SYBASE®

Installation Guide

Unwired Accelerator

8.0

[Windows 2003, Windows XP]

DOCUMENT ID: DC00082-01-0800-01

LAST REVISED: August 2006

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

Contents

About This Book ..... **v**

CHAPTER 1 **Overview** **1**
Product summary 1

CHAPTER 2 **Installation Procedures** **3**
System requirements 3
Unwired Accelerator default values 4
Pre-installation tasks 5
Installation tasks 5
Post-installation tasks 8
Starting Unwired Accelerator 9
Verifying the installation 9
Setting the SMTP server and UAMAIL gateway in MobiLink 10
Verifying the mail.host property 11
Configuring for a proxy server 11
Updating digital certificates 12
Installing the UA offline client 13
Installing RIM BlackBerry server 16
Configuring Tomcat for LDAP 17
Starting and stopping the system 17
Starting and stopping the database 18
Starting and stopping the Tomcat application server 18
Starting and stopping MobiLink 19
Uninstalling Unwired Accelerator 20
Upgrading from UA 7.0 to 8.0 (Tomcat) 21
Post-upgrade tasks 22

CHAPTER 3 **Troubleshooting** **25**
Overview 25
Installer 26
Unwired Accelerator setup 26
BlackBerry Enterprise Server setup 28

MobiLink setup 28
Mobile device setup 29
Upgrade 30

APPENDIX A **Setting Up Authentication and Authorization 31**
Overview 31
Configuring the CSI realm 32
Configuring the security provider 32
Configuring the LDAP provider 33
Restoring the PortalDB provider configuration 42
Configuring certificate authentication 43
Configuring the CSI RADIUS provider 46
Stacked CSI providers 48
Enabling debugging in the Tomcat realm 50

Index 51

About This Book

Audience

This guide is for any persons installing the Sybase® Unwired Accelerator software, who are familiar with their system's environment, networks, disk resources, and media devices.

How to use this book

This book contains these 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, and how to uninstall Unwired Accelerator.
- Chapter 3, "Troubleshooting," provides troubleshooting 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.
- The Unwired Accelerator installation guide (this document) contains installation instructions.
- The *Unwired Accelerator Quick Start Guide* shows how to deploy a Web application and a database application to either a PDA or BlackBerry device.
- The *Mobile Application Development Tutorial* provides tutorials that provide examples of how you can use Mobile Web Studio to develop and deploy mobile applications.

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

- The *Portal Interface User's Guide* describes the Portal Interface user interface and how to use Portal Interface to build and manage your enterprise's portal.
- The *Unwired Accelerator Administration Guide* provides administration topics for Unwired Accelerator and its components.
- The *Unwired Accelerator Developer's Guide* includes developer-related topics for Unwired Accelerator components, Portal Interface applications, and Java Template Framework pages.

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 on the SyBooks CD.

Adaptive Server® Anywhere documents Unwired Accelerator 8.0 includes the ASA database to store system information including security authentication and authorization information. The ASA document set is 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
%SYBASE%	Variable used to represent the Sybase Unwired Accelerator installation directory.
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."

Key	Definition
`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

The installation and post-installation instructions refer to these variables:

- %SYBASE% refers to the Unwired Accelerator installation directory; for example, *C:\Sybase\UA80*.
- %RIM% refers to the Research in Motion installation directory; for example, *C:\Program Files\Research In Motion* or *C:\RIM*.
- %CATALINA_HOME% refers to the Apache Tomcat application server installation directory. Unwired Accelerator integrates the Tomcat in its installation directory (*%SYBASE%\UA80\tomcat*).
- *%JAVA_HOME%* refers to a valid JVM directory.

If you need help

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

CHAPTER 1

Overview

This guide explains how to install, or upgrade, and configure Sybase Unwired Accelerator running on Tomcat.

Topic	Page
Product summary	1

Product summary

Unwired Accelerator mobilizes enterprise applications and data, which allows users to be productive and effective inside or outside the office. Users can access the applications and tools anytime 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:

- Microsoft Windows XP, Windows 2003
- Mobile device, online access:
  - BlackBerry, versions 4.0 and 4.1
  - PocketPC 2003 (Windows CE)
  - Motorola MPx200 (Windows Mobile OS)
  - HandSpring Treo 600 and 650 (PalmOne OS 5.x)
  - Sony Ericsson P900 (Symbian OS)
- Mobile device, offline access:
  - PocketPC
  - Palm (including M-Business Anywhere Client)

- Symbian
- RIM BlackBerry (including Proximus and Vodafone)

CHAPTER 2

Installation Procedures

This chapter describes how to install Unwired Accelerator on Windows 2003 and Windows XP.

