "Creating ConnectionPool property files" on page 27.

APPENDIX A

Setting Up Authentication and Authorization

This appendix describes how to set up authentication and authorization for Unwired Accelerator and either the portal database or a Lightweight Directory Access Protocol (LDAP) server security provider. This chapter also discusses the configuration of CSI providers that are used in UA.

Preconfigured for PortalDB Unwired Accelerator 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 appendix.

Overview

Unwired Accelerator is integrated with Common Security Infrastructure (CSI) and leverages CSI 2.5 to perform security tasks such as authentication, authorization, and auditing. For information about auditing, see the *Unwired Accelerator Administration Guide*.

CSI uses the Java Authentication and Authorization Services (JAAS) model so that UA can integrate with different security providers without requiring you to update code.

The CSI configuration file, *csi.xml*, is located in the *$UA80/tomcat/conf* directory. You can configure this file to specify which security providers to use. You can also configure several security providers, stacked together, to meet your security requirements.

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

You can use various options to require either one or more authenticators, and you can also control the order in which they are called. You can also specify whether, after authenticating to LDAP, user roles are pulled from PortalDB, or if the roles come only from LDAP. If you authenticate only to LDAP, you get roles only from LDAP.

You can also configure CSI to perform mutual certificate authentication, or 2-factor Remote Authentication Dial-In User Service (RADIUS) authentication, for example by using a PIN from a Smartcard.

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

Configuring the CSI realm

Unwired Accelerator supports authentication and authorization for the Tomcat Web application container. The CSI realm is preconfigured in the *$UA80/tomcat/conf/server.xml* file and should not be changed.

Configuring the security provider

Unwired Accelerator includes two security providers, the PortalDB provider and the LDAP provider. Initially, Unwired Accelerator 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:

- "Configuring the LDAP provider" below, or
- "Restoring the PortalDB provider configuration" on page 52.

Configuring the LDAP provider

Unwired Accelerator 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.

Table A-1 defines the options that you can use to configure the authentication provider. Enable any of the options by adding the option name and value to *csi.xml*. 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 A-1: LDAP configuration options

Configuration option	Default value	Description
AllowSelfRegistrationAndManagement	true	Controls whether or not this LDAP configuration will permit self-registration and self-management requests through a configured LDAP attributer.
AuthenticationFilter	Most LDAP servers: (&(uid={uid}) (objectclass=personal) Microsoft Active Directory: (&(userPrincipalName={uid}) (objectclass=user))	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. The second default value is designed for Microsoft Active Directory. This allows users to authenticate using their e-mail address. To allow users to authenticate using the Windows user name, set this filter to: `"(&(sAMAccountName={uid})(objectclass=user))"`

Configuration option	Default value	Description
AuthenticationMethod	simple	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 later.
AuthenticationScope	onelevel	Set this option to either "onelevel" or "subtree." If set to "onelevel," only the AuthenticationSearchBase is searched for user records; if set to "subtree," the AuthenticationSearchBase and its subtree are searched.
AuthenticationSearchBase		The location of user records. If not specified, the DefaultSearchBase is used.
BindDN	None	The DN to which to bind 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 you do not specify this property, anonymous binding is used, which works on most servers.
BindPassword		The password to which to bind when creating the initial LDAP connection. Specify a bind password only when the BindDN property is specified.
CertificateAttributes		Comma-separated list of attributes in the certificate used to authenticate the user instead of the certificate binary.

Configuration option	Default value	Description
CertificateAuthenticationFilter	Most LDAP servers: &({certattr}={0})(objectclass=person)) Microsoft Active Directory: (&({certattr}={0}(objectclass=user))	The filter used when authenticating a certificate user. The filter determines the LDAP entry that matches the supplied certificate encoded form. If the certificate attribute mapping is not defined, {cerattr} is replaced with the LDAP certificate attribute name (userCertificate) and {0} is replaced with the encoded certificate binary. If certificate attribute mapping is defined and the certificate contains a specified attribute, its value replaces {0} and the corresponding LDAP attribute name defined in the mapping replaces {certattr}.

