WebSphere® Everyplace™ Suite

Getting Started

Version 1.1.3

Note

Before using this document, read the general information under "Notices" on page 109.

Second Edition (March 2001)

This edition applies to the IBM WebSphere Everyplace Suite Version 1 Release 1 Modification Level 3 (for AIX and Solaris); 5765–E59, Enterprise Edition; 5697–G53, Service Provider Edition; and to all subsequent releases and modifications until otherwise indicated in new editions. Make sure you are using the correct edition for the level of the product.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

International Business Machines Corporation
Department CGM
P.O. Box 12195
Research Triangle Park, North Carolina
27709-2195

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

About this information

Note

This Web-based version of the *IBM® WebSphere™ Getting Started* book has been updated to include all of the material from the Everyplace Suite Version 1.1.3 README. This version is more current than the *Getting Started* document provided on CD number 1 on the Everyplace Suite Version 1.1.3 CDs.

This book contains information for the planning, installation and configuration of the IBM WebSphere Everyplace Suite (from now on referred to as the Everyplace Suite). The Everyplace Suite is an integrated, modular suite of software components that support connectivity of pervasive devices such as wireless phones, personal digital assistants (PDAs), and mobile computers, to online information. This book does not provide documentation regarding the specific Everyplace Suite components. See “Where to find Everyplace Suite component documentation” on page 4 to locate documentation about individual components.

Who should read this book

This document is intended for system administrators responsible for installing and configuring the components of the Everyplace Suite. It is also intended for individuals using the Everyplace Administration Console and administering the Everyplace Authentication Server. They should be experienced in supporting internet servers running the AIX or Solaris operating systems.

How this book is organized

This book contains the following chapters:

- “Chapter 1. Introducing the IBM WebSphere Everyplace Suite” on page 1 describes the Everyplace Suite and its components.
- “Chapter 3. Planning to implement the Everyplace Suite” on page 15 provides information about planning issues, and hardware and software requirements.
- “Chapter 4. Installing the Everyplace Suite” on page 39 gives detailed instructions about installing the Everyplace Suite.
- “Chapter 5. Configuring the Authentication Server” on page 73 gives detailed instructions about configuring the Everyplace Authentication Server.
- “Chapter 6. Configuring and administrating the Everyplace Suite” on page 87 provides information about administering and configuring the Everyplace Suite and using the Everyplace Administration Console.
- “Chapter 8. Uninstalling the Everyplace Suite components” on page 105 gives information about uninstalling the Everyplace Suite or Everyplace Suite components.

Conventions

The following conventions are used throughout this book:

Directory paths, file names, and command line commands will appear in monospace, as follows: `/pathname/directory/command`

Book titles and website URLs and links will appear in italics, as follows: *www.website.com/webpage*

Buttons, text fields, and other selectable entities will appear in **Bold Text**.

Naming conventions

The Everyplace Suite comprises many components and supporting components. The following list gives the full product name of all the components that make up the Everyplace Suite along with any short names used in this book.

- **WebSphere Everyplace Suite**: Everyplace Suite
- **Everyplace Authentication Server**: Authentication Server
- **Everyplace Wireless Gateway**: Wireless Gateway
- **MQSeries® Everyplace for Multiplatforms**: MQSeries Everyplace
- **WebSphere Edge Server Caching Proxy (Web Traffic Express)**: Edge Server Caching Proxy, Caching Proxy
- **WebSphere Edge Server Load Balancer (Network Dispatcher)**: Edge Server Load Balancer, Load Balancer
- **Tivoli® Personalized Services Manager**
- **WebSphere Transcoding Publisher**: Transcoding Publisher
- **IBM DB2® Universal Database™**: IBM DB2 UDB, DB2
- **Everyplace Administration Console**: Administration Console
- **IBM HTTP Server**: HTTP Server
- **SecureWay® Directory**
- **WebSphere Application Server**: Application Server
- **Everyplace Synchronization Manager**: Synchronization Manager

Chapter 1. Introducing the IBM WebSphere Everyplace Suite

The IBM WebSphere Everyplace Suite is an integrated, modular suite of software components. These software components provide reliable access to online information from a wide variety of pervasive devices such as cellular phones, personal digital assistants (PDAs), and mobile computers, among other wireless and traditionally connected devices. Together, the Everyplace Suite components provide solutions for connectivity, security, content handling, optimization and subscriber and device management.

The Everyplace Suite is intended for the following kinds of customers:

- **Enterprise customers** who seek to extend their intranet applications to pervasive devices. These devices include job-task devices (such as electronic package delivery and tracking systems) and multifunction devices (such as laptop computers and PDAs). These customers may also wish to deliver select Internet content to users.
- **Content providers** who wish to deliver data and applications to consumers. These customers include enterprises providing Internet commerce, finance, information sites, and Internet portals.
- **Internet service providers** who wish to provide connection services to consumers and enterprise users.

Everyplace Suite components

Each Everyplace Suite component performs a different function in extending pervasive computing connectivity. These components may either be provided iwth the Everyplace Suite CDs or purchased as third-party software components. The Everyplace Suite components provide the following services through the corresponding components:

Connectivity

- **Everyplace Wireless Gateway**: Provides a communications platform that enables Internet Protocol and Wireless Access Protocol (WAP) applications to run in a wireless environment.
- **Everyplace Authentication Server**: Acts as the point of entry to the Everyplace Suite domain for devices that do not connect through the Everyplace Wireless Gateway. Supports third-party gateway connectivity if desired.
- **MQSeries Everyplace for Multiplatforms**: Provides assured messaging capability between devices and any MQSeries family platform.
- **Everyplace Synchronization Manager**: Enables mobile computing devices to link remotely to applications such as Microsoft Exchange, Lotus Notes or DB2 databases.

Security

- **Everyplace Wireless Gateway**: Provides network access user authentication for WAP and non-WAP users, and data encryption. Supports Internet Protocol and WAP transport layer security and can be configured to use a third party RADIUS server.

- **Everyplace Authentication Server**: Authenticates users defined to the Everyplace Suite when they attempt to access Everyplace Suite services.

Subscriber and Device Management

- **Tivoli Personalized Services Manager**: Provides tools to centrally manage subscribers and their devices, and allows for the creation of discrete groups of users.

Content Handling

- **WebSphere Transcoding Publisher**: Adapts, reformats, and filters data based on the destination device or network.
- **WebSphere Edge Server Caching Proxy (Web Traffic Express)**: Retrieves Internet data for multiple browser clients and acts as a caching server and content filter.

Optimization

- **WebSphere Edge Server Load Balancer (Network Dispatcher)**: Balances requests in real time among Everyplace Suite servers to increase capacity and scalability of heavily accessed enterprises.

Note: You only need to install the components that best provide or extend the services you require. See “Understanding the Everyplace Suite components” on page 15 for more information about the Everyplace Suite components and their subcomponents.

Figure 1 shows the Everyplace Suite providing connectivity between client software on the pervasive devices and internet applications and content.

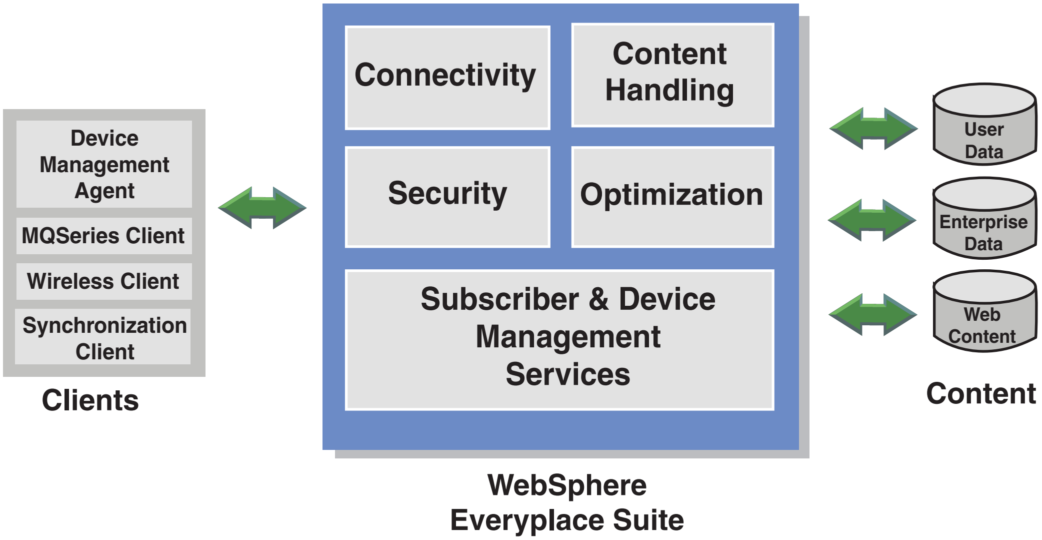


Figure 1. WebSphere Everyplace Suite connecting client devices and internet data

Everyplace Suite deployment scenarios

The Everyplace Suite components that are installed will depend on the specific services to be provided. The following examples represent three possible customer requirements and the Everyplace Suite solutions to meet them. These are just a few examples of possible Everyplace Suite solutions. Each deployment of the Everyplace Suite is intended to be a unique solution to specific user requirements. See “Everyplace Suite installation models” on page 21 for more information about Everyplace Suite deployment.

Content provider — start-up portal company

A start-up portal company wants a complete solution for device support. This is a company with no existing database of users. The company will provide content through an Internet portal page that users can customize to their personal tastes and needs. The company also wants to offer services such as e-mail and search engine capability for both wired and wireless devices. This company requires a complete suite of services including transcoding, device management, data synchronization, and assured messaging. The company also needs integrated network access support (NAS) and wireless access protocol (WAP) connectivity.

The company requires the following Everyplace Suite components:

- WebSphere Transcoding Publisher — data transcoding
- MQSeries Everyplace — assured messaging

- Everyplace Wireless Gateway — wireless device connectivity (WAP support)
- Edge Server Caching Proxy — performance optimization
- Edge Server Load Balancer — performance optimization
- Everyplace Authentication Server — user authentication and security
- Everyplace Synchronization Manager — data synchronization
- Tivoli Personalized Services Manager — subscriber and device management
- IBM DB2 Universal Database — subscriber and device management

Enterprise customer — package delivery company

An overnight delivery company wants to equip its delivery personnel with wireless devices to record and track delivery of packages in the field. The company already has a device and user support infrastructure in place, including user and subscriber management. It is not important that network access infrastructure be integrated with the rest of its device infrastructure.

The company requires the following Everyplace Suite components:

- Everyplace Wireless Gateway — wireless device connectivity
- MQSeries Everyplace — assured messaging
- Everyplace Synchronization Manager — data synchronization

Internet service provider — pervasive support

A new internet service provider wants to specialize in pervasive device services. The provider will require users to subscribe in order to obtain the new service.

The company requires the following Everyplace Suite components:

- Everyplace Wireless Gateway — wireless device connectivity
- Everyplace Authentication Server — user authentication and security
- Tivoli Personalized Services Manager — subscriber and device management
- WebSphere Transcoding Publisher — data transcoding
- Edge Server Load Balancer — performance optimization

See “Chapter 3. Planning to implement the Everyplace Suite” on page 15 for more information about the Everyplace Suite components and planning.

Where to find Everyplace Suite component documentation

The *Getting Started* book does not provide specific information on configuring and using the various Everyplace Suite components. Each Everyplace Suite component provides its own documentation to help you administer and use that component. When more information about a specific component is needed, please refer to the corresponding documentation in this section.

Note: It is important to follow the installation instructions in “Chapter 4. Installing the Everyplace Suite” on page 39 when installing the Everyplace Suite components.

Do not follow the stand-alone installation instructions in the component documentation, as the installation requirements for the component within the Everyplace Suite may vary.

The following list provides information on where to find documentation for all the Everyplace Suite components. Many of the documents can also be accessed through each component's online help.

If you cannot view the Everyplace Suite *Getting Started* or *README* documentation from the Everyplace Suite installation program, change your Netscape settings by entering the following commands from the command line:

```
xhost +localhost
PATH=$PATH:/opt/NSCPcom
export PATH
```

Everyplace Authentication Server

See "Chapter 5. Configuring the Authentication Server" on page 73.

Everyplace Wireless Gateway (Version 1.1)

Before installation, complete documentation, including the *Everyplace Wireless Gateway Administrator's Guide*, can be found on CD number 7 in:

- `/ewg/docs/en/cdread.htm`

In addition, see the Web site:

- *http://www-3.ibm.com/pvc/tech/library.shtml*

MQSeries Everyplace for Multiplatforms (Version 1.1)

Before installation, documentation can be found on CD number 4 in:

- `/mqe/read_me.txt`

The following documents can be found as pdf files in the /mqe directory:

- `READMEFirst.pdf`
- `Introduction.pdf`
- `ProgrammingGuide.pdf`
- `ProgrammingReference.pdf`

In addition, see the Web site:

- *http://www.ibm.com/software/mqseries/library/#books*

Edge Server Load Balancer (Version 1.0)

Before installation, documentation can be found on CD number 6 in:

- `/wscs/Docs/index.htm`

After installation, the *User's Guide* and other documentation can be found in:

- AIX: `/usr/lpp/nd/documentation`

- Solaris: `/opt/nd/documentation`

In addition, see the Web site:

- *http://www.ibm.com/software/webservers/edgeserver/library.html*

Edge Server Caching Proxy (Version 1.0)

Before installation, documentation can be found on CD number 6 in:

- `/wscs/Docs/index.htm`

In addition, see the Web site:

- *http://www.ibm.com/software/webservers/edgeserver/library.html*

Tivoli Personalized Services Manager (Version 1.1.1.0)

Note: The links here point to the English language version of the documents. Other languages are available. The `/en/` portion of the path can be changed (to `/ja/` for Japanese, for example) to access documentation in other languages.

Before installation, complete documentation for overall Tivoli Personalized Services Manager information on both AIX and Solaris systems can be found on CD number 8 in:

- `/tsm/doc/en/index.htm`

This index file contains links to the complete product documentation.

Additional product information not included in the product library, can be found in:

- `/tsm/aix/oracle/ReadMe11.htm`
- `/tsm/aix/oracle/TPSM-Overview.htm`

The `/aix/oracle` portion of the path can be changed to:

- `/aix/db2/`
- `/sun/oracle/` or
- `/sun/db2/`

After installation, complete documentation can be found in the following location:

On AIX systems:

- At physical address: `/usr/TivTSM/doc/en/index.htm`
- At URL: *http://server_name/doc/en/index.htm*

where *server_name* is a computer where Tivoli Personalized Services Manager is installed.

On Solaris systems:

- At physical address: `/opt/TivTSM/doc/en/index.htm`

- At URL: *http://server_name/doc/en/index.htm*

where *server_name* is a computer where Tivoli Personalized Services Manager is installed.

Device Manager feature

Before installation, complete documentation for both AIX and Solaris systems can be found on CD number 8 in:

- `/dms/doc/en/index.htm`

This index file contains links to the complete product documentation.

Additional product information not included in the product library, can be found in:

- `/dms/doc/en/dmsrbdy.htm`

After the Device Manager feature installation, complete documentation can be found in the following locations:

On AIX systems:

- At physical address: `/usr/lpp/TivDMS/doc/en/index.htm`
- At URL: *http://server_name/dmserver/en/index.htm*

where *server_name* is a computer where the Device Manager is installed.

On Solaris systems:

- At physical address: `/opt/TivDMS/doc/en/index.htm`
- At URL: *http://server_name/dmserver/en/index.htm*

where *server_name* is a computer where the Device Manager is installed.

WebSphere Transcoding Publisher (Version 3.5.0.1)

Note: The links here point to the English language version of the documents. Other languages are available. The `/en/` portion of the path can be changed (to `/jp/` for Japanese, for example) to access documentation in other languages.

Before installation, complete documentation can be found on CD number 8 in:

- `/wtp/doc/en/readme.htm`
- `/wtp/doc/en/index.htm`

This index file contains links to a number of Transcoding Publisher documents, that discuss planning, installation and configuration, and administration.

After installation, the WebSphere Transcoding Publisher *Administrator's Guide* and *Developer's Guide* can be opened from the **Help** menu of the WebSphere Transcoding Publisher Administration Console.

In addition, see the Web site:

- *http://www.ibm.com/software/webservers/transcoding/library.html/*

Everyplace Synchronization Manager (Version 1.1)

Before installation, the following documentation can be found on CD number 11 in:

- `/README_For_Sync.txt`
- `/esm/docs/English/Getting started guide.pdf`
- `/esm/docs/English/Everyplace Sync Manager (ce).pdf`
- `/esm/docs/English/Everyplace Sync Manager (palm).pdf`
- `/esm/docs/English/Everyplace End User Guide (ce).pdf`
- `/esm/docs/English/Everyplace End User Guide (palm).pdf`
- `/esm/docs/English/Everyplace End User Guide (EPOC).pdf`

Japanese Everyplace Synchronization Manager documentation is located in the following file on CD number 11:

- `/README_For_Sync_Jp.txt`
- `/esm/docs/Japanese/Everyplace End User Guide (ce).pdf`
- `/esm/docs/Japanese/Everyplace End User Guide (palm).pdf`

IBM DB2 Universal Database — Enterprise Edition (Version 7.1)

See the Web site:

- *http://www.ibm.com/software/data/db2/library/*

WebSphere Application Server — Standard Edition (Version 3.5)

Before installation, documentation can be found on CD number 5 in:

- `/was/sun/spool/WSdocen/reloc/IBMWebAS/web/InfoCenter/index.htm`
- `/was/aix/README.FIRST`
- `/was/sun/spool/README.FIRST`

In addition, see the Web site:

- *http://www.ibm.com/software/webservers/appserv/library.html*

IBM HTTP Server (Version 1.3.12)

See the Web site:

- *http://www.ibm.com/software/webservers/httpservers/library.html*

SecureWay Directory (Version 3.2)

Before installation, documentation can be found on CD number 4 in parent files `/swd/aix/start.htm` and `/swd/sun/start.htm` for AIX and Solaris, respectively.

In addition, see the Web site:

- *http://www.ibm.com/software/network/directory/library/*

Redbooks™

You can access the following Redbooks for the Everyplace Suite and Everyplace Suite components through the IBM Redbook site:

- *An Introduction to IBM WebSphere Everyplace Suite Version 1.1 Accessing Web and Enterprise Applications, SG24-5995-00*
- *Using IBM WebSphere Everyplace Suite Version 1.1.2, SG24-5996-00*
- *IBM WebSphere Transcoding Publisher V1.1: Extending Web Applications to the Pervasive World, SG24-5965-00*
- *Mobile Computing: The eNetwork Wireless Solution, SG24-5299-00*
- *Web Caching and Filtering with IBM WebSphere Performance Pack, REDP0009 (redpaper)*
- *WebSphere V3 Performance Tuning Guide, SG24-5657-00*
- *IBM WebSphere Performance Pack: Caching and Filtering with IBM Web Traffic Express, SG24-5859-00*
- *IBM WebSphere Performance Pack: Load Balancing with IBM SecureWay Network Dispatcher, SG24-5858-00*
- *Using LDAP for Directory Integration A look at IBM SecureWay Directory, Active Directory and Domino, SG24-6163-00*

A system development kit is available to help you build wireless applications that run on various Everyplace Suite components. The WebSphere Everyplace Suite System Development Kit (SDK), available through the IBM PartnerWorld® program, allows you to create and test applications, and includes WAP Client-Proxy, phone and gateway simulators, WML, Push, VoiceXML samples, and documentation. For more information, see *http://www.developer.ibm.com/pvc/index.html*

Chapter 2. Data migration

Custom data migration for Everyplace Suite Version 1.1.3 will be handled by the refreshed Everyplace Suite components. However, the Everyplace Suite installation program will automate the migration as much as possible.

Note: Data migration is not supported in a Japanese environment. If Japanese environment support is required for migrating from Everyplace Suite Version 1.1.2 to Everyplace Suite Version 1.1.3, please contact your IBM service representative.

The following table lists migration changes for Everyplace Suite Version 1.1.3:

Table 1. Everyplace Suite data migration for Corrective Service Delivery

Everyplace Suite component	Migration performed by	Notes
WebSphere Transcoding Publisher	WebSphere Transcoding Publisher	WebSphere Transcoding Publisher tools will be invoked by Everyplace Suite installation.
Everyplace Wireless Gateway	Everyplace Suite installation	Everyplace Wireless Gateway installation launches the script during Everyplace Suite installation.
Tivoli Personalized Services Manager	Everyplace Suite installation	Everyplace Suite installation migrates the Tivoli Personalized Services Manager DB2 database. See “Migrating the Oracle database for Tivoli Personalized Services Manager” on page 13 for information on migrating the Oracle database.
Everyplace Authentication Server	Follow instructions in the “Third-party gateway support” on page 90 for Everyplace Suite 1.1.3 Authentication Server configuration.	

Before you begin data migration, it is recommended that you back up the SecureWay Directory (LDAP) server. If more than one Everyplace Suite component is installed on the same system, it is recommended that you migrate one Everyplace Suite component at a time. You should migrate data for Everyplace Suite components in the following order:

1. WebSphere Transcoding Publisher
2. Tivoli Personalized Services Manager
3. Everyplace Wireless Gateway
4. Authentication Server
5. Everyplace Synchronization Manager

The following sections provide additional information for migrating each of the above Everyplace Suite components.

Migrating the WebSphere Transcoding Publisher

It is recommended that WebSphere Transcoding Publisher be the first component migrated. Before the start of WebSphere Transcoding Publisher migration make sure that WebSphere Transcoding Publisher related processes are stopped and that you have made a backup of all custom device profile and custom stylesheet files. You must also stop `AdminConsle.sh` and `RunTrancoding.sh`.

Any custom device profiles and XML stylesheets in the `/usr/lpp/IBMTrans` directory tree will be deleted during migration and may not be properly copied to the new WebSphere Transcoding Publisher installation directory. Before migrating WebSphere Transcoding Publisher, make a backup copy of all custom device profiles and custom XML stylesheets.

After starting the migration, from the component list select WebSphere Transcoding Publisher. Select **yes** to over-write the previous version of WebSphere Transcoding Publisher. After the installation is complete, load the `AdminConsole.sh` and re-enable each custom stylesheet. Start WebSphere Transcoding Publisher by running `RunTranscoding.sh`.

On Solaris systems, there should be no Everyplace Suite entries in the `/vol/dsk` directory prior to installing WebSphere Transcoding Publisher. To remove any entries, type the command `rm /vol/dsk/everypl*` before starting the Everyplace Suite installation program.

Migrating the Tivoli Personalized Services Manager

It is recommended that Tivoli Personalized Services Manager be the second component migrated. Before migrating, it is recommended that you back up the Tivoli Personalized Services Manager database data. Also you should ensure that all Tivoli Personalized Services Manager related processes are stopped. This includes IBM HTTP Server, WebSphere Application Server, Transactions server, and the RADIUS, LDAPGateway, and Active Session Table servers.

After starting the migration, select Tivoli Personalized Services Manager and all subcomponents that are shown to already be installed. You do not need to reinstall the Device Management Server as it has not been changed. Do not select the DB2 server to be reinstalled as you do not want to rebuild the DB2 database. Select for installation all Tivoli Personalized Services Manager subcomponents that are shown to be already installed. The installation program should indicate that the Tivoli Personalized Services Manager components are already installed and ask you whether to reinstall. Select **yes**.

After completing Tivoli Personalized Services Manager migration, you can start related processes manually in the following order if they are not already started:

- Transactions servers
- RADIUS Servers, Active Session Table Servers, and LDAPGateway

- IBM HTTP Server
- WebSphere Application Server

Migrating the Oracle database for Tivoli Personalized Services Manager

If you are using Tivoli Personalized Services Manager with the Oracle database, migrate the database from Everyplace Suite Version 1.1.2 to 1.1.3 as follows:

1. Log in as `root`.
2. Save the original `createEventPackage.sql` file as `oldcreateEventPackage.sql` by entering the following command:

   ```
   cd /db/app/oracle/products/8.1.5/schemas/ispb
   mv createEventPackage.sql oldcreateEventPackage.sql
   ```
3. Mount Everyplace Suite CD number 8 in the CD drive. See “From the product CD” on page 54.
4. Place the modified `createEventPackage.sql` file in the `/db/app/oracle/products/8.1.5/schemas/ispb` subdirectory by entering the following command at the `/db/app/oracle/products/8.1.5/schemas/ispb` subdirectory:
   - For AIX:

     ```
     tar -xf /cdrom/tsm/aix/oracle_schema.tar createEventPackage.sql
     ```
   - For Solaris:

     ```
     tar -xf /cdrom/cdrom0/tsm/sun/oracle_schema.tar ./createEventPackage.sql
     ```
5. Apply the new triggers by entering the following commands:

   ```
   su - oracle8
   cd schemas/ispb
   sqlplus stage_master/oracle@ispb @createEventPackage.sql
   quit
   ```

Migrating the Everyplace Wireless Gateway

It is recommended that Everyplace Wireless Gateway be the third component migrated. Before the start of Everyplace Wireless Gateway migration make sure that all Everyplace Wireless Gateway related processes have been stopped. Stop Everyplace Wireless Gateway by entering `ps -ef | grep wga` and then kill the process. If the Everyplace Wireless Gateway resource is running, the `wgated` and `wgattachd` process will also be running and must be stopped. Make sure Wireless GateKeeper (process name `wgcfg`) is stopped if it is running on the same system as Everyplace Wireless Gateway.

After starting the migration, from the component list select Everyplace Wireless Gateway for installation. Select all Everyplace Wireless Gateway subcomponents that are shown to be already installed. Do not select IBM DB2 Universal Database to be reinstalled from the components list as DB2 has not changed and you do not want to rebuild the DB2 database.

Migrating the Authentication Server

It is recommended that Authentication Server be the fourth component migrated. Before the start of Authentication Server migration make sure that all Authentication Server related processes have been stopped. Make sure the `ibmproxy` process has also been stopped before the beginning of Authentication Server migration.

After starting the migration, from the installable component list select the Everyplace Authentication Server only. Do not select to install Edge Server Caching Proxy from the component list as it has not changed. After migration, if you need default realm support, you will have to add the line ″`default_realm [YourDefaultRealm]`″ in the `ibmwesas.conf` file. Where `YourDefaultRealm` is your specific default realm.

Migrating the Everyplace Synchronization Manager

It is recommended that Everyplace Synchronization Manager be the fifth component migrated. See the Everyplace Synchronization Manager README file for information on migrating the Everyplace Synchronization Manager.

