

Release Notes for iPlanet™ Portal Server 3.0 Service Pack 5

Updated July 2003

The *Release Notes for iPlanet™ Portal Server, Version 3.0, Service Pack 5* document important information available at the time of release. Installing this product updates the iPlanet Portal Server software to include fixes from Service Pack 1, Service Pack 2, Service Pack 3, Service Pack 3a, and Service Pack 4 and Service Pack 5. The information in this document includes documentation for previous service packs.

NOTE	Upgrading from iPlanet Portal Server Service Pack 1 or Service Pack 2 to iPlanet Portal Server Service Pack 5 is not supported. Upgrades to iPlanet Portal Server Service Pack 5 should be performed only on machines that have iPlanet Portal Server Service Pack 3 or greater installed.
-------------	--

These release notes contain the following sections:

- What's New in Service Pack 5
- Previous Service Pack Enhancements
- Known Problems and Limitations
- Bugs Fixed
- Documentation Updates
- How to Report Problems
- Where to Find More Information

Read this document before you begin installing Service Pack 5. For an online version of this and other Portal Server 3.0 documentation, see the iPlanet documentation Web site at:

<http://docs.sun.com/>

After you install and start using iPlanet Portal Server 3.0, Service Pack 5, check this Web site periodically to view the most up-to-date documentation.

About This Document

This section provides details about this document. It contains the following topics:

- Typographic Conventions
- Sample Machine Names

Typographic Conventions

Table 1 is a three column table that describes the typographic conventions used in this release note. The first column describes typeface or symbol, the second column describes the meaning, and the third column provides an example of how the typeface is used.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories; on-screen computer output.	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name% You have mail.</code>
AaBbCc123	What you type, contrasted with on-screen computer output.	<code>machine_name% su</code> <code>Password:</code>
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized, or glossary terms.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.
<i>AaBbCc123</i>	Command-line placeholder; replace with a real name or value.	To delete a file, type <code>rm filename</code> . <code>http://server.domain:port/login/domain</code> where <i>domain</i> is a Portal Server domain name.

Sample Machine Names

Table 2 is a two column table that lists the machine names used in code examples and the types of iPlanet Portal Server components to which they correspond. The first column of the table contains machine names, the second column states what component is installed on the machine.

Table 2 Sample Machine Names

Machine Name	Running as . . .
server1	The primary Portal Server
server2	iPlanet Portal Server not being used as the profile server in multiple server installations
gateway	iPlanet Portal Server gateway component

What's New in Service Pack 5

This section summarizes the newest enhancements implemented in Service Pack 5.

- Template Modifications
- Tips for Customizing Templates
- Customizing Desktop Top Level TABLE Attributes
- Maximizing Desktop Channels
- Setting Cookies From A JSPPProvider Channel

See the [“Desktop and Provider Changes”](#) section of this document for details on these changes.

- Configuring Multiple Gateway Instances
- Using Wildcards In JavaScript Rewriter Rules
- Disabling Client-Side Caching of Redirected Content
- Advanced Rewriter Concepts

See the [“Gateway Changes”](#) section of this document for details on these changes.

- NetFile Internationalization and Usability Enhancements

See the “[NetFile Changes](#)” section of this document for details on these changes.

- Automatic Proxy Configuration for Netlet Connections
- Controlling Server Session Timeout When Using the Netlet

See the “[Netlet Changes](#)” section of this document for details on these changes.

- Tuning the Gateway for Optimal Performance

See the “[Performance and Tuning Changes](#)” section of this document for details on these changes.

- Disabling Synchronization of User Profile Changes

See the “[Profile Service Changes](#)” section of this document for details on these changes.

- Gateway Profile Attributes
- Non-Portal Server Cookie Management

See the “[Documentation Updates](#)” section of this document for details on these changes.

Previous Service Pack Enhancements

This section summarizes the cumulative enhancements implemented in the following previous Service Packs: iPlanet Portal Server 3.0, Service Pack 1, Service Pack 2, and Service Pack 3a, and Service Pack 4.

Authentication Changes

- A new parameter for redirecting users during login and logout is available.
- Users can be required to authenticate against more than one authentication mechanism.
- User default URLs can be set in the pluggable interface, without changing default URLs in user profiles.
- A new Desktop login channel allows users to register and receive personalized pages.
- Anonymous authentication is available.
- A user with a valid session can go directly to a login module without sending a logout URL.
- Users can change their membership login passwords.
- A user's email address can now be used as the user profile ID on the certificate.
- A persistent cookie mode is now available.

See the [“Authentication Changes”](#) section of this document for details on these changes.

Desktop and Provider Changes

- A new provider allows JavaServer Pages™ (JSP™) technology to be used to write providers for Desktop channels.
- The template scan interval, the length of time between checking to see whether disk files have been updated, can now be changed in the administration console.
- Tabs for organizing Desktop content are available for the edit page.
- The Provider API allows a channel to return either a complete HTML edit form or a subset of a complete HTML page.
- Administrators can prevent users from changing a channel's position on the Desktop.

- The Desktop can display full-width channels.
- The Desktop can display channels without frames, titles or controls.
- The Login Provider Channel template files now use the POST method when submitting login forms.
- The URL scraper can forward cookies passed in HTTP requests to the Desktop.
- Multiple cookies differing only in path or value can be used.
- Providers can access HTTP request and response headers.
- Session time-out units are now in minutes.
- Desktop applications can be run on Macintosh computers.

See the [“Desktop and Provider Changes”](#) section of this document for details on these changes.

Gateway Changes

- Gateway logging is now disabled by default.
- Administrators can set JavaScript™ variables for rewriting.
- Administrators can define JavaScript functions with a single parameter.
- Administrators can define JavaScript functions with multiple parameters.
- Rewrite Applet/Object parameter values can be changed via the administration console.
- Administrators can deny unknown certificates.
- Administrator can specify how many times the gateway should retry socket connections to a destination server.
- Outlook Web Access 2000 applications can now be used with the gateway.
- Some attribute settings are now inactive.

See the [“Gateway Changes”](#) section of this document for details on these changes.

Localization Changes

- Multiple locales for a domain are available.
- The user can select locale.
- The user can see changes in the locale of choice.

- A new properties file allows the default Desktop JSP Provider's description and title to be localized.
- A copy of the sample JSP Provider properties file is provided specifically for localizations.

See the "[Localization Changes](#)" section of this document for details on these changes.

NetFile Changes

- A generic file path search utility is now available for all data file types.
- Each channel now can identify whether it supports a client type's output format.

See the "[NetFile Changes](#)" section of this document for details on these changes.

NetFile Changes

- Improvements in using NetWare File Systems are available.
- Systems and shares can be defined at the domain, role and user level.
- NT hidden shares can be defined using the administration console.
- Shares on Windows NT systems are now alphabetized.
- NetFile usability has been improved.

See the "[NetFile Changes](#)" section of this document for details on these changes.

Netlet Changes

- The Netlet now supports an unlimited number of connections per Netlet.
- The Netlet now supports secure remote FTP transfers.
- The Netlet proxy manages communication between the gateway and target servers and offers improved security.
- Messages in Netlet windows can be changed.
- The Netlet applet can be used with Web browsers that are configured to use automatic proxy configuration (PAC) files.
- Internet Explorer can use automatic configuration files for automatic proxy services.

See the "[Netlet Changes](#)" section of this document for details on these changes.

Performance and Tuning Changes

- Netscape™ Security Services (NSS) is now supported on the gateway component.
- The Maximum Thread Pool Size parameter can be increased.
- A new method for loading multiple attributes in one profile request is available.
- Short-circuiting for session and logging requests improves performance.
- Adjusting iPlanet™ Web Server parameters can improve performance.

See the [“Performance and Tuning Changes”](#) section of this document for details on these changes.

Profile Service Changes

- A separate profile service is now used for each Portal Server instance.
- New methods for getting and setting user properties are available.

See the [“Profile Service Changes”](#) section of this document for details on these changes.

Server Changes

- Portal Server can now be run without the gateway.
- Multiple instances of the Portal Server can be run on different ports.
- The server can now access multiple instances of iPlanet Portal Server from a single server installation.
- You can run applications written using iPlanet Portal Server APIs on a server host that is not iPlanet Portal Server.

See the [“Server Changes”](#) section of this document for details on these changes.

Third-Party Software Changes

- A new parameter allows NetFile to display ISO8859-1 character sets.

See the [“Third-Party Software Changes”](#) section of this document for details on this change.

Webmail Changes

- A workaround to allow Portal Server to display Webmail is now available.

See the “[Webmail Changes](#)” section of this document for details on this change.

Authentication Changes

This section provides details about authentication changes in iPlanet Portal Server. It contains the following topics:

- Using the goto Parameter
- Authentication Chaining
- Setting Default URLs
- Login Channel
- Anonymous Authentication
- Extending Authentication
- Changing Membership Login Passwords
- Using an email Address as User Profile ID
- Setting Persistent Cookies

Using the goto Parameter

The `goto` parameter is now available. It enables applications to instruct authentication to redirect the user to a URL other than the default URL stored in the user profile upon login or logout. It is valid for the current session only, and it does not change the default URL stored in the user profile.

To be redirected to a specific URL, the application must specify the `goto` parameter in the URL.

The `goto` parameter allows the calling application to specify where the user is redirected upon successful login.

For example, if an application wanted to redirect the user to `my.sesta.com` after successful authentication, the URL would be:

`http://server1.domain:port/login?goto=http://my.sesta.com`

An API developer can use the `goto` parameter in conjunction with the logout URL to specify where the user should be redirected upon logout.

For example, if an application wanted to redirect the user to `sesta.com` after logout, the logout link would be:

```
http://server1.domain:port/logout?goto=http://sesta.com
```

Authentication Chaining

Authentication chaining can provide a higher level of security for organizations by requiring users to authenticate against more than one authentication mechanism. For example, if the membership and UNIX authentication modules are chained, Desktop users would authenticate against both to access the Desktop.

To set up authentication chaining, complete the following steps:

1. Log on to the administration console as super administrator.
2. Select Manage Domains.
3. Select the domain for which authentication chaining is to be used.
4. Select Authentication.
5. In the Authentication Chaining Modules field, enter the authentication modules to be chained, separated by spaces. For example:

Membership Unix

6. Select the Authentication Enabled check box to enable authentication chaining.
7. Select Submit. A message is displayed indicating that the profile was successfully updated.
8. Select Continue.

