WebSphere® Everyplace™ Server Version 2.1

Everyplace Cookie Proxy User’s Guide

Note

Before using this document, read the general information in “Notices” on page 17.

First Edition (July 2001)

This edition applies to the Everyplace Cookie Proxy in WebSphere Everyplace Server Version 2 Release 1 and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2001. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

About this manual

The Everyplace Cookie Proxy is a plug-in software for the WebSphere Edge Server Caching Proxy. This manual presents a general description of the Everyplace Cookie Proxy, and instructions for installing, configuring, and uninstalling it.

How this manual is organized

This manual contains the following chapters:

- "Chapter 1. Introducing the Everyplace Cookie Proxy" on page 1 describes the Everyplace Cookie Proxy and its functions.
- "Chapter 2. Installing and uninstalling the Everyplace Cookie Proxy" on page 5 explains how to install the Everyplace Cookie Proxy on your AIX or Solaris system, and how to uninstall it.
- "Chapter 3. Configuring and administering the proxies" on page 9 tells how to configure the Everyplace Cookie Proxy and the Edge Server Caching Proxy, and explains the error log.

Chapter 1. Introducing the Everyplace Cookie Proxy

The number of subscribers to wireless Internet services—services that give access to the Internet through wireless devices such as mobile phones—has been growing rapidly in the last couple of years in Japan. Since Japan's biggest wireless carrier launched its wireless Internet service in February 1999, the number of its subscribers has increased by 25,000 a day, and rapid growth continues.

Web browsers in wireless devices meet with numerous problems:

Problem	Description
Cookies are not supported.	Web applications using cookies cannot be developed for this large market, and existing service approaches that rely on cookies are unusable.
The Web browsers cannot remember the user ID or password for Basic Authentication even after authentication.	As a user, you must enter your user ID and password every time you submit an HTTP request; for example, every time you click a hyperlink of the Web site.
No IP address or other information (such as a phone number) is available to enable the Web application to identify the user. [1]	This makes it impossible to maintain a session, so session-based Web applications, such as personalized services, cannot be developed or used.
Entering a password is difficult because the input field shows only asterisks for the typed characters.	Ordinary mobile phones have only 10 numeric keys for dialing and several other keys overloaded with 3 or 4 writing systems, plus special characters. The result is that up to 5 kana (Japanese syllabic) characters are assigned to each key for input.

These problems are solved by the Everyplace™ Cookie Proxy (hereafter called the Cookie Proxy). This software is a plug-in for the WebSphere® Edge Server Caching Proxy (hereafter called the Edge Server Caching Proxy). The Edge Server Caching Proxy is a component of the IBM® WebSphere Everyplace Server (hereafter called the Everyplace Server).

WebSphere Portal Server is an example of software that uses cookie for session management.

As a part of the proxy service, the Cookie Proxy saves important information on behalf of Web browsers with limited functions. This can include cookie values and other values used for session management and Basic Authentication. The Cookie Proxy also improves the usability of Web applications by providing a customizable login form.

A typical configuration is shown in Figure 1. In this example, the authentication is handled by the Everyplace Authentication Server (hereafter called the Authentication Server), a components of the IBM WebSphere Everyplace Server (hereafter called the Everyplace Server).

[1] There are cases in which the official sites of a wireless carrier are able to identify their users' devices.

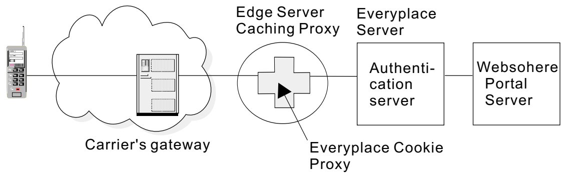

Figure 1. Relation of the Everyplace Cookie Proxy to the system: example

How the Everyplace Cookie Proxy works

Cookies

When an HTTP response is downloaded, the Cookie Proxy reads its header and saves any cookie values (that is, name=value pair, path and expires data) in its own table. Then, when the Web browser issues an HTTP request to the Web server, the Cookie Proxy retrieves the saved cookie values, adds them to the request header, and passes the request to the back-end server.