Chapter 3. Planning to implement the Everyplace Suite

This chapter provides information you need to begin planning for the Everyplace Suite installation. It identifies all hardware and software requirements and other planning issues to be considered prior to installation.

Understanding the Everyplace Suite components

The Everyplace Suite comprises a number of featured components that are installed in the Everyplace Suite domain, some of which have corresponding subcomponents. The Everyplace Suite domain consists of a group of servers running Everyplace Suite components that are under central administrative control and are within the same protection space (protected area within the same domain name). The Everyplace Suite also includes supporting components, such as IBM HTTP Server and SecureWay Directory, that may require installation. These supporting components are required by some Everyplace Suite components and provide underlying support to the primary Everyplace Suite services.

All of the components, and most of the supporting components, will be provided on the Everyplace Suite product CDs. Other components will need to be downloaded separately and installed prior to installing the Everyplace Suite.

It is important to understand the function and interrelation of the components before beginning installation. The components and their subcomponents are:

Featured Everyplace Suite components

Everyplace Authentication Server

The Authentication Server is the central point of user authentication for the Everyplace Suite. It authenticates users defined to the Everyplace Suite (through the RADIUS server) when they attempt to access Everyplace Suite services. The Authentication Server also allows you to use gateways other than the Everyplace Wireless Gateway if desired. At least one Authentication Server is required in the Everyplace Suite domain to enable integration of most Everyplace Suite components. It is the point of entry to the Everyplace Suite domain for devices that do not connect through the Everyplace Wireless Gateway, and is the next, non-firewall hop for connections through the Everyplace Wireless Gateway.

The Authentication Server runs as a plug-in to the Edge Server Caching Proxy. The Caching Proxy is a prerequisite for Authentication Server and must be installed on the same machine as the Authentication Server. The Authentication Server can be configured in one of two modes:

- **Authentication proxy**: Performs user authentication based on HTTP Authenticate headers. In an Everyplace Suite domain where the authentication proxy is installed, no other origin server (content or application server) in the Everyplace Suite domain may do its own user authentication. Users authenticated through the authentication proxy may not access content outside of the Everyplace Suite domain.

- **Transparent authentication proxy**: Performs user authentication based on HTTP Proxy-Authenticate headers. In an Everyplace Suite domain where transparent proxy is installed, origin servers (content or application servers) in the Everyplace Suite domain may do their own user authentication. The transparent authentication proxy allows users to access material outside the Everyplace Suite domain.

Note: The Authentication Server allows for single user sign-on (user ID and password) for all services within the Everyplace Suite domain. With this feature, user authentication only needs to be done once to access services requiring a user ID and password. Authentication will still be needed for services outside the Everyplace Suite domain.

For example: Users log on to an enterprise site that uses the Everyplace Suite and give their user ID and password, which is then authenticated by the Authentication Server. If users want to change their password (performed by Tivoli Personalized Services Manager) they will not have to enter a user ID and password again to access this service.

Everyplace Wireless Gateway

The Everyplace Wireless Gateway provides a communications platform that enables Internet Protocol and Wireless Access Protocol (WAP) applications to run in a wireless and wired environment. Wireless Gateway provides mobile devices containing the Wireless Client with access to host and network resources through radio and dial-up networks. It can encrypt, compress, and minimize the data that passes through the wireless link, thereby increasing the speed of messaging. The Wireless Gateway contains the following subcomponents:

- **Wireless Gatekeeper**: A Java-based administration tool for the Wireless Gateway and wireless resources. It enables an administrator to configure wireless and wireless access protocol (WAP) gateways, add users and mobile devices, define and group wireless resources, and assign administrators to wireless resources.
- **Ardis Support**: Enables use of the advanced radio data information services protocol. Motient is the network provider.
- **Dataradio Support**: Enables use of the Dataradio network provider.
- **DataTAC Support**: Enables use of the DataTAC 5000 and DataTAC 6000 networks.
- **Dial Support**: Enables use of dial-capable digital and analog networks such as global system for mobile communication (GSM), advanced mobile phone service (AMPS), public switched telephone network (PSTN), and integrated service digital network (ISDN) networks. Native point-to-point protocol (PPP) is also supported over these networks.
- **IP LAN Support**: Enables use of a LAN-based network provider and all IP-based mobile devices, such as cellular digital packet data (CDPD), and general packet radio service (GPRS), among others. IP LAN Support works for wired environments and for any two nodes on a network. Using the two network nodes, you can create a secure tunnel, which functions as a virtual private network (VPN), between the nodes.

- **Mobitex Support**: Enables use of networks that contain the Mobitex protocol. These networks include BellSouth Wireless, CanTel, and Norcom Satellite.
- **Modacom Support**: Enables use of the Modacom network provider. This subcomponent is currently only available for AIX systems.
- **Motorola PMR**: Enables communication with one or more RNC-3000 network controllers in a Motorola private mobile radio (PMR) network.
- **Wireless Client**: The interface for starting and stopping communication with a Wireless Gateway. Wireless Client shields network-specific details inside the interface layer and allows IP applications on a mobile computer to run over a wireless network. For example, a radio network would not require any specialized communication protocols for use by a mobile device.

  Note: Wireless Client is not installed on an Everyplace Suite server, but rather on the client device.

MQSeries Everyplace for Multiplatforms

MQSeries Everyplace provides assured messaging capability between devices and any MQSeries family platform. It extends secure messaging to include dependable communications with mobile workers. It connects laptops, servers, PDAs, phones, and unattended devices, such as sensors, to MQSeries networks. This enables users to perform business functions, including e-mail access, stock purchase, or order placement through their mobile devices. MQSeries Everyplace consists of Java® and C components enabling solution developers to create an MQSeries Everyplace gateway and client on a variety of devices and platforms.

The native C client version of MQSeries Everyplace is not installed with the Everyplace Suite. This version can be downloaded from:

http://www.ibm.com/software/ts/mqseries/

WebSphere Edge Server Caching Proxy (Web Traffic Express)

The Caching Proxy retrieves Internet data for multiple browser clients. It also acts as a caching server and content filter, reducing the time needed to retrieve information from the Internet and filtering Internet data for multiple browser clients.

WebSphere Edge Server Load Balancer (Network Dispatcher)

The Load Balancer provides dynamic load balancing, scalability, and high availability for servers, boosting overall server performance by automatically finding the optimal server within a group of servers to handle each incoming request. It can be used with Web servers, e-mail servers, distributed parallel database queries, and other Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) applications. The Load Balancer contains the following subcomponents:

- **Content Based Routing**: Performs balancing in one of two ways:
  - For HTTP, Content Based Routing performs balancing based on the content of an HTTP client request. This method requires the Caching Proxy on the same machine.

  - For IMAP and POP3, Content Based Routing performs balancing on IMAP or POP3 mail servers. It selects the appropriate server based on the user ID and password provided by the client and does not require the Caching Proxy.
- **Dispatcher**: An IP packet-level load balancer. It provides high performance, low latency load balancing using weights and measurements that are dynamically set. It also provides built-in support for protocols such as HTTP, FTP, SSL, NNTP, IMAP, POP3, SMTP, and Telnet, but can be extended to support both TCP and UDP.
- **Interactive Session Support**: Balances the load on servers using a domain name server. This is done by communicating with server agents that are used to monitor the load and then altering the IP address returned to the client based on this load. Interactive Session Support can also provide the same server load information to the Dispatcher subcomponent.

Tivoli Personalized Services Manager

Tivoli Personalized Services Manager enables service providers to centrally manage subscribers and devices. Management includes enrolling subscribers and devices, providing self care and customer care, maintaining and billing subscriber accounts, and submitting jobs such as software distribution to devices, among others. Tivoli Personalized Services Manager contains the following subcomponents:

- **Device Manager Feature**: Helps service providers manage their subscribers' pervasive devices, including PDAs, subnotebooks, and other devices. Device Manager can identify, configure, and distribute software to any device that the Device Manager and the service provider support.
- **Enrollment Server**: Provides a subscriber and device enrollment engine for an ISP, including a customizable set of screens with unique banners, messages, billing plans, and payment options. The enrollment server distributes Tivoli Personalized Services Manager features to every subscriber, regardless of their ISP.
- **Database Integration**: Enables the installation program or the user to create either a DB2 or Oracle database. If you install Tivoli Personalized Services Manager, you must install this subcomponent.
- **Customer Care Support**: Enables representatives to open new or child accounts and deactivate or reactivate accounts. It also enables representatives to view and update personal information, service plans, payment methods, and e-mail settings.
- **Member Self Care Support**: Enables subscribers to modify the portal pages on their mobile devices and to modify some of their profile data, including address and telephone data, billing plan, payment method, and registering for premium Tivoli Personalized Services Manager content.
- **Active Session Table**: Tracks user and session information.
- **RADIUS**: Remote Authentication Dial-In User Service. Provides user authentication in compliance with the RADIUS authentication protocol. If the user and account are valid, the session is allowed to begin.

- **System Management**: Provides the ability to set up groups of subscribers, domains, and membership plans and deals. It also enables the user to access subscriber profiles.
- **Everyplace Suite Enabler**: Allows Tivoli Personalized Services Manager to manage its subscriber database in SecureWay Directory.

WebSphere Transcoding Publisher

The Transcoding Publisher adapts Web content based on destination device characteristics and network service level. You can enhance the performance of the Transcoding Publisher by also installing Edge Server Caching Proxy, which stores transcoded material. This removes the necessity of retranscoding Web pages each time they are retrieved.

Note: WebSphere Transcoding Publisher is intended to be deployed as a proxy in the Everyplace Suite domain. It is not intended to be used as a servlet or a JavaBean within the Everyplace Suite domain.

Everyplace Synchronization Manager

Everyplace Synchronization Manager enables handheld computing devices to link remotely to desktop applications. Mobile users can easily synchronize data with Microsoft Exchange, Lotus Notes or DB2 databases (synchronization with any ODBC compliant database, such as Oracle or Sybase, will be available at a future time). The mobile device can synchronize using modem, cellular phone, Internet, Wireless, Intranet, local area network (LAN) or wide area network (WAN). Mobile users can be authenticated through existing Microsoft Exchange or Lotus Notes user data or through a list of users held internally in Everyplace Synchronization Manager. Data can be encrypted for secure transmission. Mobile devices can be automatically backed up or restored and applications can be remotely installed on these devices. Everyplace Synchronization Manager contains the following subcomponents:

- **Everyplace Synchronization Manager Service**: Handles the request from the mobile device, manages security, and performs all the data transfers between the mobile and the enterprise data sources. Runs on a Unix server.
- **Everyplace Synchronization Manager Admin**: Enables the administrator to set up or modify the synchronizations performed by the Synchronization Manager service. Uses wizards or intuitive forms. Runs on a Unix server.
- **Exchange Connector**: Enables Synchronization Manager to synchronize with Microsoft Exchange Server. Runs on Windows NT4 or 2000.
- **Notes Connector**: Enables Synchronization Manager to synchronize with Lotus Notes. Runs on a Unix server.
- **Everyplace Synchronization Proxy**: Mobile devices may synchronize either directly (through dial-up or packet network) to the Synchronization Manager Service or indirectly with a serial cable to a desktop PC which then connects to the Synchronization Manager Service. The Everyplace Synchronization Proxy must be installed and running on the desktop PC to synchronize through cable. Runs on Windows.
- **Everyplace Synchronization Client**: Enables the mobile device to synchronize with enterprise data sources through the Synchronization Manager Service. Clients are packaged with the Windows install library.

Note: The Everyplace Synchronization Manager is not installed using the Everyplace Suite installation program. It is installed independently from CD number 11 of the Everyplace Suite product CDs. See the documentation in the `/esm/docs` directory of CD 11 for installation instructions.

Everyplace Administration Console
The Administration Console provides a centralized location from which to launch the corresponding administration console of any installed Everyplace Suite component.

Supporting components

The following components are included on the product CDs and are required as supporting components for the Everyplace Suite.

SecureWay Directory
A Lightweight Directory Access Protocol (LDAP) directory that runs as a stand-alone daemon. It is based on a client/server model that provides client access to an LDAP server. SecureWay Directory provides an easy way to maintain directory information in a central location for storage, updating, retrieval, and exchange.

IBM HTTP Server
An IBM enhanced Web server based on the Apache Web server. The IBM HTTP Server supports both the secure sockets layer (SSL) version 2 and SSL version 3 protocols for secure connections. It also includes a cache accelerator for improved performance when serving static Web pages.

IBM DB2 Universal Database Enterprise Edition
DB2 is a Web-ready relational database management system, supporting many levels of complexity in database environments.

WebSphere Application Server Standard Edition
Enables Web transactions and interactions with a robust deployment environment for e-business applications. It provides a portable, Java-based Web application deployment platform focused on supporting and executing servlets, JavaBeans, JavaServer Pages (JSP) files, and enterprise beans.

Java Development Kit (AIX only)
Contains the software and tools used to compile, debug, and run applets and applications written using the Java programming language.

The following supporting components are required but not included on the product CDs. Refer to the corresponding Web sites for downloading and installation instructions.

Java Development Kit (Solaris)
Contains the software and tools used to compile, debug, and run applets and applications written using the Java programming language. See the Web site *http://www.sun.com/software/solaris/java/archive.html* for downloading and installation instructions.

Netscape Communicator — Netscape Navigator
Displays Internet Web pages and other HTML-based documents. See the Web site *http://www.netscape.com/computing/download/index.html* for downloading and installation instructions.

Everyplace Suite installation models

The installation of Everyplace Suite components will be unique for each Everyplace Suite domain. The Everyplace Suite domain consists of a group of servers in an enterprise that are under central administrative control and are within the same protection space. Typically, there will be a number of servers within a local area network (LAN) that will have one or more Everyplace Suite components installed on them. For example, there may be a cluster of four servers running WebSphere Transcoding Publisher and a cluster of eight servers running Everyplace Wireless Gateway.

A Lightweight Directory Access Protocol (LDAP) implementation is required for running the Everyplace Suite components. The Everyplace Suite components use the SecureWay Directory as a common information platform to maintain a seamless integration within the Everyplace Suite domain. The Everyplace Suite relies on a specific directory schema that is only implemented in SecureWay Directory Version 3.2. Therefore, SecureWay Directory can be seen as a prerequisite for all the Everyplace Suite components. It is strongly recommended that SecureWay Directory be deployed within any Everyplace Suite domain.

Note: Be sure to consult an IBM technical representative before attempting to install or use the Everyplace Suite with an LDAP implementation other than SecureWay Directory.

For more detailed information about network planning and design issues see the WebSphere Everyplace Suite Redbooks. They can be found online at:

http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245995.pdf and
http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245996.pdf

See *http://www.redbooks.ibm.com* for more information about obtaining hard copies of these and other IBM Redbooks.

Figure 2 and Figure 3 represent two possible implementations of the Everyplace Suite. These diagrams are for illustrative purposes only. It is unlikely that any Everyplace Suite installation will exactly resemble these examples. Even though each server cluster is represented by only one box in the following diagrams, a server cluster may contain one or more servers performing a particular service. The Edge Server Load Balancer can be deployed to distribute traffic across any cluster of servers performing the same service (authentication or transcoding for example). For every cluster of servers, a corresponding Load Balancer is implied but not shown in the following diagram.

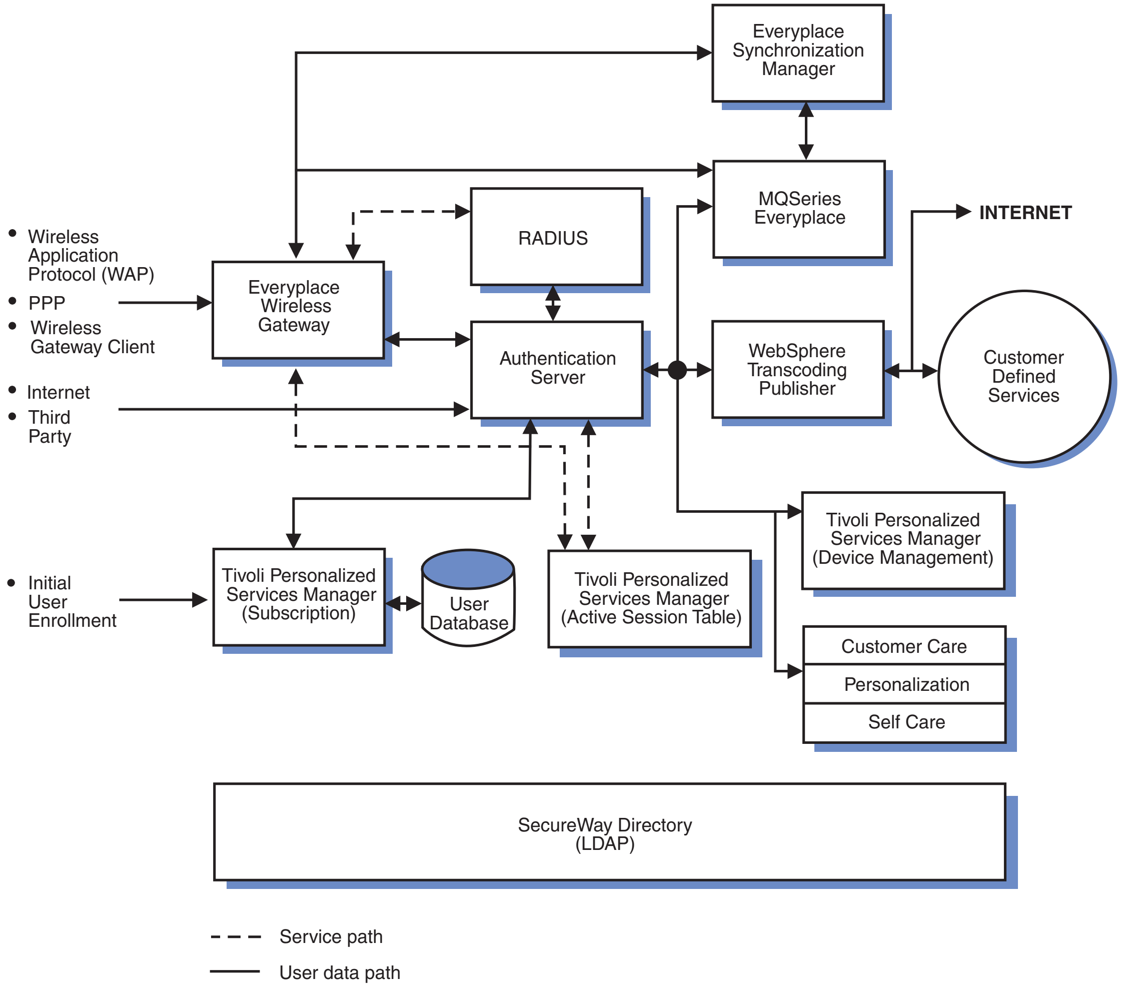

Everyplace Synchronization Manager
MQSeries Everyplace
INTERNET
RADIUS
Wireless Application Protocol (WAP)
PPP
Wireless Gateway Client
Everyplace Wireless Gateway
Authentication Server
WebSphere Transcoding Publisher
Customer Defined Services
Internet
Third Party
Tivoli Personalized Services Manager (Device Management)
Initial User Enrollment
Tivoli Personalized Services Manager (Subscription)
User Database
Tivoli Personalized Services Manager (Active Session Table)
Customer Care
Personalization
Self Care
SecureWay Directory (LDAP)
Service path
User data path

Figure 2. Complete Everyplace Suite installation

Complete Everyplace Suite installation

Figure 2 represents an Everyplace Suite domain where all key components deployed. This deployment could be typical for an enterprise that is looking for a complete solution for pervasive device support along with traditional wired internet services. See “Content provider — start-up portal company” on page 3 for a description of this kind of enterprise. One possible example of how communications flow within this Everyplace Suite domain could be:

- A user wishes to access personal e-mail using a cellular phone.
- After the connection is made, the Wireless Gateway receives the request.

- The Edge Server Load Balancer dispatches the request to the appropriate Authentication Server.
- The Authentication Server performs the authentication which allows the user access.
- The Edge Server Load Balancer dispatches the request to the appropriate WebSphere Transcoding Publisher server.
- The Transcoding Publisher forwards the request to the server handling the back end customer defined services (possibly the WebSphere Application Server).
- The Application Server returns the requested e-mail data to the Transcoding Publisher.
- The Transcoding Publisher reformats the e-mail data according to the cell phone's display specifications and returns it to the Wireless Gateway.
- The Wireless Gateway forwards the reformatted e-mail data to the cell phone user.

The Everyplace Suite components use the SecureWay Directory as a common information platform to maintain a seamless integration within the Everyplace Suite domain.

Limited Everyplace Suite installation with Wireless Gateway

Figure 3 represents a limited installation of the Everyplace Suite, centered around Wireless Gateway. This kind of installation could be typical for an enterprise that already has device and user support in place, including subscriber management. See "Enterprise customer — package delivery company" on page 4 for a description of this kind of enterprise.

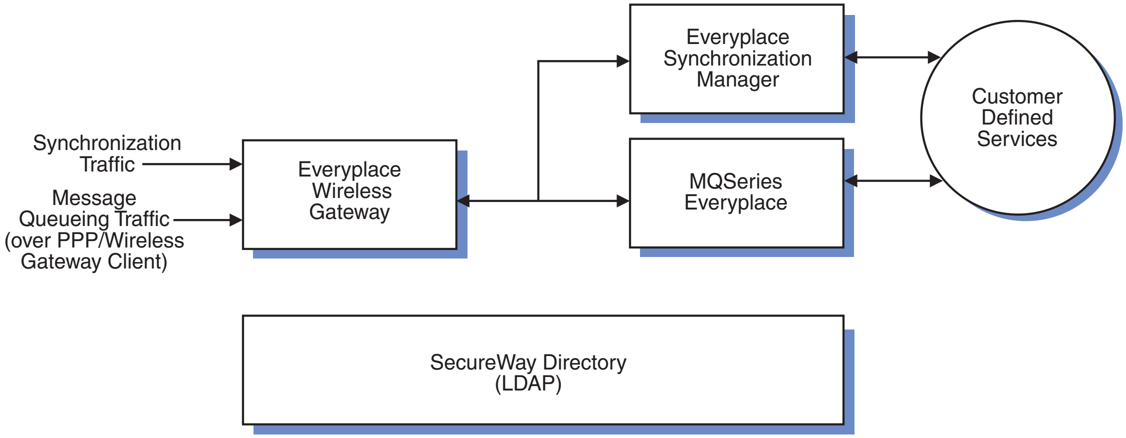

Synchronization Traffic
Message Queueing Traffic (over PPP/Wireless Gateway Client)
Everyplace Wireless Gateway
Everyplace Synchronization Manager
MQSeries Everyplace
Customer Defined Services
SecureWay Directory (LDAP)

Figure 3. Limited Everyplace Suite installation with Wireless Gateway

Pre-installation planning

Be sure to read this section carefully before installing the Everyplace Suite. This section contains information about the installation and configuration of SecureWay Directory and configuration of the Authentication Server.

Installation planning for SecureWay Directory

The Everyplace Suite uses SecureWay Directory to access and manage information in a shared directory structure. SecureWay Directory supports the Lightweight Directory Access Protocol (LDAP) Version 3. This protocol provides access to the X.500 directory over a TCP or SSL connection. LDAP lets you store information in a directory service and query it in a database fashion. Any LDAP-enabled application can store information once, such as user authentication information, and other applications using the LDAP server will recognize it.

During installation, you will be given three options for storing and sharing installation and configuration information across the Everyplace Suite domain. Each option you select will require you to provide additional information.

1. **Install SecureWay Directory**: Installs SecureWay Directory on the local server. This option requires the following information:
   - **Directory suffix**

     The directory suffix specifies a distinguished name for the root of a directory. The directory suffix is the highest-level entry stored in the directory by a server.
   - **Object type**

     The object type specifies a set of mandatory and optional attributes for a SecureWay Directory database entry. The object type also defines the location of the entry in the database.
   - **Database name**

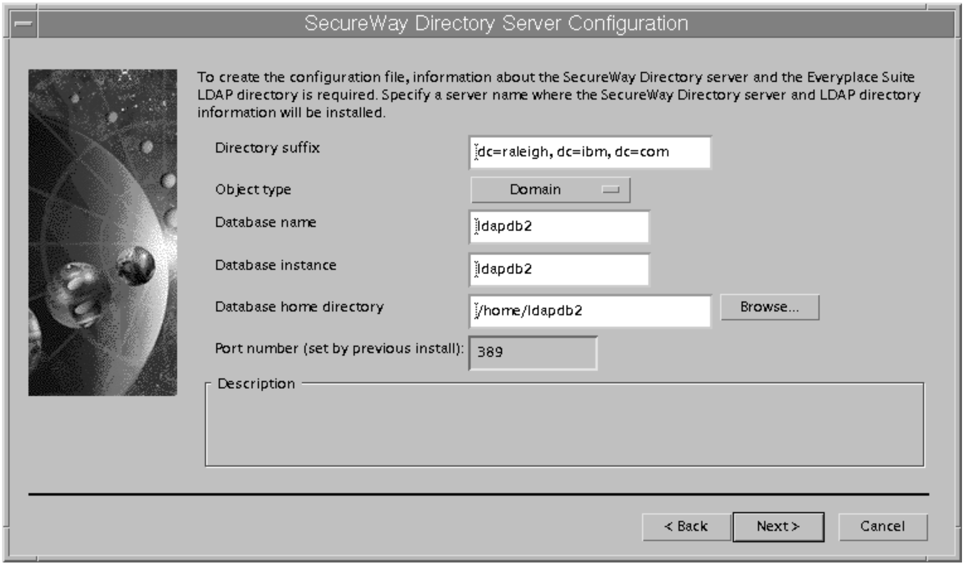
     The database name specifies the name of the SecureWay Directory database.
   - **Database instance**

     The database instance specifies the database manager environment where you can catalog databases and set configuration parameters for the SecureWay Directory database.
   - **Database home directory**

     The database home directory specifies the file path for the directory where the SecureWay Directory database is located.
   - **Port number**

     The port number specifies the network port where the SecureWay Directory database is located.

Figure 4 on page 25 shows the installation program screen for the **Install SecureWay Directory** option.


SecureWay Directory Server Configuration

To create the configuration file, information about the SecureWay Directory server and the Everyplace Suite LDAP directory is required. Specify a server name where the SecureWay Directory server and LDAP directory information will be installed.