Setting Default URLs

The user's default URL can now be set in the pluggable authentication interface, without changing the default URL in the user's profile. When the user authenticates successfully, the user is redirected to this URL.

A new method called `setDefaultURL` in the pluggable authentication API allows the authentication modules to set the user's default redirect URL on successful authentication:

```
public void setDefaultURL(java.lang.String url)
                        throws LoginException
```

TIP To use this, replace the `setDefaultURL` parameter with the user's default URL. This is an example of setting the default URL to `www.sesta.com`:

```
public void setDefaultURL("http://www.sesta.com")
```

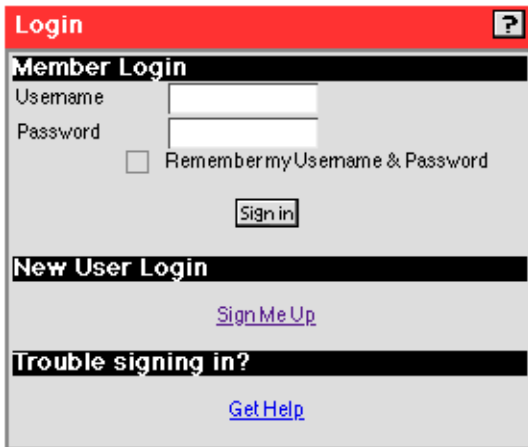
This method overrides the `goto` parameter. See [“Using the goto Parameter.”](#)

Login Channel

Portal Server now contains a membership authentication module that is useful for open portal installations. Combined with anonymous user, unregistered users can view non-personalized content in a portal, and registered users can log in and view personalized content.

The addition of a login channel on the Desktop allows registered users to access the portal, register and receive personalized pages. It allows non-registered users to view static content.

The login channel also allows the user to enable persistent cookies, if the domain allows this option. Persistent cookie support puts user login information into a cookie so that the user does not have to log in for subsequent sessions.



The screenshot shows a web browser window titled "Login" with a red header bar. Below the header, there are three main sections: "Member Login", "New User Login", and "Trouble signing in?". The "Member Login" section contains fields for "Username" and "Password", a checkbox for "Remember my Username & Password", and a "Sign in" button. The "New User Login" section contains a "Sign Me Up" link. The "Trouble signing in?" section contains a "Get Help" link.

The user interface for the login channel does not have an edit page, as user-editable preferences are not available.

Anonymous Authentication

In a typical anonymous installation, the anonymous authentication module would be the only authentication type enabled. When the URL `http://server.domain:port/login/domain` is specified, the user's browser displays the anonymous user Desktop. No user input, other than the URL, is required.

A list of user IDs authorized to log in to the anonymous user's Desktop can be specified and modified through the administration console.

When a user ID appears in the List of Anonymous Usernames, access to the anonymous user's Desktop is granted. The session is assigned to the specified userID. When user ID does not appear in the List of Anonymous Usernames, the session is assigned to the user ID specified in the Default Anonymous Username field and the anonymous Desktop is displayed.

Modifying Default Anonymous User Names

To change the default anonymous user name, complete the following steps:

1. Log on to the administration console as super administrator.
2. From the left frame, select the Manage Domains link to display the Portal Server Domains page.

3. Select the domain to display the Role and Users page.
4. Expand the Profiles link and expand the Authentication link.
5. From the Authentication menu, select Anonymous.
6. Select Show Advanced Options at the bottom of the page.
7. In the List of Anonymous User Names, change default value `anonymous` to the desired user ID.
8. Select Submit at the bottom of the page to commit these changes to the profile server.
9. On the Profile Successfully Updated page, select Continue.

Setting Default Anonymous User Names

To define the default anonymous user name, complete the following steps:

1. Log on to the administration console as super administrator.
2. From the left frame, select the Manage Domains link.
3. In the Domain, Role and Users page, expand the Profiles link and expand the Authentication link.
4. From the Authentication Menu, select Anonymous.
5. Select Show Advanced Options at the bottom of the page.
6. In the Default Anonymous User Name field, change the default user ID `anonymous` to the desired user ID.
7. Select Submit at the bottom of the page to commit these changes to the profile server.
8. On the Profile Successfully Updated page, select Continue.

Enabling Anonymous Desktop

Use the administration console to enable an anonymous Desktop using the Anonymous Authentication Module and Login Channel.

To enable the anonymous Desktop, complete the following steps:

1. Log on to the administration console as super administrator.
2. From the left frame, select the Manage Domains link to display the Portal Server Domains page.
3. Select the domain to display the Domain, Role and Users page.
4. Expand Profiles link.
5. Select Authentication link.

6. From the Authentication Menu, select Anonymous and de-select all other authentication modules.

Portal Server is now defaulted to the Anonymous authentication module in all cases and displays the anonymous Desktop by default.

7. Select Submit at the bottom of the page to commit these changes to the profile server.
8. Select Continue on the Profile Successfully Updated page.
9. Select Show Advanced Options at the bottom of the page.
10. In the Non Interactive Modules, add Membership.

This enables users to use the login channel to use Membership authentication instead of having to use the provided membership login page.

11. Select Enable Persistent Cookie Mode, if persistent cookies are desired.
12. Select Submit at the bottom of the page to commit these changes to the profile server.
13. Select Continue on the Profile Successfully Updated page.

Customizing Anonymous Desktop Templates

You can customize templates for the anonymous Desktop by editing the `menubar.html` file and changing settings in the administration console.

To customize a user logout from the Desktop redirect to the anonymous user Desktop, complete the following steps:

1. Edit the `HREF` definition for the Log Out link in the `/etc/opt/SUNWips/desktop/default/iwtDesktop/menubar.html` file.

TIP Use this format to set the logout from the Desktop to be redirected to the anonymous Desktop in all cases:

```
<A HREF="/logout?goto=/login/Anonymous?domain=mydomain">
```

To customize the Help page for the anonymous Desktop, complete the following steps:

1. Log on to the administration console as super administrator.
2. Select the Anonymous User Desktop.
3. From the left frame, select the Manage Domains link.
4. Select the domain.

5. Select Default Role.
6. Select Users.
7. Select Anonymous.
8. Expand Applications.
9. Select Desktop.
10. Scroll down and select Show Advanced Options.
11. Modify the value for Front Page Help.

The default English locale value in Front Page Help is assumed to be relative from the `/opt/SUNWips/public_html/docs/en_US/online_help` directory.

12. Select Submit at the bottom of the page to commit these changes to the profile server.
13. Select Continue on the Profile Successfully Updated page.

Enabling Anonymous Desktop for Other Domains

To create an anonymous user for any other domain, complete the following steps:

1. Use this command to copy the `/var/opt/SUNWips/iwtAnonymousUser.xml-orig` file to a temporary location (`/tmp`):

```
# cp /var/opt/SUNWips/iwtAnonymousUser.xml-orig /tmp/iwtAnonymousUser.xml-orig
```

2. Change the string `INST_DEFAULT_DOMAIN` in the `/tmp/iwtAnonymousUser.xml-orig` file to the name of the other domain:

```
<iwt:Att name="iwtUser-role"
  userConfigurable="true"
  >
  <Val>/INST_DEFAULT_DOMAIN/defaultRole</Val>
</iwt:Att>
```

3. Use these commands to load the new anonymous user profile to the primary server service:

```
# cd /opt/SUNWips/bin
# ipsadmin create user /other_domain/anonymous /tmp/iwtAnonymousUser.xml-orig
```

4. Use this URL to access the authentication menu for the new domain in the browser:

```
http://server1.domain:port/login?domain=/other_domain
```

Disabling Anonymous Desktop

To disable anonymous Desktop, complete the following steps:

1. Log on to the administration console as super administrator.
2. From the left frame, select the Manage Domains link to display the Portal Server Domains page.
3. Select the domain to display the Domain, Role and Users page.
4. Expand Profiles link.
5. Select Authentication link.
6. In the Authentication Menu, de-select the Anonymous auth module.
At least one auth module entry must be selected in the field after you de-select any module.
7. Select Submit at the bottom of the page to commit these changes to the profile server.
8. Select Continue on the Profile Successfully Updated page.

Modifying the Login Channel

The login channel can be modified to work with other authentication modules. A sample template is available to illustrate how the login channel can be changed to work with the Unix authentication module, rather than the Membership authentication module.

To enable Unix authentication for the login channel, complete the following steps:

NOTE	When replacing files to modify the operation of the Desktop, make copies of the files being replaced, first, so that they can be reinstated at any later date.
-------------	--

1. As root, use these commands to make a copy of the `display.html` file:

```
# cd /etc/opt/SUNWips/desktop/default/iwtLoginProvider
# mv display.html display_iwtAuthMembership.html
```

2. Replace the `display.html` file with

`/etc/opt/SUNWips/desktop/default/iwtLoginProvider/display_iwtAuthUnix.html`.

```
# cp display_iwtAuthUnix.html display.html
```

3. Log on to the administration console as super administrator.
4. From the left frame, select the Manage Domains link to display the Portal Server Domains page.
5. Select the domain to display the Domain, Role and Users page.
6. Expand the Profiles link and select the Authentication link.
7. Scroll down to and select Show Advanced Options.
8. In the Non Interactive Modules field, add Unix.
9. Select Submit at the bottom of the page to commit these changes to the profile server.
10. Select Continue on the Profile Successfully Updated page.

The login channel now uses UNIX authentication.

The template file, `display_iwtAuthUnix.html`, is an example of how templates could be created to enable other authentication modules for the login channel. The contents of the built-in login page for a given authentication method provide an example of the correct parameters to include in the `display.html` template.

Extending Authentication

When a registered user authenticates from the anonymous Desktop, Portal Server obtains information about the user and presents the user Desktop from the user profile. When a new user registers from the anonymous Desktop, the user's current session from the anonymous Desktop is destroyed before the `auth` module in the URL for the user's default Desktop is called.

This allows a user with a valid iPlanet Portal Server session to directly go to a login module without sending a logout URL. For example, a login channel sends the following URL to allow an anonymous user to register with the membership module:

```
http://server.domain:port/login/Membership?domain=/mydomain&arg=newsession
```

The `arg=newsession` parameter instructs the authentication module to destroy the current session before calling the authentication module in the URL.

Previously, if a user wanted to switch from anonymous user to registered user, it was impossible to authenticate the user using another authentication module such as the Membership module since an anonymous user has a valid session.

Changing Membership Login Passwords

Users can now change their membership login passwords.