DefaultSearchBase	None	The search base 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 example, for a machine in the Sybase organization, the previous two syntax options map to:
		`dc=sybase,dc=com`
		`o=Sybase,c=us`

DigestMD5AuthenticationFormat	DN	The DIGEST-MD5 bind authentication identity format. The value is set to Username for OpenLDAP server.
EnableCertificateAuthentication	false	Enables or disables certificate authentication in addition to the user name/password authentication.
InitialContextFactory	com.sun.jndi.ldap.LdapCtxFactory	Specifies the JNDI provider to use. If you are using a Sun Java VM version 1.3 or later, the default value should work. If you are using an IBM or other third-party VM, adjust this value accordingly.
ldapAttributes		Comma-separated list of attributes that map to the certificate attributes specified to be used to select the LDAP entry that matches the value in the certificate.
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. The format of this parameter is ldap://<*hostname*>:<*port*>.

Configuration option	Default value	Description
Referral	ignore	Specifies how to handle a referral. The valid values are “follow,” “ignore,” and “throw.”
RoleFilter	SunONE: (&(objectclass=ldapsubentry) (objectclass=nsroledefinition)) Netscape Directory Server: (|(objectclass=groupofnames) (objectclass=groupofuniquenames)) Microsoft Active Directory: (|(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. You may want to set RoleMemberAttributes if you use LDAP groups as placeholders for roles. **Note** The default value applies only to Netscape Directory Server; other servers do not have a default value.
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.
SelfRegistrationSearchBase		The search base used to retrieve the list of self-registered users. If not specified, the DefaultSearchBase is used.
SecurityProtocol		Specifies the protocol to use when connecting to the LDAP server. If you are using the SSL protocol, set the SecurityProtocol to “ssl” instead of “ldap” in the URL. Active Directory requires the use of the SSL protocol when setting the value for the password attribute. This occurs when creating a user or updating the password of an existing user.

Configuration option	Default value	Description
ServerType	None	The type of LDAP server you are connecting to. Supported server types are: • "msad2k" – Microsoft Active Directory. For Windows 2000—see "Limitations of Microsoft Active Directory LDAP servers" on page 51. • "nsds4" – Netscape Directory Server 4.*x*. • "sunone5" – SunONE Directory Server 5.*x* or iPlanet 5.*x*. • "openldap" – OpenLDAP Directory Server 2.*x*. ServerType does not require a value, but if one is provided, it establishes default values for the following configuration properties: • AuthenticationFilter • RoleFilter • RoleMembershipAttributes • UserRoleMembershipAttributes • MD5AuthenticationFormat • UseUserAccountControlAttribute
UnmappedAttributePrefix	LDAP	Prefix assigned to unmapped LDAP attributes when moving them into the CSI attribute namespace. A period (.) is appended to the specified value, followed by the LDAP attribute name. For example, the employeeNumber attribute will be converted to LDAP.employeeNumber. Specify a blank value for map LDAP attributes directly into the CSI attribute namespace with no prefix.
UseUserAccountControl Attribute	false true when ServerType is set to msad2k	Specifies that the UserAccountControl attribute should be used for detecting disabled user accounts, account expiration, password expiration, and so on. Microsoft Active Directory uses this attribute to store the above information.
UseUserCredentials ToBind	false	Enables the LDAP attributer to use the stored user credentials to bind to the LDAP server for self-update operations. If this is set to true, the login module configuration should be such that the user credentials are saved and available to the LDAP attributer.

Configuration option	Default value	Description
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 is granted roles whose names are “sales” and “consulting.” If you are using a SunONE Directory Server 5, set up the above example as follows: 1 From the LDAP Administration console’s Generic Editor, add a multi-value 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 Active Directory: 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 Active Directory, 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 Active Directory. 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 A-1 on page 43:

- RoleFilter
- RoleNameAttribute
- RoleSearchBase
- RoleScope
- UserRoleMembershipAttributes

- LDAP group role definitions – are supported by almost all LDAP servers and are a common construct in older LDAP servers. Use LDAP group role definitions 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 A-1 on page 43 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 – are 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 A-1 on page 43.