Directory suffix: dc=raleigh, dc=ibm, dc=com

Object type: Domain

Database name: ldapdb2

Database instance: ldapdb2

Database home directory: /home/ldapdb2

Port number (set by previous install): 389

Description

Figure 4. SecureWay Directory configuration parameter panel

2. **Retrieve Everyplace Suite information from a SecureWay Directory server**: Instructs the installation program to retrieve the information from the existing SecureWay Directory (LDAP) server in the Everyplace Suite domain. This option requires the following information:
   - Server name
   - User ID
   - Password
   - Port
3. **Retrieve existing Everyplace Suite information from a file**: This will allow the installation to be performed without using SecureWay Directory. Installation information will be retrieved from the file system or diskette media at a later time. Use this option for:
   - Installation on a server isolated from the existing SecureWay Directory domain.
   - Installation of Everyplace Suite components prior to the installation of SecureWay Directory.

   If you select this option, SecureWay Directory will appear on the component selection panel of the installation wizard. You will then have the option of installing SecureWay Directory on any machine in the Everyplace Suite domain.

   After selecting this option, you will be prompted to input the file name for the Everyplace Suite LDAP Data Interchange Format (LDIF) file. This file is used to represent SecureWay Directory entries in text form. This file will serve as a temporary holder for installation and configuration information that will be imported into the SecureWay Directory at a later time. The default filename and path is `/tmp/everyplace/everyplace`. Use the default file or enter the name and path of the file you wish to use.

Notes:

a. It is strongly recommended that the same LDIF file be used on subsequent installations within the Everyplace Suite domain.

b. If you are installing Tivoli Personalized Services Manager using the LDIF file, you will not be able to install using a remote DB2 database server, since SecureWay Directory is not available for the Everyplace Suite installation program. Therefore, do not use this option unless you are installing Tivoli Personalized Services Manager on a local DB2 database server.

Importing the LDIF file into SecureWay Directory

If any Everyplace Suite components were installed prior to the installation of SecureWay Directory (using the **Retrieve existing Everyplace Suite information from a file** option), then the installation and configuration information must be imported into SecureWay Directory after it is installed and running in the domain. This import will be done automatically by the installation wizard when SecureWay Directory is installed.

If there is a need to do this import manually, use the `ldif2db` utility. The following command must be run on the SecureWay Directory server:

```
ldif2db -i file_name
```

where `file_name` is the full path of the LDIF file that was specified during installation.

Backing up the Everyplace Suite Directory for SecureWay Directory refresh

If you want to refresh SecureWay Directory and back up the existing Everyplace Suite LDAP Directory that was created during the installation, you can do this using the following command:

```
db2ldif -o backup_file_name -s suffix_name
```

where `backup_file_name` is the name of the backup file being created, and `suffix_name` is the directory suffix is the distinguished name provided during SecureWay Directory installation. This will store the directory information in an LDIF file.

After SecureWay Directory has been refreshed, be sure to import the information from the LDIF file back into SecureWay Directory as discussed in “Importing the LDIF file into SecureWay Directory”.

Authentication Server configuration parameters

If you install the Authentication Server in transparent proxy mode, you must set the server address and port number of the Edge Server - Caching Proxy in the Netscape Navigator HTTP proxy setting panel before attempting to open the Caching Proxy from the Everyplace Administration Console.

If you install the Authentication Server, the Everyplace Suite installation program will prompt you for configuration information. Some of this information will be common across all instances of the Authentication Server within the Everyplace Suite domain. Other information will be unique to each instance of the Authentication Server. After installation, you can reassign these configuration parameters from common to unique or from unique to common. See Table 7 on page 77 for a description of these Authentication Server configuration entries.

You must provide the following common information:

- Primary Active Session Table (AST) server name
- Secondary Active Session Table (AST) server name
- Maximum RADIUS retries
- RADIUS shared secret
- Maximum RADIUS retry timeout (milliseconds)
- Maximum session age (minutes)
- Default retry after delay (seconds)

The Authentication Server can be configured in one of two modes: as an authentication proxy that intercepts all requests made to resources within the Everyplace Suite, or as a transparent authentication proxy that allows access to content provided by third-party content servers while taking advantage of Everyplace Suite authentication and transcoding. This can be done by specifying the **Authentication Server role** in the unique Authentication Server panel during installation.

Sample configuration files for the authentication proxy and transparent authentication proxy modes (ibmproxy_ap.conf.sample and ibmproxy_tp.conf.sample, respectively) are located in `src/wes_auth/samples/`. The file entries that pertain to the Everyplace Suite are designated by 'WES' in the associated comments.

You must provide the following information for each server installing the Authentication Server. This information will be unique to each server.

- Authentication Server role
- Primary RADIUS server name
- Secondary RADIUS server name
- Maximum session cache size
- Active Session Table (AST) daemon cleanup interval

You can modify Authentication Server configuration parameters after installation using the Directory Management Tool. For more information about the Authentication Server configuration and using the Directory Management Tool, see "Configuring Authentication Server information in SecureWay Directory" on page 73.

Note: When configuring the Authentication Server to deploy WebSphere Transcoding Publisher in your Everyplace Suite environment, there may be performance penalties when routing content through Transcoding Publisher. Be careful to only use transcoding when it is needed.

Pre-installation requirements for Tivoli Personalized Services Manager

Software prerequisite information including JDK versions for installing Tivoli Personalized Services Manager is located on CD number 8 in /tsm/aix/oracle/TPSM-Overview.htm. The /aix/oracle/ portion of the path can be changed to /aix/db2/, /sun/oracle/ or /sun/db2.

Be sure to review the following items before installing Tivoli Personalized Services Manager:

- If you are installing Tivoli Personalized Services Manager on AIX systems with a DB2 database, the IBM AIX Developer Kit, Java 2 Technology Edition, Version 1.2.2 will be automatically installed. See "Applying the AIX PTFs for Java Version 1.2.2" on page 34 for information on installing the AIX PTF files required to run Java Version 1.2.2.
- If you are using DB2 database, you must install a C compiler prior to the installation of Tivoli Personalized Services Manager.

  Note: It is very important that this compiler be installed and the license be activated before installing Tivoli Personalized Services Manager.

  For AIX:

  Install the IBM C for AIX Compiler Version 5.0 or higher. This product can be purchased from the Web site: *http://www2.software.ibm.com/prodindex/prodindex.nsf/H2BPages/DMUR-4CPLLN?opendocument*

  For Solaris:

  Install the Sun WorkShop Version 5.0 C Compiler. This product can be purchased from the Web site: *http://www.sun.com/990209/workshop/*
- If you are installing Tivoli Personalized Services Manager using an LDIF file (without an active SecureWay Directory), you will not be able to install using a remote DB2 database server, since SecureWay Directory is not available for the Everyplace Suite installation program. Therefore, do not use this option unless you are installing Tivoli Personalized Services Manager on a local DB2 database server.

Special file system requirements for Tivoli Personalized Services Manager

If you are installing Tivoli Personalized Services Manager on AIX systems, you will need to create the /var/adm/logs file system. You can do this with the following command:

```
crfs -v jfs -g'rootvg' -asize='49152'  -m'/var/adm/logs' -Ayes
mount /var/adm/logs
```

If you are installing the Oracle database, you will need to create the Oracle volume group oravg on hdisk1 as follows:

```
mkvg -f -y'oravg' -s'8' hdisk1
```

Note: -s8 is the physical partition size, you must use 1, 2, 4, 8, 16, or 32 depending on the size of the drive.

Now you can create the file system /db on the oravg volume group with the command:

```
crfs -v jfs -g'oravg' -asize=' 4128768' -m'/db' -Ayes
mount /db
```

Pre-installation requirement for installing Tivoli Personalized Services Manager or Everyplace Wireless Gateway on a remote DB2 server

If you install Tivoli Personalized Services Manager or Everyplace Wireless Gateway using a remote DB2 server, you must determine whether the db2inst1 user ID exists on the local machine before running the Everyplace Suite installation program.

For AIX:

- Enter SMIT to check the user ID.

For Solaris:

- Enter admintool to check the user ID.

If the db2inst1 user ID exists on the local machine, but the /home/db2inst1 directory does NOT exist on the local machine, you must erase the db2inst1 user ID, using SMIT for AIX or admintool for Solaris.

Swing Libraries pre-installation requirement for the Everyplace Administration Console

If you install the Everyplace Administration Console, be sure that the Swing Libraries for Java Version 1.1.8 are installed on the target system in the wesconsole.sh file. The following default paths are prepared for the Swing Libraries in the wesconsole.sh file:

- /usr/java1.1/lib
- /Swing-1.1.1
- /opt/Swing-1.1.1
- /usr/local/Swing-1.1.1

If you install the Swing Libraries in other directories, you must set the directory to the SWING_HOME environment variable in the wesconsole.sh file, or the following error message will appear when you attempt to use the Everyplace Administration Console: ″Swing 1.1.1 needed for Java 1.1.8 is not found.″

System requirements

Many Everyplace Suite components have specific system requirements and prerequisites that need to be understood prior to installation. Component prerequisites and automatic installation of components are discussed in this section. The hardware and software requirements and prerequisites for the Everyplace Suite components are listed in Table 2 on page 30.

Component specific requirements and prerequisites

Before installing any of the Everyplace Suite components, it is important to review and understand which installation prerequisites are required for the components you intend to install. In some instances, an older version of a prerequisite may already be installed. The installation program will detect this and ask if you want to upgrade to the recommended version. Not upgrading to the recommended version can result in unpredictable performance.

There may also be instances where downgrading to a previous version (or refreshing a current version) of the prerequisite software will be recommended by the installation program. This will ensure reliable integration of the Everyplace Suite components.

The following table displays the system requirements and prerequisites for each component. For additional prerequisite information, see the specific component documentation listed in "Where to find Everyplace Suite component documentation" on page 4.

Table 2. Hardware and software requirements and prerequisites

Everyplace Suite Component	Requirements and prerequisites
Everyplace Authentication Server	• Edge Server Caching Proxy (for each instance) • Tivoli Personalized Services Manager (within the domain)
Everyplace Wireless Gateway	• DB2 UDB Enterprise Edition 7.1 or Oracle8i database version 8.1.5 • MERANT Data Direct Connect ODBC 3.6.0 if using Oracle8i • IBM GSKit SSL Library • IBM X.25 co-processor card if you are connecting to any of the following packet radio networks: – ARDIS-X.25 – DataTAC-5000 – Mobitex – Modacom-SCR – MCA-bus RS/6000® machines: IBM X.25 Interface Co-processor/2 card – ISA-bus RS/6000 machines: IBM X.25 Interface Co-Processor/1 card **Note:** If you connect to ARDIS, DataTAC-SCR, or Mobitex by IP instead of X.25, you do not need an X.25 Interface co-processor card. • Asynchronous adapter and modem if you connect to a circuit-switched cellular network using RS232 communication (for example PSTN, GSM, or AMPS) • LAN adapter for connection to the IP network and to the RNG of a DataTAC-TCP, Mobitex-TCP, or RNC3000 radio network • AIXLinkX.25 1.1.5 (if using X.25 connectivity)

Table 2. Hardware and software requirements and prerequisites (continued)

Everyplace Suite Component	Requirements and prerequisites
Edge Server Load Balancer	• Edge Server Caching Proxy — if installing Content Based Routing (CBR) subcomponent
Edge Server Caching Proxy	• Edge Server Load Balancer — administration package and device driver • IBM GSKit SSL Library • 4GB Ultra SCSI disk or 16GB SSA disk
Tivoli Personalized Services Manager	• WebSphere Application Server, Standard Edition, 3.5 • DB2 UDB 7.1 or Oracle8i database version 8.1.5 • 8.1.6.0.1 JDBC driver for use with JDK 1.2.x (if using Oracle) • IBM C for AIX Compiler Version 5.0 (for AIX) • Sun WorkShop Version 5.0 C Compiler (for Solaris) • DBI/DB Perl module to Perl 5 • IBM HTTP Server 1.3.12 • 2GB RAM, 2GB hard disk space (separate volume ID is recommended)
Everyplace Synchronization Manager	• DB2 Client 7.1 • Lotus Notes/Domino 5 server (on local machine) if synchronizing with Lotus Notes (UNIX server) • Microsoft Exchange Server 5.5 (Windows NT 4 or Windows 2000 server) if synchronizing with Microsoft Exchange
Everyplace Administration Console	• Netscape Navigator 4.08, or • Netscape Communicator 4.5 or higher • Swing Libraries for Java 1.1.8

Note: A Lightweight Directory Access Protocol (LDAP) implementation is required for running the Everyplace Suite components. The Everyplace Suite relies on a specific directory schema that is only implemented in SecureWay Directory Version 3.2. Therefore, SecureWay Directory can be seen as a prerequisite for all the Everyplace Suite components. It is strongly recommended that SecureWay Directory be installed within the Everyplace Suite domain. Be sure to consult an IBM technical representative before attempting to install or use the Everyplace Suite with an LDAP implementation other than SecureWay Directory.

Automatic prerequisite installation

There are instances when supporting software will automatically be installed, depending on which components and system configuration options you have selected in the installation program. Installation of the following components will automatically result in the installation of the corresponding components:

- **SecureWay Directory**: When this component is installed, IBM DB2 and the IBM HTTP Server are automatically installed on the server.

- **Tivoli Personalized Services Manager**: When this component is installed, WebSphere Application Server and the IBM HTTP Server are automatically installed.
- **Everyplace Authentication Server**: When this component is installed, the Caching Proxy is automatically installed.
- **Edge Server Caching Proxy**: When this component is installed, the Edge Server Load Balancer administration package and device driver are automatically installed.

Hardware and software requirements

The Everyplace Suite only runs on AIX version 4.3.3 and Solaris Version 7 platforms.

Everyplace Suite components must be installed on an AIX or Solaris X-Window workstation. Installation from a remote X-Window session or emulator is not supported and may cause problems.

The Everyplace Suite also requires that the Sun Microsystems Java® Development Kit (JDK) Version 1.1.8 be installed on all servers where Everyplace Suite components will be installed.

- On AIX systems, the JDK is included on the Everyplace Suite CD and will automatically be installed.
- On Solaris systems, the JDK will need to be installed separately. See the Web site *http://www.sun.com/software/solaris/java/archive.html* for downloading and installation instructions.

If you are installing the Everyplace Suite in an AIX environment, you should ensure that AIX Version 4.3.3 Modification Level 10 is installed for all AIX software packages. The following Everyplace Suite components require specific AIX PTFs or filesets which are available in AIX Version 4.3.3 Modification Level 10:

- SecureWay Directory
- Tivoli Personalized Services Manager
- WebSphere Transcoding Publisher

If this level of modification has not been applied to your AIX system, and you intend to use any of the above components, you must ensure that the AIX PTFs or filesets noted in the following sections are applied before installing the Everyplace Suite.

Applying the AIX program temporary fixes (PTFs)

Before installing the Everyplace Suite on AIX systems you must apply the following PTFs to your system using SMIT. Be sure to install the listed version numbers or higher. Base level filesets corresponding to those listed below are required to be installed before the PTFs are installed. They can be found on the AIX 4.3.3 installation media.

- X11.adt.lib 4.3.3.10
- bos.adt.include 4.3.3.10
- X11.adt.motif 4.3.3.10
- bos.adt.prof 4.3.3.10

Applying the AIX PTFs for SecureWay Directory

If you are installing Everyplace Authentication Server, Tivoli Personalized Services Manager or SecureWay Directory, the SecureWay Directory client will be installed. This client requires the following PTFs installed on the machine:

- X11.Dt.lib 4.3.3.10
- X11.Dt.rte 4.3.3.10
- X11.base.lib 4.3.3.10
- X11.base.rte 4.3.3.10
- X11.compat.lib.X11R5 4.3.3.10
- X11.motif.lib 4.3.3.10
- X11.motif.mwm 4.3.3.10
- bos.rte.libpthreads 4.3.3.10

In addition, SecureWay Directory also needs the following PTFs installed:

- bos.adt.include 4.3.3.10
- bos.adt.prof 4.3.3.10
- bos.adt.samples 4.3.3.12
- bos.diag.com 4.3.3.13
- bos.diag.rte 4.3.3.13
- bos.net.ipsec.keymgt 4.3.3.10
- bos.net.nfs.client 4.3.3.10
- bos.net.tcp.client 4.3.3.14
- bos.net.tcp.server 4.3.3.14
- bos.rte.aio 4.3.3.11
- bos.rte.control 4.3.3.10
- bos.rte.libc 4.3.3.13
- bos.rte.net 4.3.3.1
- bos.rte.tty 4.3.3.10
- bos.sysmgt.serv_aid 4.3.3.13
- bos.sysmgt.trace 4.3.3.11
- bos.up 4.3.3.16 (or bos.mp 4.3.3.16)
- devices.chrp.base.rte 4.3.3.12
- devices.common.base.diag 4.3.3.10
- devices.ssa.disk.rte 4.3.3.10
- perfagent.tools 2.2.33.10
- bos.diag.util 4.3.3.11
- X11.adt.motif 4.3.3.12
- X11.adt.lib 4.3.3.10
- bos.rte.methods 4.3.3.13

Applying the AIX PTFs for Java Version 1.2.2

If you are installing Tivoli Personalized Services Manager or WebSphere Transcoding Publisher on AIX you will be prompted during installation to install the IBM AIX Developer Kit, Java 2 Technology Edition, Version 1.2.2. The following AIX PTFs are required to run Java Version 1.2.2. Be sure to install the listed version numbers or higher.

- bos.adt.include 4.3.3.1
- bos.net.tcp.client 4.3.3.3
- bos.sysmgt.serv_aid 4.3.3.2
- X11.base.lib 4.3.3.2
- X11.adt.motif 4.3.3.1
- X11.base.rte 4.3.3.2
- X11.Dt.rte 4.3.3.3
- X11.motif.mwm 4.3.3.1
- X11.motif.lib 4.3.3.2
- X11.compat.lib.X11R5 4.3.3.2
- bos.rte.libpthreads 4.3.3.3
- bos.adt.prof 4.3.3.3
- X11.Dt.lib 4.3.3.2

And one of the following depending on whether your system is a uniprocessor or multiprocessor machine:

- bos.up 4.3.3.3 (uniprocessor)
- bos.mp 4.3.3.3 (multiprocessor)

The above PTFs are for all locales and are not on the AIX 4.3.3 installation media. They can be obtained from IBM if they are not already on your AIX system. The easiest way to do the upgrade is by using the FixDist tool, available from: *http://service.software.ibm.com/cgi-bin/support/rs6000.support/downloads*

The Java 2 Technology Edition, Version 1.2.2, requires the following AIX base level filesets for specific locales or for double-byte character set (DBCS) locales. If they are not already installed, they can be found on the AIX 4.3.3 installation media.

- bos.loc.com.utf 4.3.3.0
- bos.iconv.Vi_VN 4.3.0.0
- bos.loc.iso.zh_TW 4.3.3.0

In addition, Java Version 1.2.2 requires that the following PTFs be applied to your AIX system for specific locales or DBCS locales, with the base level filesets listed above already installed:

- bos.loc.iso.th_TH 4.3.3.1
- bos.loc.iso.Vi_VN 4.3.3.1
- bos.loc.iso.zh_TW 4.3.3.1

Applying AIX PTFs for Oracle Database

If you are installing Tivoli Personalized Services Manager with Oracle Database, you must apply the following AIX filesets. They can be found on the AIX V4.3.3 installation media:

- bos.adt.*
- xlC.rte.*
- X11.adt.*
- X11.base.*
- perl.rte.*
- bos.compat.termcap
- bos.sysmgt.trace
- devices.ssa.disk.rte
- Update all AIX components to AIX 4.3.3 Maintenance Level 02(IY06844) or higher

You also need to install the following filesets to use Java 2:

- Java_dev2.rte.* (Java Runtime Environment)
- Java_dev2.ext.plugin (Java PlugIn for Netscape)
- Update all Java filesets to PTF 07 (IY12075)

Note: In the above filesets, the * denotes all the filesets that begin with the preceding text. For example, `bos.adt.*` refers to all of the filesets starting with `bos.adt`.

Applying AIX PTFs for WebSphere Transcoding Publisher

If you are installing WebSphere Transcoding Publisher on AIX systems, you will need to install the following PTF:

- `bos.rte 4.3.3.10`

In addition, if you are using AIX with a double-byte language, you will need to install the following fileset:

- `X11.fnt.ucs.ttf`

Disk space requirements

Table 3 shows the minimum disk space requirements for the Everyplace Suite components and key directories. The amount of disk space needed will depend on which components are installed. The following disk space requirements needed for component installation are for the `/usr` directory on AIX systems and the `/opt` directory for Solaris systems.

Table 3. Everyplace Suite disk space requirements

Everyplace Suite component	Minimum disk space requirement
Everyplace Authentication Server	20MB
Wireless Gateway	Gateway 250MB Gatekeeper 50MB
MQSeries Everyplace	11MB

Table 3. Everyplace Suite disk space requirements (continued)

Edge Server Load Balancer	60MB
Edge Server Caching Proxy	100MB
Tivoli Personalized Services Manager	Subscription Manager 75MB Device Manager 45MB
WebSphere Transcoding Publisher	80MB
IBM DB2 Universal Database	Server 350MB Client 150MB
WebSphere Application Server	100MB
IBM HTTP Server	40MB
SecureWay Directory	100MB
Everyplace Synchronization Manager	190MB
Everyplace Administration Console	1MB
Local Directory	
/ (AIX only)	40MB
/ (Solaris only)	140MB
/usr (AIX only)	Total MB for all components being installed
/opt (AIX only)	100MB If installing Edge Server Caching Proxy
/opt (Solaris only)	Total MB for all components being installed
/db	1500MB
/dbfiles (Solaris Tivoli Personalized Services Manager for Oracle only)	1000MB
/home (AIX only)	100MB
/tmp	100MB
/var	50MB
/var/adm/logs (Tivoli only)	30MB

Supported pervasive devices and network types

The Everyplace Suite components support the devices and network types listed in Table 4. Except where noted, the Everyplace Suite includes wireless client code on the specified platforms for full security, connectivity and optimization functions.

Table 4. Supported devices and network types

Everyplace Suite Component	Supported Platforms and Network Types
Everyplace Wireless Gateway	• Microsoft® Windows® CE 2.0 and 2.11 • Windows CE (PPC)[1] • Windows CE V3.0[1] • Microsoft Windows 95 and 98 • Microsoft Windows NT • Microsoft Windows 2000 • Palm OS • EPOC[1] • Pre-EPOC WAP phones • QNX/Neutrino • WAP phones (1.1 and 1.2)[2]
WebSphere Transcoding Publisher	• Windows CE • Microsoft Windows 95 • Microsoft Windows 98 • Microsoft Windows NT • Microsoft Windows 2000 • Palm OS • EPOC • Pre-EPOC WAP phones • i-mode
Tivoli Personalized Services Manager (Device Manager)	• Windows CE • Palm OS • QNX/Neutrino
MQSeries Everyplace	• Windows CE • Microsoft Windows 95 • Microsoft Windows 98 • Microsoft Windows NT • Microsoft Windows 2000 • Palm OS • EPOC • Any device running Java JVM 1.1 or later

Table 4. Supported devices and network types (continued)

Everyplace Suite Component	Supported Platforms and Network Types
Everyplace Synchronization Manager	• Palm OS • Windows CE • Pocket PC • EPOC (will be supported at a future time)

Note: 1. These devices are supported as WAP-capable clients (with no IBM code needed on the device), or as a standard PPP-capable client. Full connectivity is supported but with somewhat less optimization, and security and no data encryption.

Note: 2. These devices are supported as WAP-capable clients only (with no IBM code needed on the device).

Where to find additional planning information

Network planning and design issues are discussed in detail in the following WebSphere Everyplace Suite Redbooks:

- *An Introduction to WebSphere Everyplace Suite Version 1.1* discusses the services and functions the Everyplace Suite provides, as well as the administrative tasks involved with the Everyplace Suite.
- *Implementing WebSphere Everyplace Suite Version 1.1* discusses performance expectations and planning, as well as security and authentication issues.

They are available online at *http://www.redbooks.ibm.com*

Migrating existing products into the Everyplace Suite environment

In some instances, an older version of an Everyplace Suite component or prerequisite will already be installed. The installation wizard will detect this and ask if you want to upgrade to the recommended version. Not upgrading to the recommended version can result in unpredictable performance.

There may also be instances where downgrading to a previous version (or refreshing a current version) of the component or prerequisite being installed will be recommended by the wizard. This will ensure reliable integration of the Everyplace Suite components.

It is strongly recommended that SecureWay Directory be installed within the Everyplace Suite domain.

Chapter 4. Installing the Everyplace Suite

This chapter provides information and instructions needed to install and configure the Everyplace Suite.

Pre-installation checklist

It is important to review the following information before beginning the installation process to avoid any problems or errors during the installation.

__ 1. Before installing any Everyplace Suite components, review “Hardware and software requirements” on page 32.

__ 2. Be sure to exit all running programs prior to starting Everyplace Suite installation.

__ 3. On Solaris systems, JDK 1.1.8 must be installed separately. See the Web site *http://www.sun.com/software/solaris/java/archive.html* for downloading and installation instructions.

__ 4. Either Netscape Navigator 4.08 or higher or Netscape Communicator 4.5 or higher needs to be installed to run the Everyplace Administration Console.

__ 5. Be prepared to provide a user ID, group, and password for the following Everyplace Suite components at the time of installation:

- SecureWay Directory
- Edge Server Caching Proxy
- Tivoli Personalized Services Manager
- Tivoli Personalized Services Manager — Device Management Server
- IBM HTTP Server
- IBM DB2 UDB™
- WebSphere Application Server
- WebSphere Transcoding Publisher
- Everyplace Administration Console

Notes:

a. You may use only lower case letters (a-z) or numbers (0-9) for the user ID, group, and password.

b. WebSphere Transcoding Publisher only requires a user ID and password.

__ 6. Install the appropriate pre-requisites. See “Component specific requirements and prerequisites” on page 30.

__ 7. Ensure the Swing Libraries are installed on the Everyplace Administration Console. See “Swing Libraries pre-installation requirement for the Everyplace Administration Console” on page 29.

__ 8. If you are installing Tivoli Personalized Services Manager, be sure to review “Special file system requirements for Tivoli Personalized Services Manager” on page 28 and “Pre-installation requirements for Tivoli Personalized Services Manager” on page 28 before installation.

__ 9. If you are using the Oracle Database, be sure to install the Tivoli Oracle integration package and the Oracle8i before installing the Everyplace Suite. See “Installation of Oracle Database software” on page 43 for more information. If you are installing the RADIUS subcomponent of Tivoli Personalized Services Manager be sure to install the Oracle client from the Oracle8i installation CD prior to installing Tivoli Personalized Services Manager. See “Installing the Oracle client on the RADIUS server” on page 49.