Topic	Page
System requirements	3
Unwired Accelerator default values	4
Pre-installation tasks	5
Installation tasks	5
Post-installation tasks	8
Starting and stopping the system	17
Uninstalling Unwired Accelerator	20
Upgrading from UA 7.0 to 8.0 (Tomcat)	21

System requirements

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

Table 2-1: System requirements

Platform and OS	Release level	RAM	Disk space	Network protocol	Web browser
Windows XP, 2003 minimum 750Mhz	XP – Service Pack 2	512MB recommended	500MB minimum, 1GB recommended	TCP, IPX/SPX, and Named Pipes	To access Portal Interface, use Internet Explorer 5.5+, or Netscape Navigator 7.01+. To access Mobile Web Studio, use Internet Explorer 6.0.

Unwired Accelerator default values

UA includes defaults for many of its setup values. You can accept the defaults, or change them, if necessary.

Table 2-2: Unwired Accelerator default installation values

Component	Default values	Description
Local host machine		
Local host machine name	(demo)	The name of the machine on which you are installing Unwired Accelerator; for example, “lab2k”
Unwired Accelerator HTTP port	4040	
Unwired Accelerator HTTPS port	4443 **Note** If you have M-Business Anywhere server installed on the same machine as Tomcat, there is a conflict with port 4443, so you must use a different port for HTTPS.	
Adaptive Server Anywhere 9.0.2		
ASA port	4747	
ASA administrator user name	dba	The name used to log in to Adaptive Server Anywhere
ASA administrator password	SQL	The password used to log in to Adaptive Server Anywhere
MobiLink		
Notification port	8777	
Database port	4747	
Database user name	dba	
Password		
Mobile Web Studio		
User name/password	masuper/m8super	Created automatically during installation
M-Business Anywhere 6.0 (optional)		
Administrative user name	admin	The name used to log in to M-Business Server as an administrator
Administrative password	none	
Admin port	8091	
JDBC connection port	8099	Default AGDB database port

Component	Default values	Description
M-Business client port	8092	M-Business Anywhere “synch” port

Pre-installation tasks

Before you install Unwired Accelerator:

- Verify that you have 512MB free space in your temporary directory, otherwise, the installation fails.
- Verify that you have write permission on the directory where you install the software, and on the *x:\tmp\logs* directory (where *x:* is the installation drive). If the *logs* directory does not exist, the Installer creates it.
- 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:

  ```
  ipconfig /all
  ```

  Your domain displays in the “Connection-specific DNS Suffix” setting; for example, sybase.com.
- Verify that reg.exe exists on your machine by opening a Command Prompt window and entering:

  ```
  reg.exe
  ```

  If you do not have reg.exe on your machine, get the instructions for installing reg.exe at http://support.microsoft.com/kb/301423/.

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.

Note See “Upgrading from UA 7.0 to 8.0 (Tomcat)” on page 21 if you are upgrading Unwired Accelerator software on Tomcat.

❖ **Installing Unwired Accelerator**

1 Insert the installation CD. If AutoStart is enabled, the InstallShield wizard starts and the Welcome window displays. This may take a few moments. If AutoStart is disabled, launch the installer from the CD by double-clicking *ua80setup.exe*. The Welcome screen appears.

Note Remote installation of UA 8.0 is not supported. You must install UA 8.0 using the installation CD or by copying all the installation files to the machine on which you are installing UA 8.0.

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

3 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 agree to the terms of the Sybase license for the installation location specified." Click Next.

4 In the Installation Directory window, enter the installation directory where you want to install Unwired Accelerator, for example, *C:\Sybase\UA80*.

Note The installation directory is referred to as *%SYBASE%* in this guide.

Do not select an installation directory that uses double-byte characters or spaces anywhere in the path name.

Click Next.

5 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.

6 In the next window, enter:

Note If you are performing an upgrade from UA 7.0, you must use the same domain name, host name, database port, HTTP port, and HTTPS port as you configured for your 7.0 installation.