Note: The Cookie Proxy checks the expiration value of a cookie only when it is saved in its own table, and it does not check the expiration value of any cookies when they are retrieved. All saved cookie values remain in the Cookie Proxy's table until the session is cleaned up by the cleanup daemon. This means that a cookie is passed to the back-end server as long as the cookie entry remains in the table, and monitoring for expiration is the responsibility of the back-end server.

Session management

When a user tries to get access to a Web application for the first time in a session (or after the expiration of a timeout delay since this user last had access to this application), the Cookie Proxy generates a session ID. If the host name of the URL is that of the back-end server or the Cookie Proxy, this session ID is added to the URLs of the hyperlinks in the HTTP response. Every time an HTTP request is submitted, the Cookie Proxy checks whether the incoming session ID is valid. This session information is stored in the table of Cookie Proxy until the session cleanup daemon removes it. The session expiration period and the cleanup interval can be defined during the configuration of the Cookie Proxy.

Basic Authentication

If the Web browser submits an HTTP request and the back-end server requires Basic Authentication, but the Cookie Proxy has not yet stored a valid user ID and password, the Cookie Proxy sends a login form to the Web browser. (This form can be customized by the back-end web application developer or the administrator who sets up the Cookie Proxy.) When the user logs in, the Cookie Proxy reads the body of the HTTP request and saves the user ID and password. Then, throughout the rest of the session, whenever the browser submits an HTTP request, the Cookie Proxy retrieves the user ID and password; adds the default realm after the user ID if the realm is specified in its configuration file; encodes the resulting string, using BASE64; adds the string to the request header; and passes the header to the back-end server.

Performance and scalability

When the Cookie Proxy is set up with the Edge Server Caching Proxy, the Everyplace Server, and the back-end server, the physical architecture will have an important effect on both performance and scalability. For better throughput and security, the Edge Server Caching Proxy, including the Cookie Proxy, should be installed on another machine, separate from the other components of the Everyplace Server. For more information about the performance and scalability of the Edge Server Caching Proxy, and the Everyplace Server, refer to the guidebook for each of those programs.

The use of the Secure Socket Layer (SSL) is one factor that affects the number of HTTP requests processed per unit time and the turnaround time per request. In general, the overhead for processing SSL is much larger than the overhead for cookie processing by the Cookie Proxy.

For the best use of memory, *MaxSession*, defined in the configuration file for the Cookie Proxy, *jpas.conf*, should not be too large relative to the estimated user accesses.

When you configure the system, you must consider security along with performance and scalability. For security considerations, refer to “Security considerations”.

Devices supported

NTT DoCoMo’s i-mode phones.

Markup languages supported

The Cookie Proxy has native support for the compact HTML in Shift-JIS code. If the WebSphere Transcoding Publisher is used, other markup languages can be supported. For details about the Transcoding Publisher, refer to http://www.jp.ibm.com/software/network/transcoding/library.html

Security considerations

To prevent the system from being attacked by an intriguer who uses powerful personal computers with highly functional Web browsers, the proxy server, including the Cookie Proxy, should be directly connected to an NTT DoCoMo gateway via a leased line network. Then only i-mode phones can get access to these Web applications.

Limitation

The Cookie Proxy does not support any Java applications (iappli).

Chapter 2. Installing and uninstalling the Everyplace Cookie Proxy

Hardware requirements

The Everyplace Cookie Proxy can be used with the following hardware for each platform:

For AIX system: IBM RS/6000®
For Solaris system: SPARC™ or UltraSPARC

A minimum of 512 megabytes of memory is recommended for the Everyplace Cookie Proxy and Edge Server Caching Proxy server machine when the other components are installed in separate machines.

For more information about the hardware requirements, refer to the *WebSphere Edge Server for Multiplatforms—Web Traffic Express User's Guide*.