__ 10. The Everyplace Synchronization Manager is not installed using the Everyplace Suite installation program. It is installed independently from CD number 11 of the Everyplace Suite product CDs. See the documentation in the `/esm/docs` directory of CD number 11 for installation instructions and requirements.

__ 11. The Everyplace Suite relies on a specific directory schema that is only implemented in SecureWay Directory Version 3.2. Therefore, SecureWay Directory is a prerequisite for all the Everyplace Suite components. It is strongly recommended that SecureWay Directory be deployed within any Everyplace Suite domain.

Building the installation image

If you already have the Everyplace Suite installation CDs you can ignore this section and go to “Installation CD directory structure”. The Everyplace Suite is made up of eleven large files that are downloaded from the Internet. These files correspond to the eleven CDs or CD images used to install the Everyplace Suite. The files are in a compressed tar format (with a `.taz` extension) and have to be extracted. Be sure that there is at least 5GB of local disk space on the target machine that you want to unbundle the install CD images. To build the install image, follow these steps:

1. Create the directory for each CD image to be extracted into by entering:

   ```
   mkdir /cd1
   mkdir /cd2
   mkdir /cd3
   ```

   and so on for all the CD images. Download the CD images into the corresponding directories.
2. Uncompress each compressed CD image by entering the command:

   ```
   gzip -dvf cdXimage.taz
   ```

   where `cdXimage.taz` is the name of the downloaded CD image and X is the CD image number corresponding to each of the eleven product CDs. Be sure to maintain the numeric order of the file names from the compressed files to the eleven CD install images, creating ordered file names such as: `cd1,cd2,cd3...cd10`.
3. Extract the files from each CD image. For example, for CD number 1, enter:

   ```
   tar -hxvf cd1image.taz
   ```
4. At this point you can create the eleven CDs that will be used for installation or install directly from the extracted install images.

Installation CD directory structure

The Everyplace Suite (Version 1 Release 1 Modification 3) will provide the existing Everyplace Suite Version 1.1.2 customers with a set of refreshed Everyplace Suite components and some corrective service defect fixes. The Everyplace Suite Version 1.1.3 installation program will also allow new Everyplace Suite customers to install Everyplace Suite in a new environment.

The following components will be refreshed:

- WebSphere Transcoding Publisher
- Tivoli® Personalized Services Manager (not including the Device Manager subcomponent)
- Everyplace Authentication Server
- Everyplace Wireless Gateway
- Everyplace Administration Console
- IBM WebSphere Everyplace Suite installation program
- Everyplace Synchronization Manager

The Everyplace Suite is comprised of eleven CDs. CD number 1 contains the Everyplace Suite documentation, including the README file (readme.htm) and *Getting Started* (everyplace.htm), and the install program. The structure of CD number 1 is as follows:

`/info` Everyplace Suite documentation, including the README file (readme.htm) and *Getting Started* (everyplace.htm).

`/install` Installation programs and files

You must use the following CDs to install the Everyplace Suite in a new environment. No other levels of the Everyplace Suite are supported:

Table 5 lists the product CDs and their contents.

Table 5. Everyplace Suite 1.1.3 CDs

CD Number	Content	Level
CD number 1	Install IBM WebSphere Everyplace Suite/IBM HTTP Server Everyplace Suite Documentation, including *Getting Started* and the README	Everyplace Suite Version 1.1.3
CD number 2	AIX® DB2®	Everyplace Suite Version 1.1.3
CD number 3	Solaris DB2	Everyplace Suite Version 1.1.3
CD number 4	SecureWay® Directory, MQSeries® Everyplace	Everyplace Suite Version 1.1.3
CD number 5	WebSphere Application Server	Everyplace Suite Version 1.1.3

Table 5. Everyplace Suite 1.1.3 CDs (continued)

CD number 6	Edge Server Caching Proxy, Edge Server Load Balancer	Everyplace Suite Version 1.1.3
CD number 7	Everyplace Wireless Gateway (except for the Wireless Client subcomponent) WebSphere Transcoding Publisher	Everyplace Suite Version 1.1.3
CD number 8	Tivoli Personalized Services Manager, Everyplace Administration Console Everyplace Authentication Server	Everyplace Suite Version 1.1.3
CD number 9	DBCS AIX DB2	Everyplace Suite Version 1.1.3
CD number 10	DBCS Solaris DB2	Everyplace Suite Version 1.1.3
CD number 11	Everyplace Synchronization Manager Cookie Proxy for WebSphere Portal Server (Japanese only) Everyplace Wireless Gateway — Wireless Client subcomponent	Everyplace Suite Version 1.1.3

This release of Everyplace Suite includes a Japanese only Cookie Proxy for WebSphere Portal Server Version 1.1 on CD number 11. This proxy, provided on the AIX platform only, enables users to use i-mode phones when accessing portals built with the WebSphere Portal Server. Messages and other information displayed in the interface are in Japanese only (English is not supported). Installation of this feature is handled through a separate install script and not by the Everyplace Suite installation program. For more information about i-mode support, and for instructions on installation and configuration, refer to the documentation listed in the following README files on CD number 11:

- `/jpas/readme_Ja.txt`: Japanese version of the README file
- `/jpas/readme_En.txt`: English version of the README file

Backup files

Backup configuration files for the refreshed Everyplace Suite components will be renamed as follows:

Table 6. Everyplace Suite component backup files

Component	1.1.2 Configuration file	1.1.2 Backup file
WebSphere Transcoding Publisher	`wbi.boot`	`wbi.boot.112` in `/usr/IBMTrans` for AIX or `/opt/IBMTrans` for Solaris

Tivoli Personalized Services Manager	`schema/trigger/createPItrigger.sql`	For AIX:
		`usr/TivTsm/install/db/db2/schema/trigger/createPItriggler.sql.wes112`
		For Solaris:
		`opt/TivTsm/install/db/db2/schema/trigger/createPItriggler.sql.wes112`

Everyplace Authentication Server	`ibmwesas.conf` `ibmproxy.conf`	`/tmp/IBMEPS/ibmwesas.conf.112` `/etc/ibmporxy.conf.112`

Everyplace Wireless Gateway	`wgmgrd.conf`
	`wgated.conf`
		For AIX:
		`/usr/lpp/wireless/wgmgrd.conf.112`
		`/usr/lpp/wireless/wgated.conf.112`
		For Solaris:
		`/opt/wireless/wgmgrd.conf.112`
		`/opt/wireless/wgated.conf.112`

WebSphere Suite files	`install.conf` `wgated.conf`	`/tmp/IBMEPS/install.conf.112` `/tmp/IBMEPS/suiteadmin.conf.112`

Installation of Oracle Database software

If you plan to use Oracle Database software for your database management system instead of IBM DB2 Universal Database, follow the instructions in this section to install the Oracle Database.

If you plan to install the Tivoli Personalized Services Manager RADIUS subcomponent, you must install the Oracle client from the Oracle8i installation CD prior to installing Tivoli Personalized Services Manager.

If you plan to install any Tivoli Personalized Services Manager subcomponents (except RADIUS or the Oracle database integration package) you must place a copy of the Oracle JDBC driver (`classes12_01.zip`) on the same machine where the subcomponent will be installed. See step 20 on page 49 or 18 on page 54 for instructions on how to do this on AIX or Sun systems, respectively.

Installing the Tivoli Oracle integration package on AIX

Installing the Tivoli Oracle integration package

Before installing the Oracle Database management system for the Everyplace Suite, the Tivoli Internet Services Management - Oracle Database Integration package (1.1.1.0) must be installed on any machine where the Oracle Database will be installed to facilitate the integration of the Oracle Database software with the Tivoli Personalized Services Manager environment.

Install the Tivoli Oracle integration package on AIX as follows:

1. Log in as root.
2. Place the Everyplace Suite CD number 8 in the CD drive.
3. Mount the CD.
   - Create the directory `/cdrom` (if it does not exist) by entering the following command:

     ```
     mkdir /cdrom
     ```

     in the root directory. To get to the root directory, enter:

     ```
     cd /
     ```

   - Enter the command:

     ```
     mount -rv cdrfs /dev/cd0 /cdrom
     ```

     To remove the CD enter the command:

     ```
     unmount /cdrom
     ```

4. Run SMIT by entering:

   ```
   SMIT
   ```

   - Select **Software Installation and Maintenance**.
   - Select **Install and Update Software**.
   - Select **Install and Update from LATEST Available Software**.
   - Enter:

     ```
     /cdrom/tsm/aix/oracle/sm
     ```

     for the device/directory for software.

5. Select the list under **SOFTWARE to Install**. If you plan to use either the English or the Japanese locale environment, select 1.1.1.0 Tivoli Internet Services Manager - Oracle Database Integration. If you plan to use the Japanese locale environment, you must also select 1.1.1.0 Tivoli Internet services Manager - Japanese Language Files.
6. Edit the `/usr/TivTSM/install/db/oracle/tool/batchInstall.sql` file by modifying the line:

   ```
   @batchSubmitJob   tsmreport.submitAll(&job_2 parm)   &job_2 hour
   ```

   to

   ```
   @batchSubmitJob   tsmreport.submitAll()  &job_2 hour
   ```

7. Enter:

   ```
   cp /cdrom/tsm/aix/oracle_schema.tar  /usr/TivTSM/install/db/oracle
   ```

8. When the install is finished, unmount the CD by entering:

   ```
   unmount /cdrom
   ```

   and remove it from the CD drive.

Installing the Oracle Database using the Oracle8i CD

Once the Tivoli package has been installed, you can proceed with the installation of the Oracle8i database software by following these steps:

1. At the command line, enter the following command (in the Korn shell):

   ```
   export DISPLAY=:0.0
   ```

   then enter:

   ```
   xhost +
   ```

   You should see the message:

   ```
   Access control disabled, clients can connect from any host.
   ```

   If you do not, and instead you see the message:

   ```
   1346-217 xhost:  must be on local machine to enable or disable access control.
   ```

   Enter the following command (in the Korn shell):

   ```
   export DISPLAY=HOSTNAME:0.0
   ```

   then enter:

   ```
   xhost + HOSTNAME
   ```

2. Place the Oracle8i CD in the CD-ROM drive and enter the following commands:
   - `cd /usr/TivTSM/install/db/oracle`
   - `export PATH=$PATH:/usr/TivTSM/install/db/oracle`
   - `./TSMOracle8i`
3. Press **Enter** after you see the message:

   ```
   Please place the Oracle CD in Drive
   ```

4. Answer **yes** when asked to create the **dba** group and the **oracle** user.
5. You will then be asked:

   ```
   What is the 'mount point' for Oracle user's home?
   ```

   Enter:

   ```
   /db
   ```

Note: It is very important that the mount point be specified as `/db`

At this point, you should see messages indicating:

```
Installing Oracle8i software.
Initializing Java Virtual Machine. This may take up to 10 minutes.
```

After this time, you should see the message:

```
Install phase starts, updates every 15 seconds.
```

If you don’t see this message after 10–15 minutes, stop the installation program and check the error log for possible errors. The installation can take from 20 to 90 minutes from this point, depending on your hardware.

6. After the installation completes, you will be prompted for the full path name of the local bin directory. Accept the default value of the following:

   ```
   /usr/local/bin
   ```

7. You will then be asked:

   ```
   Enter instance name to be created, or 'q' to abort:
   ```

   Enter the instance name `ispb` and press **Enter**.

8. You will then be asked:

   ```
   How many subscribers in this database?
   ```

   Enter a number between 10000 and the maximum, which is dictated by your disk space (16 kilobytes per user).

9. You will then be asked:

   ```
   Do you want logging on or off for this install? (n/f)
   ```

   Enter **n**.

10. You will then be told:

    ```
    Press 'Enter' to review update file /db/creispblv.ksh.
    ```

    Press **Enter**. The script file `creispblv.ksh` will appear. If the information is accurate, exit the file without saving. The information is automatically saved in the `/usr/TivTSM/install/db/oracle/dbcalc.log` file.

    To change the default settings, you need to edit the file as follows:

    a. When editing the file, you must change the values to match those in the `/usr/TivTSM/install/db/oracle/dbcalc.log` file. An example `dbcalc.log` file is shown below:

    ```
    Disk    Free PPs
    ====    ========
    hdisk0  166
    Physical Partition Size: 16MB

    File       Units      Size
    ======     ===== =========
    Data:          8   127999K
    Index:         6    95999K
    Temp:          2    31999K
    System:       11
    ```

```
User:          1
Rbs:           1
Drsystem:      6
Oem:           1
Redo:          1
Ctrl:          1
```

If you have more than one volume group, you will see information for all volume groups on the system. Use the information under the volume group that you will use for your database space.

b. There are three columns named **FILE**, **UNITS**, and **SIZE**, respectively, as shown in the previous example: Use this information to edit the `creispblv.ksh` file. Only edit lines that begin with `mklv`. The following is a sample line from `creispblv.ksh`:

```
mklv -a c -y lvispbdata -ex -u1  rootvg 8 hdisk0
             (1)            (2) (3)   (4) (5)

mklv -a c -y lvispbindex -ex -u1 rootvg 6 hdisk0
mklv -a c -y lvispbrbs1          rootvg 1 hdisk0
mklv -a c -y lvispbrbs2          rootvg 1 hdisk0
mklv -a c -y lvispbredo11        rootvg  1 hdisk0
mklv -a c -y lvispbredo12        rootvg  1 hdisk0
mklv -a c -y lvispbredo13        rootvg  1 hdisk0
mklv -a c -y lvispbredo21        rootvg  1 hdisk0
mklv -a c -y lvispbredo22        rootvg  1 hdisk0
mklv -a c -y lvispbredo23        rootvg  1 hdisk0
mklv -a c -y lvispbsys           rootvg 11 hdisk0
mklv -a c -y lvispbdrsys         rootvg 6 hdisk0
mklv -a c -y lvispbtemp          rootvg 2 hdisk0
mklv -a c -y lvispbctrl1         rootvg  1 hdisk0
mklv -a c -y lvispbctrl2         rootvg  1 hdisk0
mklv -a c -y lvispbctrl3         rootvg  1 hdisk0
mklv -a c -y lvispbuser          rootvg  1 hdisk0
mklv -a c -y lvispboem           rootvg 1 hdisk0
```

Notes:

1) Mapping with values from `dbcalc` is done using `lvispb` **(1)** as a reference. `lvispbdata` maps to the `Data` value (**8** in the example shown in Step 10a). `lvispbindex` maps to the `Index` value (**6** in the example shown in Step 10a).

2) `-u1` is the number of hard drives used for the table space (`1`=1 hard drive).

3) The number following any `-u` flag **(2)** must be equal to the number of disks **(5)** listed on that line. You may remove both `-ex` and `-un` flags if only one disk is listed.

4) `rootvg` **(3)** is the name of the volume group that hard drive belongs to.

5) `8` **(4)** is the number that must match the number on the screen or in the `dbcalc.log` file.

6) `hdisk0` is the physical hard drive, which must be part of the volume group named before it.

11. Enter **y** when asked if you want to continue. The script will continue to run and create the logical volume. If you use `ispb` as the instance name, you can see the details by viewing `tail -f /usr/TivTSM/install/db/oracle/./sqlispb.log`.
12. You will be asked for the following entries (accept the default values):
    - locale: default = `en` (`ja` for Japanese)
    - password for db user 'system': default = `manager`
    - schema owner: default = `stage_master`
    - schema user: default = `stage_user`

    Note: If you plan to enter `ja` for **default locale**, you must first open another console and perform the following:

    a. Enter:

    ```
    su - oracle8
    ```

    b. Add the following lines to `.profile`:

    ```
    export LANG=JA_JP
    export NLS_LANG=Japanese_Japan.UTF8
    ```

    c. Save the changes.
13. Enter **y** when asked if you are ready to create the schema.
14. The following messages will appear:
    - `Loading tables...`
    - `Done loading...`
    - `Checking results...OK.`
15. You will then be asked:

    ```
    Do you need to include the Device Schema?
    ```

    Enter **y** if you are going to use the Device Management Server.
16. You will then be asked:

    ```
    Do you need to load the zip codes table?
    ```

    Enter **y**.
17. You will then be asked:

    ```
    Configure LDAP Integration?
    ```

    Enter **y**.
18. You will then be asked:

    ```
    Configure eBill?
    ```

    Enter **y**.
19. You will then be asked:

    ```
    Configure Web Hosting?
    ```

    Enter **n**.

20. You must copy the Oracle JDBC driver file (`classes12_01.zip`) into the appropriate directories. The file can be located on CD number 8 in the `/tsm/aix/oracle/prereqs` directory and copied into the following directories:
    - `mkdir /usr/TivTSM/classes`
    - `cp classes12_01.zip  /usr/TivTSM/classes/.`
    - `cp /usr/TivTSM/classes/classes12_01.zip  ~oracle8/jdbc/lib/.`

    If you are installing the Device Manager feature, then copy the following file:

    ```
    cp classes12_01.zip /usr/lpp/TivDMS/doc/.
    ```

Before installing Tivoli Personalized Services Manager with Oracle Database be sure to apply the following AIX PTFs:

- bos.sysmgt.trace 4.3.3.11
- devices.ssa.disk.rte 4.3.3.10

Now you are ready to install Tivoli Personalized Services Manager with the Everyplace Suite installation program.

Note: Do not select **Database Integration** in the Everyplace Suite installation program, or the Tivoli Personalized Services Manager installation will fail.

Installing the Oracle client on the RADIUS server

If you are installing the RADIUS subcomponent of Tivoli Personalized Services Manager install the Oracle client on the RADIUS server prior to installing Tivoli Personalized Services Manager as follows:

1. Mount the Oracle8i CD by entering:

   ```
   mount -rv cdrfs /dev/cd0 /cdrom
   ```
2. Enter:

   ```
   mkdir -p /db/app/oracle/products/8.1.5
   ```
3. Create group `dba`.
4. Create user `oracle8` who belongs to the `dba` group.
5. Enter:

   ```
   /db/app/oracle/products/8.1.5
   ```

   for the home directory.
6. Enter:

   ```
   chown -R oracle8:dba /db
   ```
7. Follow the instructions in “Installing the Oracle Database using the Oracle8i CD” on page 45 to install the Oracle database. Use `-c` to install only the Oracle client, as in `TSMOracle8i -c`.

   Note: If you install the Oracle client and Oracle server on separate machines, a setup inconsistency may occur between the two machines which could prevent successful database connections from client to server. This inconsistency will cause difficulty in using the reporting and RADIUS scripts on the client machine. The affected scripts are as follows:

```
reporting_job_ora.ksh
reporting_deljob_ora.ksh
start_radius.ksh
reload_radius.ksh
```

To solve this problem, copy the following files from the Oracle server machine to the Oracle client machine, replacing the original files on the client:

```
/db/app/oracle/product/8.1.5/network/admin/tnsnames.ora
/db/app/oracle/product/8.1.5/network/admin/sqlnet.ora
```

Installing the Tivoli Oracle integration package on Solaris

Installing the Tivoli Oracle integration package

If you install the Tivoli Personalized Services Manager RADIUS subcomponent on a Solaris system which is not the Oracle DB Server, you must install the Oracle Client prior to RADIUS installation by the Everyplace Suite installer.

To install Oracle on Solaris, you must install both the RADIUS server and the Oracle integration package on a single machine.

For Oracle Software installation on Solaris, the following Operating System Packages are required:

- SUNWarc
- SUNWbtool
- SUNWhea
- SUNWlibm
- SUNWlibms
- SUNWsprot
- SUNWtoo

You must add the following parameters at `/etc/system` and reboot the system before Oracle installation:

- set shmsys:shminfo_shmmax=536870912 (half of physical memory)
- set shmsys:shminfo_shmmin=1
- set shmsys:shminfo_shmmni=200
- set shmsys:shminfo_shmseg=20
- set semsys:seminfo_semmni=1000
- set semsys:seminfo_semmsl=100
- set semsys:seminfo_semmns= the sum of all the processes (1000 per db) X 2 + System requirements (Usually 10%) = total value of semmns
- set semsys:seminfo_semopm=100
- set semsys:seminfo_semvmx=32767

Refer to the Oracle documentation located in `index.htm` in the root directory of the Oracle8i SPARC 8.1.5 CD for more details.

Before installing the Oracle Database management system for the Everyplace Suite, the Tivoli Internet Services Management - Oracle Database Integration package (1.1.1.0) must be installed to facilitate the integration of the Oracle Database software with the Tivoli Personalized Services Manager environment.

Install the Tivoli Oracle integration package on Solaris as follows:

1. Log in as root.
2. Place the Everyplace Suite CD number 8 in the CD drive.
3. Mount the CD. On Solaris, the CD will automatically mount and appear in the file manager.
4. Install 1.1.1.0 Tivoli Internet Services Management - Oracle Database Integration as follows:

   ```
   admintool
   ```

   or

   ```
   pkgadd -d
   ```

   - To install in the English locale, enter the following command to obtain the device/directory for software:

     ```
     /cdrom/everypl_suite-8/tsm/sun/oracle/sm TivTISMO8
     ```

   - To install in the Japanese locale, enter the following command to obtain the device/directory for software:

     ```
     /cdrom/everypl_suite-8/tsm/sun/oracle/sm TivTISMO8
     /cdrom/everypl_suite-8/tsm/sun/oracle/sm TivTISMJa
     ```

5. Enter:

   ```
   cp /cdrom/everypl_suite-8/tsm/sun/oracle_schema.tar /opt/TivTSM/install/db/oracle
   ```

6. When the install is finished, enter:

   ```
   eject
   ```

   and umount and remove the CD from the CD drive.

Installing the Oracle Database using the Oracle8i CD

Once the Tivoli package has been installed, you can proceed with the installation of the Oracle8i database software by following these steps:

1. At the command line, enter the following command (in the Korn shell):

   ```
   export DISPLAY=:0.0
   ```

   Enter:

   ```
   xhost +
   ```

   You should see the message:

   ```
   Access control disabled, clients can connect from any host.
   ```

If you do not, and instead you see the message:

```
1346-217 xhost:  must be on local machine to enable or disable access control.
```

Enter the following command in the Korn shell:

```
export DISPLAY=HOSTNAME:0.0
```

Enter:

```
xhost + HOSTNAME
```

2. Place the Oracle8i CD in the CD-ROM drive and enter the commands:
   - `cd /opt/TivTSM/install/db/oracle`
   - `export PATH=$PATH:/opt/TivTSM/install/db/oracle`
   - `./TSMOracle8i`
3. Press **Enter** after you see the message:

   ```
   Please place the Oracle CD in Drive. Press 'Enter' to continue.
   ```
4. Enter **y** when asked to create the `dba` group and the `oracle8` user.
5. When asked:

   ```
   What is the 'mount point' for Oracle user's home?
   ```

   Enter:

   ```
   /db
   ```

   Note: It is very important that the mount point be specified as `/db`

   At this point, you should see messages indicating:

   ```
   Installing Oracle8i software.
   Initializing Java Virtual Machine. This may take up to 10 minutes.
   ```

   After this time, you should see the message:

   ```
   Install phase starts, updates every 15 seconds.
   ```

   If you don't see this message after 10–15 minutes, stop the installation program and check the error log for possible errors. The installation can take from 20 to 90 minutes from this point, depending on your hardware.
6. After the installation completes, you will be asked for the full path name of the local bin directory. Accept the default value of the following:

   ```
   /opt/local/bin
   ```
7. You will then be asked:

   ```
   Enter instance name to be created, or 'q' to abort:
   ```

   Enter the instance name `ispb` and press **Enter**.
8. You will then be asked:

   ```
   How many subscribers in this database?
   ```

Enter a number between 10000 and the maximum, which is limited by your disk space (16 kilobytes per user).

9. You will then be asked:

   ```
   Do you want logging on or off for this install? (n/f?)
   ```

   Enter **n**.

10. You will be asked for the following entries (accept the default values):

    - locale: default = `en` (`ja` for Japanese)
    - password for database user 'system': default = `manager`
    - schema owner: default = `stage_master`
    - schema user: default = `stage_user`

    Note: If you plan to enter `ja` for **default locale**, you must first open another console and perform the following:

    a. Enter:

       ```
       su - oracle8
       ```

    b. Add the following lines to `.profile`:

       ```
       LANG=ja_JP.UTF-8
       export LANG
       NLS_LANG=Japanese_Japan.UTF8
       export NLS_LANG
       ```

    c. Save the changes.

11. You will then be asked:

    ```
    Ready to create the schema?
    ```

    Enter **y**.

12. The following messages will appear:

    - `Loading tables...`
    - `Done loading...`
    - `Checking results...OK.`

13. You will then be asked:

    ```
    Do you need to include the Device Schema?
    ```

    Enter **y** if you are going to use the Device Management Server.

14. You will then be asked:

    ```
    Do you need to load the zip codes table?
    ```

    Enter **y**.

15. You will then be asked:

    ```
    Configure LDAP Integration?
    ```

    Enter **y**.

16. You will then be asked:

```
Configure eBill?
```

Enter **y**.

17. You will then be asked:

    ```
    Configure Web Hosting?
    ```

    Enter **n**.

18. You must copy the Oracle JDBC driver file (`classes12_01.zip`), located on CD number 8 in the `/tsm/sun/oracle/prereqs` directory into the following directories:

    ```
    cp classes12_01.zip /opt/TivTSM/classes/.
    cp /opt/TivTSM/classes/classes12_01.zip ~oracle8/jdbc/lib/.
    ```

    If you are installing the Device Manager feature then copy the file into the following directory as well:

    ```
    cp classes12_01.zip /opt/TivDMS/doc/.
    ```

Now you are ready to install Tivoli Personalized Services Manager with the Everyplace Suite installation.

Note: Do not select **Database Integration** in the Everyplace Suite installation program, or the Tivoli Personalized Services Manager installation will fail.

Starting the installation program

Installation can be done from CDs burned from the downloaded files or directly from the extracted CD image files.

From the product CD

To start the Everyplace Suite installation program from the product CD, follow these steps:

1. Log in as root.
2. Place CD number 1 in the CD drive.
3. Mount the CD.
   - In the root directory, create the directory `/cdrom` (if it does not exist) by entering the command:

     ```
     mkdir /cdrom
     ```

     Note: To get to the root directory, enter: `cd /`
   - For AIX, enter the command:

     ```
     mount -rv cdrfs /dev/cd0 /cdrom
     ```

     To remove the CD, enter the command:

     ```
     umount /cdrom
     ```

or click the **Unmount** button when prompted by the Everyplace Suite installation program.
- On Solaris, the CD will automatically mount and appear in the file manager.