LDAP authorization configuration

UA requires all authenticated users to have the "everybody" role to access UA. An authorizer called com.sybase.security.helpers.EveryobodyRoleAuthorizer is available to facilitate this task. This authorizer passes the "everybody" role check for any user. Thus, you can configure the LDAP providers as follows:

```
<config:authenticationProvidername="com.sybase.security.ldap.LDAPLoginModule"
     controlFlag="optional" />

<config:provider name="com.sybase.security.ldap.LDAPAttributer"
type="attributer" />

<config:provider name="com.sybase.security.core.RoleCheckAuthorizer"
     type="authorizer" />

<config:provider name="com.sybase.security.helpers.EverybodyRoleAuthorizer"
     type="authorizer" />
```

Additionally, there is an authorizer called com.sybase.security.portaldb.PortalDBAuthorizer, which extends from RoleCheckAuthorizer and processes the "everybody" role as EverybodyRoleAuthorizer.

If you are using only the LDAP server to perform user role checks, the configuration is similar to:

```
<config:authenticationProvidername="com.sybase.security.ldap.LDAPLoginModule"
     controlFlag="optional" />

<config:provider name="com.sybase.security.ldap.LDAPAttributer"
type="attributer" />

<config:provider name="com.sybase.security.portaldb.PortalDBAuthorizer"
     type="authorizer" >
     <config:options name="AlwaysUsePortalDBRoles" value="false" />
     <config:options name="AlwaysUsePortalDBPermissions" value="false"/>

</config:provider>
```

The authorizer also provides two configuration options:

- AlwaysUsePortalDBRoles – if an administrator uses Mobile Web Studio to manage user roles, the role check process should be against the LDAP server as well as PortalDB. The configuration for this option looks like this:

```
<config:provider name="com.sybase.security.portaldb.PortalDBAuthorizer"
     type="authorizer" >
     <config:options name="AlwaysUsePortalDBRoles" value="true" />
     <config:options name="AlwaysUsePortalDBPermissions"
value="false"/>
```

- AlwaysUsePortalDBPermissions – if you want users to undergo PortalDB access permissions check in addition to role-based checks, you can configure the option this way:

```
<config:provider name="com.sybase.security.portaldb.PortalDBAuthorizer"
     type="authorizer" >
     <config:options name="AlwaysUsePortalDBRoles" value="true" />
     <config:options name="AlwaysUsePortalDBPermissions" value="true"/>
```

Limitations of Microsoft Active Directory LDAP servers

If you are using the Microsoft Active Directory 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 Active Directory Users and Computers console, you can create users and groups, then add users to the groups so they are authorized to perform tasks in Unwired Accelerator. Create the following groups, then add users to these groups:
  - everybody

- PortalAdmin
- PortalGuest
- PortalUser
- StudioAdmin
- superuser

Restoring the PortalDB provider configuration

By default, Unwired Accelerator is configured to use the PortalDB security provider. If your system has been changed to use the LDAP security provider, you can restore the PortalDB configuration.

1 Change to the location of the *csi.xml* file:

   - Tomcat – $CATALINA_HOME/conf, where $CATALINA_HOME represents the Tomcat root installation directory.

2 Open *csi.xml*, and verify that the PortalDB provider definitions are not commented out. The sample *csi.xml* file that is installed with Unwired Accelerator 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 Unwired Accelerator creates this JNDI name automatically during deployment. If the DatasourceName configuration option is missing, the default value is used.

3 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.

Configuring certificate authentication

To log in to UA with certificate authentication use http://hostname:port/certAuth/index.jsp.There are both HTTP and HTTPS port number configurations for certificate authentication in the *config.txt* file located in $UA80/tomcat/webapps/certAuth. Ensure the port numbers are configured correctly in terms of Tomcat listener configuration.