- Host Name – by default, the Installer inserts the machine name listed in the Windows Registry. Accept the default, or enter the name of the machine on which you are installing Unwired Accelerator; for example, `lab2k`.

- Domain Name – by default, the Installer inserts the domain listed in the Windows Registry. Accept the default or enter the domain (and subdomain if used).

Click Next.

7 The parameters window displays. Enter the values for these parameters or accept the defaults.

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

  Note If you are using Netscape 7.0.*x* for Web browser access, and using HTTPS to protect passwords during login, use port 80 for the Unwired Accelerator HTTP port.

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

  Note Before accepting the default values, keep in mind:

  - If you are using Netscape 7.0.*x* for Web browser access, and using HTTPS to protect passwords during login, use port 443 for the Unwired Accelerator HTTPS port.
  - If you have M-Business Anywhere server installed on the same machine you are installing Tomcat on, there is a conflict with port 4443, so you must use a different port for HTTPS.

This window also shows the ports used by Unwired Accelerator:

- Database Port – `4747`
- Tomcat Administration Port – `8005`
- MobiLink Database Port – `2439`

Click Next. The installer starts.

8 The Installation Progress window displays.

The installer starts the Adaptive Server Anywhere database.

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

9 Click Finish.

10 To start UA, you must restart your machine. In the next window, select from these options:

- Yes, restart my computer, or
- No, I will restart my computer at a later time

11 The Unwired Accelerator installation is complete. After restarting your machine, see “Verifying the installation” on page 9 to verify the network installation works correctly

Post-installation tasks

This section describes post-installation tasks. Perform only the procedures for the features needed in your installation.

- Verifying the installation
- Setting the SMTP server and UAMAIL gateway in MobiLink
- Configuring for a proxy server
- Updating digital certificates
- Installing RIM BlackBerry server
- Configuring Tomcat for LDAP

See the *Unwired Accelerator Administration Guide* for information about additional post-installation configuration tasks, including:

- Installing M-Business Anywhere server and client software
- Installing Answers Anywhere server software
- Setting up a SAP connection
- Setting up a Domino connection
- Installing the .NET container client

Starting Unwired Accelerator

To start UA, select Start | Programs | Sybase | Unwired Accelerator | Start UA (Windows Services).

Verifying the installation

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

❖ **Checking the installations**

1 To verify the Mobile Web Studio installation, go to Start | Programs | Sybase | Unwired Accelerator | Start UA Studio. An Internet Explorer browser window opens and the Mobile Web Studio login page displays.

You can also access Mobile Web Studio by entering the following URL in an Internet Explorer browser window:

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

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

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

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

If the Mobile Web Studio window does not display, see Table 3-2 on page 26 for information.

2 In Mobile Web Studio, log in using `masuper` as the user name, and `m8super` as the password.

3 To verify the Portal Interface installation, 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, "lab2k."

- *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 example:

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

The Portal Interface Welcome window displays.

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

Setting the SMTP server and UAMAIL gateway in MobiLink

If you want to send mail from UA or the UAMAIL gateway in MobiLink, you must configure the ASA port and SMTP server in the *configML.sql* file.

1 Navigate to the UA installation directory and open *configML.sql* with a text editor.

2 Search for the line that says:

```
call ml_add_property( 'SIS',
'com.sybase.ua.gateway.SMSGateway(UASMS)',
'database_url',
'jdbc:sybase:Tds:localhost:4747?servicename=portaldata
base' );
```

Replace the `4747` with the port number your ASA is listening on.

3 Search for the line that says `call ml_add_property( 'SIS', 'com.sybase.ua.gateway.MailGateway(UAMAIL)', 'server', 'localhost' );` and replace `localhost` with the host name of the machine in your network that handles your SMTP requests.

4 Save and close the *configML.sql file*.

5 Run *configML.bat*.

6 Restart MobiLink. See “Starting and stopping MobiLink” on page 19.

Verifying the mail.host property

When you create a new user in Mobile Web Studio, you are sent a verification e-mail message that contains the user's password. Verify the mail.host property in the *global.properties.xml* file is pointing 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 verify that the value of the IP address or fully qualified DNS matches 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%\UA80\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.