4. Enter the following command:
   - For AIX:

     ```
     /cdrom/install.sh
     ```

   - For Solaris:

     ```
      /cdrom/cdrom0/install.sh
     ```

5. At the command line, you will be prompted for the `JAVA_HOME` directory. Press **Enter** or enter a different `JAVA_HOME` directory to start the installation program.
6. You will then be asked if you are installing Tivoli Personalized Services Manager. If so, the IBM AIX Developer Kit, Java 2 Technology Edition, Version 1.2.2. will be installed.

Note: Be sure to issue these commands from the root directory. Enter `cd /` to get to the root directory. If any command window is in the `/cdrom` directory, you will not be able to unmount the CD.

From the file system

Use these instructions only if you are installing directly from the downloaded files instead of the product CDs. To start the Everyplace Suite installation program from the file system, follow these steps:

1. Go to the directory for CD number one by entering:

   ```
   cd cd1name
   ```

   Where `cd1name` is the name of the directory where the downloaded CD image file was extracted.
2. Enter the command:

   ```
   ./install.sh
   ```

3. At the command line, you will be prompted for the `JAVA_HOME` directory. Press **Enter** or enter a different `JAVA_HOME` directory to start the installation.
4. You will then be asked if you are installing Tivoli Personalized Services Manager. If so, the IBM AIX Developer Kit, Java 2 Technology Edition, Version 1.2.2 will be installed.

Java exception messages

If you install the Everyplace Suite on Solaris, several Java exceptions messages may appear when you start `install.sh`. These messages are cosmetic in nature and are related to the JDK. They will not affect installation of the Everyplace Suite components. The messages are as follows:

- java.lang.NoSuchMethodError: java.lang.Object: method postEvent(Ljava/awt/AWTEvent;)V not found at java.lang.Thread.run(Compiled Code)
- java.lang.NoSuchMethodError: java.lang.Object: method postEvent(Ljava/awt/AWTEvent;)V not found at java.lang.Thread.run(Compiled Code)

- java.lang.NoSuchMethodError: java.lang.Object: method postEvent(Ljava/awt/AWTEvent;)V not found at java.lang.Thread.run(Compiled Code)
- java.lang.NoSuchMethodError: java.lang.Object: method postEvent(Ljava/awt/AWTEvent;)V not found at java.lang.Thread.run(Compiled Code)

The following additional messages may appear when you click **Finish** to complete the installation:

- java.lang.NoSuchMethodError: java.lang.String: method postEvent(Ljava/awt/AWTEvent;)V not found at java.lang.Thread.run(Compiled Code)
- java.lang.NoSuchMethodError: java.lang.String: method postEvent(Ljava/awt/AWTEvent;)V not found at java.lang.Thread.run(Compiled Code)

Installing the Everyplace Suite

Installation of the Everyplace Suite is made easy with the installation program. The installation program prompts you for all the necessary information to complete the installation.

For all of the components in the Everyplace Suite, the installation program automatically uses that component's installation program to properly install that component. The Everyplace Suite installation program also uses the information to provide limited configuration of each component after it is installed.

Everyplace Suite installation is not supported in an NIS (Network Information Service) environment for either Solaris or AIX.

If you cancel the Everyplace Suite installation prior to installing any of the Everyplace Suite components, you must use SMIT, SMITTY, or admintool to remove the Everyplace Suite files.

You must disable the Operating System Password Rules prior to the Everyplace Suite installation. After the installation is complete, you can reenable the password rules.

If you install an application that uses JDK 1.2.2, such as the WebSphere Application Server, and then start the Everyplace Suite, the font will appear larger than it should, and items will appear to be missing from the panels. You can either enlarge the panel by dragging, or reboot the machine to resolve the issue.

Notes:

1. The Everyplace Synchronization Manager is not installed using the Everyplace Suite installation program. It is installed independently from CD number 11 of the Everyplace Suite product CDs. See the documentation in the `/esm/docs` directory of CD number 11 for installation instructions and requirements.
2. It is important to follow these installation instructions when installing the Everyplace Suite components. Do not follow the stand-alone installation instructions in the component documentation (with the exception of Everyplace Synchronization Manager), as the installation requirements for the component within the Everyplace Synchronization Manager may vary.

Installation steps

At any time during the installation process, you can click the **Back** button to go back to previous panels to review or change the information. You have the opportunity to review all entries on the **Final Selection Confirmation** window before the installation actually begins.

1. **View documentation:** To view the README or the *Getting Started* book before starting the installation, click the **README** or the **Getting Started** buttons on the View Documentation panel that is presented.

   Note: On Solaris systems: If you click in the background area outside the install window, the install window will go to the background and not be visible. To bring the install window back in view, press the **Alt-Tab** keys simultaneously.
2. **Select SecureWay Directory option:** Select one of the three SecureWay Directory information sharing options. The three options are:
   - **Install SecureWay Directory**: This installs the SecureWay Directory on the local server.
   - **Retrieve Everyplace Suite information from a SecureWay Directory server**: This instructs the installation program to retrieve the information from the existing SecureWay Directory (LDAP) server in the Everyplace Suite domain.
   - **Retrieve existing Everyplace Suite information from a file**: This allows the installation to be performed without using SecureWay Directory. Installation information is retrieved from the file system or diskette media at a later time. If you select this option, SecureWay Directory appears on the component selection panel as a selectable component. If you install SecureWay Directory using this option, you cannot install the Tivoli Personalized Services Manager component if you are using a remote DB2 database server. You must either use a local DB2 database server or a local or remote Oracle database server. If you install SecureWay Directory using this option, the LDIF file generated by the Everyplace Suite installation cannot be shared between the AIX and Solaris systems. For example, if the LDIF file is generated on AIX, the LDIF file must be imported into the SecureWay Directory AIX server. It cannot be imported into the SecureWay Directory Solaris server.

   When you are prompted to enter a user ID for access to SecureWay Directory, be sure to include `cn=` before the user ID value (for example `cn=xxxxx`).

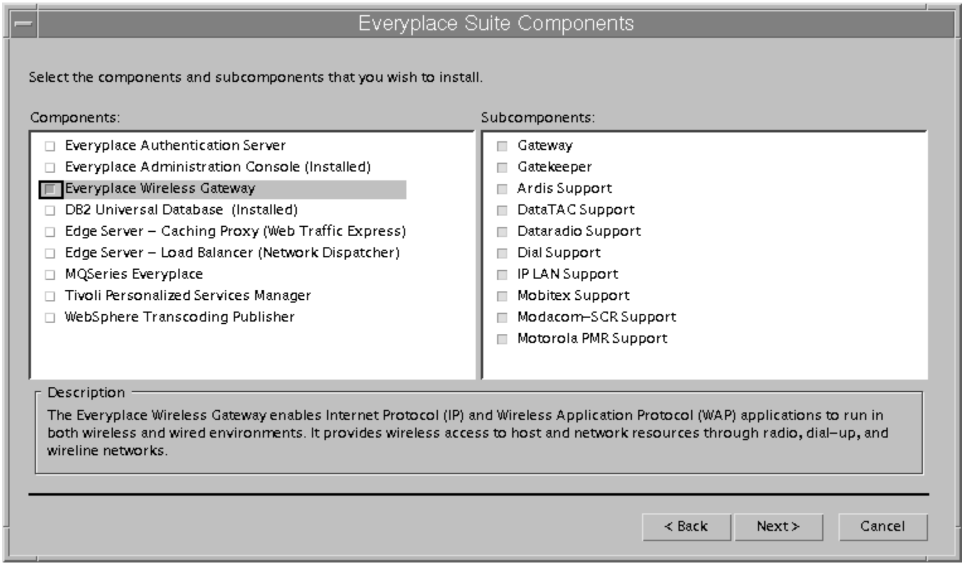
   You will be prompted for specific information depending on the option you select.
3. **Select components to install:** Choose the Everyplace Suite components by selecting the check boxes of the components you wish to install. All the Everyplace Suite components are displayed in the panel. You may select any combination for installation.

   Some of the components have subcomponents that appear in the right pane. These subcomponents can be individually selected.

   Figure 5 shows the component selection panel of the installation wizard. The subcomponents of the currently highlighted component (in this example, Everyplace Wireless Gateway) are shown in the right pane.

The installation wizard will verify that all prerequisite and corequisite software is installed before beginning the actual installation. The installation wizard will notify you of any problems or of software requirements that need to be met prior to completing the installation.

Note: It may be necessary to upgrade component or prerequisite software to complete the Everyplace Suite installation properly. Follow the instructions on the installation panels to verify and upgrade the necessary software. In some circumstances, it may be necessary to downgrade to an earlier version of the component software to ensure the Everyplace Suite software runs properly. Without the recommended versions of prerequisite and component software installed, the Everyplace Suite may not work as expected.



Everyplace Suite Components

Select the components and subcomponents that you wish to install.

Components:

- □ Everyplace Authentication Server
- □ Everyplace Administration Console (Installed)
- □ Everyplace Wireless Gateway
- □ DB2 Universal Database (Installed)
- □ Edge Server – Caching Proxy (Web Traffic Express)
- □ Edge Server – Load Balancer (Network Dispatcher)
- □ MQSeries Everyplace
- □ Tivoli Personalized Services Manager
- □ WebSphere Transcoding Publisher

Subcomponents:

- □ Gateway
- □ Gatekeeper
- □ Ardis Support
- □ DataTAC Support
- □ Dataradio Support
- □ Dial Support
- □ IP LAN Support
- □ Mobitex Support
- □ Modacom–SCR Support
- □ Motorola PMR Support

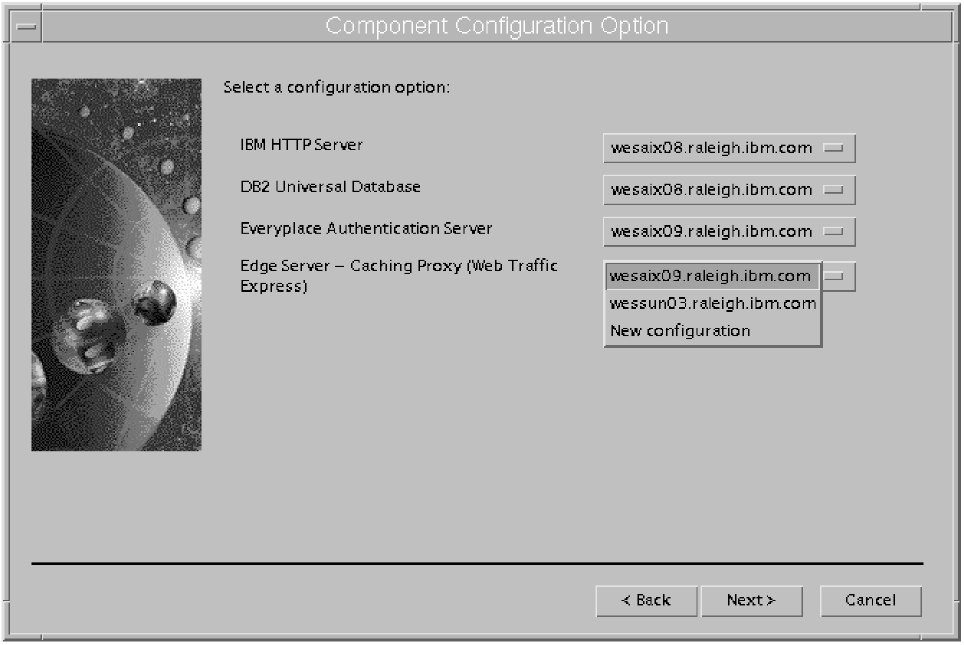
Description

The Everyplace Wireless Gateway enables Internet Protocol (IP) and Wireless Application Protocol (WAP) applications to run in both wireless and wired environments. It provides wireless access to host and network resources through radio, dial–up, and wireline networks.

Figure 5. Selecting the Everyplace Suite components

4. **Select database management system:** If you select either Tivoli Personalized Services Manager or Everyplace Wireless Gateway from the component list, then you must select either DB2 UDB or Oracle as the database management system.

   Both of these components require either IBM DB2 Universal Database 7.1 or Oracle database 8.1.5 to be installed in the Everyplace Suite domain.
5. **Select component configuration options:** If there are other instances of components that you are currently installing in the Everyplace Suite, you will be given configuration options for each component with other instances already in the domain. Figure 6 on page 59 shows how each instance is listed by server name. You can select one of the instances to configure the current selected component with the same parameters, or you can select **New configuration** if you don't want to use any of the pre-installed configuration parameters.



Component Configuration Option

Select a configuration option:

IBM HTTP Server: wesaix08.raleigh.ibm.com

DB2 Universal Database: wesaix08.raleigh.ibm.com

Everyplace Authentication Server: wesaix09.raleigh.ibm.com

Edge Server – Caching Proxy (Web Traffic Express): wesaix09.raleigh.ibm.com

Figure 6. Select component configuration options

6. **Select user ID option:** Select either single or multiple user IDs for component administration.

   Some of the Everyplace Suite components require a user ID, group ID, and password for configuration. You have the option of configuring these with one ID for all the components that require an ID, or unique ID for each component that requires an ID.

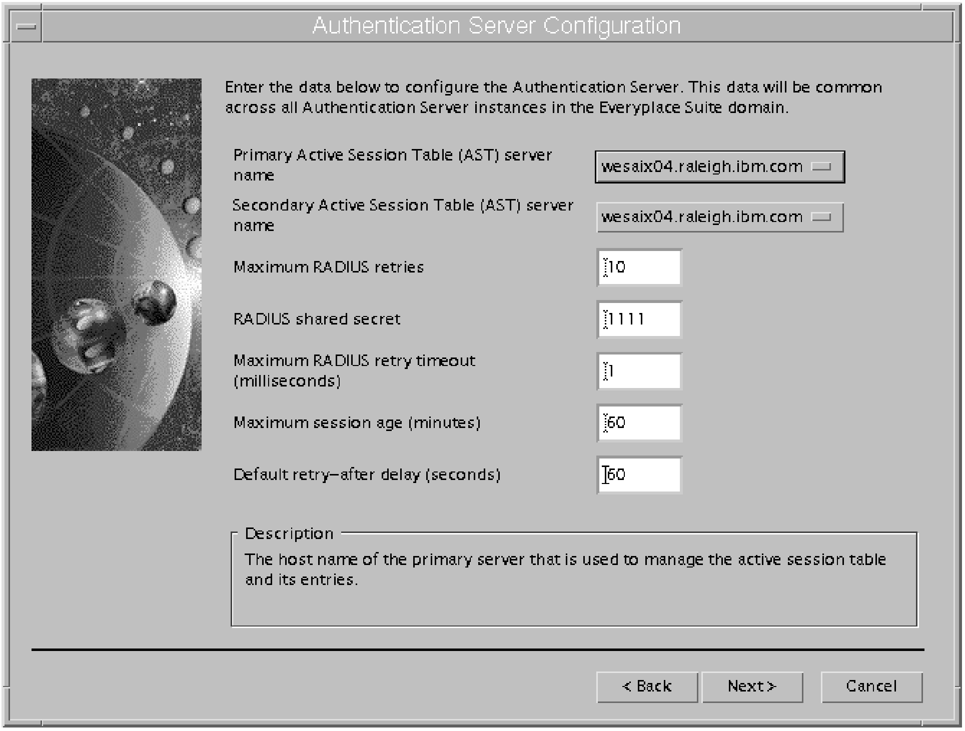
   If you select the single user ID option, you will be prompted once for the user and group IDs and password.

   If you select different IDs for each component, you will be prompted to enter the user ID, group ID, password and other component-specific information.

7. **Specify Authentication Server configuration information:** If the Authentication Server has been selected, you will be prompted to input the necessary configuration information. You will be presented with two panels to accomplish this:

   - The first panel prompts you for information that is common to all Authentication Servers in the domain. This information will be stored in SecureWay Directory and will only need to be entered once. See Figure 7 on page 60.
   - The second panel will prompt you for information that is specific to a particular Authentication Server. This panel will also present the option of configuring the Authentication Server as an authentication proxy or as a transparent authentication proxy.

For more information about supplying configuration information for the Authentication Server, see “Configuring Authentication Server information in SecureWay Directory” on page 73.


Authentication Server Configuration

Enter the data below to configure the Authentication Server. This data will be common across all Authentication Server instances in the Everyplace Suite domain.

Primary Active Session Table (AST) server name: wesaix04.raleigh.ibm.com

Secondary Active Session Table (AST) server name: wesaix04.raleigh.ibm.com

Maximum RADIUS retries: 10

RADIUS shared secret: 1111

Maximum RADIUS retry timeout (milliseconds): 1

Maximum session age (minutes): 60

Default retry–after delay (seconds): 60

Description

The host name of the primary server that is used to manage the active session table and its entries.

Figure 7. Common Authentication Server configuration information

8. **Specify Webmaster user ID:** If you have selected Tivoli Personalized Services Manager, specify the Webmaster user ID in the form of `webmasterid@domain_name.com`.
9. **Confirm component selections:** Confirm the component selections by reviewing the list of selected components.

   All selected components, subcomponents, and configuration information will be displayed. You can click the **Back** button to go back to the component selection panel to add or remove components from the list or to change other configuration information. When the **Install** button is clicked, the installation will begin.

Note: If any Everyplace Suite components have been installed using the LDIF file (option three in the SecureWay Directory Information Sharing Options installation panel) instead of SecureWay Directory then SecureWay Directory must be installed and information imported from the LDIF file into SecureWay Directory.

Installation progress

As the installation process commences, a progress indicator is displayed that shows the status of the install. Any errors or problems that happen during the install are displayed here, as well as logged in the Everyplace Suite log file. See “Troubleshooting” on page 71.

Installing Tivoli Personalized Services Manager with DB2 on AIX

In Everyplace Suite Version 1.1.3, the installation will launch the Tivoli Personalized Services Manager `Createdb.ksh` file without modifying the original file. The **Subscriber Entry** fields have been removed from the Everyplace Suite installation panels because that information is now captured during the runtime of `Createdb.ksh`. The database name `ispb` is automatically entered, however, you must manually configure several options, including the number of subscribers, the locale (for example, `en`, `de`, `ja`, `zh`), and other integrators (for example, eBill or WebHosting). You must also modify various script files. The administrator will have the option of modifying the volume group information for the database that is about to be defined.

During installation of Tivoli Personalized Services Manager with DB2 on an AIX platform, the `Createdb` window will open while you are running the Everyplace Suite installation program. You must perform the following steps:

1. You will be asked:
   ```
   How many subscribers in this database?
   ```
2. Enter a number between 10000 and the maximum, which is dictated by your disk space (16 kilobytes per user).
3. Press **Enter** to see information for `rootvg`. The information you receive will depend on your system configuration. An example of possible output information is shown below:
   ```
   Disk Free PPs
   ======= =====
   hdisk0: 34
   Physical partition size: 8 MB

   File Units Size
   ======= ===== =========
   Data:     16   16001
   Index:    12   12001
   ```
   This information is also saved in the `dbcalc.log` in the `/usr/TivTSM/install/db/db2` directory.
4. Press **Enter** to see information for `oravg`. The following is an example of the information that you will see if you are using more than one hard drive:
   ```
   Disk Free PPs
   ======= =====
   hdisk1:  40
   hdisk2: 366
   Physical partition size: 8 MB
   ```

```
File Units Size
======= ===== =========
Data:     16   16001
Index:    12   12001
```

5. Open another window to update the `/usr/TivTSM/install/db/db2/creispblv.ksh` and `/usr/TivTSM/install/db/db2/schema/ddl/createdb2_db2_ispb.sql` files.

   When editing the files, you must change the values to match those in the table displayed. You can also view this table in the `/db/db2/install/dbcalc.log` file. If you have more than one volume group, you will see information for all volume groups on the system. Use the information under the volume group that you will use for your database space.
6. Edit the `/usr/TivTSM/install/db/db2/creispblv.ksh` file as follows:
   - There are three columns named **FILE**, **UNITS**, and **SIZE**, respectively. Use this information to edit the`/db/db2/install/creispblv.ksh` file. Only edit lines that begin with `mklv`. The following is a sample line from `creispblv.ksh`:

     ```
     mklv -a c -y lvispbdata -ex -u1 oravg 16 hdisk1
                     (1)         (2)  (3)  (4) (5)
     ```

     Notes:

     a. Mapping with values from `dbcalc` is done using `lvispb` **(1)** as a reference. `lvispbdata` maps to the `Data` value (**16** in the example shown in Step 4). `lvispbindex` maps to the `Index` value (**12** in the example shown in Step 4).
     b. `-u1` is the number of hard drives used for the table space (`1`=1 hard drive).
     c. The number following any `-u` flag **(2)** must be equal to the number of disks **(5)** listed on that line. You may remove both `-ex` and `-un` flags if only one disk is listed.
     d. `oravg` **(3)** is the name of the volume group that hard drive belongs to.
     e. `16` **(4)** is the number that must match the number on the screen or in the `dbcalc.log` file.
     f. `hdisk1` is the physical hard drive, which must be part of the volume group named before it.
7. Go to `/usr/TivTSM/install/db/db2/schema/ddl` and modify the following lines in the `createdb2_db2_ispb.sql` script:

   ```
   USING (device '/dev/rlvispbdata' xxxxx)
   USING (device '/dev/rlvispbindex' yyyyy )
   ```

   * Replace the variable information, represented here by **xxxxx** and **yyyyy** with information from the volume group. Using the information from the example volume group above, you would enter **16001** in place of **xxxxx** and **12001** in place of **yyyyy**.
8. If you have just installed DB2, and are not using a C compiler trial license, you must run the `chmod -R 777` command in the `/var/ifor` directory before typing `exit`.
9. Enter **exit** from the `Createdb` window to continue the DB2 installation procedure.
10. You will then be told:

    ```
    Enter default locale for your system:(en,ja..2 letters):
    ```

Enter `en` for English, `ja` for Japanese, etc.

11. You will then be asked:

    ```
    Configure LDAP integration (y/n)?
    ```

    Enter **y**.

12. You will then be asked:

    ```
    Configure eBill?
    ```

    Enter **y**.

13. You will then be asked:

    ```
    Configure Web Hosting?
    ```

    Enter **n**.

    Note: The Everyplace Suite does not support Web hosting. However, you may still use Web hosting if you desire. To use Web hosting, enter **y** for this question.

14. The `Createdb` window will close automatically, and installation will continue.

Installing Tivoli Personalized Services Manager with DB2 on Solaris

If you are installing Tivoli Personalized Services Manager with DB2 on a Solaris platform, the `Createdb` window will open while you are running the Everyplace Suite installation program. You must perform the following steps:

1. You will be asked:

   ```
   How many subscribers in this database?
   ```

2. Enter a number between 10000 and the maximum, which is dictated by your disk space (16 kilobytes per user).

3. Needed disk size information is displayed as follows:

   ```
   File    Size(In 8k Pages)
   ====      ================
   Data:     10240
   Index:    7680
   ```

4. Open another window to update `/opt/TivTSM/install/db/db2/./schema/ddl/createdb2_db2_ispb.sql`.

5. Go to `/usr/TivTSM/install/db/db2/schema/ddl` and modify the following lines in the `createdb2_db2_ispb.sql` script:

   ```
   USING (file '/db/db2/ispbdata' xxxxx)
   USING (file '/db/db2/ispbindex' yyyyy )
   ```

   * Replace the variable information, represented here by **xxxxx** and **yyyyy** with information from the volume group. Using the information from the example volume group above, you would enter **10240** in place of **xxxxx** and **7680** in place of **yyyyy**.

6. Enter **exit** in the `Createdb` window to continue the DB2 installation procedure.

7. You will then be told:

```
Enter default locale for your system:(en,ja..2 letters):
```

Enter `en` for English, `ja` for Japanese, etc.

You will then be asked:

```
Configure LDAP integration (y/n)?
```

Enter **y**.

You will then be asked:

```
Configure eBill?
```

Enter **y**.

You will then be asked:

```
Configure Web Hosting?
```

Enter **n**.

Note: The Everyplace Suite does not support Web hosting. However, you may still use Web hosting if you desire. To use Web hosting, enter **y** for this question.

The `Createdb` window will close automatically, and installation will continue.

Everyplace Suite component installation hints and tips

Installing Everyplace Wireless Gateway

You may not have the ability to access the Authentication Server from Netscape Navigator if it is launched in a machine where Everyplace Wireless Gateway is installed. If that is the case, use other machines to access the Authentication Server.

You may not have the ability to launch the Caching Proxy's administration console from the Everyplace Administration Console in a machine where Everyplace Wireless Gateway is installed. If that is the case, launch the Everyplace Administration Console from another server.

Installing Everyplace Wireless Gateway with DB2 on Solaris

If you install Everyplace Wireless Gateway with DB2 on Solaris, you must copy the `NetQ` directory from the installation CD to the DB2 directory on the Everyplace Wireless Gateway machine after installing the Everyplace Wireless Gateway. For example, using WebSphere Everyplace Suite installation CD number 3, copy the contents of `db2/sun/NetQ` to `/opt/IBMdb2/NetQ`.

Installing DB2 on Solaris

If you install DB2 on Solaris, which is required if you wish to select SecureWay Directory or Everyplace Wireless Gateway, the Everyplace Suite install

(Installer.class) will check if the file system /home is writable. If /home is not writable, you will receive an error message and the install will end. To avoid this occurrence, you must edit the following files:

- /etc/auto_master
- /etc/auto_home

Comment out the line starting with /home in auto_master, and remove the line reading +auto_home from auto_home, and restart the machine.

If you install DB2 on Solaris, the following messages may appear on the terminal where the shell script install.sh is running:

```
UX: usermod: ERROR: Invalid syntax.
UX: usermod: ERROR: root is in use. Cannot change it.
```

Ignore these messages.

Launching the DB2 Universal Database Control Center on Solaris

To launch the DB2 Universal Database Control Center on Solaris, you must issue the following command from the terminal window:

```
 ln -s /home/db2as /export/home/db2as
```

You will then be able to launch the DB2 Universal Database Control Center from the Everyplace Administration Console.

Removing DB2 from Solaris

There are many combinations of Everyplace Suite installations, and the following instructions will work in most cases. However, there may be a configuration that was not completely tested. Any deviation from these steps will probably result in what appears to be a successful uninstall. An unsuccessful uninstall will not be detected until the reinstall fails. If the reinstall fails, try the uninstall process again.