To change the membership login password, the user must complete the following steps:

1. Select the Edit icon from the User Information channel menu.
2. Enter the original password and the new password and confirm the new password.

Password checking is subject to the same rules as the membership authentication module. The user must authenticate via Membership for changes to the Membership password.

Using an email Address as User Profile ID

A user's email address can now be used as the user profile ID on the certificate. When the email address is selected, the `cert_auth` module searches for the `emailAddr` field in the certificate's user subject `dn` field for the attribute tag `emailaddr` and uses its value to access the user's profile ID.

The tag `emailAddr` is stored in the `iwtAuthCert.properties` file. It can be replaced with a different value, depending on the site or the certificate issuer.

To use the email address as profile ID, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select your domain and select Profiles and Authentication.
3. Select Cert from the list.
4. Select email address from the What field in cert to use to access user info in profile field.
5. Select Submit.

Setting Persistent Cookies

Persistent cookies are now supported. If the persistent cookie mode is enabled, the user:

- Is not required to log in to Portal Server after relaunching the browser
- Can display the Desktop immediately without logging in

NOTE If the user explicitly logs out when persistent cookie mode is enabled, logging in is required on the next visit.

To set up persistent cookie mode for an individual user, the user must select the Remember My Username and Password check box using the Login Channel.

Administrators can set a persistent cookie for a domain. To do this, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select your domain and select Profiles and Authentication.
3. In the Profile:Auth page, select Show Advanced Options.
4. In The Persistent Cookie MaxAge Value text box, specify the maximum age of the cookie in seconds.
5. Select the Enable Persistent Cookie Mode check box to enable the persistent cookie mode for users in this domain.

Desktop and Provider Changes

This section provides details about Desktop changes in iPlanet Portal Server. It contains the following topics:

- Template Modifications
- Tips for Customizing Templates
- Customizing Desktop Top Level TABLE Attributes
- JavaServer Pages Provider
- Setting Cookies From A JSPPProvider Channel
- Reloading Templates without a Server Restart

- Tabbed Desktop
- Using Form Control
- Maximizing Desktop Channels
- Locking Channel Positions
- Setting Up Full-Width Channels
- Setting Up Frameless Channels
- Default Login Channel Templates Changes
- Forwarding Cookies
- Using Non-iPlanet Portal Server Cookie Management
- Enabling Access to HTTP Requests and Responses
- Setting Session Time-out Units
- Running Desktop Applications on Macintosh Clients

Template Modifications

The patch installer attempts to preserve customized template information and to automate the update of that information. However, since the contents of the files cannot be accurately predetermined, any modified template files are backed up in the same directory as their updated counterparts, with the patch name postfixed to the template name. For example,

```
/etc/opt/SUNWips/desktop/default/iwtBookmarkProvider/display.template
```

might be backed up to

```
/etc/opt/SUNWips/desktop/default/iwtBookmarkProvider/display.template.preSP5.
```

The backup files are also copied back to their original location upon service pack removal.

To help avoid potential content-related customization problems, refer to the [“Tips for Customizing Templates”](#) section of this document.

Table 3 is a three column table that lists the template files, `.properties` files, `xml` files, and platform files that are modified by this service pack. The first column of the table contains the template or flatfile names. The second column contains the component with which the template is associated. The third column describes the change to the template.

Table 3 Template Modifications

Template or Flatfile Name	Component	Change
/etc/opt/SUNWips/platform.conf	Gateway and Platform	<p>Added <code>ips.gateway.newDomainLogic</code> entry to support single and double level domains.</p> <p>Added <code>allow.desktop.caching.in.client</code> to allow the caching of the iPlanet Portal Server Desktop by the browser.</p> <p>Note: By default, the value for this option is set to false and must be set to true in order to cache the Desktop.</p> <p>Added <code>ips.gateway.logging.hostlookup</code> to control whether reverse DNS lookup occurs during logging calls.</p>
/etc/opt/SUNWips/properties.file	Platform	<p>Added <code>domainlist.refresh.interval</code> to reduce LDAP traffic retrieving primarily static data.</p> <p>This option enables the list of Portal domains (which is normally retrieved at every login) to be cached, and refreshed with the given interval in milliseconds. This reduces the load on the LADP server.</p> <p>By enabling caching , new domains will not be visible to users until the next refresh. For test and development systems this value should be left at 0. However, on stable production systems, the value should be increased. A reasonable value is 1800000 (30 minutes).</p> <p>Note: By default, the value for this option is set to 0, thus the behavior will remain the same as in Service Pack 4 unless this value is changed.</p>

Table 3 Template Modifications (*Continued*)

Template or Flatfile Name	Component	Change
<i>install_dir</i> /SUNWips/locale/iwtNetFileApplet.properties	Platform	<p>Added <code>systemencoding=System</code> Encoding function</p> <p>Added country names used in add host and edit host info</p>
<i>install_dir</i> /SUNWips/locale/iwtNetFileServlet.properties	Platform	<p>Added <code>error43=Share</code> does not exist or you do not have permission to access</p> <p>Added country name labels for NetFile Lite function</p> <p>Added <code>macie50=<FONT</code> <code>COLOR=FF0000></code></p> <p>Note: The <code></code> tag on Internet Explorer 5.0 on a Macintosh computer is not a supported browser version. Please update the browser to Internet Explorer 5.1.5 or greater.</p>
<i>/etc/opt/SUNWips/desktop/*</i> /iwtDesktop/userTemplate.html	Platform	<p>Added top level table definitions previously rendered internally by the FrontProvider Servlet.</p> <p>Removed content tag [tag:content]</p> <p>Note: if content tag has already been removed the changes will have to be made manually.</p>
<i>/etc/opt/SUNWips/xml</i> /iwtDesktop.xml	Profile	Added attribute <code>iwtMaximizeProvider</code> to <code>iwtDesktop</code> profile
<i>/etc/opt/SUNWips/xml</i> /iwtGateway.xml	Profile	Added attribute <code>iwtGateway=UnencodedURLCharset</code> to gateway profile
<i>template_dir</i> /iwtBookmarkProvider/display.template	Platform	Added <code>openSavedBookmarkURL</code> function

Table 3 Template Modifications (*Continued*)

Template or Flatfile Name	Component	Change
<i>install_dir</i> /SUNWips/locale/iwtGateway.properties	Platform	<p>Added X-x11=Rewrite JavaScript Function Parameters in Fractured HTML entry</p> <p>Added X-x17=Rewrite JavaScript Function Parameters in JavaScript or a URL entry</p> <p>Added X-x18=Extend Portal Session for Clientbound Netlet Traffic entry</p>
<i>install_dir</i> /SUNWips/public_html/third_party /	Platform	Replaced citrix_start.html
<i>install_dir</i> /SUNWips/locale/iwtNetletServlet.properties	Platform	<p>Added</p> <p>macloopbackhost=http://127.0.0.1 entry</p>
<i>install_dir</i> /SUNWips/bin/ipshttpd	Platform	Overwrote IPS_CLASSES value to include additional jar entries
/etc/opt/SUNWips/platform.conf*	Platform and Gateway	<p>Added</p> <p>ips.gateway.sockretries=3 entry</p> <p>Addedallow.client.caching=true entry</p> <p>Added</p> <p>netlet.session.extension=true entry</p> <p>Added</p> <p>ips.gateway.mem_management_option=false entry</p> <p>Added</p> <p>ips.gateway.mem_management_interval=30 entry</p> <p>Added</p> <p>ips.gateway.mem_threshold=70 entry</p> <p>Removed</p> <p>netlet.session.extension.for.\clientbound.traffic entry</p> <p>Removed blank lines</p>

Table 3 Template Modifications (*Continued*)

Template or Flatfile Name	Component	Change
/etc/opt/SUNWips/xml/iwtGateway.xml	Profile	<p>Added openSavedBookmarkURL:y value to iwtGateway-JavaScriptRewrite attribute</p> <p>Added window.location to iwtGateway-JavaScriptVariableConvert attribute</p> <p>Added new Attribute:</p> <p>iwtGateway-JavaScriptFracturedHTML</p> <p>Added new Attribute</p> <p>iwtGateway-JavaScriptFunctionParameterJavaScriptOrURL</p> <p>Added new Attribute</p> <p>iwtGateway-ThirdPartySessExt</p> <p>Modified rules for NetMail and NetFile in Rewrite Applet Parameters Values List of the Gateway Profile.</p>
install_dir/SUNWips/bin/ipsgateway	Gateway	<p>Overwrote IPS_CLASSES value to add additional jar entries</p> <p>Changed gateway specific Java Virtual Machine™ (JVM™) parameters in CMD value</p> <p>Note: These changes have been added for the multiple gateway instance support. This script is now much longer than the previous script.</p>
/etc/init.d/ipsgateway	Gateway	<p>Overwrote IPS_CLASSES value to add additional jar entries</p> <p>Changed gateway specific JVM parameters in CMD value</p> <p>Note: These changes have been added for the multiple gateway instance support. This script is now much longer than the previous script.</p>

Tips for Customizing Templates

Because the Portal Server itself is so customizable, you should follow some precautions to ensure that any customizations made to the iPlanet Portal Server product are preserved after a product upgrade. First, set up a customized template directory if you have not already done so. While this directory might be an entire subset of the default template directory, it is advisable to copy over only those template files that you will be customizing. This particular scheme would then use the default directory as a base for all templates and would help ensure that customized templates are not accidentally overwritten when the default templates are modified.

Creating a Customized Template Directory

1. Create a directory at the same level as the `/etc/opt/SUNWips/desktop/default/` directory with a new name such as `mytemplates`. In that directory, put only copies of the templates you need to modify. The other templates will be retrieved from the default directory.
2. Edit the templates in the `mytemplates` directory according to your own preference. Refer to the [“Desktop Template and Tag Index”](#) section of this document for additional template-related information.
3. Log into the administration console.
4. Select Manage Domains.
5. Select the domain you want to administer.
6. Go to Applications | Desktop.
7. In the Display/Layout section, change the value of the Template Directory field to match the name of the directory you just created—for example, `mytemplates`.
8. Click Submit at the bottom of the page.

In general, avoid modifying templates that have only a functional purpose rather than a look and feel purpose. One example of a template that should not need modifications is the `iwtNetletProvider/display.template`. This template contains only JavaScript necessary for the launching of the Netlet. The contents of the Netlet pop-up window should instead be customized by modifying the associated `.properties` file (`install_dir/SUNWips/locale/iwtNetletServlet.properties`). This is because the product might have a functional change that would overwrite a customization done specifically to that particular template file. This example also exhibits why it is important to keep only customized files in the customized template directory.