❖ **Using Unwired Accelerator behind a proxy server**

1 Navigate to *%SYBASE%\UA80\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 that should 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"/
```

Updating digital certificates

User authentication for the portal uses HTTPS, which uses Secure Sockets Layer (SSL) to post the user names and passwords that users enter in an encrypted form over a secure channel. SSL and HTTPS rely on 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 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 Uwired 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 14.

❖ **Obtaining the offline client OTA**

1. On the BlackBerry device, use the BlackBerry browser to navigate to `http://hostname.domain:port/onepage/ota/bb`.
2. First download: *Uaframework.jad*. This downloads the UA framework, needed for push synchronization.
3. Then download the following to install the UA client, and the UA listener also needed for push synchronization:
   - *Uaclient.jad*
   - *Ualistener.jad*

❖ **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 Download link, select BlackBerry Device 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 14.

Installing RIM BlackBerry server

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

Installing BlackBerry server

Skip this section if you plan to use M-Business Anywhere server to deploy applications to mobile devices, instead of the RIM BlackBerry Enterprise Server (BES). The 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 instead of using M-Business Anywhere server, 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.

Setting up BlackBerry users

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

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 his or her 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 Unwired Accelerator.

❖ **Starting Unwired Accelerator**

- Select Start | Programs | Sybase | Unwired Accelerator | Start UA (Windows Services). This starts the ASA database, the Tomcat application server, and MobiLink.

❖ **Stopping Unwired Accelerator**

- Select Start | Programs | Sybase | Unwired Accelerator | Stop UA (Windows Services). This stops MobiLink, the Tomcat application server, and the ASA database.

Typically, you leave the application server and database running, but you may need to stop and start the application server or database to modify the system or initialize a configuration change. If you stop and start the ASA database or Tomcat server independently, start the UA components in this order:

1 ASA database

2 Tomcat server

3 MobiLink

Stop UA components in this order:

1 MobiLink

2 Tomcat server

3 ASA database

Starting and stopping the database

This section describes how to start and stop the Adaptive Server Anywhere database. The security provider—portaldatabase (or PortalDB)—is included with ASA as a default.

❖ **Starting and stopping the ASA database using Windows Services**

ASA starts as a Windows Service automatically. If you shut it down and need to restart it:

1 Select Start | Settings | Control Panel.

2 In the Control Panel window, double-click Administrative Tools.

3 In the Administrative Tools window, double-click Services.

4 In the Services window, scroll down the list and select Unwired Accelerator ASA Database.

5 Select Action | Start to start the ASA database.
Select Action | Stop to stop the ASA database.

❖ **Starting the ASA database using the Command Prompt window**

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

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

When the database starts, the icon for the Sybase ASA database appears in your taskbar.

❖ **Shutting down the ASA database**

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

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

Starting and stopping the Tomcat application server

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

❖ **Starting and stopping the Tomcat application server using Windows Services**

ASA starts as a Windows Service automatically. If you shut it down and need to restart it:

1 Select Start | Settings | Control Panel.

2 In the Control Panel window, double-click Administrative Tools.

3 In the Administrative Tools window, double-click Services.

4 In the Services window, scroll down the list and select Unwired Accelerator Tomcat Server.

5 Select Action | Start to start the Tomcat Server.
Select Action | Stop to stop the Tomcat Server.

❖ **Starting the Tomcat application server**

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

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

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