1. Stop all the UDB processes as follows:
   a. Switch to the Solaris instance user ID. If SecureWay Directory is installed, then the user ID is normally ldapdb2. For the other products (Tivoli Personalized Services Manager and Everyplace Wireless Gateway), the user ID is normally db2as. For example:

      If SecureWay Directory is installed, enter: `su - ldapdb2`

      If the other products are installed, enter: `su - db2as`

   b. Stop the instance processes. For example, enter:

      `db2 force applications all`

      `db2 terminate`

      `db2stop`

      `db2licd end`

      `exit` (ldapdb2 only)

   c. Switch to the Solaris DB administrator user ID. The user ID is normally db2as, but it may not have been created. For example, enter:

```
su - db2as
```

   d. Stop the administrator process. For example, enter:

```
db2admin stop
exit
```

2. Drop the DB2 instances as follows:

   a. From the root user ID, change to the DB2 directory. This is normally /opt/IBMdb2/V7.1.

   b. Confirm the instance name(s). The name displayed is normally db2inst1, but it may also show ldapdb2 or wgdb. For example, enter:

```
./bin/db2ilist
```

   c. Drop the instance name(s). For example, enter:

```
./instance/db2idrop  db2inst1
./instance/db2idrop  ldapdb2
./instance/db2idrop  wgdb
```

   Use the force option, -f, if necessary.

   d. Confirm the DB administrator name. The name displayed is normally db2as. For example, enter:

```
./bin/dasilist
```

   e. Drop the DB2 instance. For example, enter:

```
./instance/dasidrop  db2as
```

3. Use the ADMINTOOL to delete the DB2 user IDs that correspond to the DB2 instances found above. This is normally db2inst1, db2as, ldapdb2, and wgdb. Select the /home directory to be deleted. Do not delete any other user IDs.

4. Remove the Everyplace Suite products, clean up the system, and reinstall the Everyplace Suite products as follows:

   a. Run the Everyplace Suite uninstall program to remove the products. For example, enter:

```
/opt/IBMEPSIn/uninstall.sh
```

   b. Remove the files not removed by the uninstall. Depending on the product group, some files and directories may not exist. Save any configuration files prior to running the remove commands. For example, enter:

```
rm -r /opt/IBM*
rm -r /db/db2
rm -r /var/db2
rm -r /var/ldap
```

   c. Reboot the machine to clean up running processes.

   d. Run the Everyplace Suite install program to reinstall the products. For example, enter:

```
/cdrom/cdrom0/install.sh
```

Installing Tivoli Personalized Services Manager

Verify that links are set to the IBM C for AIX Compiler Version 5.0 or higher prior to installing Tivoli Personalized Services Manager, so that the system can access the compiler during Tivoli Personalized Services Manager installation and configuration. To reestablish all the links on AIX, execute the following script:

```
/usr/vac/bin/replaceCSET
```

If you install Tivoli Personalized Services Manager in a distributed environment, the System Management subcomponent's Reporting application must be able to connect to the Tivoli Personalized Services Manager database. To use the Reporting application, you must install the System Management subcomponent on the same machine as the Database Integration subcomponent or with the RADIUS subcomponent that uses a database client.

Device Agents

Device agents for Windows CE, used in the Tivoli Personalized Services Manager Device Manager subcomponent, are contained in the following directories:

- For AIX:

  ```
  /usr/lpp/TivDMS/agents/wince
  ```

- Solaris:

  ```
  /opt/TivDMS/agents/wince
  ```

If you experience difficulty in downloading these agents, contact your IBM service representative and request the application of APAR IY14335.

You may find the device agent `aero8000.CAB` in one of the following directories:

- For AIX:

  ```
  /usr/lpp/TivDMS/agents/aero8000
  ```

- Solaris:

  ```
  /opt/TivDMS/agents/aero8000
  ```

Do not use this agent. Instead, use `ceagent.sh4.CAB`. Contact your IBM service representative and request the application of APAR IY14335 as described in the preceding paragraph.

Device Management Server

Following Device Management Server installation, it is recommended that you stop and restart the WebSphere Application Server and the IBM HTTP Server in the following order:

1. Restart IBM HTTP Server.
2. Restart WebSphere Application Server.

Installing the Tivoli Personalized Services Manager RADIUS subcomponent on a Solaris system

Install the Tivoli Personalized Services Manager RADIUS subcomponent on a Solaris system as follows:

1. Install the Tivoli Oracle integration package on Solaris from CD number 8. See “Installing the Oracle Database using the Oracle8i CD” on page 51.
2. Create a destination directory for the Oracle Client by entering:

   ```
   mkdir /db
   ```

3. Insert the Oracle CD and verify that the CD is automatically mounted correctly. If not, eject and reinsert the Oracle CD.
4. Enter:

   ```
   cd /opt/TivTSM/install/db/oracle
   ```

5. At the command line, enter the commands:

   ```
   DISPLAY=:0.0
   xhost +
   PATH=$PATH:/opt/TivTSM/install/db/oracle
   ./TSMOracle8i -c
   ```

6. After the Tivoli Personalized Services Manager RADIUS subcomponent is installed by the Everyplace Suite installer, edit file `/opt/TivTSM/radius/bin/start_radius.ksh` as follows:

   Add line:

   ```
   TNS_ADMIN=$ORACLE_HOME/network/admin; export TNS_ADMIN
   ```

   immediately after line:

   ```
   ORACLE_HOME=/db/app/oracle/products/8.1.5; export ORACLE_HOME
   ```

   Note: If you install the Oracle client and Oracle server on separate machines, a setup inconsistency may occur between the two machines which could prevent successful database connections from client to server. This inconsistency will cause difficulty in using the reporting and RADIUS scripts on the client machine. The affected scripts are as follows:

   ```
   reporting_job_ora.ksh
   reporting_deljob_ora.ksh
   start_radius.ksh
   reload_radius.ksh
   ```

   To solve this problem, copy the following files from the Oracle server machine to the Oracle client machine, replacing the original files on the client:

   ```
   /db/app/oracle/product/8.1.5/network/admin/tnsnames.ora
   /db/app/oracle/product/8.1.5/network/admin/sqlnet.ora
   ```

Enabling the JDBC app driver for Tivoli Personalized Services Manager

You can improve Tivoli Personalized Services Manager performance by using the app driver as the JDBC driver for DB2. The procedure used to enable the DB2 app driver depends on the location of the Tivoli Personalized Services Manager applications and DB2 server.

If the Tivoli Personalized Services Manager applications and DB2 server are installed on the same machine, you only have to change the properties and scripts.

If the Tivoli Personalized Services Manager applications and DB2 server are installed on different machines, perform the following:

1. Install and set up a DB2 client.
2. Change properties and scripts.

For either scenario, refer to the following sections in the *TPSM-Overview.htm (Tivoli Personalized Services Manager Documentation) Planning and Installation* section located on CD number 8 (`tsm/aix/db2/TPSM-Overview.htm` or `tsm/sun/db2/TPSM-Overview.htm`):

- Installing DB2 Database
- Post-Installation

Installing Tivoli Personalized Services Manager with DB2 or Oracle on Solaris

If you install Tivoli Personalized Services Manager with DB2 or Oracle on Solaris, the installation process incorrectly creates a hard link between the `/opt/TivTSM/doc` and `/opt/TivTSM/sysmgmt/content/doc` directories by running the `link` command as follows:

```
link /opt/TivTSM/doc /opt/TivTSM/sysmgmt/content/doc
```

After installing Tivoli Personalized Services Manager with either DB2 or Oracle on Solaris, run the following two commands to break the link between the directories:

```
unlink /opt/TivTSM/sysmgmt/content/doc
ln -s /opt/TivTSM/doc /opt/TivTSM/sysmgmt/content/doc
```

Installing WebSphere Transcoding Publisher

Any time that you install WebSphere Transcoding Publisher, contact your IBM service representative and request the application of APAR IC29792.

Installing WebSphere Transcoding Publisher on Solaris

Installing WebSphere Transcoding Publisher on Solaris in an Everyplace Suite environment requires the installation of different versions of JDK. Everyplace Suite requires JDK 1.1.8 and WebSphere Transcoding Publisher requires JDK 1.2.2. WebSphere Transcoding Publisher scripts set the JAVA_HOME variable to `/usr/java`. The `/usr/java` directories may be linked to the `/usr/java1.1` for JDK 1.1.8, thus causing JAVA errors when running the scripts.

To resolve this problem, either define the JAVA_HOME environment variable to be either `/usr/java1.2` or `/usr/java_dev2` prior to invoking the scripts, or manually modify the scripts in the `/opt/IBMTrans` directory and change the setting of the JAVA_HOME variable inside the script files. There are many script files in `/opt/IBMTrans` which define JAVA_HOME that may need to be updated, such as `RunTranscoding.sh`, `AdminConsole.sh`, `SetupWizard.sh` and `RASCollect.sh`.

Installation of device clients and applications

The following Everyplace Suite components have associated clients and client development applications that must be installed on pervasive devices or other platforms. Refer to the corresponding documentation for information on installing and working with these clients and applications.

Everyplace Wireless Gateway

The Everyplace Wireless Gateway includes the Wireless Client, which is used to connect pervasive devices to the Wireless Gateway. The client information can be found in the *Everyplace Wireless Gateway Administrator's Guide.* This book and additional information can be found at:

http://www.ibm.com/pvc/enterprise

The Wireless Client driver is located on CD number 11 in the following directory:

```
/ewg/clients
```

Tivoli Personalized Services Manager (Device Manager)

The Device Manager (a feature of Tivoli Personalized Services Manager) includes device agents that are installed on target pervasive devices. Information about installing these agents can be found in the Device Manager: Device Plug-in Notes. See 6 for instructions on accessing the Device Manager Plug-in Notes.

MQSeries Everyplace

MQSeries Everyplace consists of Java and C components that enable solution developers to create an MQSeries Everyplace gateway and client on a variety of devices and platforms.

The native C client version of MQSeries Everyplace is not installed with the Everyplace Suite. It can be downloaded from:

http://www.ibm.com/software/ts/mqseries/

The following MQSeries Everyplace technical documentation is available online:

- *Introduction*
- *Programming Guide* (for Java)
- *Programming Reference* (for Java)
- *Native Client Information* (for C)

These books and additional information can be found at:

http://www.ibm.com/software/mqseries/library/#books

Everyplace Synchronization Manager

For installation instructions for the Synchronization Manager clients, see the documentation in `/esm/docs` on CD number 11 of the Everyplace Suite product CDs.

Troubleshooting

If errors occur during installation, you will be notified of the specific problem. Follow the instructions indicated by the error message. Some problems may require termination of the installation program. During installation, all actions and outcomes are logged to an install log file in `/tmp/everyplace.log`. This file contains a sequence of information that can assist you in identifying and analyzing problems. The `everyplace_install.trace` file is also available in the /tmp directory and contains details about the program execution. These files are in ASCII text format and can be viewed using any text editor.

Note the following items to avoid or resolve any problems installing the Everyplace Suite.

- **Install window disappears on Solaris systems:** If you click in the background area outside the install window, the install window goes to the background and is not visible. To bring the install window back in view, press the **Alt-Tab** keys simultaneously.
- **Remote X-Window session install does not work:** Installation of Everyplace Suite components must be done on an AIX or Solaris X-Window workstation. Installation from a remote X-Window session or emulator is not supported and may cause problems.
- **Trouble installing WebSphere Transcoding Publisher on Solaris systems:** On Solaris systems, there should be no Everyplace Suite entries in the `/vol/dsk` directory prior to installing WebSphere Transcoding Publisher. To remove any entries, type the command `rm /vol/dsk/everypl*` before starting the Everyplace Suite installation program.

The `everyplace.log` file is cumulative over multiple Everyplace Suite installations. However, the `everyplace_install.trace` file is reinitialized on each Everyplace Suite installation. If you want to keep the problem determination information from an install, you must save the `everyplace_install.trace` file before a new Everyplace Suite installation.

Chapter 5. Configuring the Authentication Server

This chapter provides information on configuring the Authentication Server. You can perform the following configuration tasks:

- Edit Authentication Server information in SecureWay Directory for all Authentication Servers within an Everyplace Suite domain.
- Configure the Authentication Server as a reverse proxy. This configuration enables the Authentication Server to route client requests to another server.
- Configure the Authentication Server for redirection. This configuration enables the Authentication Server to route client requests to one of several servers.
- Perform operations tasks, including suspend, resume, refresh, display, flush, and starting and stopping the active session table (AST) cleanup daemon.

Note: If you install the Authentication Server in transparent proxy mode, you must set the server address and port number of the Edge Server Caching Proxy in the Netscape Navigator HTTP proxy setting panel before attempting to open the Caching Proxy from the Everyplace Administration Console.

Configuring Authentication Server information in SecureWay Directory

Common and unique Authentication Server settings are initially configured during installation. Common entries can be accessed and administered from SecureWay Directory for all Authentication Servers within an Everyplace Suite domain after configuration on one Authentication Server within the domain. Unique entries must be configured for each Authentication Server installed within the domain.

After installation, if the Authentication Server requires a particular configuration setting, it will search first the unique and then the common settings of SecureWay Directory. If the setting is not located within SecureWay Directory, the Authentication Server will search its configuration file `ibmwesas.conf`.

If the configuration setting is not located in the configuration file, the Authentication Server will use a hard-coded default value for some numeric configuration settings, such as **maximum RADIUS retries**.

To change Authentication Server settings after installation is complete, you must edit the settings in SecureWay Directory. You can use the Directory Management Tool to locate Authentication Server settings in SecureWay Directory. Refer to *http://www.ibm.com/software/network/directory/library/publications/31/dmt/dparent.htm* for instructions on using the Directory Management Tool.

To configure the Directory Management Tool, edit the `/etc/dmt.conf` DMT configuration file. For example, if the property file contains these lines:

```
#browser=
#tolbar=both
server1.url=ldap://localhost:389
#server1.security.bindDN=
#server1.security.password=
#server1.security.ssl.keyclass=
#server1.secuirty.ssl.keyclass.password=
#server1.admin.url=http://webserver:80
```

You need to set the bindDN and password entries and remove ″#″ at the beginning of those lines to effect your changes. For example:

```
server1.security.bindDN=cn=adminusr
server1.security.password=pssword
```

To start dmt, type `dmt` at the command line.

The Directory Management Tool opens a tree view of SecureWay Directory as shown in Figure 8 on page 75:

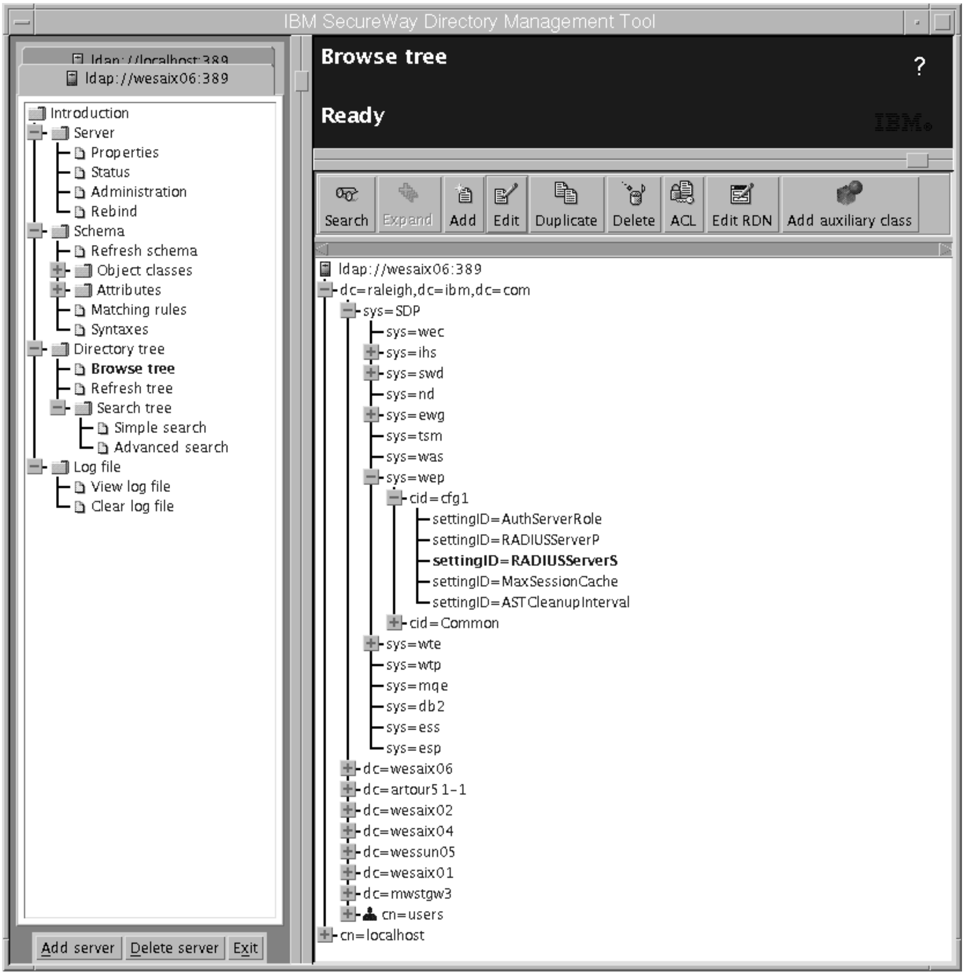


Figure 8. Directory Management Tool view of Everyplace Suite Information in SecureWay Directory

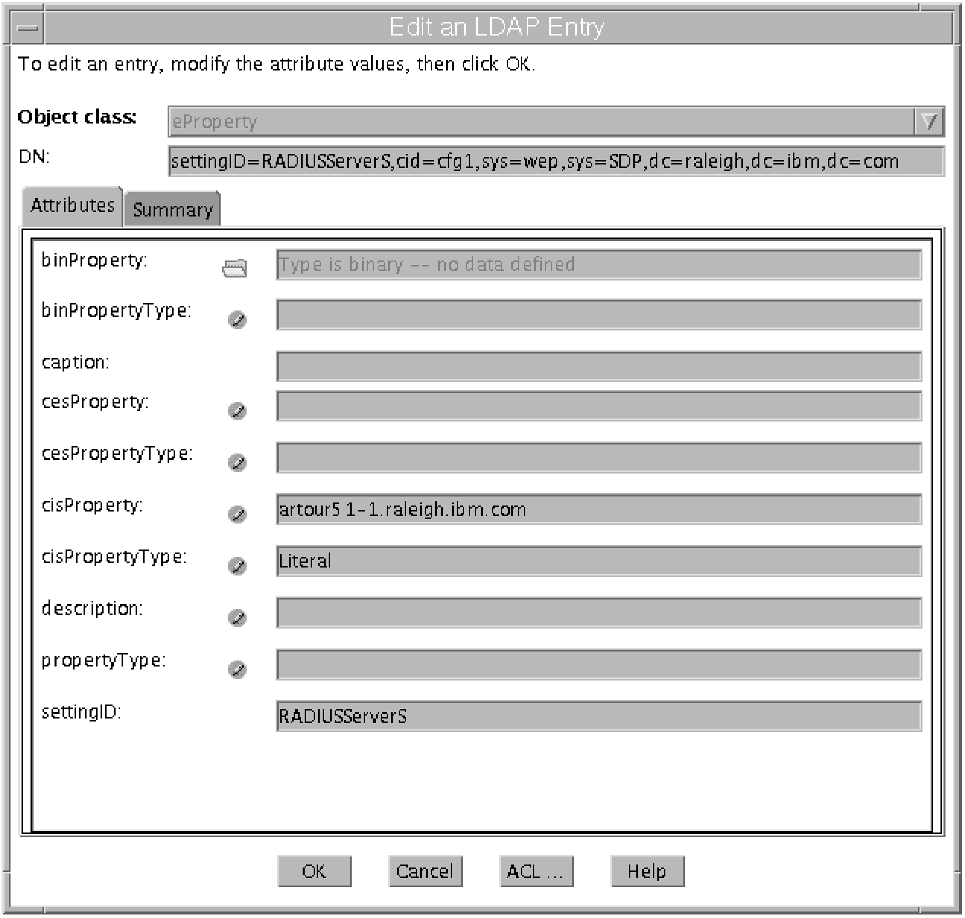
The **cid** object indicates the type of Authentication Server setting. The **cid** for all common Everyplace Suite Authentication Server settings is *common*. The **cid** for unique Everyplace Suite Authentication Server settings is a generated token with an *eServicePtr* attribute that matches the hostname of the Authentication Server.

The **sys** object indicates the name of the Authentication Server subsystem. The **sys** for all Everyplace Suite Authentication Server settings is *wep*.

In order to change an Authentication Server setting, perform the following:

1. Use Directory Management Tool to open a tree view of SecureWay Directory.
2. Click the **Search** button in the right-hand pane of the tree view to bring up a query screen.
3. Specify the following information to locate the setting:

   - object class: The object class for all Authentication Server settings is *eProperty*.
   - settingID: Name of the Authentication Server setting you want to change.
4. If the search results in multiple Authentication Server settings, use the **cid** and **sys** objects to locate the desired setting. For a unique Authentication Server setting, perform a search on the *eServicePtr* attribute of the **cid** object, which will match the hostname of the Authentication Server.
5. After you locate an Authentication Server setting, a configuration dialog is displayed, as shown in Figure 9.



Edit an LDAP Entry

To edit an entry, modify the attribute values, then click OK.

Object class: eProperty

DN: settingID=RADIUSServerS,cid=cfg1,sys=wep,sys=SDP,dc=raleigh,dc=ibm,dc=com

binProperty: Type is binary -- no data defined

binPropertyType:

caption:

cesProperty:

cesPropertyType:

cisProperty: artour51-1.raleigh.ibm.com

cisPropertyType: Literal

description:

propertyType:

settingID: RADIUSServerS

Figure 9. SecureWay Directory entry configuration dialog

Edit the **cisProperty** field to configure the Authentication Server setting.

You must use the correct format to configure Authentication Server settings. For example, in the figure above, you must use a literal (character) format to configure the **RADIUSServerS** setting. The **cisPropertyType** field indicates the format you will use to configure the setting.

A description of the Authentication Server settings, the settingID, and the cisPropertyType for each setting is provided in Table 7.

Table 7. Authentication Server entries

Authentication Server Entry	Description	SettingID	cisProperty Type
Maximum RADIUS Retries	The maximum number of times the Authentication Server sends a UDP authentication request to a RADIUS server before it stops trying.	MaxRADIUSRetries	Number
RADIUS Shared Secret	The password shared between the RADIUS server and RADIUS client that allows them to perform mutual authentication.	RADIUSSharedSecret	Literal
Maximum RADIUS Retry Timeout	The maximum amount of time, in milliseconds, an Authentication Server waits for a response from a RADIUS server before sending another request for access. The Authentication Server will wait for a response as many times as the specified maximum number of RADIUS retries.	MaxRADIUSTimeout	Number
Maximum Session Age	The maximum amount of time, in minutes, an Authentication Server maintains information about a user's session. After this time has passed, the Authentication Server will clear the information. Authentication Server resources, such as disk space, are used while the information is maintained. But once the information is cleared, additional time may be necessary to recreate it.	MaxSessionAge	Number
Default Retry After Delay	When the Authentication Server is suspended by the administrator, requests to the RADIUS server are rejected. Default Retry After Delay is the default amount of time, in seconds, the device should wait to retry the request.	DefaultRetryDelay	Number

Table 7. Authentication Server entries (continued)

Authentication Server Entry	Description	SettingID	cisProperty Type
Authentication Server Role	The Authentication Server may serve as one of two proxy types or roles: as an authentication proxy that intercepts all requests made to resources within the Everyplace Suite, or as a transparent authentication proxy that allows access to content provided by third-party content servers while taking advantage of Everyplace Suite authentication and transcoding.	AuthServerRole	Literal
Primary AST Server Name	The host name of the primary server that is used to manage the active session table and its entries.	ASTServerP	Literal
Secondary AST Server Name	The host name of the backup server, if applicable, that is used to manage the active session table and its entries.	ASTServerS	Literal
Primary RADIUS Server Name	The host name of the primary RADIUS Authentication Server.	RADIUSServerP	Literal
Secondary RADIUS Server Name	The host name of the backup RADIUS Authentication Server, if applicable.	RADIUSServerS	Literal
Maximum Session Cache Size	The maximum size of the local in-memory cache for a particular proxy.	MaxSessionCache	Number
AST Daemon Cleanup Interval	The amount of time, in seconds, in which session information should be cleared from the active session table server.	ASTCleanupInterval	Number

Selecting a Secondary Active Session Table server

If you select **None** for the Secondary Active Session Table (AST) server name on the Authentication Server **Configuration** panel, the following message is logged in to the `/opt/IBMWTE/usr/internet/server_root/logs.error`, `(DATE)` file.

```
wesauth0501: Invalid hostname for Active Session Table Server: None.
```

Ensure the host domain name resolution is working correctly. If you select a valid Primary Active Session Table Server, you can ignore this message.

Configuring device and network types

The Authentication Server identifies devices associated with incoming requests based on mapping rules defined in the device profiles stored in SecureWay Directory (see the *WebSphere Transcoding Publisher Administrator's Guide* for information about configuring device profiles and the device mapping rules). If the Authentication Server cannot determine a device type based on the available mapping rules, the Authentication Server will use a default network or device type to implement transcoding. The default network type is GENERIC_WIRELESS. The default device type is `default`.

To change the default network or device type, open the file where the SecureWay Directory parameters are stored and search for the following:

```
default_device_type
```

or

```
default_network_type
```

You can select one of the following options for the default device type.

Note: The device type names are case-sensitive.

- WML-Device: Any WAP-compliant device (pre-defined default)
- Palm-Pilot3 HandWeb11: Palm Pilot HandWeb Browser
- NT.InternetExplorer4: MS Internet Explorer browser (version 4)
- NT.InternetExplorer: MS Internet Explorer browser (version 5)
- NT.Netscape45: Netscape Navigator browser (version 4+)
- WinCE.PocketIE20: MS Windows CE-compatible device
- I-Mode 501: Wireless Phone - I-Mode Model 501i
- I-Mode 2 Color Phone: Wireless Phone - I-Mode 2 Color Model
- I-Mode 2 Monochrome: Wireless Phone - I-Mode 2 Monochrome Model

Note: Any valid device type as defined in the WebSphere Transcoding Publisher device preference profiles is allowed.

You can select one of the following options for the default network type:

- GENERIC_WIRELESS: Any wireless network (pre-defined default)
- GENERIC_DIAL: Dial-up network
- LAN: Direct-connected or LAN

Note: Generally, you should choose a network type with the lowest bandwidth that your enterprise supports as the default.