For instance, in the iPlanet Portal Server Service Pack 3 product, the Netlet launching behavior changed. Therefore, for customers who use the Netlet, and upgraded from the iPlanet Portal Server Service Pack 2 product to iPlanet Portal Server Service Pack 3, and have an entire copy of the default template directory, the functional change was not propagated to the customized template directory.

The following sections contain instructions for some simple template modifications that may help you get you started with your new customized template directory.

Customizing the Channel Border Look

To modify the look of all the channels (for example, where the buttons are and how the border looks) do the following:

1. Edit the file

```
/etc/opt/SUNWips/desktop/mytemplates/iwtDesktop/providerWrapper.html
```

2. Edit the file

```
/etc/opt/SUNWips/desktop/mytemplates/iwtDesktop/minimize.html
```

3. Logout of the Desktop and then log back in again.

Changing the Desktop Background Colors, Images, and Product Name

1. Edit the file `/etc/opt/SUNWips/desktop/mytemplates/banner.html` to:

- o Point to different graphics files with your company name or logo.
- o Change the background color and layout to match that of your portal's look.

If you change the red background color in `banner.html`, you should also change the background color in the following files wherever the HTML tag attribute `BGCOLOR` appears:

- o `contentTemplate.html`
- o `layout1Template.html`
- o `layout2Template.html`
- o `layout3Template.html`
- o `layout4Template.html`
- o `minimized.html`
- o `optionsTemplate.html`
- o `providerWrapper.html`

2. If you want to change the iPlanet Portal Server 3.0 product name that appears on the Desktop in the menubar, you must remove the tag `[tag:productName]` that appears in the following files and replace it with the text you prefer. The files are:

- `banner.html`
- `contentTemplate.html`
- `editTemplate.html`
- `errorTemplate.html`
- `layout1Template.html`
- `layout2Template.html`
- `layout3Template.html`
- `layout4Template.html`
- `menubar.html`
- `optionsTemplate.html`
- `popupMenubar.html`
- `popupTemplate.html`
- `userTemplate.html`

This text can be changed in the profile store, but it is system-wide and not specific to any one domain. To change the value system-wide, do the following:

- a. From the profile server command line, as root type:

```
install_dir/SUNWips/bin/ipsadmin get component iwtPlatform > /tmp/file
```

- b. Edit the file and delete all the attributes except for `iwtPlatform-productName`. Change the attribute value between the `<Val></Val>` tags to be the value you want-- most likely the title of your company portal. Save that file with just that attribute in it.

- c. From the command line, enter the following:

```
install_dir/SUNWips/bin/ipsadmin change component iwtPlatform /tmp/file
```

3. Remove the `iwtSampleRSS` and `iwtIPInfo` channels. These channels both contain iPlanet information, so they can be removed from the installation by removing them from the available providers.

These channels are sourced from the RSS Provider and URL Scraper providers, respectively, and are examples of how the iPlanet Portal Server can pull content from other sources. The `iwtIPInfo` channel is simply an HTML page and a GIF file displayed by the URLScraper. The `iwtSampleRSS` channel is an RDF file with an accompanying GIF file. You can set up channels like this quickly for your own portal by using the Channel Wizard in the iPlanet Portal Server Administration Console.

4. Restart the server for any changes you have made to take effect

Changing the Channel Buttons:

The links and image tags for the channel buttons are generated dynamically by the Desktop, but the actual image file sources are taken from the Desktop properties file. To change the button images, do the following:

1. Edit the file `/opt/SUNWips/locale/iwtDesktop.properties` and change the properties entries:
 - `ProviderCommands-helpIcon`
 - `ProviderCommands-minimizeIcon`
 - `ProviderCommands-maximizeIcon`
 - `ProviderCommands-editIcon`
 - `ProviderCommands-removeIcon`
 - `ProviderCommands-attachIcon`—all relative to *install_dir*/SUNWips/public_html/
2. Edit the following entries in the same `.properties` file as above to change the ALT text for the IMG tags in the channel buttons.
 - `ProviderCommands-help`
 - `ProviderCommands-minimize`
 - `ProviderCommands-maximize`
 - `ProviderCommands-edit`
 - `ProviderCommands-remove`
 - `ProviderCommands-attach`

Using Images for Channel Titles

1. In the `providerWrapper.html` file, replace `[tag:title]` with the following:

```
<script>
drawTitle('[tag:title]');
</script>
```

2. In the <HEAD> section of the `userTemplate.html` file, insert the following:

```
<script>
function drawTitle(title)
{
    if (title == 'special title') {
        document.write('<img src=/images/specialtitle.gif>');
    }
    else {
        document.write(title);
    }
}
</script>
```

Changing The Link Color in The Desktop

Edit the following line in `userTemplate.html` to change link colors for the page:

```
<BODY BGCOLOR="#FFFFFF">
```

Desktop Template and Tag Index

Table 4 is two column table that contains a list of templates and tag descriptions. The first column lists the template name. The second column provides a tag description.

Table 4 Desktop Template and Tag Index

Template	Tag Description
iwtAppProvider	
display.template - Contains the JavaScript that launches the windows that the HTML applications are displayed in.	[tag:apps] - Replaced with the application listings
iwtBookmarkProvider	

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
display.template - Contains JavaScript language for the Bookmark Provider to open new windows launched from the form submittal or from saved bookmark links in the provider window. JavaScript also performs redirection of URLs to avoid burdening the gateway with unnecessary requests for content that can be retrieved directly by the browser.	<p>[tag:bookmarks] - List of bookmark links</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag>windowOption] - JavaScript variable default for method of launching bookmark windows (taken from iPlanet Portal Server user preferences).</p>
edit.template - contains the edit screen formatting for the Bookmark provider. It contains four tags.	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:resourceList] - Selectable list of bookmarks for the edit page</p> <p>[tag:resourceCount] - Total number of bookmarks</p> <p>[tag>windowOptions] - Default for checkboxes defining how the bookmark should be opened (new window, existing window, etc.)</p>
iwtMailCheckProvider	
display.template - Mail check layout provider content	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:mailStatColor] - Color of status text, based on actual mail status</p> <p>[tag:mailStatus] - Status text</p> <p>[tag:mailCount] - Total count of unread messages</p>
iwtNetletProvider	
display.template - Contains JavaScript necessary to launch a Netlet session.	[tag:content] - Appropriate JavaScript for launching the correct Netlet type based on the Netlet rules
edit.template - Contains the formatting for the edit of the Netlet provider.	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:newRuleSelect] - HTML section for adding new dynamic rules</p> <p>[tag:targetList] - Section of HTML table listing existing dynamic rules</p> <p>[tag:targetCount] - Total number of dynamic rules</p>

Table 4 Desktop Template and Tag Index *(Continued)*

Template	Tag Description
<code>wtUserInfoProvider</code>	
<code>content.html</code> - Content page for the UserInfo provider.	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop</p> <p>[tag:iwtUserInfoProvider-greeting] - User's greeting</p> <p>[tag:iwtUserInfoProvider-firstname] - User's first name</p> <p>[tag:iwtUserInfoProvider-lastName] - User's last name</p> <p>[tag:iwtUserInfoProvider-currentDate] - Current date</p> <p>[tag:iwtUserInfoProvider-timeLeft] - Time left in user's session</p> <p>[tag:iwtUserInfoProvider-maxIdle] - Maximum idle time</p>

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
edit.template - Edit page for the UserInfo provider.	<p>[tag:iwtDesktop-fontFacel] - Default font for the Desktop (sans-serif)</p> <p>[tag:iwtUserInfoProvider-greeting] - User's greeting</p> <p>[tag:iwtUserInfoProvider-firstname] - User's first name</p> <p>[tag:iwtUserInfoProvider-lastName] - User's last name</p> <p>[tag:iwtUserInfoProvider-currentDate] - Date</p> <p>[tag:iwtUserInfoProvider-timeLeft] - Time left in user's session</p> <p>[tag:iwtUserInfoProvider-maxIdle] - Maximum idle time</p> <p>[tag:iwtUserInfoProvider-timeZoneList] - List of timezones</p> <p>[tag:iwtUserInfoProvider-IMAPServerName] - IMAP server name</p> <p>[tag:iwtUserInfoProvider-SMTPServerName] - SMTP server name</p> <p>[tag:iwtUserInfoProvider-IMAPPassword] - IMAP server password</p> <p>[tag:iwtUserInfoProvider-IMAPUserId] - IMAP username</p> <p>[tag:iwtUserInfoProvider-localeList] - List of available locales</p> <p>[tag:iwtUserInfoProvider-passwordHandler] - HTML code to change membership password, if available</p>
passwordHandler-Membership.html - Partial template inserted into edit.template if membership authentication is used. This allows the user to change password.	[tag:iwtDesktop-fontFacel] - Default font for the Desktop (sans-serif)
iwtDesktop	
alertTemplate.html - Not used.	No tags

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
<code>arrangeProvider.js</code> - Javascript used in the Desktop Layout page	No tags
<code>bareProviderWrapper.html</code> - Template for each provider wrapper with no titlebar.	<p>[tag:borderSize] - size of border (CELLPADDING) around provider HTML table</p> <p>[tag:size] - size of border, (BORDER) around provider HTML table</p> <p>[tag:bgColor] - provider background color</p> <p>[tag:content] - provider content</p>
<code>banner.html</code> - the banner across the top of the Desktop pages, including the edit, layout, and content pages.	No tags
<code>contentTemplate.html</code> - the HTML template for the Content (Channels) page	<p>[tag:noCache] - Inserts <code>noCache.html</code> template</p> <p>[tag:productName] - Product name</p> <p>[tag:openFrontPage] - Inserts <code>openFrontPage.js</code> template</p> <p>[tag:style] - Inserts <code>style.html</code> template</p> <p>[tag:banner] - Inserts <code>banner.html</code> template</p> <p>[tag:menubar] - Inserts <code>menubar.html</code> template</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:thinProviders] - Checkbox list of available thin providers to add to Desktop</p> <p>[tag:wideProviders] - Checkbox list of available wide providers to add to Desktop</p> <p>[tag:fullProviders] - Checkbox list of available full width providers to add to Desktop</p>