```
Dbconnectionbroker:init<>
[dba@jdbc:sybase:Tds:lab2k:4747 <op portal asa>]
DataManager created
Review datamanager.log in C:/Sybase/UA80/logs
```

When you see this message, minimize the Tomcat window but do not close it. If you do not see this message, check the *datamanager.log* file, located in *x:\tmp\logs*.

❖ **Shutting down the Tomcat application server**

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

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

Starting and stopping MobiLink

This section describes how to start and stop MobiLink.

❖ **Starting and stopping MobiLink using Windows Services**

ASA starts as a Windows Service automatically. If you shut it down and need to restart it:

1 Select Start | Settings | Control Panel.

2 In the Control Panel window, double-click Administrative Tools.

3 In the Administrative Tools window, double-click Services.

4 In the Services window, scroll down the list and select Unwired Accelerator MobiLink Server.

5 Select Action | Start to start the MobiLink server.
Select Action | Stop to stop the MobiLink server.

❖ **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

---

Note You cannot cancel the uninstallation after clicking Next in the uninstaller Welcome window, so be sure you want to proceed with the uninstallation before clicking Next in the initial Welcome window of the uninstaller.

❖ **Removing Unwired Accelerator**

Before beginning the uninstallation, close the Administrative Tools | Services window if it is open. Otherwise, the uninstaller is not able to completely remove UA 8.0 from Windows Services.

1 Select Start | Programs | Sybase | UnwiredAccelerator | Uninstall UA.

Alternatively, select Start | Settings | Control Panel | Add or Remove Programs, and remove Unwired Accelerator.

2 A prompt notifies you that a file has been modified and asks if you want to proceed with removing it. Click Yes to All.

3 The uninstallation summary window displays. Click Finish.

4 Delete the *%SYBASE%\UA80* installation directory to remove any residual files.

Upgrading from UA 7.0 to 8.0 (Tomcat)

This section describes how to update from Unwired Accelerator 7.0 to 8.0 when running in the Tomcat application server.

❖ **Pre-upgrade tasks**

Before beginning the upgrade:

1 Back up your UA 7.0 installation. The upgrade process does not preserve the UA 7.0 installation. If you uninstall Unwired Accelerator 8.0 after you upgrade, everything is uninstalled, including anything from your UA 7.0 installation.

2 Shut down Tomcat. See “Starting and stopping the Tomcat application server” on page 18.

3 Open a Command Prompt window, and navigate to your UA 7.0 installation directory and start the ASA database by entering:

```
startdb.bat
```

❖ **Upgrading UA 7.0 to 8.0 (Tomcat)**

1 Insert the Unwired Accelerator installation CD into your CD drive.

2 Perform an installation as described in “Installing Unwired Accelerator” on page 6.

Note You must use the same domain name, host name, database port, HTTP port, and HTTPS port as you configured for your 7.0 installation. The installer does not verify this information and will proceed with the installation but UA will not start properly after the installation.

Select your existing UA installation directory as the installation directory. The Installer notifies you that you are performing an upgrade. During the upgrade, the Installer:

- Overwrites unchanged UA 7.0 files with UA 8.0 files.
- Renames files changed by both Sybase and the user with the *.ChangedByUser* file extension.

  You must open each of the *.changedByUser* files listed in the installer window and manually merge each one according to the information contained within the file.
- Keeps files that are unchanged by Sybase from version 7.0 to version 8.0, but modified by the user, and copies the corresponding UA 8.0 files with the file extension *.ua8*.
- Retains the database files unchanged.
- Updates the *global.properties.xml* file where necessary.
- Creates a *tomcat.old/webapps* directory.

3 The Installation Progress window displays.

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

Click Finish.

4 Click Yes, restart the computer now. UA starts as a Windows Service after the computer restarts.

5 Log in to Unwired Accelerator as described in “Verifying the installation” on page 9.

Post-upgrade tasks

After perfoming the upgrade, there are some additional tasks you may need to perform.

- Log in to Mobile Web Studio and change the action type of linked applications you upgraded from 7.0 to 8.0 to Update.
- If you have created or changed the following files or applications, either re-create them or manually merge them:
  - If you have any customized *.jsp* files from *onepage\fw\baseApps*, manually merge them.

- If you change the location of the installation, manually copy custom *.jsp* files to the same subdirectory in the new installation directory.
- If you modified the main *index.jsp* file from the *onepage* directory, manually merge them.
- If you have created a *cobrand* directory, verify the installer retained the directory.
- If you have customized images, check them, and if necessary, copy them from your backup.
- Verify that any advanced applications you created, such as server-side click-across linked applications with update, charting, offline BlackBerry, and so on are working correctly. If they are not, you must re-create them.
- Check the DefaultResourceID in the *global.properties.xml* file to verify that it is 21. If it is not 21, change the property manually to duplicate the same UA look and feel when you create new resources.
- If you use the CellularModemController (CMC), after performing the upgrade, run:

```
run -logLevel FINEST -initDatabase true
```

- Check the *tomcat.old/webapps* directory created by the installer. If you need the files contained in the directory, you must manually deploy them into the new version of Tomcat. You may need to modify these files, as UA 8.0 uses version 5.5 of Tomcat as opposed to version 4.0 used by UA 7.0
- Check the templates associated with any applications you imported from version 7.0 and verify the associated template is appropriate for version 8.0 to avoid execution failures. For example, the BlackBerry Online template has changed with 8.0, the Nokia Online template is new, and applications created in 7.0 may use XSL templates that no longer work with 8.0.

  To fix the templates, either edit the application so that each device type points to the correct template; or edit the template itself so that it is correct. If you edit the template, there is no need to edit the application. Decide which method to use based on whether the problem is with the template definition, or with the application pointing to the wrong template.

CHAPTER 3

Troubleshooting

This chapter describes how to troubleshoot Unwired Accelerator installation and configuration problems.

Topic	Page
Overview	25
Installer	26
Unwired Accelerator setup	26
BlackBerry Enterprise Server setup	28
MobiLink setup	28
Mobile device setup	29
Upgrade	30

Overview

To help troubleshoot installation and configuration problems:

- View log files, typically found in *x:\tmp\logs*
- View error messages
- Check port numbers
- Check configuration files (especially *global.properties.xml*, *server.xml*)
- Test connections
- Run the Portal Interface and Mobile Web Studio
- Run the M-Business Anywhere server and client
- Run mobile device applications

Installer

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

Table 3-1: Troubleshooting installation problems

Problem	Try this
During installation, you see a `configASA.err` listed in the config error files in the second to last window of the installer..	Windows 2000 is not a supported, nor certified, operating system on which to run UA 8.0. This error is caused when reg.exe is not found on your Windows 2000 machine. You must install reg.exe, then run the following scripts: • *createdsn.bat* • *installasaodbc.bat* • *configasa.bat* This problem might also occur if you previously uninstalled ASA improperly, i.e. by deleting the ASA directory instead of using the uninstaller. You can find the instructions for installing *reg.exe* on the Microsoft support Web site at http://support.microsoft.com/kb/301423/.

Unwired Accelerator setup

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

Table 3-2: Troubleshooting Unwired Accelerator problems

Problem	Try this
Cannot start ASA database: `Connection error: Unable to initialize requested communication links`	If you receive this error when trying to start the ASA database, check the *global.properties.xml* and *server.xml* files to make sure the ASA port number is set to the correct value, and to the same value in both files. The default is 4747. You can also check the *datamanager.log* file, located in *x:\tmp\logs*, for database-related error messages.
Missing database in the ASA process.	Verify that the database files specified to start in *startdb.bat* and *uadbservice.bat* are in sync. If Windows services is used to start ASA, you must reinstall the service.

Problem	Try this
Cannot connect to Mobile Web Studio: • Receiving 404 error codes • Having authentication problems and the Tomcat log/console shows connection exceptions.	The host and/or domain name may not have been entered correctly for your environment during installation. Verify the following configuration files contain the correct host and domain names: • *global.properties.xml*, located in *%SYBASE%\tomcat\webapps\onepage\config* • *domain.js*, located in *%SYBASE%\tomcat\webapps\onepage\javascript* • *context.xml*, located in *%SYBASE%\tomcat\webapps\onepage\META-INF* • *config.txt*, located in *%SYBASE%\tomcat\webapps\certAuth* The above files can be corrected by executing *%SYBASE%\UA80\config.bat [domain name]*. **Note** *config.bat* uses %COMPUTERNAME% as the host name. • *server.xml*, located in *%SYBASE%\tomcat\conf* After modifying these files, you must restart the Tomcat application server.
Cannot start Portal Interface: `File Not Found 404 error`	Check the *global.properties.xml*, *domain.js*, and *server.xml* files to make sure the *localhost*, *domain*, and *port* values are set to the correct values, and to the same values in all files. If you receive this error when trying to start Portal Interface, make sure you: • Entered the URL correctly to access Portal Interface as described in "Verifying the installation" on page 9. • Are using the correct port number; for example, 4040.
Cannot start Mobile Web Studio	Verify that you are using: • Internet Explorer and not Netscape. • The correct version of Internet Explorer as described in Table 2-1 on page 3. • The correct port number, for example, 4040 when running in Tomcat.