Software requirements

The following software is required for the Cookie Proxy:

For AIX system:

- AIX® 4.3.3
- WebSphere Edge Server Caching Proxy version 1.0.3 (Web Traffic Express 3.6)

For Solaris system:

- Solaris version 7 or 8 (32-bit only)
- WebSphere Edge Server Caching Proxy version 1.0.3 (Web Traffic Express 3.6)

For the requirements for the Edge Server Caching Proxy, refer to the *WebSphere Edge Server for Multiplatforms—Web Traffic Express User's Guide*. For the latest information about the required updates, read the README file in the installation package.

Required disk space

To manage the software and documentation for the Edge Server Caching Proxy and the Cookie Proxy, you will need 50 megabytes of free disk space, plus space for logs. For more information, refer to the *WebSphere Edge Server for Multiplatforms - Getting Started*.

Installing the Everyplace Cookie Proxy

Before you begin to install the Cookie Proxy, be sure to read the README file. The README file is on the 10th CD-ROM for the WebSphere Everyplace Server. The version in English is (cd_root)/jpas/readme_En.html; the version in Japanese is (cd_root)/jpas/readme_Ja.html.

On an AIX system

To install the Cookie Proxy from the CD-ROM, follow these steps:

1. Log in as root.

2. Stop the Edge Server Caching Proxy by the procedure given in “Starting and stopping the proxies” on page 14.
3. Place CD number 10 in the CD drive.
4. Mount the CD.

   For example, type the command: mount -rv cdrfs /dev/cd0 /mnt

5. Change the current directory to *(cd_root)*/jpas/aix
6. Type ./install.sh to run the installation shell script.
7. Modify the configuration file for the Cookie Proxy, */etc/jpas.conf*, by the procedure given in “Chapter 3. Configuring and administering the proxies” on page 9.

On a Solaris system

To install the Cookie Proxy from the CD-ROM, follow these steps:

1. Log in as root.
2. Stop the Edge Server Caching Proxy by the procedure given in “Starting and stopping the proxies” on page 14.
3. Place CD number 10 in the CD drive.
4. Change the current directory to *(cd_root)*/jpas/solaris
5. Type ./install.sh to run the installation shell script.
6. Modify the configuration file for the Cookie Proxy, */etc/jpas.conf*, by the procedure given in “Chapter 3. Configuring and administering the proxies” on page 9.

Uninstalling the Everyplace Cookie Proxy

Note: After you uninstall the Everyplace Cookie Proxy, the configuration file (*ibmproxy.conf*) of the Edge Server Caching Proxy is replaced with the one that was saved when Everyplace Cookie Proxy was installed.

On an AIX system

To uninstall the Cookie Proxy with the product CD, follow these steps:

1. Log in as root.
2. Stop the Edge Server Caching Proxy by the procedure given in “Starting and stopping the proxies” on page 14.
3. Place CD number 10 in the CD drive.
4. Mount the CD.

   For example, type the command: mount -rv cdrfs /dev/cd0 /mnt

5. Change the current directory to *(cd_root)*/jpas/aix
6. Type ./uninstall.sh to run the uninstallation shell script.

On a Solaris system

To uninstall the Cookie Proxy with the product CD, follow these steps:

1. Log in as root.
2. Stop the Edge Server Caching Proxy by the procedure given in “Starting and stopping the proxies” on page 14.
3. Place CD number 10 in the CD drive.

4. Change the current directory to *(cd_root)*/jpas/solaris
5. Type ./uninstall.sh to run the uninstallation shell script.

Chapter 3. Configuring and administering the proxies

The Edge Server Caching Proxy and the Everyplace Cookie Proxy read their respective configurations at startup time. If any configuration data is updated during a session, the Edge Server Caching Proxy must be stopped and then restarted so that the update will take effect.