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
editTemplate.html - Generic edit page template.	<p>[tag:noCache] - Inserts noCache.html template</p> <p>[tag:productName] - Product Name</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:openFrontPage] - Inserts openFrontPage.js template</p> <p>[tag:style] - Inserts style.html template</p> <p>[tag:banner] - Inserts banner.html template</p> <p>[tag:menubar] - Inserts menubar.html template</p> <p>[tag:providerName] - The name of the provider or channel</p> <p>[tag:inlineError] - Replaced with inlineError.html template if error has occurred</p> <p>[tag:title] - The title of the provider or channel</p> <p>[tag:contentOptions] - The edit page content from the provider or channel</p>
errorTemplate.html - Error template. Used when an internal Desktop error (usually a provider error) has occurred making display of the providers impossible.	<p>[tag:noCache] - Inserts noCache.html template</p> <p>[tag:productName] - Product name</p> <p>[tag:style] - Inserts style.html template</p> <p>[tag:banner] - Inserts banner.html template</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:productName] - Product name</p> <p>[tag:helpFile] - URL or directory path to the Help file</p> <p>[tag:helpTag] - String for link to Help file</p>
inlineError.html - HTML to show an error message	[tag:errorMessage] - The error message
launchPopup.js - JavaScript to launch a popup window.	No tags

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
layout1Template.html - left/thin, right/wide.	<p>[tag:noCache] - Inserts noCache.html template</p> <p>[tag:productName] - Product name</p> <p>[tag:openFrontPage] - Inserts openFrontPage.js template</p> <p>[tag:arrangeProvider] - Inserts arrangeProvider.js template</p> <p>[tag:performSubstitution] - Inserts performSubstitution.js template</p> <p>[tag:performColumnSubstitution] - Inserts performColumnSubstitution.js template</p> <p>[tag:selectAll] - Inserts selectAll.js template</p> <p>[tag:switchColumns] - Inserts switchColumns.js template</p> <p>[tag:style] - Inserts style.html template</p> <p>[tag:banner] - Inserts banner.html template</p> <p>[tag:menubar] - Inserts menubar.html template</p> <p>[tag:iwtDesktop-fontFacel] - Default font for the Desktop (sans-serif)</p> <p>[tag:layoutFullTop] - Inserts layoutFullTop.html template</p> <p>[tag:leftUserProviderList] - List that shows left column channels</p> <p>[tag:rightUserProviderList] - List that shows right column channels</p> <p>[tag:layoutFullBottom] - Inserts layoutFullBottom.html template</p>

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
layout2Template.html - left/wide, right/thin.	[tag:noCache] - Inserts noCache.html template
	[tag:productName] - Product name
	[tag:openFrontPage] - Inserts openFrontPage.js template
	[tag:arrangeProvider] - Inserts arrangeProvider.js template
	[tag:performSubstitution] - Inserts performSubstitution.js template
	[tag:performColumnSubstitution] - Inserts performColumnSubstitution.js template
	[tag:selectAll] - Inserts selectAll.js template
	[tag:switchColumns] - Inserts switchColumns.js template
	[tag:style] - Inserts style.html template
	[tag:banner] - Inserts banner.html template
	[tag:menubar] - Inserts menubar.html template
	[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)
	[tag:layoutFullTop] - Inserts layoutFullTop.html template
	[tag:leftUserProviderList] - List that shows left column channels
	[tag:rightUserProviderList] - List that shows right column channels
	[tag:layoutFullBottom] - Inserts layoutFullBottom.html template

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
layout3Template.html - left/thin, center/wide, right/thin.	[tag:noCache] - Inserts noCache.html template
	[tag:productName] - Product name
	[tag:openFrontPage] - Inserts openFrontPage.js template
	[tag:arrangeProvider] - Inserts arrangeProvider.js template
	[tag:performSubstitution] - Inserts performSubstitution.js template
	[tag:performColumnSubstitution] - Inserts performColumnSubstitution.js template
	[tag:selectAll] - Inserts selectAll.js template
	[tag:switchColumns] - Inserts switchColumns.js template
	[tag:style] - Inserts style.html template
	[tag:banner] - Inserts banner.html template
	[tag:menubar] - Inserts menubar.html template
	[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)
	[tag:layoutFullTop] - Inserts layoutFullTop.html template
	[tag:leftUserProviderList] - List that shows left column channels
	[tag:rightUserProviderList] - List that shows right column channels
	[tag:layoutFullBottom] - Inserts layoutFullBottom.html template
	[tag:centerUserProviderList] - List that shows center column channels

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
layout4Template.html - left/thin, center/thin, right/thin.	[tag:noCache] - Inserts noCache.html template
	[tag:productName] - Product name
	[tag:openFrontPage] - Inserts openFrontPage.js template
	[tag:arrangeProvider] - Inserts arrangeProvider.js template
	[tag:performSubstitution] - Inserts performSubstitution.js template
	[tag:performColumnSubstitution] - Inserts performColumnSubstitution.js template
	[tag:selectAll] - Inserts selectAll.js template
	[tag:switchColumns] - Inserts switchColumns.js template
	[tag:style] - Inserts style.html template
	[tag:banner] - Inserts banner.html template
	[tag:menubar] - Inserts menubar.html template
	[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)
	[tag:layoutFullTop] - Inserts layoutFullTop.html template
	[tag:leftUserProviderList] - List that shows left columns channels
	[tag:rightUserProviderList] - List that shows right column channels
layoutFullBottom.html - Partial HTML template for layout pages when the user has a full-width channel available at the bottom of the layout.	[tag:centerUserProviderList] - List that shows center column channels
	[tag:layoutFullBottom] - Inserts layoutFullBottom.html template
	[tag:fullbottomUserProviderList] - List of Full Width (Bottom) Channels to move
	[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
layoutFullTop.html - Partial HTML template for layout pages when the user has a full width channel available at the top of the layout.	<p>[tag:fulltopUserProviderList] - List of Full Width (Top) Channels to move</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p>
menubar.html - HTML for the menubar containing the Home, Options, Content, Layout, Help, and Logout links	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:productName] - Product name</p> <p>[tag:help_link] - Link to help from Desktop</p>
minimized.html - Template of a provider when it is in its minimized state - just the title and button bar showing, no content area showing.	<p>[tag:borderSize] - The border size of the channel (default 0)</p> <p>[tag:size] - Table width, fixed at 100%</p> <p>[tag:title] - The title of the provider or channel</p> <p>[tag:provider_cmds] - Inserts the channel command button links, for example, minimize and detach.</p>
noCache.html - HTML META headers to prevent browser caching of the pages.	No tags
openFrontPage.js - Javascript to go back to the Desktop page.	No tags
openURLInParent.js - Javascript to open a URL in the parent window. Used in popup windows.	No tags

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
optionsTemplate.html - Template for the Options page of the Desktop.	<p>[tag:noCache] - Inserts noCache.html template</p> <p>[tag:productName] - Product name</p> <p>[tag:openFrontPage] - Inserts openFrontPage.js template</p> <p>[tag:style] - Inserts style.html template</p> <p>[tag:banner] - Inserts banner.html template</p> <p>[tag:menubar] - Inserts menubar.html template</p> <p>[tag:inlineError] - Replaced with inlineError.html template if error has occurred</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:serviceTimeout] - Provider Timeout in seconds</p> <p>[tag:layoutOneChecked] - Makes Radio button for layout one the default</p> <p>[tag:layoutTwoChecked] - Makes Radio button for layout two the default</p> <p>[tag:layoutThreeChecked] - Makes Radio button for layout three the default</p> <p>[tag:layoutFourChecked] - Makes Radio button for layout four the default</p>
performColumnSubstitution.js - JavaScript used on the Layout page.	No tags
performSubstitution.js - JavaScript used on the Layout page.	No tags
popupMenubar.html - Menubar to be used in popup windows.	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:productName] - Product name</p>

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
popupTemplate.html - Used to show provider and channel content in detached windows. Similar to providerWrapper, but not in a table structure.	<p>[tag:noCache] - Inserts noCache.html template</p> <p>[tag:productName] - Product name</p> <p>[tag:providerTitle] - Provider or Channel title</p> <p>[tag:openURLInParent] - Inserts openURLInParent.js template</p> <p>[tag:style] - Inserts style.html template</p> <p>[tag:popupMenubar] - Inserts popupMenubar.html template</p> <p>[tag:providerContent] - Content of the provider</p>
providerWrapper.html - Template that all providers and channels use for layout on Desktop. Defines the look of the border of the providers and channels on the screen.	<p>[tag:borderSize] - The border size of the channel</p> <p>[tag:size] - Table width, fixed at 100%</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:title] - Provider title</p> <p>[tag:provider_cmds] - Inserts the channel command button links, for example, minimize or detach.</p> <p>[tag:bgColor] - Background color</p> <p>[tag:content] - Provider or channel content inserted here</p>
removeProvider.js - Not used.	No tags
selectAll.js - Javascript used on the Layout page.	No tags
style.html - Stylesheet/CSS information for the HTML pages.	No tags
switchColumns.js - Javascript used on the Layout page.	No tags

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
userTemplate.html - The base Desktop layout structure document. There is very little content in this file, since most of the the Desktop is swapped in during processing in the servlets. This is a good place to put global JavaScript variable initializations which may need to be used by the providers.	<p>[tag:noCache] - Inserts noCache.html template.</p> <p>[tag:launchPopup] - Inserts launchPopup.js template</p> <p>[tag:detachedContent] - Provider content</p> <p>[tag:productName] - Product name</p> <p>[tag:style] - Inserts style.html template</p> <p>[tag:banner] - Inserts banner.html template</p> <p>[tag:inlineError] - Replaced with inlineError.html template if error has occurred</p> <p>[tag:content] - Provider or channel content (HTML table) inserted here</p> <p>[tag:menubar] - Inserts menubar.html template</p>
iwtTabProvider	
editForm.html - Edit page template for creating and removing tabs.	<p>[tag:iwtTabProvider.makeNewTab] - Inserts makeNewTab.html template</p> <p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:iwtTabProvider.removeRenameTab] - Inserts removeRenameTab.html template</p>
makeNewTab.html - HTML used in editForm.html for creating a new tab.	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:iwtTabProvider.tabTopics] - HTML for selecting a tab topic</p>
removeRenameTab.html - HTML used in editForm.html for removing or renaming existing tabs.	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:iwtTabProvider.tabList] - List of available tabs to remove</p>
selectedTab.html - HTML used to show the currently selected tab on the Desktop.	<p>[tag:iwtDesktop-fontFace1] - Default font for the Desktop (sans-serif)</p> <p>[tag:iwtTabProvider.tabName] - Tab name</p>
tabs.html - Template of the tab provider on the Desktop.	<p>[tag:tabs] - Inserts either tab.html or selectedTab.html depending on whether the current tab being drawn is selected</p> <p>[tag:editTabs] - Inserts editTabs.html template</p>

Table 4 Desktop Template and Tag Index (*Continued*)

Template	Tag Description
tab.html - HTML used to show the unselected tab or tabs on the Desktop.	<p>[tag:iwtDesktop-fontFace1] – Default font for the Desktop (sans-serif)</p> <p>[tag:iwtTabProvider.tabURL] – Tab URL (When Tab is clicked)</p> <p>[tag:iwtTabProvider.tabName] – Tab name</p>
iwtWeatherProvider	
This directory is not used	No tags

Customizing Desktop Top Level TABLE Attributes

The top level TABLE attribute definitions have been moved from being emitted directly by the FrontProvider Servlet to the userTemplate Desktop template file. All customized template directories under /etc/opt/SUNWips/desktop/ that contain an iwtDesktop/userTemplate.html file will be modified automatically by the installer to include the default TABLE attributes which were already being set by the FrontProvider.