In the following example certificate authentication is used against the LDAP server in UA 8.0 to illustrate the configuration options.

You must first import the appropriate certificate into the IE browser. In UA 8.0, Tomcat does not come configured with a client authentication-enabled HTTPS listener. You must configure *$UA80/tomcat/conf/server.xml* to create this type of listener as shown in the following procedure.

❖ **Importing the certificate into IE**

1 In IE, select Tools | Internet Options | Content | Certificates | Import.

If you are using Tomcat, the Java VM the certificate uses should trust the Certificate Authority that issued the certificate.

2 Go to *$UA80/jdk1.5.0_05/jre/lib/security* and use the keytool command to import the CA certificate into the cacerts keystore.

3 Tomcat is not configured with a client authentication-enabled HTTPS listener, so you must configure the *server.xml* file located in *$UA80/tomcat/conf* to create the listener as shown in this example:

```
<!-- Define a SSL HTTP/1.1 Connector on port 4444 -->
<Connector port="4444" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
       enableLookups="false" disableUploadTimeout="true"
       acceptCount="100" scheme="https" secure="true"
       clientAuth="want" sslProtocol="TLS" keystoreFile=".keystore"/>
```

Make sure clientAuth is assigned the want value. After creating the listener, update the *config.txt* file located in *$UA80/tomcat/webapps/certAuth* accordingly. Then, configure the CSI LDAP provider to support certificate authentication.

There are two ways to map a certificate to a record in the LDAP directory:

- Binary Certificate Registration – the user certificate is registered with an LDAP user record using an LDAP administration tool such as the SunONE Server Console. In this case, the CSI LDAP authentication provider is configured to match the certificate binary supplied by the user and locate a record in the LDAP server with the same registered binary certificate in order to authenticate the user.
- Certificate Attribute Mapping – use this technique to map certificates that do not, or cannot, hold the actual certificate data into the LDAP directory. Configuring the mappings between the certificate and LDAP attributes is done through modifications to the following two configuration properties:

```
<config:authenticationProvidername="com.sybase.security.ldap.
LDAPLoginModule" controlFlag="requisite">

<!-- snipped other options for brevity -->
<config:options name="certificateAttributes" value="" />
<config:options name="ldapAttributes" value=""/>

</config:authenticationProvider>
```

For example, to define a mapping between the e-mail attributes, you can use a configuration like this:

```
<config:options name="certificateAttributes" value="EMAIL" />
<config:options name="ldapAttributes" value="mail" />
```

You can add a secondary search attribute by separating the attribute names with a comma. For example:

```
<config:options name="certificateAttributes" value="EMAIL,CN"/>
<config:options name="ldapAttributes" value="mail,cn" />
```

Following is an example of a complete CSI configuration for LDAP certificate authentication:

```
?xml version="1.0" encoding="UTF-8"?>
<config:configuration xmlns:config="http://www.sybase.com/csi/2.5/config"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<!-- Certificate validation moduel -->
<config:authenticationProvider
name="com.sybase.security.core.CertificateValidationLoginModule"
       controlFlag = "optional" >
</config:authenticationProvider>

<!-- LDAP authenticator -->
<config:authenticationProvidername="com.sybase.security.ldap.LDAPLoginModule"
  controlFlag="optional" />
<config:options name="ServerType" value="sunone5" />
  <config:options name="ProviderURL"value="ldap://tyuanxp.sybase.com:59889" />
  <config:options name="DefaultSearchBase" value="dc=sybase,dc=com" />
  <config:options name="enableCertificateAuthentication" value="true" />
  <config:options name="CertificateAuthenticationFilter"
          value="(&amp;({certattr}={0})(objectclass=person))" />
</config:authenticationProvider>

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

<config:provider name="com.sybase.security.portaldb.PortalDBAuthorizer"
  type="authorizer" >
  <config:options name="AlwaysUsePortalDBRoles" value="false" />
  <config:options name="AlwaysUsePortalDBPermissions" value="false" />
</config:provider>
</config:configuration>
```

com.sybase.security.core.CertificateValidationLoginModule is configured preceding the LDAP authentication provider. This provider is used to validate the certificate. In the above configuration, CertificateValidationLoginModule is not configured with any option, so it validates only whether the certificate to be authenticated is within the valid time period.