Configuring the Edge Server Caching Proxy

The Edge Server Caching Proxy can be configured as a forward, reverse, or transparent proxy. To use the Cookie Proxy, you must set the Edge Server Caching Proxy as a reverse proxy. The procedure is given in the chapter that explains the proxy settings in the *WebSphere Edge Server for Multiplatforms—Web Traffic Express User’s Guide*.

In addition, the following steps are required.

1. Setting mapping rules

   To enable users to get access to a Web application via the Cookie Proxy without knowing the Web server’s host name, specify the Proxy directive in the Mapping Rules section of the Edge Server Caching Proxy’s configuration file, *ibmproxy.conf*.

   Proxy *<Cookie Proxy’s path> <back-end server’s name and path to be mapped into Cookie Proxy’s path>*

   An example of the statement for a reverse proxy is:

```
Proxy          /*                http://wps.yamato.ibm.com/*
```

2. Setting caching off

   To make sure that Web browsers get fresh data every access, disable the caching by editing the *ibmproxy.conf* in the configuration file for the Edge Server Caching Proxy, as follows:

   Caching OFF
   Comment out **CacheMemory**

   The Cookie Proxy’s installation program does this change automatically.

3. Setting the names of plug-in function

   The following statements must be included in the API directives section of the Edge Server Caching Proxy’s configuration file, *ibmproxy.conf*.

   ServerInit /opt/IBMJPAS/lib/libjpas.so:JpasInit *[<Cookie Proxy’s configuration file name>]*

   PreExit /opt/IBMJPAS/lib/libjpas.so:JpasPreExit

Transmogrifier /opt/IBMJPAS/lib/libjpas.so:JpasTOpen:JpasTWrite:JpasTClose: JpasTError

ServerTerm /opt/IBMJPAS/lib/libjpas.so:JpasTerm

Note: Each of these statements must be typed without a line break, even though lines have had to be broken here.

If the name of the configuration file for the Cookie Proxy is not specified after ***JpasInit***, the default file path, */etc/jpas.conf*, is used. These statements are automatically added in *ibmproxy.conf* by the Cookie Proxy's installer. If you want to use another name for the configuration file, manually modify the argument after ***JpasInit***. If the configuration file for the Cookie Proxy is not present under the name specified, the initialization fails and the Cookie Proxy is not activated.

Configuring the Everyplace Cookie Proxy

When the Edge Server Caching Proxy starts up, the Cookie Proxy reads its configuration file, *jpas.conf*. This file contains the definitions shown in the following table. The keys are case-sensitive.

key	Descriptions	Required or default value	Example
ServerId	Cookie Proxy server ID. Any letters (a-z) and digits (0-9). If the Cookie Proxy servers are configured as a cluster, each of them must have a unique server ID.	Required	ServerId = a
ProxyHostname	Cookie Proxy server's host name. If the Cookie Proxy servers are configured as a cluster, do not specify a cluster name.	Required	ProxyHostname = www.jpas.ibm.com

BackendHostname.*n*	Host name of the back-end server. "*n*" denotes any number starting from 0 to 63, which is the maximum number of backended hosts.	Required	BackendHostname.0 = www0. jpas.ibm.com
			BackendHostname.1 = www1. jpas.ibm.com

AssumeHTML	Turn on in case the Content-type header field is missing from the response and the Cookie Proxy needs to assume that Content-type is "text/html."	off	AssumeHTML=on
Clustering	Turn on if the Cookie Proxy servers are configured as a cluster with network dispatcher.	off	Clustering = on
DefaultRealm	Realm string used in the back-end server. If specified, it affects the basic authentication string in the authentication header.	Optional	DefaultRealm = mycompany.com
MaxSession	Maximum number of sessions the Cookie Proxy can hold at a time.	200	MaxSession = 45
SessionTimeout	Time interval in minutes after which, if the user takes no action during a session, the session ends automatically. The minimum value is 5.	15	SessionTimeout = 25
CleanupInterval	Time interval in minutes: between cleanups of the session table. The minimum value is 1.	5	CleanupInterval = 45
MaxCookie	Maximum number of cookies per session.	20	MaxCookie = 10