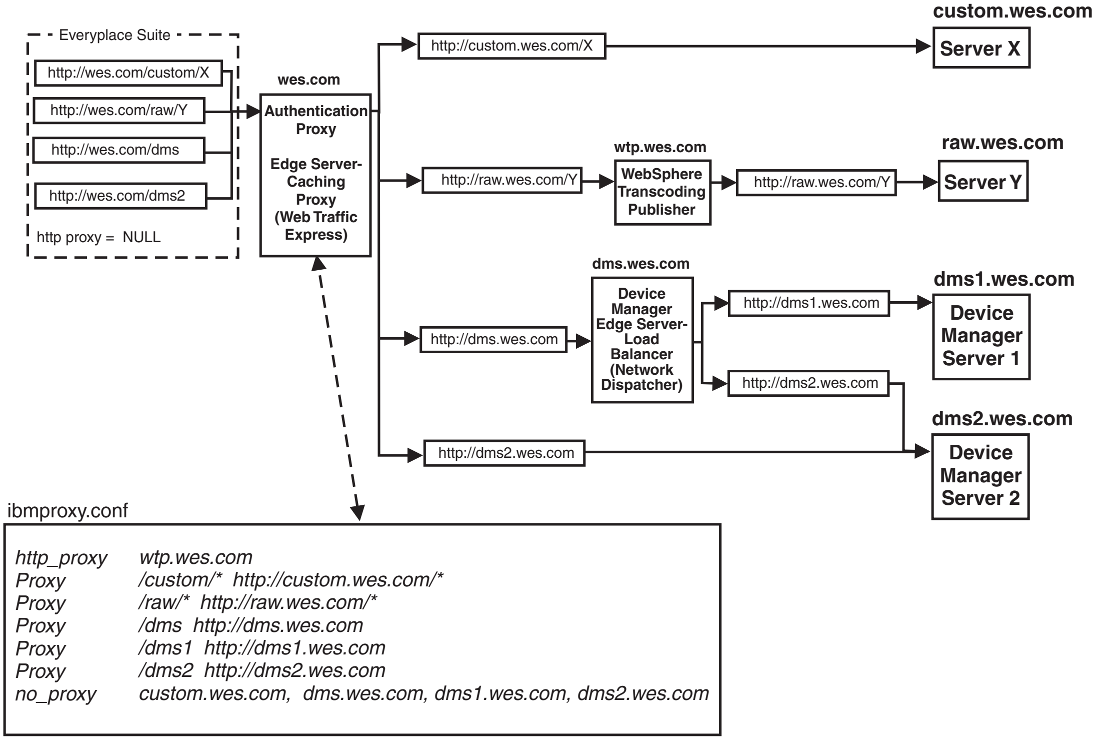
Configuring the authentication proxy as a reverse proxy

If you are using the Everyplace Suite Authentication Server in authentication proxy mode, then you must configure the authentication proxy as a reverse proxy. In this configuration, the authentication proxy accepts client requests, then routes those requests to another server. The authentication proxy appears to the client to be the content server, and the client is not aware that the request has been sent to another server. For more information regarding reverse proxy configuration, refer to the *Edge Server Caching Proxy (Web Traffic Express) User's Guide*, which can be found at *http://www.ibm.com/software/webservers/edgeserver/library.html*

There are two sample configuration files available on CD number 8 to help with configuring the Authentication Server. There is one each for both the authentication proxy mode and for the transparent proxy mode. The files are:

- `ibmproxy_ap.conf` - authentication proxy
- `ibmproxy_tp.conf` - transparent proxy

Figure 10 on page 81 shows the configuration of the authentication proxy as a reverse proxy.



```
http_proxy    wtp.wes.com
Proxy         /custom/*  http://custom.wes.com/*
Proxy         /raw/*  http://raw.wes.com/*
Proxy         /dms  http://dms.wes.com
Proxy         /dms1  http://dms1.wes.com
Proxy         /dms2  http://dms2.wes.com
no_proxy      custom.wes.com,  dms.wes.com, dms1.wes.com, dms2.wes.com
```

Figure 10. Configuring the authentication proxy as a reverse proxy

Proxy statements, shown in the *ibmproxy.conf* portion of Figure 10, are used to route Everyplace Suite client requests from the authentication proxy (*wes.com*, above) to the application servers. You must create a proxy statement in the *ibmproxy.conf* file for each distinct URL that is used by an application. The proxy statement consists of the authentication proxy path name (for example, */custom/**, Figure 10) and the distinct URL (*http://custom.wes.com/**, Figure 10). Caching Proxy maps the URL in the Everyplace Suite domain through the authentication proxy to the actual content or application on the server.

You must also create two additional proxy statements that indicate whether the request will use transcoding after it goes through the authentication proxy.

1. The first proxy statement in the *ibmproxy.conf* file must be an **http_proxy** statement. This statement is used for requests that pass through a transcoder and consists of the host name of the WebSphere Transcoding Publisher instance that is used as the default Everyplace Suite transcoder (*wtp.wes.com*, above).
2. The last proxy statement in the *ibmproxy.conf* file must be a **no_proxy** statement. This statement is used for requests that do not pass through a transcoder (for example, the Tivoli Personalized Services Manager Device Manager feature, MQSeries Everyplace, or any custom content services). This statement, shown in

the bottom line in the *ibmproxy.conf* portion of the figure, consists of a list of domains and causes the Caching Proxy to override the **http_proxy** directive for those domains.

Additional configuration required for redirection

Redirection occurs when a client request is routed to another server, such as for load balancing or to obtain information or services from another server. To maintain Everyplace Suite single sign-on capability, redirected target URLs must be to the same host as the authentication proxy.

For example, if a user requests a device management operation, and there are multiple device management servers (managed by Load Balancer) which can service the request, the redirected requests must be routed back through the authentication proxy. In order to enable this capability, you must specify a parameter value for an authentication proxy URL, **authProxyDmsUrl**, during creation of the Device Manager server, which occurs during the configuration of the WebSphere Application Server.

During enrollment, when the Device Manager attempts to redirect a device, it checks the application server to determine whether **authProxyDmsUrl** was defined. If so, Device Manager uses the parameter value specified for **authProxyDmsUrl** to compose a redirection URL. If **authProxyDmsUrl** was not defined, Device Manager computes the redirection URL as it always has.

During redirection, the redirection URL computed especially for authentication proxy support causes the device to be rerouted through the authentication proxy and on to the correct destination, usually Tivoli Personalized Services Manager’s subscription services or a particular Device Manager server.

For additional details on how Device Manager handles authentication and redirection, refer to *Device Manager: Planning and Installation*.

Enabling the Authentication Server to access the RADIUS and active session table servers

After installing the Authentication Server, you must configure Tivoli Personalized Services Manager so that the network access server (NAS) password matches the SHARED_SECRET Authentication Server entry. This configuration adds the Authentication Server to the RADIUS and active session table servers as a client and enables the Authentication Server to acess the RADIUS and active session table servers. If necessary, you can look up the value of the SHARED_SECRET Authentication Server entry using the Directory Management Tool (see “Configuring Authentication Server information in SecureWay Directory” on page 73 for more information on using the Directory Management Tool). The parameters you need to know to locate the SHARED_SECRET entry are:

- settingID=RADIUS_SHARED_SECRET
- cid=common
- sys=wep
- sys=SDP, <your suffix>

Configure the Tivoli Personalized Services Manager as follows:

1. Use the Tivoli Personalized Services Manager Director Tool to add a RADIUS client that will enable the Authentication Server to access the RADIUS server. To do this:
   a. Open the Director Tool and double-click **TISM**.
   b. Select **RADIUS**, then expand the RADIUS tree view.
   c. Select **Clients**.
   d. Right-click **Clients**, then select **Add**.
   e. Enter the following data:
      - Frame ID and NASID=Authentication Server IP Address
      - NAS Name=Authentication Server Host Name
      - NAS Password=Value of RADIUS_SHARED_SECRET
      - Select the default values for the remaining arguements.
   f. Click **Add**.
   g. Restart the RADIUS Server as follows:
      1) From the Tivoli Personalized Services Manager RADIUS server, enter the `su - tsmuser` command (for Oracle database root userid is sufficient).
      2) Enter the command:`cd /usr/TivTSM/radius/bin`
      3) Run the "`./reload_radius_db2.ksh`" script (for Oracle database, use the command: `./reload_radius.ksh`).
2. Modify the Tivoli Personalized Services Manager active session table server as follows:
   a. From the active session table console, enter the `exit` command.
   b. Enter the `cd/usr/TivTSM/ast/bin` command.
   c. Modify the active session table server's `AST.properties` file to add the Authentication Server's IP address to the active session table server's client list.
   d. Restart the active session table server by entering the `/ASTServer.ksh` script.
3. Stop and restart the Authentication Server as follows:
   a. Check for any Caching Proxy processes by entering the (`ps –ef | grep ibmproxy`) command.
   b. If any Caching Proxy processes are found, enter the `stopsrc -s ibmpproxy` or `kill -9 <process id>` command to stop the process.
   c. Restart the Authentication Server by entering the `ibmproxy` command.

Authentication proxy error messages in Solaris

After you finish configuring the authentication proxy in Solaris, check the Caching Proxy console and log for error messages (refer to the *Edge Server Caching Proxy User's Guide* at *http://www.ibm.com/software/webservers/edgeserver/library.html* for more information). If an error message occurs, you should stop and restart the Caching Proxy process. You should also shut down and restart the Solaris system after each reconfiguration of the authentication proxy.

Debugging the Authentication Server

The Authentication Server contains two modules: `wesauth.so` and `wesauth.so.debug`. Use the `wesauth.so.debug` module to debug the Authentication Server. In order to switch to the debug module, rename the `wesauth.so` module to any desired name, and then rename the `wesauth.so.debug` module as `wesauth.so`.

The `ibmwesas.conf` file should have the following statement to enable debugging: `debugLevel 10`. This statement should be the first statement in the file to allow debugging for processing the rest of the file. The number 10 specifies a level which tells how much output will be given. A higher number specifies more output.

Performing operations tasks

The Authentication Server `authserv` command line utility can be used to control and monitor the Authentication Server plug-in while it is running. For security reasons, the utility must run on the same system as the Authentication Server. The *authserv* utility lets you perform certain operations tasks on the Authentication Server, including suspending and resuming the Authentication Server, refreshing configuration settings, and displaying operational statistics.

The *authserv* program has the following syntax:

```
authsrv [-?| -help] [-p:serverPort] [funcname[args,,,]] ]
```

Arguments:

- —? or —help: Displays help information for the program. Issuing the *help* function name will display a list of functions supported by the server.
- —p: Sets the TCP port on which to connect to the server. The port is configured in *ibmwesas.conf*. A default port of 9734 is used.
- *funcname*: The function to be executed on the server. See Table 8 on page 85 for more information.
- *args*: Any arguments for the function.

If you specify a function name on the command line, that function will be sent to the server. Once the response and output is received, the client will terminate the session and exit.

If you do not specify a function name or help options, the program will establish a session with the server, enter a command loop reading from standard input (stdin), and wait for you to enter a function name with optional arguments. You can exit the program by specifying one of the following function names:

```
quit
```

or

```
exit
```

The operations tasks that you can perform using the `authserv` program are shown in Table 8 on page 85:

Table 8. Operations tasks for the authserv program

Function Name	Argument(s)	Description
suspend	[Retry-After delay (seconds)]	Stops normal operation of the Authentication Server instance. Any requests received while suspended are rejected with a 503 status code specifying a Retry-After value as passed in. If no value is specified, then the default Retry-After value is used.
resume		Begins normal operation of the Authentication Server instance after suspension.
refresh	[configuration file path]	Updates the Authentication Server's active configuration settings by forcing a read of the specified configuration file and of SecureWay Directory. If no configuration file is specified, only a SecureWay Directory read is performed. Refresh performs an implicit suspension of the Authentication Server. The Caching Proxy must be shut down separately to refresh the Caching Proxy settings.
display		Returns operational statistics.
flush		Flushes the session cache for all users.
start_daemon		Starts the active session table clean-up daemon.
stop_daemon		Stops the active session table clean-up daemon.
help		Returns a list of functions supported by the server.
quit		Causes the session with the client to be terminated.

If an operations command fails, information on the failure will be reported to either the command line console or to the Caching Proxy console.

Chapter 6. Configuring and administrating the Everyplace Suite

This chapter provides information on performing the following tasks for the Everyplace Suite:

- "Rebooting"
- "Enrolling subscribers and adding mobile devices" on page 88
- "Third-party gateway support" on page 90
- "Changing the SecureWay Directory and administrator passwords" on page 95
- "Configuring Tivoli Personalized Services Manager" on page 96
- "Configuring Everyplace Wireless Gateway" on page 97
- "Using the Everyplace Administration Console" on page 99

Rebooting

IBM HTTP

If you reboot a server where IBM HTTP is installed, you must restart the IBM HTTP server by entering the following command:

- For AIX:

  ```
  /usr/HTTPServer/bin/adminctl start
  ```

- For Solaris:

  ```
  /opt/IBMHTTPD/bin/adminctl start
  ```

SecureWay Directory server

In the Everyplace Suite environment, the SecureWay Directory server is configured to start automatically when the system reboots; however, it may not always restart automatically. After a reboot, ensure the SecureWay Directory server has started by entering the following:

```
ps -ef | grep slapd*
```

If the SecureWay Directory server is running, the following messages should appear:

```
/bin/slapd -f /etc/slapd32.conf
```

If the SecureWay Directory server does not start automatically after rebooting, you must start it manually as follows:

1. For AIX, enter the following at the command line:

   ```
   chgrpmem -m + root dbsysadm
   chgrpmem -m + root db2asgrp
   ```

2. After typing the commands in Step 1 (AIX only), use the instructions in the following locations to start the SecureWay Directory manually:

   - For AIX:

     ```
     /usr/ldap/web/en_US/config/aparent.htm
     ```

   - For Solaris:

```
/opt/IBMldaps/web/en_US/config/sparent.htm
```

DB2 listener

For Tivoli Personalized Services Manager to connect to DB2, the DB2 listener must be listening on port 6789. The DB2 listener must also be running on any system where a Tivoli Personalized Services Manager component is installed. If you reboot the system, or if the DB2 listener is not running, you must start the DB2 listener `db2jstrt 6789` manually before starting the `/etc/rc.txservers` transaction server.

You can determine whether the DB2 listener is running, by issuing the following command:

```
ps -ef | grep db2jd
```

You can start the DB2 listener by issuing the following commands:

```
su - db2inst1
db2jstrt 6789
```

WebSphere Application Server

If WebSphere Application Server is installed on a machine, you must stop WebSphere Application Server before rebooting that machine. You will stop the WebSphere Application Server as follows:

1. Start the WebSphere Application Server administration console from either the Everyplace Administration Console or by issuing the `./IBMWebAS/bin/adminclient.sh` command from the command line.
2. Stop the node (for example, the hostname of the machine) on the console.
3. After the machine reboots, you will restart the WebSphere Application Server by issuing the `./IBMWebAS/bin/startupServer.sh` command, and waiting until an `open for e-business` message is logged in the `./IBMWebAS/logs/tracefile` file.

Restarting Oracle on Solaris

After rebooting a Solaris machine that contains the Tivoli Personalized Services Manager Oracle database server, the Oracle database may not start. You can start the Oracle database manually as follows:

1. Log in as the root user on the Oracle database server machine.
2. Issue the following command:

   ```
   /etc/rc.oracle
   ```

Enrolling subscribers and adding mobile devices

You can enroll subscribers (also known as users) through Everyplace Suite using either Tivoli Personalized Services Manager or Everyplace Wireless Gateway. If you install both Tivoli Personalized Services Manager and Everyplace Wireless Gateway, you must define subscribers in Tivoli Personalized Services Manager. You can then view subscribers in Everyplace Wireless Gateway, using Gatekeeper. If you install Everyplace Wireless Gateway as the only component in the Everyplace Suite domain (stand-alone component), you can define subscribers in Gatekeeper.

You can add mobile devices using either Tivoli Personalized Services Manager or Everyplace Wireless Gateway. Use Gatekeeper to add mobile devices through the Everyplace Wireless Gateway.

Subscriber and device information can be found in the following documentation:

- Information on enrolling subscribers or adding mobile devices through the Everyplace Wireless Gateway is available through the Everyplace Wireless Gateway Administrator's Guide, which can be found at:

  dochttp://www.ibm.com/pvc/enterprise/mobile/references.shtml
- Information on enrolling subscribers through Tivoli Personalized Services Manager is available in the *Tivoli Personalized Services Manager Operations and Administration Guide*.
- Information on adding devices through Tivoli Personalized Services Manager is available through the following Device Manager Plug-In Notes:
  - Device Manager: PalmOS Plug-In Notes
  - Device Manager: Windows CE Plug-In Notes
  - Device Manager: Aero 8000 Plug-In Notes
  - Device Manager: NetVista Internet Appliance Plug-In Notes

Adding a device profile using WebSphere Transcoding Publisher

If you add a new device profile to Everyplace Suite using WebSphere Transcoding Publisher's Administration Console, you must stop and restart WebSphere Transcoding Publisher to make the new device profile be recognized by WebSphere Transcoding Publisher. You must also perform the following steps in order for the profile to be recognized in the system:

1. Choose any existing device profile cid entry (under the directory information tree's cn=″Device Profiles″ section) in the SecureWay Directory directory information tree and export it to a temporary file using `db2ldif`. Try to choose a device profile whose name has the same number of characters as the new profile's name in order to make editing easier. For example:

   ```
   db2ldif -o /tmp/newprof.ldif -s cid=WML-Device,cn="Device Profiles",
   sys=SDP,dc=raleigh,dc=ibm,dc=com
   ```
2. Edit the output file using any text editor as follows:
   - Delete all dn entries for settingID EXCEPT the one for ″deviceRule″.
   - Change the value for the deviceRule settingID (next to cesProperty) to the deviceRule value as entered in the WebSphere Transcoding Publisher Administration Console.
   - Change all occurrences of the old device name to the new device name as entered in WebSphere Transcoding Publisher Administration Console.

   Be careful when editing to maintain the line length for broken and continued lines to be 80 characters and to maintain the single space character at the beginning of continuation lines. This process is much easier if the copied profile's name and the new profile's name have the same number of characters.
3. Save the changes.

4. Import the changed file using ldif2db. For example:

   ```
   ldif2db -i /tmp/newprof.ldif
   ```

5. Refresh the Authentication Server's configuration or stop and restart the Authentication Server in order to make the change take effect.

Third-party gateway support

Version 1.1.3 of the Everyplace Suite allows the use of third-party gateways, which are gateways other than the Everyplace Wireless Gateway, if desired. The use of third-party gateways is supported by new function of the Authentication Server.

The Authentication Server will search SecureWay Directory for third-party gateway definitions and use that information to invoke a customer-supplied, gateway-specific C or C++ plugin routine that returns a client ID (for example, a phone number or device number) that identifies the user who initiated the HTTP request coming through the gateway. The Authentication Server uses the client ID to search the *cn=users* portion of SecureWay Directory for the ePerson entry whose client ID attribute matches the client ID returned by the plugin. The client ID attribute is configurable and is contained in the third-party gateway definition.

The plugin has access to Edge Server Caching Proxy (Web Traffic Express) APIs that return a specific HTTP header, the URL, the query string, and other information about the current request. If a matching ePerson entry is found, its user ID and organizational unit attributes are used to construct the ID placed on the X-IBM-PVC-User HTTP header, and the client ID is placed on an X-IBM-PVC-Client-id HTTP header. Both of these headers are then available for use by downstream components.

The Authentication Server will invoke the appropriate plugin when handling a request from a third-party gateway. The actual gateway-specific plugins will be written by IBM, the gateway providers, or customers.

Installing third-party gateway support

Install third-party gateway as follows:

1. Code the plugin routine for each third-party gateway you plan to use. Create a shared library containing the plugin and place it in an appropriate directory with appropriate file ownership and permissions. Shared libraries typically have an `.so` file extension and reside in `/usr/lib/`. Detailed plugin information is shown in "Customer-supplied, gateway-specific client ID plugin" on page 93.
2. Shut down Caching Proxy, so that the Authentication Server is no longer running. Make a backup copy of your existing Authentication Server shared library. The library is shipped with the Everyplace Suite as `wesauth.so` and is typically installed in `/usr/bin/`. Replace the library with `wesauth.so.debug` if you want to capture additional debugging information in the Caching Proxy log files. The file ownership and permissions must match those of the original `wesauth.so` library.
3. Choose a location in SecureWay Directory for each type of third-party gateway you plan to use.

Note: You do not have to choose a SecureWay Directory location for each instance of a particular type of third-party gateway.

This location must be under the baseDN (the Distinguished Name) specified in your Authentication Server configuration file, but **NOT** under the *cn=root*, *sys=ewg* entry, because that section is reserved for use by the Everyplace Wireless Gateway.

The configuration file is usually called `ibmwesas.conf`, and is installed in the following locations:

- For AIX:

  `/usr/lpp/IBMEPS.Auth/`
- For Solaris:

  `/opt/IBMEPSAu/`

For each gateway, add a gatewayDN statement to your Authentication Server configuration file. This statement specifies the gateway's location in the SecureWay Directory tree, relative to the baseDN. The syntax for this statement is:

```
gatewayDN DN_relative_to_baseDN
```

(for example: `gatewayDN cn=mygateway`).

4. Add the *wlGateway* and *wlMni* object classes if they are not already located within your SecureWay Directory schema. Use the SecureWay Directory administration Web pages to make a backup copy of the SecureWay Directory tree and schema (LDIF). Run the `wg_schema` program to add these object classes. To access the SecureWay Directory administration Web pages, point your browser to `/ldap` on the machine running the SecureWay Directory server (for example `http://dirserver2.company.com/ldap`). You must have a Web server running on the same machine as the SecureWay Directory server. The syntax is:

   ```
   wg_schema -h <ldap_server_hostname> -D <admin_DN> -w <admin_pw>
   ```
5. Use the Directory Management Tool (see Web site *http://www-4.ibm.com/software/network/directory/library/publications/31/dmt/dparent.htm* for instructions on using the Directory Management Tool). Add entries to the SecureWay Directory as follows:

   a. Add a container entry at the spot in the tree you identified on the *gatewayDN* statement in the configuration file. The RDN (Relative Distinguished Name) for this entry must match that on the *gatewayDN* statement. Continuing with the example above, you would use *cn=mygateway* as the RDN.

   b. Under the container entry add an ePropertySet. A typical RDN for this entry might be *cid=Common*, but the RDN is not important.

   c. Under the ePropertySet add the following eProperty entries:

      An entry with an RDN of *settingID=pluginName*. Set the entry's *cesProperty* attribute to the name of your plugin for this gateway. The plugin name must be of the form: `library_name:function_name` where *library_name* is the name of the shared library that contains `function_name`. An example plugin name is `myLibrary.so:getClientID`.

      An entry with an RDN of *settingID=clientIDAttributeName*. Set the entry's *cisProperty* attribute to the name of the attribute in the ePerson object that you will use to locate, in SecureWay Directory, the user associated with the client ID returned from your plugin. For example, if your plugin returns an MSISDN number, you could set this eProperty to internationalISDNNumber.

(optional) An entry with an RDN of *settingID=pluginToken*. Set the entry's *cesProperty* to a string token that you want passed to your plugin. Any use of the string token is defined solely by your plugin. For example, it could be used to pass in the name of an HTTP header, a gateway type, or a plugin version number.

d. Under the **container** entry, add *wlGateway* or *wlMni* entries to identify specific instances of the type of third-party gateway that you have installed. The RDN is not important (for example, `cn=mygateway1`). When adding a *wlGateway*, specify a structural object class of *wlGateway* and an auxiliary object class of *ibm-wlResource*. When adding a *wlMni*, specify a structural object class of *wlMni* and an auxiliary object class of *ibm-wlResource*.

   The *wlGateway* entry identifies a single gateway machine, while the *wlMni* entry can identify a range of IP addresses running such gateways. If you add a *wlGateway* entry, you must specify its hostname or IP address in the host attribute. If you add a *wlMni* entry, you must specify an IP address in the *netaddr* attribute and a mask in the *netmask* attribute; the mask is applied to the IP address to define a range of IP addresses.

6. Restart Web Traffic Express. If you installed the debug version of `wesauth.so`, you can set the debug message level via the `debugLevel` statement in the Authentication Server configuration file to provide debugging/progress information in one of the Caching Proxy log files.
7. As with all SecureWay Directory information used by the Authentication Server, if you change any of the SecureWay Directory information used in Authentication Server's third-party gateway, you must either issue an `authsrv refresh` command or stop and restart Caching Proxy. If you don't, the changes might not have any effect on Authentication Server operation.
8. You must now integrate ClientID support into the Tivoli Personalized Services Manager applications to assign unique IDs to Everyplace Suite users. For example, you could configure Customer Care to use ClientIDs as follows:
   a. For AIX, update the `/usr/TivTSM/custcare/content/JPanSearch.cfg` file to modify the following two lines.

   ```
   SP_Defined_1=MSISDN
   SP_Defined_2=
   ```

   b. Save the file.

   c. Re-start the customer care servlet using the WebSphere adminclient tool.

   d. When a customer service representative logs into CustomerCare, they will have the option to add or modify the value of the **MSISDN** field of any user.

   Note: **MSISDN** is the name of the field where the client ID is specified. You may give this field another name (for example, **ClientID**).

   e. For Solaris, update the `/opt/TivTSM/custcare/content/JPanSearch.cfg` as shown above and follow the procedure used for AIX.

Unique Client ID support

If using client ID as the third-party authentication mechanism in the Everyplace Suite environment, you must add further validation to the Tivoli Personalized Services Manager sub-components to ensure that client IDs are unique. By default, there is no data validation of end-user input for client ID, which allows duplicate or incorrect client IDs to be created. For additional information about validating profile extensions, please contact your IBM service representative.

Performance considerations

To improve the performance of the SecureWay Directory search for ePerson entries with a client ID attribute that matches that returned from your plugin, you can create a DB2 index for that relationship. The Authentication Server will cache the result of these lookups in memory, so that not every request from your third-party gateways involves an SecureWay Directory search, but the DB2 index will still be beneficial to performance.

This support adds one or more caches for SecureWay Directory information mapping client IDs to user information. The size and cleanup interval of these caches is the same as for the active session table cache and is controlled by the *MaxSessionCache* and *ASTCleanupInterval* configuration values, respectively. These new caches are flushed when an `authsrv flush` or `authsrv refresh` command is issued.