As a result, the attributes can now be modified to provide more flexible control over the look and feel of the entire iPlanet Portal Server Desktop in addition to providing a means to use Cascading Style Sheets for themes, or JavaScript to change the TABLE attributes dynamically.

If the content tag ([tag:content]) was already removed from the userTemplate.html file prior to the service pack installation, the template will need to be updated manually in order for the portal contents to be displayed correctly.

Just below the inlineError tag ([tag:inlineError]) of each customized userTemplate.html file, add the following:

```
<!-- BEGIN TOP FULL PROVIDERS -->
<TABLE WIDTH=100% BORDER=0 CELLPADDING=2 CELLSPACING=0><TR><TD
VALIGN=TOP><CENTER>
[tag:fullTopContent]
</CENTER></TD></TR></TABLE>
<!-- END TOP FULL PROVIDERS -->

<TABLE WIDTH=100% BORDER=0 CELLPADDING=0 CELLSPACING=4><TR>
<TD WIDTH=[tag:leftWidth]% VALIGN=TOP>
<!-- BEGIN LEFT PROVIDERS -->
[tag:leftContent]
<!-- END LEFT PROVIDERS -->
</TD>
```

```

<TD WIDTH=[tag:centerWidth]% VALIGN=TOP>
<!-- BEGIN CENTER PROVIDERS -->
[tag:centerContent]
<!-- END CENTER PROVIDERS -->
</TD>

<TD WIDTH=[tag:rightWidth]% VALIGN=TOP>
<!-- BEGIN RIGHT PROVIDERS -->
[tag:rightContent]
<!-- END RIGHT PROVIDERS -->
</TD></TR></TABLE>

<!-- BEGIN BOTTOM FULL PROVIDERS -->
<TABLE WIDTH=100% BORDER=0 CELLPADDING=2 CELLSPACING=0><TR><TD
VALIGN=TOP><CENTER>
[tag:fullBottomContent]
</CENTER></TD></TR></TABLE>
<!-- END BOTTOM FULL PROVIDERS -->

```

Maximizing Desktop Channels

Individual channels on the iPlanet Portal Server Desktop can now be maximized. Maximizing a channel means that it is displayed on entire Desktop space between the horizontal menu bars. When a channel has been maximized, the banner and the menu bars are still visible.

If a channel is edited in the maximized state, its previous size will be restored once the edit is completed. Additionally, if the provider is detached while maximized, it will be re-attached in a restored state. This feature is also extended by adding the ability to tag-swap the `providerName` tag (`[tag:providerName]`) in the provider Desktop templates.

In order to maximize a provider channel, a URL should be constructed so that the channel's name appears at the end of the query string. The following is an example of a relative URL for a stocks channel:

```
/DesktopServlet?action=content&provider=iwtMaximizeProvider&targetprovider=stocks
```

Selecting this link from anywhere on the Desktop or explicitly setting it in the URL field of the web browser, after being fully qualified, will result in the stocks channel being maximized.

This maximize feature differs from the maximize functionality already built in to the Desktop as a provider command. When a provider has been minimized, the menu bar for the provider will contain a maximize button. Maximize, in this instance, will merely restore the provider to its original position and size on the Portal Desktop.

One example of how to use this new feature on the Desktop would be to create the maximize URL dynamically using the tag-swapping capability of the iPlanet Portal Server from within the `providerWrapper.html` template. The provider commands available are determined based on the policy for that provider and user. However, a maximize button could be inserted just prior to the `provider_cmds` tag so each provider could be independently maximized.

For example:

```
...
<TD BGCOLOR="#999999" NOWRAP>
  <P ALIGN="RIGHT">
    <A HREF="/DesktopServlet?action=content&provider
      =iwtMaximizeProvider&targetprovider
      =[tag:providerName]">
    <IMG SRC="/desktop/images/b_maximize.gif" ALT="Maximize" BORDER=0></A>
    <A HREF="/DesktopServlet?action=content&provider=iwtFrontProvider">
    <IMG SRC="/desktop/images/b_attach.gif" ALT="Restore"
    BORDER=0>[tag:provider_cmds]
  </TD>
...
```

In this example, default Desktop images were used for two additional buttons—one to maximize the provider, and one to restore it to its original size. To avoid potential confusion for the end users, these buttons should be made unique if the providers will be allowed to minimize or detach.

Both the `providerWrapper.html` and `userTemplate.html` files could be changed to have only one image which would represent the current state of the provider (maximized or restored).

For example:

Add the following to the `HEAD` element of the `userTemplate.html` file:

```
...
<SCRIPT>
var pageLoc=this.location.href;
var isMaximized=pageLoc.search(/provider=iwtMaximizeProvider/);
function setProvState(provName) {
  if (isMaximized == -1) {
    document.location.href="/DesktopServlet?action=content&provider
      =iwtMaximizeProvider&targetprovider="+provName;
  }
  else {
    document.location.href="/DesktopServlet?action=content&provider
      =iwtFrontProvider"
  }
}
function setImgState() {
  if (isMaximized == -1) {
    document.images.provState.alt="Maximize";
    document.images.provState.src="/desktop/images/b_maximize.gif";
  }
  else {
    document.images.provState.alt="Restore";
    document.images.provState.src="/desktop/images/b_attach.gif";
  }
}
```

```

}
</SCRIPT>
...

```

Edit the `providerWrapper.html` template to look like the following:

```

...
<TD BGCOLOR="#999999" NOWRAP>
<P ALIGN="RIGHT">
  <A HREF="javascript:setProvState(' [tag:providerName] ')">
    <IMG SRC="/desktop/images/b_maximize.gif"
      ALT="Maximize" NAME="provState" BORDER=0></A>
  [tag:provider_cmds]
</TD>
...

```

The preceding example uses JavaScript to determine whether the provider is maximized or not and to dynamically update the button and corresponding URL.

NOTE The Netscape Navigator™ 4.x browser does not correctly update the ALT text of the image object. For example, the ALT text for the restore button will say “maximize.”

This example demonstrates how the provider maximization feature might be generally applied to the Desktop. Many other applications are possible. If Secure Remote Access Pack has been installed, verify that any reference to the maximize or restore URLs are rewritten correctly.

JavaServer Pages Provider

The JSP Provider allows you to use JavaServer Pages technology to write providers for Desktop channels. JSP Provider-based channels have the following attributes in addition to the attributes of other channels:

- `contentPage` - the JavaServer Page specification used to generate the HTML content for the channel through the provider's `getContent` method. The generated HTML must contain only those tags that are appropriate for display within a channel.

- `editPage` - the JavaServer Page specification used to generate the internal content for the edit form through the provider's `getContent` method displayed when the user selects the channel's Edit function. This page is optional, and if it is not specified, the `isEditable` method for the provider returns false.
- `processPage` - the JavaServer Page specification used to process the results of an edit page using the `processEdit` method.

The `contentPage` and `editPage` JSP specifications can be used in various combinations. For example, you can use a JSP specification to generate content while you can use Java™ code in the provider class to generate the edit page. Both have access to iPlanet Portal Server platform services.

Processing of the edit form consists of Java code that checks validity of the form entry and updates user preferences for the channel. The result is a display of the Desktop in the case of success or a display of the edit page in the case of a failure, possibly with some error information for the user.

To handle the processing of an edit form, the JSP-based provider has these options:

- Defining a `processPage` JSP. If defined, this JSP is invoked via a `POST` request and the JSP processes the results, either using a script or a bean or other Java class. The JSP must produce a redirect in the response. This redirect then becomes the return value for the provider's `processEdit` method.
- Extending the `JSPProvider` class and implementing the `processEdit` method. The `processPage` attribute is left blank.

Support for JSP-based channels is provided through a class called `JSPProvider`. The `JSPProvider` extends the `ProfileProviderAdapter` class to support other attributes for the channel by using the profile service.

When specifying a JSP in one of the JSP attributes, the path name is interpreted relative to the Desktop template directory using the same algorithm as for other Desktop templates, including the locale setting.

If the user's locale is `de_DE`, the Desktop type is `SunBlue`, and a JSP attribute is set to `myChan/chan.jsp`, the system would search for these JSP files:

```
/etc/opt/SUNWips/desktop/SunBlue_de_DE/myChan/chan.jsp
/etc/opt/SUNWips/desktop/SunBlue_de_DE/chan.jsp
/etc/opt/SUNWips/desktop/SunBlue/myChan/chan.jsp
/etc/opt/SUNWips/desktop/SunBlue/chan.jsp
/etc/opt/SUNWips/desktop/default_de_DE/myChan/chan.jsp
/etc/opt/SUNWips/desktop/default_de_DE/chan.jsp
/etc/opt/SUNWips/desktop/default/myChan/chan.jsp
/etc/opt/SUNWips/desktop/default/chan.jsp
```

TIP For more information on implementing JSP-based channels, see the Javadoc™ software shipped with Service Pack 5.