key	Descriptions	Required or default value	Example
AddHeader.*n*.name AddHeader.*n*.value	Header field name and value, to be added when the Cookie Proxy passes a message to a back-end server. Each "*n*" denotes any number starting from 0 to 15, which is the maximum. The setting takes effect only if name and value are specified at the same time.	Optional	AddHeader.0.name = Accept-Encoding AddHeader.0.value = compress, gzip
UserAgent.n	List of supported user agents. ″n″ denotes a whole number starting from 0.	Required	UserAgent.0 = DoCoMo/1.0/P501i UserAgent.1 = DoCoMo/1.0/D502i
LoginPath	Login request path. This is used as a part of the URL to login. Specify a path that does not already exist.	Required	LoginPath = / login.jpas
LogoutPath	Logout request path. This is used as a part of the URL to logout.	Optional	LogoutPath = / logout.jpas
HomepageUrl	Home page URL. This page is opened when the Cookie Proxy is unable to determine which page it should jump to after a login or logout process.	Required	HomepageUrl = /welcom/index.html
LoginForm	Login form name to indicate where in the Cookie Proxy the login form is.	Required	LoginForm = /opt/IBMJPAS/etc/ Ja_JP/login.html
ErrorPage.General	HTML file path for ″general error.″ This is used when the Cookie Proxy detects an error.	Required	ErrorPage.General = /opt /IBMJPAS/etc/ Ja_JP/error.html
ErrorPage.Busy	HTML file path for ″busy.″ This is used when the Cookie Proxy is in a busy state.	Required	ErrorPage.Busy = /opt/IBMPAS/etc/ Ja_JP/error_busy.html
ErrorPage.BadReq	HTML file path for ″bad request.″ This is used when the Cookie Proxy detects an invalid input from the Web browser.	Required	ErrorPage.BadReq = /opt/IBMJPAS/etc/ Ja_JP/error_badreq.html
TraceLevel	One of the following trace levels: 0 = errors only 1 = errors and notices 2 = errors, notices, and other information 3 = all (errors, notices, other information, and debugs)	0	TraceLevel = 3
Syslog	Whether or not the syslog function is to be enabled for the Cookie Proxy trace. If this is on, trace messages are sent to the syslogd daemon.	off	Syslog = on
TraceFile	Full path name of the trace file. This can be used in addition to the Syslog parameter.	Required if Syslog = off	TraceFile = /var/jpas/logs/jpas.log

- Each parameter is to be specified in "key=value" format in the configuration file. Spaces are allowed before and after "=".
- Lines starting with "#" are regarded as comments.
- 255 characters per statement including the new line are allowed.
- If any required parameter is missing, the initialization fails and the Cookie Proxy is not activated.

For an example of configuration file, look at */opt/IBMJPAS/etc/jpas.conf* (symbolic-linked by */etc/jpas.conf*) after installation.

Customizing login

If a user tries to open a page that requires authentication, but you do not have a session active, a login form requesting that the user logs in appears in the user’s Web browser.

A login form must be available according to the LoginForm parameter in the configuration file for the Cookie Proxy. If there is no such form, the initialization fails and the Cookie Proxy is not activated.

The HTML login form must include the following strings:

- method=“post” action=“$$$LOGINPATH$$$;ZZLOGIN” in a FORM tag.
- name=“jpasuid” maxlength=“16” in an INPUT tag of this FORM definition.
- name=“jpaspw” maxlength=“16” in another INPUT tag of this FORM definition.

A sample login form is shown below.

```
<html>
<head>
<META http-equiv=“Content-Type” content=“text/html; charset=shift_jis”>
</head>
<body>
<form method=“post” action=“$$$LOGINPATH$$$;ZZLOGIN”>
User ID:<br>
<input type=“text” name=“jpasuid” size=“14” maxlength=“16”><br>
Password:<br>
<input type=“text” name=“jpaspw” size=“14” maxlength=“16”><br>
<input type=“submit” value=“Login”>
</form>
</body>
</html>
```

Customizing error messages

Three types of error messages can be written in HTML files. The messages appear in the Web browser.