Since the plugin will be called for every request coming through a third-party gateway, it is important that the plugin be efficient and not perform lengthy operations unless absolutely necessary.

Customer-supplied, gateway-specific client ID plugin

The customer-supplied gateway-specific plugin is responsible for returning a client ID for the current request. This routine will run as part of the same process and thread as the Authentication Server. Because Caching Proxy plugins run in a multithreaded environment, the gateway-specific plugin must be thread-safe. The plugin will have access to the HTTP headers, URL and query string, and other information about the current request through the same Caching Proxy plugin APIs as the Authentication Server. API `httpd_getvar()` will be used to obtain the request information.

The plugin can use `HTTPD_log_error()` to write information to the Web Traffic Express error log, which is identified on the ErrorLog directive in the Caching Proxy configuration file. Caching Proxy API information is available in the *Web Traffic Express Programming Guide* available from: http://www.ibm.com/software/webservers/edgeserver/library.html

You can have multiple plugins in the same library and coded in the same source code file. However, they must have different function names.

Interface

The plugin will receive a buffer into which it must place the client ID. The plugin must also set a return code indicating its success or failure.

The C++ prototype for this function is:

```
extern "C" int function_name(const unsigned char *logHandle, char *buffer, int
*bufferSize, const char *token);
```

The C prototype for this function is:

```
int function_name(const unsigned char *logHandle, char *buffer,
int *bufferSize, const char *token);
```

The variables you will enter are defined as follows:

- logHandle: handle to the WTE log. Used on WTE APIs only.
- buffer: pointer to a buffer provided by the caller to hold the client ID upon return from this function
- bufferSize: pointer to a variable containing the size, in bytes, of the buffer provided by the caller
- token: pointer to a string token that was fetched from the *pluginToken* eProperty in this gateway's configuration section in SecureWay Directory. This token's content, format and use are under complete control of the plugin. If the *pluginToken* eProperty is not defined in SecureWay Directory or has no value, the token argument is NULL when this plugin is called.

Output will be shown in the form of the following return codes indicating the function's success or failure:

- 0: The client ID was obtained and copied to the caller-supplied buffer as a null-terminated string.
- 1: The caller-supplied buffer is too small to hold the entire client ID. When returning this code, this function must first update the size variable pointed to by the *bufferSize* property to contain the size of the buffer required to hold the result. In that case, the caller will acquire a buffer of the requested size and call this function again.
- 2: This function was unable to return the client ID. No specific reason is implied by this return code.
- 100-199: These return codes are reserved for plugin use. They may be used to indicate a specific error instead of returning return code 2. They are treated the same as return code 2 by the caller.

Creating the shared library

The plugin must reside in a shared library accessible to the Authentication Server during request processing. A shared library containing a C++ plugin can be created using compile and link commands similar to the following:

- C++ plugin using IBM CSet++® on AIX:

  ```
  xlC_r -c myPlugin.cxx -I/usr/samples/internet_server/API
  makeC++SharedLib -p0 -o myPluginLibrary.so
  -bI:/usr/samples/internet_server/API/libhttpdapi.exp myPlugin.
  ```

- C++ plugin using Sun Workshop on Solaris:

  ```
  CC -c -mt myPlugin.cxx -I/usr/samples/internet_server/API
  CC -G -mt -o myPluginLibrary.so myPlugin.o
  -L/usr/samples/internet_server/API -lhttpdapi
  ```

- C plugin using IBM CSet++® on AIX:

```
xlc_r -c myPlugin.c -qcpluscmt -I/usr/samples/internet_server/API
makeC++SharedLib -p0 -o myPluginLibrary.so
-bI:/usr/samples/internet_server/API/libhttpdapi.exp myPlugin.o
```

- C plugin using Sun Workshop on Solaris:

  ```
  cc -c -mt myPlugin.c -I/usr/samples/internet_server/API
  cc -G -mt -o myPluginLibrary.so myPlugin.o
  -L/usr/samples/internet_server/API -lhttpdapi
  ```

These commands create a shared library called `myPluginLibrary.so` from a single source file (`myPlugin.cxx`) using Caching Proxy API files in the `/usr/samples/internet_server/API` directory.

Changing the SecureWay Directory and administrator passwords

The SecureWay Directory user ID and password are established during Everyplace Suite installation. The password can be either the same or different for each Everyplace Suite component that accesses SecureWay Directory.

Note: After you change the password at the SecureWay Directory server, you must also change this password for all of the other servers in the Everyplace Suite domain, or you will not be able to access SecureWay Directory from those servers.

You can change the SecureWay Directory password (the SecureWay Directory user ID cannot be changed) using the following command-line statement:

For AIX:

```
cd /usr/lpp/IBMEPS.Inst
./ChangePassword.sh 'component' 'userid' 'current password'
'new password' 'confirm new password'
```

For Solaris:

```
cd /opt/IBMEPSIn
./ChangePassword.sh 'component' 'userid' 'current password'
'new password' 'confirm new password'
```

For example, if you want to change the SecureWay Directory password for WebSphere Transcoding Publisher type:

```
./ChangePassword.sh Transcoding old_uid old_password new_password new_password
```

To change the password for Tivoli Personalized Services Manager, you would enter:

```
./ChangePassword.sh Tivoli old_uid old_password new_password new_password
```

Alternately, you can enter:

```
./ChangePassword.sh
```

and press **Enter**. You will be prompted for each of the above parameters in turn.

You can use the corresponding component keyword to change the password for the following components:

`Gateway` — Everyplace Wireless Gateway server
`Gatekeeper` — Everyplace Wireless Gateway Gatekeeper
`Transcoding` — WebSphere Transcoding Publisher
`Tivoli` — Tivoli Personalized Services Manager
`Proxy` — Everyplace Authentication Server
`Console` — Everyplace Administration Console
`uninstall` — Everyplace Suite uninstall program

Note: The SecureWay Directory paswords can also be changed using a Netscape browser. Instructions about doing this can be found in the SecureWay Directory documentation online at: *http://www.ibm.com/software/network/directory/library/*

Do not confuse the SecureWay Directory user ID and password with the administrator user ID and password, which are also established during Everyplace Suite installation (they are used to access the installed Everyplace Suite components). You can change the administrator password for a component through that component's administration console by following instructions in the online help for that component. See “Where to find Everyplace Suite component documentation” on page 4 for more information.

Configuring Tivoli Personalized Services Manager

Enabling the JDBC app driver for Tivoli Personalized Services Manager

You can improve Tivoli Personalized Services Manager performance by using the app driver as the JDBC driver for DB2. The procedure used to enable the DB2 app driver depends on the location of the Tivoli Personalized Services Manager applications and DB2 server.

If the Tivoli Personalized Services Manager applications and DB2 server are installed on the same machine, you only have to change the properties and scripts.

If the Tivoli Personalized Services Manager applications and DB2 server are installed on different machines, perform the following:

1. Install and set up a DB2 client.
2. Change properties and scripts.

For either scenario, refer to the following sections in the *TPSM-Overview.htm (Tivoli Personalized Services Manager Documentation) Planning and Installation* section located on CD number 8 (`tsm/aix/db2/TPSM-Overview.htm` or `tsm/sun/db2/TPSM-Overview.htm`):

- Installing DB2 Database
- Post-Installation

Configuring Everyplace Wireless Gateway

Enabling the Everyplace Wireless Gateway to access the RADIUS and active session table servers

After installing the Everyplace Wireless Gateway, you must configure both the Everyplace Wireless Gateway and the Tivoli Personalized Services Manager so that the network access server (NAS) password matches the Everyplace Wireless Gateway SHAREDSECRET entry. This configuration adds the Everyplace Wireless Gateway to the RADIUS and active session table servers as a client and enables the Everyplace Wireless Gateway to access the RADIUS and active session table servers. If necessary, you can look up the value of the SHAREDSECRET Everyplace Wireless Gateway entry using the Directory Management Tool (see “Configuring Authentication Server information in SecureWay Directory” on page 73 for more information on using the Directory Management Tool). The parameters you need to know to locate the SHAREDSECRET entry are:

- cn=<Gateway Resource Hostname>,
- cn=root, sys
- sys=ewg
- sys=SDP, <your suffix>

Then locate the **radiussharedsecret**: entry.

Configuration will occur both during and after creation of the Gateway resource in Everyplace Wireless Gateway,

Configuring during creation of the Gateway resource

You must perform the following configuration steps when creating a Gateway resource for the Everyplace Wireless Gateway in an Everyplace Suite environment:

1. Configure the Everyplace Wireless Gateway to run in Everyplace Suite mode.
2. Configure the Everyplace Wireless Gateway to authenticate using RADIUS. This should be the default selection if Everyplace Suite mode is on.
3. Configure both Wireless Access Protocol (WAP) and non-WAP resources to perform user validation.
4. For WAP resources, configure the Authentication Server or its load balancer as the next hop for HTTP traffic from the WAP gateway.

Refer to the *Wireless Gateway Administrator’s Guide* for information on creating a Gateway resource.

Configuring after creation of the Gateway resource

Perform the following configuration steps after installing the Everyplace Wireless Gateway and creating the Gateway resource:

1. Change the default value of the Gateway resource from *1812* to the value of the Tivoli Personalized Services Manager’s RADIUS listening port. The default value of the listening port is *1645*.
2. Specify a SHAREDSECRET setting for the RADIUS server.

3. Use the Tivoli Personalized Services Manager Director Tool to add a RADIUS client that will enable the Everyplace Wireless Gateway to access the RADIUS server. To do this:
   a. Double-click **TISM**.
   b. Select **RADIUS**, then expand the RADIUS tree view.
   c. Select **Clients**.
   d. Right-click **Clients**, then select **Add**.
   e. Enter the following data:
      - Frame ID and NASID=Everyplace Wireless Gateway IP Address
      - NAS Name=Everyplace Wireless Gateway Host Name
      - NAS Password=Value of RADIUSSHAREDSECRET
      - Select the default values for the remaining arguments.

   f. Select **Add**.
   g. Restart the RADIUS Server as follows:
      1) From the Tivoli Personalized Services Manager RADIUS server, enter the `su - tsmuser` command (for Oracle database root userid is sufficient).
      2) Enter the command:`cd /usr/TivTSM/radius/bin`
      3) Issue the `./reload_radius_db2.ksh` script (for Oracle database, use the command: `./reload_radius.ksh`).
4. Modify the Tivoli Personalized Services Manager active session table server as follows:
   a. From the active session table console, enter the `exit` command.
   b. Enter the `cd/usr/TivTSM/ast/bin` command.
   c. Modify the active session table server's *AST.properties* file to add the Everyplace Wireless Gateway's IP address to the active session table server's client list.
   d. Restart the active session table server by entering the `/ASTSever.ksh` script.
5. Stop and restart the Everyplace Wireless Gateway as follows:
   - For AIX:
     a. From the command line, enter the `stopsrc -s wgated` command to stop the process.
     b. Issue the `ps -ef | grep wgated` command and verify the process is stopped.
     c. Restart the Everyplace Wireless Gateway by entering the `startsrc -s wgated` command.
   - For Solaris:
     a. Issue the `ps -ef | grep wgated` command to get the process number for `wgated`.
     b. Issue the `kill` command using the process number for `wgated`.
     c. Restart the Everyplace Wireless Gateway by entering the `wgated` command.

     Note: You can also start and stop the resource gateway via the Gatekeeper.

Note: You can also start and stop the resource gateway via the Gatekeeper.

Setting user classification flags for the Everyplace Wireless Gateway

Two fields are included in the WebSphere Everyplace Suite LDAP schema which can be used to classify users of the suite. These fields can be set either TRUE or FALSE. This classification might allow fewer users to be displayed when using the Everyplace Wireless Gateway's Gatekeeper tool to display users, since the Gatekeeper tool uses these two fields to reduce the scope of user list queries. The fields are:

- **ibm-WGclient**: this field classifies a user as a user of the Everyplace Wireless Gateway. Gatekeeper displays only users with this field set to TRUE.
- **ibm-WAPclient**: this field classifies a user as a wireless access protocol (WAP) user. Gatekeeper displays WAP characteristics only for users with this field set to TRUE.

By default when a user is enrolled, these two fields are set to TRUE by the Tivoli Internet Services Manager LDAP provisioning gateway (LDAPGateway) via a setting in the `LDAPGateway.properties` file.

You can customize the setting of these fields using techniques such as defining user profile extensions and using the LDAPGateway to provision the user profile extensions. See the Tivoli Internet Services Manager documentation for the LDAPGateway and User Profile Extensions for more details.

Using the Everyplace Administration Console

The Everyplace Administration Console provides a centralized method for launching the administration consoles of the installed Everyplace Suite components. When invoked, the Everyplace Administration Console accesses SecureWay Directory, obtains information regarding the installed components and the servers where they are installed, and displays that information on the Everyplace Administration Console.

The hostname and the port number are displayed in the right pane next to the corresponding Everyplace Suite components. Java-based administration consoles (such as WebSphere Transcoding Publisher and WebSphere Application Server) are not listed, even though they are installed on the remote hosts.

When the user selects a component and a server, the Everyplace Administration Console launches the component's administration console on the selected server.

Starting the Everyplace Administration Console

There are three ways to start the Everyplace Administration Console:

- You will be given the option to start the console at the end of the Everyplace Suite installation process.
- After installation, you can start the console by clicking the console icon, which was created during the installation process. On AIX, the icon can be found in `/home/`admin_userID`/wesconsole`, and on Solaris in `/export/home/`admin_userID`/wesconsole`. Where admin_userID is the user ID specified in the Everyplace Administration Console installation.

- After installation, you can also start the console from the command line as follows:
  1. Log on with the Administration Console user ID specified during the installation (the Everyplace Administration Console can also be started using the root userID).
  2. Open a terminal window.
  3. Execute the following commands:
     – For AIX:

       ```
       cd /usr/lpp/IBMEPS.Admin

       ./wesconsole.sh
       ```
     – For Solaris:

       ```
       cd /opt/IBMEPSAd

       ./wesconsole.sh
       ```

The Everyplace Administration Console ensures that all of the conditions for use, such as user privilege and prerequisite software, are correct. If the conditions are met, the Everyplace Administration Console displays a list of the installed Everyplace Suite components.

Launching a component administration console

A component administration console can be launched from the Everyplace Administration Console as follows:

1. Select the component whose administration console you want to launch. The rest of the component list is grayed out, and a list of servers where the selected component is installed is displayed.
2. Double-click the server containing the desired component instance to launch that component's administration console.

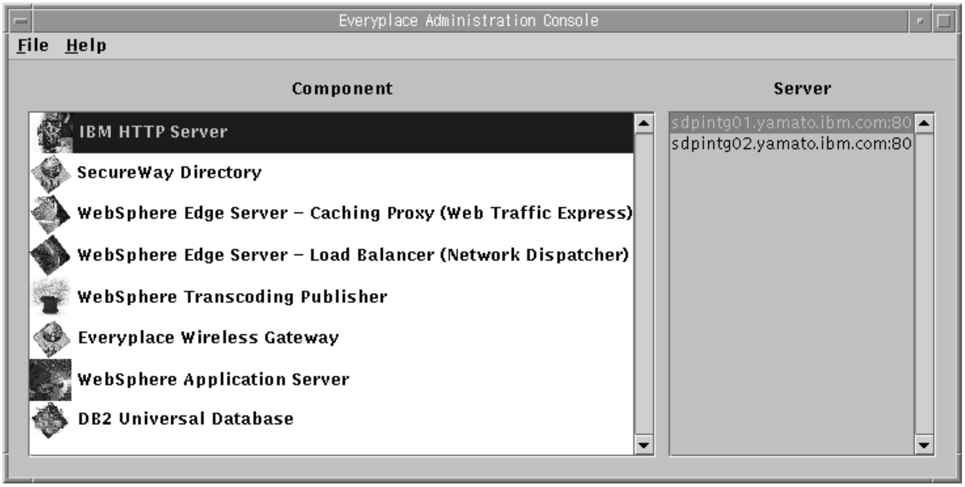

Everyplace Administration Console
File
Help
Component
Server
IBM HTTP Server
SecureWay Directory
WebSphere Edge Server – Caching Proxy (Web Traffic Express)
WebSphere Edge Server – Load Balancer (Network Dispatcher)
WebSphere Transcoding Publisher
Everyplace Wireless Gateway
WebSphere Application Server
DB2 Universal Database
sdpintg01.yamato.ibm.com:80
sdpintg02.yamato.ibm.com:80

Figure 11. Everyplace Administration Console

Changing the port number for the HTTP Server and Caching Proxy

You can change both the IBM HTTP Server and the Caching Proxy's port numbers after installation, using the Everyplace Administration Console as follows:

1. Select either the IBM HTTP Server or the Caching Proxy from the list of components. A list of all the servers where that component is installed will be displayed in the right hand panel.
2. Highlight the server you wish to change by clicking on that server (do not double click the name, as that will launch the component's administration console).
3. Right click on the server name (or press the **Shift-F10** keys simultaneously). This will display a dialog with the selected server and port number listed.
4. Enter the new port number in the **Port Number** field and then click **OK**. You can not edit the **Server** field.
5. After clicking OK, the new port number will be displayed in the list of servers in the Everyplace Administration Console.

Troubleshooting

If the Everyplace Administration Console does not launch the component's administration console, ensure that the following conditions are met:

- The login user ID has the required privilege to access the SecureWay Directory server and to launch the component's administration console. See "Installation planning for SecureWay Directory" on page 24 for more information.
- The prerequisite software for the component is installed. See "System requirements" on page 29 for more information.

- The Everyplace Administration Console configuration file (`/usr/lpp/IBMEPS.Admin/suiteadmin.conf` for AIX, `/opt/IBMEPSAd/suiteadmin.conf` for Solaris) is available, and the user ID, password, and SecureWay Directory server name are set correctly in the file.
- The SecureWay Directory server is started and connected properly.

Chapter 7. Japanese-specific information

The Everyplace Suite supports the following language environments for Japanese:

- AIX: Primary Language Environment : Japanese PC (`Ja_JP`)
- Solaris: Default Language : Japanese EUC (`ja`)

If you install the Everyplace Suite with the Japanese locale on AIX (`Ja_JP`), or Solaris (`ja`), garbage characters will appear in the following trace file:

```
/tmp/everyplace_install.trace
```

Only Japanese output characters from the AIX `installp` and Solaris `pkgadd` commands are broken.

If you install Everyplace Wireless Gateway on a Japanese AIX system, you must install the Japanese EUC (`ja_JP`) system locale.

If you install Tivoli Personalized Services Manager on a Japanese system, you must install the Japanese UTF-8 (`JA_JP`) system locale for AIX or the Japanese UTF-8 (`ja_JP.UTF-8`) system locale for Solaris.

Starting Edge Server Caching Proxy (Web Traffic Express) in a Japanese environment

If you install Edge Server Caching Proxy (Web Traffic Express) in a Japanese environment, you must enter the following before starting Caching Proxy:

- For AIX:

  ```
  cp /opt/IBMWTE/usr/internet/etc/en_US/rc.ibmproxy /opt/IBMWTE/usr/internet/etc/Ja_JP
  cd /opt/IBMWTE/usr/internet/etc/Ja_JP
  rm ibmproxy.conf
  ln -sf /opt/IBMWTE/usr/internet/etc/Ja_JP/rc.ibmproxy /etc/rc.ibmproxy
  ```

- For Solaris:

  ```
  cp /opt/IBMWTE/usr/internet/etc/en_US/ibmproxy /opt/IBMWTE/usr/internet/etc/ja
  cd /opt/IBMWTE/usr/internet/etc/ja
  rm ibmproxy.conf
  cd /etc/init.d
  rm ibmproxy
  ln -sf /opt/IBMWTE/usr/internet/etc/ja/ibmproxy /etc/init.d/ibmproxy
  ```

Using the Tivoli Personalized Services Manager Member Self Care Support subcomponent in a Japanese environment

To use the Tivoli Personalized Services Manager Member Self Care Support subcomponent in a Japanese environment, you must perform the following:

1. On the Authentication Server, edit the following file:

   ```
   /opt/IBMWTE/usr/internet/etc/ibmproxy.conf
   ```

Refer to the description of the ″ibmproxy_ap.conf.sample″ file in “Chapter 5. Configuring the Authentication Server” on page 73.

2. Add the following lines to the ″SELFCARE″ section of the `ibmproxy.conf` file:

```
##### Request URL:http://authserver:port/tsm_sc/ja/selfcare.html
Proxy    /tsm_sc/ja/*      http://<hostname>.<domain>:15080/ja/*
```

|

Chapter 8. Uninstalling the Everyplace Suite components

Any of the Everyplace Suite components can be removed using the Everyplace Suite uninstall program. This program allows users to select any combination of Everyplace Suite components and subcomponents to be removed. Only components installed on the local server where the uninstall program is being run can be uninstalled.

Note: The Everyplace Synchronization Manager can not be uninstalled with the Everyplace Suite uninstall program. See the documentation in `/esm/docs` on CD number 11 of the Everyplace Suite product CDs for information on uninstalling the Synchronization Manager.

Starting the uninstall program

To start the uninstall program, type the following at the command line:

- On AIX systems: `/usr/lpp/IBMEPS.Inst/uninstall.sh`
- On Solaris systems: `/opt/IBMEPSIn/uninstall.sh`

Selecting and uninstalling components

Follow these steps to uninstall Everyplace Suite components:

1. After starting the uninstall program, a list of all the currently installed components and their corresponding subcomponents is displayed. The subcomponents appear in the right-hand panel. These subcomponents can be individually selected.

   Note: If any selected components are required for other components not being uninstalled, you will be notified of this problem before any uninstall takes place.
2. You will be given the option of uninstalling supporting components (such as IBM HTTP Server and WebSphere Application Server) when they are no longer needed as prerequisites by components you are uninstalling.
3. After all the components have been selected for uninstall, click the **Next** button. A list of all the components and subcomponents to be uninstalled will be presented. To proceed with the uninstall, click the **Uninstall** button.

   Note: Uninstallation of IBM DB2 Universal Database will not be allowed until there are no instances of SecureWay Directory, Tivoli Personalized Services Manager, Everyplace Synchronization Manager, or Everyplace Wireless Gateway found in the Everyplace Suite domain.
4. A progress screen will display the progress of the uninstall and inform you when it is complete.

All actions and outcomes are logged to the file `/tmp/everyplace.log` during the uninstall. This file contains a sequence of information that can assist you in identifying and analyzing problems. The `everyplace_install.trace` file is also available in the /tmp directory and contains details about the program execution. These files are in ASCII text format and can be viewed using any text editor.

The uninstall program will not remove any customer data files. Only files installed during Everyplace Suite component installation will be removed. Components not installed with the Everyplace Suite installation program may not uninstall properly.

Note: After uninstalling Everyplace Suite components that use a user ID and a group ID, be sure to delete these IDs from the system to avoid any problems.

Uninstallation tips for Everyplace Suite components

Uninstall SecureWay Directory

The uninstall program will determine which components are required by the remaining installed components. This will be done by retrieving the Everyplace Suite install and configuration information from the SecureWay Directory server. Therefore, the active SecureWay Directory server must be available when the uninstall program is running to ensure the integrity of the Everyplace Suite environment.

Note: If components are uninstalled without the SecureWay Directory server active, system consistency will be compromised and unexpected results may occur.

Uninstall Everyplace Wireless Gateway

If you uninstall Everyplace Wireless Gateway and reinstall it on the same server, you may get a message indicating that ″the server exists″ during Gatekeeper configuration. Disregard this message. The Gatekeeper configuration will perform correctly because the existing resource in the LDAP directory is reused.

Uninstall Tivoli Personalized Services Manager

The DB2 database is not completely removed during uninstallation of Tivoli Personalized Services Manager with a DB2 database on AIX. You must manually remove the `/db/db2` directory before reinstalling Tivoli Personalized Services Manager with DB2.

You must stop all Tivoli Personalized Services Manager servelets before refreshing or removing Tivoli Personalized Services Manager. If the following components are running on the machine in which Tivoli Personalized Services Manager is installed, you must stop them before refreshing or removing Tivoli Personalized Services Manager:

- AST Server
- LDAP Gateway
- RADIUS Server
- Transactions Server

Terminating the Tivoli Personalized Services Manager LDAPGateway daemon on Solaris

The Tivoli Personalized Services Manager LDAPGateway Daemon does not terminate on Solaris when `stop-LDAPGateway.ksh` is issued on Solaris because the script is trying to kill an LDAPGateway process that was truncated in the called ″LDAPGateway″.

The `stop-LDAPGateway.ksh` script queries for processes with arguments that have the name `LDAPGateway` in them. If the process ID has an argument greater than 80 bytes, the LDAPGateway value is truncated and the LDAPGateway daemon is not terminated correctly.

To terminate the LDAPGateway daemon correctly, you must perform the following:

1. Enter:

   ```
   # ps -ef | grep LDAP
   ```

   and stop the resulting processes that contain *LDAPGateway*.
2. Enter:

   ```
   # ps -ef | grep tsm.l
   ```

   and end the resulting processes that contain *tsm.1*.

The following is an example of this procedure:

```
# ps -ef | grep LDAP
root  6588  5574  0 13:34:32 pts/3    0:00 /bin/ksh ./LDAPGateway.ksh
root  6650  6190  0 14:56:46 pts/4    0:00 grep LDAP
# kill -9 6588

# ps -ef | grep tsm.l
root  6589  6588  0 13:34:32 pts/3    0:13 /usr/java_dev2/bin/../jre/bin/../bin/sparc/
native_threads/javacom.tivoli.tsm.l
root  6648  6190  0 14:56:36 pts/4    0:00 grep tsm.l
# kill -9 6589
```

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504–1785
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX
CSet++
DB2
DB2 Universal Database
Everyplace
IBM
PartnerWorld
SecureWay
MQSeries
REDBOOKS
RS/6000
ThinkPad
Tivoli
WebSphere
WorkPad

The following terms are trademarks of other companies:

Sun, Sun Microsystems, all Sun-based trademarks and logos, Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Incorporated.

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

Domino, Lotus, and Lotus Notes are trademarks of the Lotus Development Corporation.

Netscape, Netscape Navigator, Netscape Communicator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

Microsoft, Windows, Windows NT, Windows 98, the Windows 95 logo, and/or other Microsoft products referenced herein are either trademarks or registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or services marks of others.

Index

Readers' Comments — We'd Like to Hear from You

WebSphere® Everyplace™Suite
Getting Started
Version 1.1.3

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You

IBM®

Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department 3JQA
P.O. Box 12195
Research Triangle Park, NC 27709-9990

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line