Setting Cookies From A JSPProvider Channel

Cookies can now be set from JSP provider channels using `response.addCookie(cookie_name)` to amend the Set-Cookie response from the Desktop Servlet. For example, a personal cookie-based counter could be added to the out-of-box `samplecontent.jsp` by adding the following code to `/etc/opt/SUNWips/desktop/desktop_name/samplecontent.jsp`:

```
<%
int value=0;
Cookie[] cookArr = request.getCookies();
for ( int i=0; i < cookArr.length ; i++ ) {
    Cookie acookie = cookArr[i];
    if ( acookie.getName().equals("Counter") ) {
        try
        {
            value= Integer.parseInt(acookie.getValue() );
            value++;
            out.println("According to your cookie counter, you have been here <B>" +
                value + "</B> times.");
        }
        catch(Exception ex){}
    }
}
Cookie nCook = new Cookie("Counter",String.valueOf(value));
nCook.setMaxAge(1500);
response.addCookie(nCook);
%>
```

When the default JSP provider channel is accessed, a cookie will now be set and the provider will indicate the cookie value plus one which represents the current number of visits to the page.

Reloading Templates without a Server Restart

When the Desktop accesses templates to generate content, it reads them from disk and caches them. All subsequent requests for the template are served from the cache.

The Desktop periodically checks to see if the disk files have been updated. If the disk file is newer than the cache, the template is re-cached based on the updated disk file.

The length of time between checking to see if the disk files have been updated is the template scan interval. This interval can now be changed in the administration console. Changing the template scan interval causes the Desktop to immediately check for changes to the disk files and then wait for the new interval value before re-checking again.

To change the template scan interval, complete the following steps:

1. Log on to the administration console as super administrator.
2. From the left frame, select the Management Platform Settings link.
3. Expand the Applications link.
4. Select the Desktop link.
5. In the Component Profile: Desktop page, edit the Template Scan Interval Field.

TIP The default value for the template scan interval is 900 seconds, or 15 minutes.

6. Select the Submit button, at the bottom of the page, and save the changes.
7. Select the Continue button on the Profile Successfully Updated page.

Tabbed Desktop

The Desktop can now use tabs to organize content. Tabbed Desktop pages can be individually modified to customize the Desktop.

The tab feature must be turned on for any given domain. By default, it is not active. The super administrator must enable the Tab Provider and then configure or remove tabs in a chosen domain.

Configuring the Tab Desktop

To enable Desktop tabs in a particular domain, complete the following steps:

1. Log on to the administration console as super administrator.
2. From the left frame, select the Manage Domains link.
3. Select a domain.
4. Expand the Applications link in the right frame.
5. Select the Desktop link.
6. At the bottom of the Profile: Desktop page, select Show Advanced Options.

7. In the Profile: Desktop page, scroll down to the Channels Field.
8. If the `iwtTabProvider` *is shown* in the Available Channels list, complete the following steps:
 - a. Highlight `iwtTabProvider` in the Available Channels list.
 - b. Select the arrow to move `iwtTabProvider` to the Selected Channels field.
9. If the `iwtTabProvider` *is not shown* in the Available Channels list, then complete the following steps:
 - a. In the New Channel Name window, enter a new channel name, `iwtTabProvider`.
 - b. In the Provider Class Name field, enter a new provider class:


```
com.iplanet.portalserver.providers.tab.TabProvider
```
 - c. In the Available Channels list, select Add to display `iwtTabProvider` in the Available Channels list.
 - d. In the Available Channels list, highlight `iwtTabProvider`.
 - e. Select the arrow to move `iwtTabProvider` to the Selected Channels field.

10. Scroll down the page and confirm that the Active Channel List Module contains a Tab Channel List entry. The Tab Channel List Module must be selected. For example:

```
com.iplanet.portalserver.desktop.util.channellist.TabChannelList
```

11. In the Start Tab field, enter a tab name. The first tab default name is My Front Page.

This Tab is always present on every Desktop in the domain and is not user configured.

12. In the Available Tabs field, edit the default tab conditions that the tab contains. Change the name, providers, and description to create a custom tab. For example:

```
name=new tab|channels=iwtTabProvider;iwtUserInfoProvider;
iwtIPInfoProvider;iwtSampleRss|desc=new tab description|
removable=true|renamable=true
```

13. In the Tab Pattern field, enter the name of a tab content template, and the providers to be included.
14. In the Make From Scratch Tab field, enter a suitable heading and all content providers that appear on the Edit Tab Provider page. For example:

```
name=Make From Scratch ...|channels=iwtTabProvider;iwtUserInfoProvider;
iwtBookmarkProvider;iwtIPInfoProvider|desc=Design a tab from the ground up|
removable=true|renamable=true
```

15. In the Maximum Number of Tabs field, provide the total number of tabs that can be on the Desktop.

TIP The default value is 4.

16. Select Submit to save the changes.

17. On the Profile Successfully Updated page, select Continue.

Configuring the Tab Provider on the Desktop

Users can configure the tabs on their Desktops. The tab's channel edit page allows users to create, rename, or remove tabs from their Desktops. In addition, users can select which tab should be present on the initial Desktop page.

To configure tabs, the user must complete the following steps:

1. As a user, log in to the iPlanet Portal Server Desktop.
2. From the tab banner, select Edit.

In the Edit Tab Provider page, the user can use a predefined tab content template by topic, or by choosing each channel for the new tab manually.

Creating Customized Tabs

To create custom tabs, the user must complete the following steps:

1. In the Edit Tab Provider page's Tab Name field, enter the name of the tab being created.
2. In the Tab Topics field, select Make From Scratch.
3. Select Finished at the bottom of the page.
4. In the Channels page, select the channels to display on the Desktop.

TIP During configuration of Desktop pages and layout, the administrator uses the administration console to determine which channels are thin and thick.

5. Select Finished at the bottom of the page to return to the Desktop.

Creating Default Content Tabs

To create a default content for a tab, the user must complete the following steps:

1. In the Edit Tab Provider's Tab Name field, enter the name of the tab being created.
2. In the Tab Topics field, select a pre-made Tab Content Provider.
3. Select Finished at the bottom of the page to return to the Desktop.

Aligning Tabs

Desktop tabs can now be aligned from the left side or the right side of the Desktop. By default, tabs are left-aligned.

To use tabs, the super administrator must enable the Tab Provider and then configure or remove tabs in a selected domain.

To change to right-to-left ordering of Desktop tabs, complete the following steps:

1. Log in to the administration console.
2. Select Manage Domains.
3. Select the domain for which you want to apply the changes.
4. Select the key next to Applications to expand the Application list.
5. Select Desktop to display the Profile: Desktop page.
6. From the Available Channels list, select iwtTabProvider.
7. Select Edit Channel to display the Profile: Tab Provider page.
8. Select Show Advanced Options at the bottom of the page.
9. Put a check mark in the check box labeled RTL Presentation.
10. Select Submit.
11. Select Continue when the console displays the `Profile was successfully updated` message.

Using Form Control

The Provider API now allows a channel to return either a complete HTML edit form, or a subset of a complete HTML page in response to a request for the edit page.

Provider API

Integer constants are added to the Provider interface that return values from the `getEditType()` method. These integer constants define the form type, return type, from the `getEditType()` method:

```
public static final int provider.EDIT_SUBSET ;  
public static final int provider.EDIT_COMPLETE ;
```

New methods query and set the form type.

```
public int getEditType();
```

The Desktop uses the `getEditType()` method so that it knows to expect either a complete or subset HTML form to be returned when calling `channel.getEdit()`.

These restrictions apply to what can be returned from `getEdit()` when the edit type is equal to `EDIT_COMPLETE`:

- This method returns a complete, valid, HTML form.
- The form is an encoding type of `application/x-www-form-urlencoded`.
- The form must contain the correct parameters for instructing the Desktop to process the page, as defined in `editTemplate.html`.
- The following parameters must be present in the submitted form:
 - `action=process`
 - `provider="iwtEditProvider"`
 - `targetprovider=`*target channel name*
- The form action must be `/DesktopServlet`. When returning a complete HTML form, a channel must submit valid actions to the Desktop as defined in the Desktop URL Javadoc software.

Provider Attributes

For channels that extend the `ProfileProviderAdapter` class, a new attribute can be defined in the profile component:

```
</iwt:Att>
<iwt:Att name="iwtProvider-editType"
        desc="Edit Form Type"
        type="singlechoice"
        idx=" "
        userConfigurable="TRUE">
  <Val>edit_subset</Val>
  <CVal>edit_subset</CVal>
  <CVal>edit_complete</CVal>
  <Rperm>ADMIN</Rperm><Rperm>OWNER</Rperm>
  <Wperm>ADMIN</Wperm>
</iwt:Att>
```

The default value is different for each provider. Variations to this might include turning off write permission for `OWNER`, if one or the other edit type was not implemented.

All iPlanet Portal Server default channels return `Provider.EDIT_SUBSET`. Modifying the `-editType` attribute causes a malfunction. A new channel must return `Provider.EDIT_SUBSET`, or `Provider.EDIT_COMPLETE` depending on how the `getEdit()` method is implemented.

Locking Channel Positions

Administrators can now lock a channel's position so that the user cannot change its position or remove it from the Desktop. The purpose is to force the user to see particular content.

The Layout page that allows the user to arrange channels on the Desktop does not list locked channels.

To lock a channel's position, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select the domain and select Profiles and Policy.
3. Deselect the Movable check box for the channel to lock the channel's position.

TIP If you select the Movable check box, the user can move channels around in the Desktop.

4. Deselect the Removable check box, so that the channel cannot be removed from the Desktop.

TIP If you select the Removable check box, the user can remove channels from the Desktop.

5. Select Submit.

To unlock a channel's position, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select the domain and select Profiles and Policy.
3. Select the Movable check box for the channel to unlock the channel's position.

TIP If you select the Movable check box, the user can move channels around in the Desktop.

4. Select the Removable check box so the channel can be removed from the Desktop.

TIP If you select the Removable check box, the user can remove channels from the Desktop.

5. Select Submit.

Setting Up Full-Width Channels

The Portal Server Desktop can now display full-width channels. A full-width channel spans the width of the Desktop, either at the top or bottom.

To configure a full-width channel, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select your domain and select Applications and Desktop.
3. Select the channel to modify and select Edit Channel.
4. Select Show Advanced Options.
5. Modify Width to either `full_top` or `full_bottom`.
6. Select Submit.

Setting Up Frameless Channels

The Portal Server Desktop can now display unframed channels. A frameless channel is one that is displayed without a title, controls, and a border or frame.

To configure a frameless channel, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select your domain and select Applications and Desktop.
3. From the list of available channels, select the channel you want to present without a border.
4. Select Edit Channel and select Show Advanced Options.
5. Deselect the Framed? check box if it is selected.

TIP If the Framed? check box is selected, the channel is displayed with a title, controls, and border.