- “JPAS200E General server error”
- “JPAS300E Server busy”
- “JPAS400E Bad request”

The “JPAS200E General server error” message file is used when the Cookie Proxy detects an error, such as a system error. Do not delete “JPAS200E” from the first line of the body element; keep it for use in reporting the error. Where to place this file is defined in the ***ErrorPage.General*** parameter in the configuration file. An example of the “JPAS200E General server error” message HTML file, /opt/IBMJPAS/etc/Ja_JP/err_general.html, is:

```
<html>
<head>
<META http-equiv=“Content-Type” content=“text/html; charset=shift_jis”>
</head>
<body>
Error:JPAS200E<br>
The Cookie Proxy detected an error. Please contact your provider’s administrator.
```

```
</body>
</html>
```

The “JPAS300E Server busy” error message file is used when the Cookie Proxy is in a busy state. For example, receiving too many requests for session establishment, it will result in a “Server busy” state. Do not delete “JPAS300E” from the first line of the body element; keep it for use in reporting the error. Where to place this file is defined in the ***ErrorPage.Busy*** parameter in the configuration file. An example of the “JPAS300E Busy” error message HTML file, /opt/IBMJPAS/etc/Ja_JP/err_busy.html, is:

```
<html>
<head>
<META http-equiv=“Content-Type” content=“text/html; charset=shift_jis”>
</head>
<body>
Error:JPAS300E<br>
The server is currently busy. Please try again later.
</body>
</html>
```

The “JPAS400E Bad request” error message file is used when the Cookie Proxy detects an invalid input from the Web browser, such as an invalid session ID created by an intruder. Do not delete “JPAS400E” from the first line of the body element; keep it for use in reporting the error. Where to place this file is defined in the ***ErrorPage.BadReq*** parameter in the configuration file. An example of the “JPAS400E Bad request” error message file in HTML, /opt/IBMJPAS/etc/Ja_JP/err_badreq.html, is:

```
<html>
<head>
<META http-equiv=“Content-Type” content=“text/html; charset=shift_jis”>
</head>
<body>
Error:JPAS400E<br>
An unexpected request has been detected.
</body>
</html>
```

Getting access to a Web application by use of the Everyplace Cookie Proxy

The host name that you use for getting access to the host is a part of the URL, and is the name not of the back-end server, but of the Cookie Proxy server. For example, if the Cookie Proxy’s host name is:

> *www.jpas.ibm.com*

then home page of the back-end WebSphere Portal Server is

> *http://wps.yamato.ibm.com/commerce/index.html*

and the mapping rule defined in the Edge Server Caching Proxy configuration file (ibmproxy.conf) is

Proxy / http://wps.yamato.ibm.com/**

The mapped URL that you should type in is

http://www.jpas.ibm.com/commerce/index.html

Starting and stopping the proxies

When the Edge Server Caching Proxy starts up, the Cookie Proxy is automatically initialized. If any problem occurs during the start, the Cookie Proxy is not activated. The Edge Server Caching Proxy, however, does not stop automatically; it must be stopped manually and restarted.

When the Edge Server Caching Proxy is shut down, the Cookie Proxy is shut down with it.

To start the Edge Server Caching Proxy, follow these steps:

For AIX system:

1. Login as root.
2. Enter **startsrc -s ibmproxy**.

For Solaris system:

1. Login as root.
2. Enter **/etc/init.d/ibmproxy start**.

To stop the Edge Server Caching Proxy, follow these steps:

For AIX system: Enter **stopsrc -s ibmproxy**.
For Solaris system: Enter **/etc/init.d/ibmproxy stop**.

For more details about how to start and stop the Edge Server Caching Proxy, refer to the *WebSphere Edge Server for Multiplatforms—Web Traffic Express User's Guide*.