Table A-2 lists available configuration options for CertificateValidationLoginModule.

Table A-2: CertificateValidationLoginModule configuration options

Configuration option	Default value	Definition
crl.[index].uri		Specifies the uri of the CRL. Multiple CRLs can be configured using different values for the index. If the CRL is to be retrieved from an LDAP directory then the LDAP url specified should point to the certificationAuthority entry and should include the query parameters to retrieve the certificateRevocationList attribute of that entry. For example if an organizational unit (say ou=certCAou,dc=sybase,dc=com) is designated as a CA by adding the auxiliary object class certificationAuthority to it, then the LDAP URL specified should look like this: `ldap://localhost:389/ou=certCAou,dc=sybase,dc=com?certificaterevocationlist`
validateCertPath	false	Enables or disables certificate path validation.
trustedCertStore		Specifies the key store containing the trusted CA certificates. Required when certPathValidation is set to true.
trustedCertStorePassword		Password to access the specified trusted certificate store.
trustedCertStoreType	Obtained at runtime KeyStore.getDefaultType()	Specifies the type of key store.
trustedCertStoreProvider		Specifies the provider for the key store.
validatedCertificateIsIdentity	false	Specifies if certificate should be set as the ID for the authenticated subject. Set to false if the CertificateValidationLoginModule is used in conjunction with other login modules that establish user identity based on the validated certificate.

Configuring the CSI RADIUS provider

UA 8.0 supports authentication against RADIUS servers. RADIUS is an authentication protocol widely used by ISPs and corporate networks. To enable RADIUS authentication, you can configure a CSI RADIUS provider as shown in this example:

```
... ...
<config:authenticationProvider
name="com.sybase.security.radius.RadiusLoginModule"
```

```
controlFlag="optional" />
<config:options name="RadiusServerHostName" value="localhost" />
<config:options name="RadiusServerAuthPort" value="1812" />
<config:options name="AuthenticationMethod" value="PAP" />
<config:options name="SharedSecret" value="secret" />
<config:options name="MaxChallenges" value="3" />
-->
```

Table A-3 shows supported CSI RADIUS provider configuration options:

Table A-3: CSI RADIUS provider configuration options

Configuration option	Default value	Definition
AuthenticationMethod	PAP	Authentication method to use. Valid values are PAP and CHAP.
SharedSecret		The secret shared between the RADIUS server and the host where the login module is executed.
RadiusServerHostName		Name of the host to connect to the RADIUS server.
RadiusServerAuthPort	1812	Radius server authentication port.
MaxChallenges	3	Maximum number of challenge prompts propagated to the client.

ErrorMsgMapping.[index].regex		Specifies the regular expression to match a RADIUS server error message. For example:
		`ErrorMsgMapping.1.regex=someRegEx`
		`ErrorMsgMapping.1.failureCode=failureCodeValue`
		The properties with the same index map the someRegEx to the failureCodeValue. The index is used only to map the regular expression to the failure code; it does not signify the order in which the regular expressions are used to match the RADIUS server error message. The order in which the regular expressions are defined determines the order in which they are used. The index can also be a string value as follows:
		`ErrorMsgMapping.map.regex=someRegEx`
		`ErrorMsgMapping.map.failureCode=`
		`failureCodeValue2`

Configuration option	Default value	Definition
ErrorMsgMapping.[index].failureCode		Specifies the error code that a regular expression specified with the same index maps to. You can specify the failure code as an integer or a string. If a string value is specified it should correspond to the constant defined in com.sybase.security.core.AuthenticationFailureWarning with any of the following valid prefixes: • FAILURE_CODE.1, 15 • ACCOUNT_LOCKED • PASSWORD_EXPIRED If an invalid value is specified, the corresponding regular expression is ignored.
caseSensitiveMatching	false	Specifies case sensitive matching to use when matching the RADIUS server error messages using the regular expressions.