Mobile Web Studio window does not display	Make sure you do not have pop-ups disabled in the Web browser. The Mobile Web Studio application requires pop-ups. If you do not want to enable pop-ups, you can access Mobile Web Studio by entering the following in the Web browser `http://hostname.domain:port/onepage/loader.jsp`
Cannot play back applications using the Active X capture method.	You must start Tomcat using *starttomcat.bat*. See "Starting and stopping the Tomcat application server" on page 18.

BlackBerry Enterprise Server setup

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

Table 3-3: Troubleshooting BES setup 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.
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.

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 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 proeprties for the uam1 data source are set correctly.
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 excecute *configML.bat*. See “Setting the SMTP server and UAMAIL gateway in MobiLink” on page 10.
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 excecute *configML.bat*. See “Setting the SMTP server and UAMAIL gateway in MobiLink.”

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.

Mobile device setup

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

Table 3-5: Troubleshooting Unwired Accelerator problems

Problem	Try this
Cannot create a personal channel	Check the *global.properties.xml* file to make sure the alwaysValidateSession parameter is set to false. See the *Unwired Accelerator Administration Guide* for information about *global.properties.xml*.
Cannot access mobile application: `Your submission has been recorded and will be sent during the next Synchronization`	If you see this message when trying to access an application on a mobile device, check the alwaysValidateSession parameter in the *global.properties.xml* file. The parameter is probably set to true, but should be set to false to enable personal channels to work. See the*Unwired Accelerator Administration Guide* for information about *global.properties.xml*.
Mobile application does not appear on the mobile device	Verify that: • The mobile application is deployed to the group. In Mobile Web Studio, select Manage | M-Business | Groups, and check the groups. • The M-Business Anywhere user name/password and server properties are set correctly in M-Business Client. M-Business Clients use M-Business users, not Mobile Web Studio users. See the *Unwired Accelerator Administration Guide* for information about M-Business Anywhere and M-Business Client software. • The user belongs to the group that contains the mobile application. • For BlackBerry devices, make sure the Offline BlackBerry option is selected for the application, and that the application is in a grid/table format.

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 client logo does not appear on the BlackBerry device	Make sure you installed the offline client on the BlackBerry device (or BlackBerry simulator), as described in “Installing an offline client on a BlackBerry device using BlackBerry Desktop Manager” on page 13 (or “Installing an offline client on a BlackBerry simulator” on page 15).

Upgrade

Table 3-6: Troubleshooting upgrade problems

Problem	Try this
Linked applications do not work after upgrade	If you exported linked applications from UA 7.0 to UA 8.0, the action type property changes from update to insert. To fix the linked applications, log in to Mobile Web Studio, manually drop and relink the applications that are not working and change the type to update.

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.

Topic	Page
Overview	31
Configuring the CSI realm	32
Configuring the security provider	32
Configuring certificate authentication	43
Configuring the CSI RADIUS provider	46
Stacked CSI providers	48
Enabling debugging in the Tomcat realm	50

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 both 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 42.

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 41. • "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 33:

- 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 33 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 33.

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 in 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, open the *logging.properties* file located in *%CATALINA_HOME%\tomcat\conf*, 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, *C:\%SYBASE%\UnwiredAccelerator80\tomcat\logs\security_debug.log*.

Initially, the Tomcat CSI realm is configured to use the PortalDB provider. To use the LDAP provider, see “Configuring the LDAP provider” on page 33.

Index

Symbols

#, beginning comment lines in properties file 50
& (ampersand), Boolean operator 33, 36
< and > (angle brackets)