Logging

The Cookie Proxy can be configured to produce trace data either by writing data to the system log (syslog) or by writing log files especially for Cookie Proxy.

If you prefer to use syslog, you must specify ***Syslog=on*** in the configuration file for the Cookie Proxy, *jpas.conf*. Before trace data can be recorded in the syslog output file specified, in */etc/syslog.conf*, you must set up the syslog output file and have the syslog daemon (syslogd) running.

To report an error to the syslog, for example, add the following line to the /etc/syslog.conf file:

daemon.err [*syslog output file*]

The location of the syslog output file for each system is as follows:

AIX:	/var/adm/*name_of_syslog_file*
Solaris:	/var/adm/messages

After you create the syslog file, restart the syslog with the following command:

```
Kill -HUP `cat/etc/syslog.pid`
```

If you prefer to use Cookie Proxy's own log files, you must specify the ***TraceFile*** parameter in the configuration file for the Cookie Proxy, jpas.conf. If you specify ***TraceFile =/var/jpas/logs/jpas.log***, for example, the /var/jpas/logs directory must be set to permit "nobody" class users to write. The date is automatically inserted between name and extension of the specified file name. For example, the date March 1, 2001, appears as jpas 20010301.log.

You can use both syslog and the Cookie Proxy's own log files. In this case, however, you cannot control the trace levels of these two output files separately; the ***TraceLevel*** parameter affects both output files. For more information about these parameters, refer to "Configuring the Everyplace Cookie Proxy" on page 10.

Note for Solaris users:

If you specify the ***LogToSyslog*** parameter in the ibmproxy.conf file, the Edge Server Caching Proxy writes a message in the syslog. Then the message facility becomes "user," and the ID becomes "ibmproxy." When the Cookie Proxy writes the message in the syslog, however, the message facility changes to "daemon" and the ID changes to "JPAS."

Troubleshooting

Error messages in Web browsers

Four types of error messages can appear in the Web browsers if a problem occurs.

Message ID	Default messages
JPAS100E	Not active. This message cannot be customized.
JPAS200E	The Cookie Proxy detected an error. Contact your provider's administrator.
JPAS300E	The server is currently busy. Try again later.
JPAS400E	An unexpected request has been detected.

To customize messages JPAS200E, JPAS300E, and JPAS400E, refer to "Customizing error messages" on page 12.

″JPAS100E Cookie Proxy: Not active″ error message

The error message "JPAS100E Cookie Proxy: Not active" means that the activation of the Cookie Proxy has failed. If this happens, look at the syslog and/or Cookie Proxy's own log file to find the error messages. If nothing has been written in either log file, see the ErrorLog file for the Edge Server Caching Proxy. Instructions for configuring the logging for the Edge Server Caching Proxy are given in "WebSphere Edge Server for Multiplatforms—Web Traffic Express User's Guide." In the trace log, one of the following error statements may appear just before the message “!!!!! JPAS Initialization Error !!!!!.” Do whatever is needed to start the Cookie Proxy successfully.

- Cannot read config file
  - The configuration file for the Cookie Proxy (*jpas.conf*) does not exist. Place the *jpas.conf* file either where the ***ServerInit*** statement in *ibmproxy. conf* specifies (refer to “Configuring the Edge Server Caching Proxy” on page 9) or at the default location (*/etc/jpas.conf*). Then stop and restart the Edge Server Caching Proxy.
  - The configuration file for the Cookie Proxy does exist, but cannot be read. Change the file permissions so that this file can be read by “nobody” class users, and stop and restart the Edge Server Caching Proxy.
- <*Parameter name*> not specified
  - A mandatory parameter is missing from the configuration file. Edit the *jpas.conf* file to specify all the required parameters, and stop and restart the Edge Server Caching Proxy.

Notices

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
Everyplace
IBM
RS/6000
WebSphere

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.

Other company, product, and service names may be trademarks or services marks of others.