Note The CSI RADIUS provider does not support any authorization function.

Stacked CSI providers

CSI providers can be stacked together to provide a security solution to meet special security requirements. Every CSI authentication provider has a controlFlag attribute that is used to control overall behavior when authentication proceeds through stacked authentication providers.

The control flag value and its meaning is the same as that defined in the JAAS, as shown in Table A-4.

Table A-4: JAAS control flag values

Control flag value	Description
required	The LoginModule is required to succeed. If it succeeds or fails, authentication proceeds down the LoginModule list.
requisite	The LoginModule is required to succeed. If it succeeds, authentication continues down the LoginModule list. If it fails, control returns immediately to the application (authentication does not proceed down the LoginModule list).
sufficient	The LoginModule is not required to succeed. If it does succeed, control returns immediately to the application (authentication does not proceed down the LoginModule list). If it fails, authentication continues down the LoginModule list.
optional	The LoginModule is not required to succeed. If it succeeds or fails, authentication proceeds down the LoginModule list.

Like the authentication provider, the CSI attributer and authorizer can also be stacked together. Normally there are CSI attributers and authorizers corresponding to an authentication provider in order to provide complete security service of backend security systems. However, attributers and authorizers do not have to be bound to a specific authenticator.

In UA 8.0, the PortalDB provider and LDAP provider are most probably stacked together to enforce UA security. For example, UA users are normally authenticated against the LDAP server. At the same time, the default “masuper” user defined in PortalDB can be used to log in to Mobile Web Studio to perform administration and development tasks. Following is a sample of stacked PortalDB providers and LDAP providers:

```
<?xml version="1.0" encoding="UTF-8"?>
<config:configuration xmlns:config="http://www.sybase.com/csi/2.5/config"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<!-- portaldatabase authentication -->
<config:authenticationProvider
name="com.sybase.security.portaldb.PortalDBLoginModule"
controlFlag="optional">
<config:options name="DatasourceName" value="java:comp/env/jdbc/portaldb" />
</config:authenticationProvider>
<!-- LDAP authenticator -->
<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>
<config:provider name="com.sybase.security.portaldb.PortalDBAttributer"
type="attributer" />

<!-- LDAP attributer  -->

<config:provider name="com.sybase.security.ldap.LDAPAttributer"
type="attributer" />
<config:provider name="com.sybase.security.portaldb.PortalDBAuthorizer"
type="authorizer" >
<config:options name="AlwaysUsePortalDBRoles" value="true" />
<config:options name="AlwaysUsePortalDBPermissions" value="true" />
</config:provider>
</config:configuration>
```

Enabling debugging in the Tomcat realm

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

❖ **To enable debugging in the Tomcat CSI realm**

1. Open the *logging.properties* file located in *$CATALINA_HOME/server/classes*, where *$CATALINA_HOME* represents the Tomcat root installation directory, and add the property:

   ```
   com.sybase.security.level = FINE
   ```

   You can set the security level to any of these: OFF, SEVERE, WARNING, CONFIG, INFO, FINE, FINER, FINEST, or ALL.

   The debugging output is written to the file whose name and location are specified by the logging.properties.appender.SecurityAppender.File property; in the example above, */opt/sybase/UA80/tomcat/logs/security_debug.log*.

2. Create a *log4j.properties* file in $SYBASE/.../tomcat/common/classes to turn on debug tracing of CSI. The following gets you "DEBUG" and higher level tracing on the tomcat console:

```
#Tomcat server Logging Configuration
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
```

Initially, the Tomcat CSI realm is configured to use the PortalDB provider. To use the LDAP provider, see “Configuring the LDAP provider” on page 43.

Index

Symbols

A

B

C

D

E

F

G

I

J

L

M

N

O

P

R

S

T

U