  <!-- ... -->, XML comment delimiters 43
  <? ... ?>, in XML processing instructions 42
| (vertical bar)
  Boolean operator 36

A

ASA
  starting the database 18
  stopping the database 18
authentication and authorization, setting up 31
authentication providers
  LDAP 33
  PortalDB 42
AuthenticationFilter, LDAP configuration option 33
AuthenticationMethod, LDAP configuration option 34
AuthenticationScope, LDAP configuration option 34
AuthenticationSearchBase, LDAP configuration option 34

B

BindDN, LDAP configuration option 34
BindPassword, LDAP configuration option 34
BlackBerry device
  installing an offline client application 13
  installing an offline client application OTA 13, 14
  troubleshooting 29
BlackBerry simulator
  troubleshooting 29

C

CATALINA_HOME environment variable ix, 50
certificates 12
CertificateValidationLoginModule
  configuration options 46
channels 29
commands
  ipconfig 5
configuring
  CSI with LDAP (Tomcat) 17
  LDAP security provider 33
  PortalDB security provider 42
  proxy server 11
  Tomcat CSI realm 50
CSI
  LDAP provider 17
  PortalDB provider (default) 17
CSI RADIUS
  configuration options 47
CSI realm
  configuring 32
csi.xml, security provider configuration file
  PortalDB provider definition 42

D

datamanager.log file 26
DefaultSearchBase, LDAP configuration option 35
digital certificates 12
disk space requirements 3
displaying
  domain name 5
documentation
  Adaptive Server Anywere vi
  jConnect for JDBC vi
  Unwired Accelerator vi
domain name 5

E

environment variables
CATALINA_HOME ix, 50
JAVA_HOME ix
RIM ix
SYBASE viii, ix

F

files
global.properties.xml file 11

G

global.properties.xml
configuring a proxy server 11

H

HTTP port 4
HTTPS port 4

I

InitialContextFactory, LDAP configuration option 35
installation
administrator privileges, required 5
installation tasks 5
post-installation tasks 8
pre-installation tasks 5
installing
offline client application on BlackBerry device 13
offline client application on BlackBerry device (OTA) 13, 14
Unwired Accelerator 3, 6

J

JAVA_HOME environment variable ix

L

LDAP security provider
configuration options 33
role computation 38
setting up 33
Lightweight Directory Access Protocol. *See* LDAP security provider
log files
datamanager.log 26
default location 5, 25

M

Microsoft ActiveDirectory server, restrictions 41

O

operating system, requirements 3
overview
authentication and authorization 31
Unwired Accelerator product 1

P

personal channels 29
PortalDB
included with ASA 18
PortalDB security provider
configuring 42
included with ASA 18
ports
4040 (UA HTTP, in Tomcat) 4, 10
4443 (UA HTTPS, in Tomcat) 4
4747 (UA ASA connection port) 4
80 (UA HTTP, with Netscape) 7
8091 (M-Business admin) 4
8092 (M-Business client "synch") 5
8099 (M-Business JDBC connection) 4
post-installation tasks
configuring a proxy server 11
configuring Tomcat for LDAP 17
installing RIM BlackBerry server/client 16
overview 8

updating digital certificates 12
verifying the installation 9
pre-installation tasks 5
checking disk space 5
checking *tmp* directory permissions 5
knowing the domain name 5
overview 5
ProviderURL, LDAP configuration option 35
proxy server 11

R

resource
user profile 14
RIM environment variable ix
role computation for LDAP 38
RoleFilter, LDAP configuration option 36
RoleMemberAttributes, LDAP configuration option 36
RoleNameAttribute, LDAP configuration option 36
RoleScope, LDAP configuration option 36
RoleSearchBase, LDAP configuration option 36

S

security
CSI with LDAP provider 17
CSI with PortalDB provider 17
ServerType, LDAP configuration option 37
setting up authentication and authorization 31
starting
ASA database 18
Tomcat application server 19, 20
stopping
Tomcat application server 19, 20
stoppping
ASA database 18
SYBASE environment variable viii, ix
system requirements
disk space 3
network protocols 3
operating system 3
system release level 3
Web browser 3

T

Tomcat
configured with CSI and PortalDB provider 17
configuring CSI realm 50
configuring LDAP 17
debugging CSI realm 50
installation directory 50
Tomcat application server
starting the application server 19, 20
stopping the application server 19, 20
troubleshooting
cannot access mobile application 29
cannot create personal channels 29
cannot start Mobile Web Studio 27
cannot start Portal Interface 27
File Not Found 404 error 27
JVM error when loading UA client on BlackBerry device 30
mobile application does not appear on PDA 29
Mobile Web Studio window does not display 27
resources 25
UA cannot connect to BlackBerry Desktop Manager 28
UA client logo does not appear on BlackBerry device 30

U

uninstalling
Unwired Accelerator (Tomcat) 20
Unwired Accelerator
default ports 4
network protocol for 3
overview 1
product description 1
verifying the installation 10
updating, digital certificates 12
upgrading
from UA 6.5 to UA 7.0 (Tomcat) 21
UserFreeformRoleMembershipAttributes, LDAP configuration option 38
UserRoleMembershipAttributes, LDAP configuration option 38