6. Select Submit.

NOTE To modify just the border of the channel, edit the `hasBorder` attribute in the Policy page.

Default Login Channel Templates Changes

The Login Provider Channel template files now use the `POST` method for improved security when submitting the login forms. This change provides the choice of using the `POST` or `GET` methods in customized login channels.

Using the `POST` method is more secure because it prevents the password from showing up in the server logs, URLs and bookmarks.

Forwarding Cookies

The URL scraper can now forward cookies passed in the HTTP request to the Desktop. That is, the URL scraper sends cookies when it makes a connection to the target site to retrieve the content it is scraping. The URL scraper also sends set-cookie requests to the browser. That is, it gets all cookies from set-cookie headers and adds them to the HTTP response to the client browser.

By default, no cookies are forwarded. For the affected domain, role or user, the administrator must use the administration console to set the list of cookies to forward.

To forward cookies, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select your domain and select Profiles and Policy.
3. Change the entries in the allow and deny lists for the Cookies To Forward privilege for the channel.

A * entry allows or denies all cookies. Other entries are compared using a prefix match.

Using Non-iPlanet Portal Server Cookie Management

Multiple cookies containing the same name and the same path can be stored, as long as the domain is not explicitly set to the same value. By default, the domain value is the fully qualified hostname of the server that originally set the cookie.

To set your own cookies:

1. Log in to the iPlanet Portal Server administration console.
2. Select Gateway Management.
3. Select Manage Gateway Profile.
4. Select the Non Portal Server Cookie Management check box.

If the cookie is in a different domain from the server (for example, if scraping a page to the iPlanet Portal Server Desktop that sets its own cookie), complete the following steps:

1. Add that cookie to the Forward Cookie URL List.
2. Select Submit.
3. Select Continue when the console displays the message `Profile was successfully updated`.
4. Select Server Management.
5. Select Manage Server Profile.
6. Add the cookie domain name to the Cookie Domain List and select Add.

TIP Use this format to add the domain name:

`.domain_name.com`

Note the `.` that precedes the name.

For example:

`.sesta.com`

7. Select Submit.
8. Select Continue when the console displays the `Profile was successfully updated message`
9. Log out of the administration console and restart the server and gateway.

If the cookie is set from the same domain as the server, complete the following steps:

1. Select Submit.

2. Select Continue when the console displays the Profile was successfully updated message
3. Log out of the administration console and restart the server and gateway.

Enabling Access to HTTP Requests and Responses

Providers can now access HTTP request and response headers. This change is desirable for single sign-on, setting cookies, getting parameters from the HTTP headers, and for inserting data into the headers.

Three new methods in the Content Provider interface are available to provide this. The methods are:

- `public StringBuffer getContent(HttpServletRequest req, HttpServletResponse res);`
- `public StringBuffer getEdit(HttpServletRequest req, HttpServletResponse res);`
- `public URL processEdit(HttpServletRequest req, HttpServletResponse res);`

These methods in the `ProviderAdapter` and `ProfileProviderAdapter` classes call the `getContent`, `getEdit`, and `processEdit` methods.

Table 5 is a two column table that lists the indicated methods for the `HttpServletRequest` and `HttpServletResponse` objects. The first column lists the method name and the second column lists the return values.

Table 5 `HttpServletRequest` and `HttpServletResponse`

<code>getSession(boolean)</code>	Null
<code>isRequestedSessionIdFromCookie()</code>	False
<code>isRequestedSessionIdFromUrl()</code>	False
<code>isRequestedSessionIdValid()</code>	False
<code>getContentLength()</code>	-1
<code>getInputStream()</code>	<code>UnsupportedOperationException</code>
<code>getParameter(String)</code>	uses internal Map to return parameter
<code>getParameterNames()</code>	uses internal Map to return names
<code>getParameterValues(String)</code>	uses internal Map to return values
<code>getReader()</code>	<code>UnsupportedOperationException</code>
<code>encodeRedirectUrl(String)</code>	arg
<code>encodeUrl(String)</code>	arg

Table 5 HttpServletRequest and HttpServletResponses (*Continued*)

getSession(boolean)	Null
sendError(int)	UnsupportedOperationException
sendError(int, String)	UnsupportedOperationException
sendRedirect(String)	UnsupportedOperationException
setStatus(int)	UnsupportedOperationException
setStatus(int, String)	UnsupportedOperationException
getOutputStream()	UnsupportedOperationException
getWriter()	UnsupportedOperationException
setContentLength(int)	UnsupportedOperationException
setContentType(String)	UnsupportedOperationException

Setting Session Time-out Units

The session time out unit of measurement is now in minutes.

To set the session time-out to the maximum possible value, complete the following steps:

1. Log on to the administration console as super administrator.
2. Select Manage Domains.
3. Select the name of the desired domain.
4. Select Session under Profiles.
5. Make value of Maximum Idle Time to the maximum value of: 153722867280912930.
6. Make value of Maximum Session Time to the maximum value of: 153722867280912930.
7. Select Submit.

Running Desktop Applications on Macintosh Clients

NetFile and NetMail applications now work on a Macintosh similarly to the way they work on other supported platforms.

The Netlet application, when used on a Macintosh, however, does not support the dynamic loading feature. If the Netlet is enabled, Macintosh clients automatically load the Netlet when the Netlet Channel is enabled on the Desktop.

Table 6 is a two column table that lists the minimum system requirements for running the Netlet, NetMail, and NetFile applications on Macintosh clients. The first column contains the system component name, and the second column describes the minimum requirements for that component.

Table 6 Minimum system requirements for running Portal Server applications on Macintosh clients

Component	Description
Operating environment	Macintosh 8.6 – 9.2.2
Browser	Microsoft Internet Explorer 5.0
Java Virtual Machine	Macintosh OS Runtime for Java (MRJ) 2.2.3

NOTE When using Internet Explorer 5.0 on a Macintosh client, the client cannot make SSL connections to the gateway with the default self-signed certificate. This certificate is installed when the iPlanet Portal Server installer is run. Any other certificate can be used.

The NetMail local installer does not work on Macintosh clients.

Gateway Changes

This section provides details about gateway changes in iPlanet Portal Server. It contains the following topics:

- Configuring Multiple Gateway Instances
- Using Wildcards In JavaScript Rewriter Rules
- Disabling Client-Side Caching of Redirected Content
- Advanced Rewriter Concepts
- Gateway Logging
- Rewriting JavaScript Variables in JavaScript
- Rewriting JavaScript Functions with a Single Parameter
- Rewriting Javascript Functions with Multiple Parameters

- Editing Rewrite Applet/Object Parameter Values
- Denying Unknown Certificate Authorities
- Setting the Number of Socket Connection Retries
- Using Outlook Web Access 2000
- Inactive Attributes

Configuring Multiple Gateway Instances

It is now possible to configure multiple gateway instances on a single system, with the following caveats:

- All instances on a single system must be associated with the same profile and platform server instances.
- Each gateway instance needs a unique IP address to bind to, with a hostname in DNS.
- All gateway instances associated with the same profile server instance must listen on the same port, for example, 443, and use the same protocol, for example, HTTPS.

Updated Command Options

The `ipsgateway` script in `install_base/SUNWips/bin` now supports several new options. Table 7 is a two column table that describes the new `ipsgateway` command options. The first column contains the command, and the second column provides a description of the new command.

The following examples assume that the commands are being run from the directory in which they reside.

Table 7 New Command Options

Command	Description
<code>ipsgateway create</code> <i>fully_qualified_instance_name</i>	Adds a new gateway instance listening on <i>fully_qualified_instance_name</i>
<code>ipsgateway delete</code> <i>fully_qualified_instance_name</i>	Deletes the instance listening on <i>fully_qualified_instance_name</i>
<code>ipsgateway startall</code>	Starts all instances
<code>ipsgateway stopall</code>	Stops all instances

In addition, the following commands in `install_base/SUNWips/bin` now accept an optional instance name argument to specify the instance to target:

- `ipsgateway start [fully_qualified_instance_name]`
- `ipsgateway stop [fully_qualified_instance_name]`
- `ipsgateway watchdog on|off [fully_qualified_instance_name]`
- `certadmin [fully_qualified_instance_name]`
- `checkipsgw [fully_qualified_instance_name]`

The instance created at install time is considered the default instance, and is addressed using the above commands with no hostname argument. The default instance cannot be deleted.

There is also a copy of the `ipsgateway` script in the `/etc/init.d` directory.

NOTE	The gateway instance name must be the fully qualified hostname in DNS for the IP address to which this instance will bind.
-------------	--

Creating Multiple Gateway Instances

You can create multiple instances of the iPlanet Portal Server gateway, after you install the iPlanet Portal Server gateway.

Unless you have a multi-homed system and wish to have individual gateway instances for each physical interface, you will need to configure a virtual interface for each gateway instance to bind to. For more information on configuring virtual interfaces, refer to InfoDoc 15659 at <http://www.sunsolve.sun.com>.

By default, the minimum and maximum JVM heapsize value for the default instance is 512Mb and 768Mb respectively, and for additional instances is 256Mb and 384Mb respectively. If you configure a large number of instances, you may want to change these values in the `ipsgateway` script, to avoid exhausting physical memory.

To create a new gateway instance, perform the following steps.

1. Configure a virtual interface for the new IP address. Refer to InfoDoc 15659.
2. Add a forward and reverse entry in DNS for this IP address. When creating a new gateway instance, use the fully qualified hostname that you gave this IP address in DNS as the instance name.

After the iPlanet Portal Server gateway has been installed, and the appropriate interfaces are established, do the following to create a new gateway instance:

3. As root enter the following commands:

```
# cd /opt/SUNWips/bin
# ipsgateway create fully_qualified_instance_name
```

4. When prompted, answer the questions.

NOTE If the gateway is listening on all interfaces, the script prompts you to choose only one interface. You can accept the default gateway interface or enter another one for the gateway to listen on.

```
Your default instance currently binds to all IP addresses.
Enter the FQDN of the IP address it should bind to. [gateway.sesta.com]:
IP address in DNS for gateway.sesta.com: 192.168.01.03.
```

```
Restart default instance, and start new instance when complete? [y/n]: y
```

```
About to create new gateway instance:
  Hostname    = gwinstance2.sesta.com
  IP address  = 192.168.01.07
```

```
About to reconfigure default gateway instance:
  Hostname    = gateway.sesta.com
  IP address  = 192.168.01.03
```

```
Continue? [y/n]: y
```

```
Creating self-signed certificate for gwinstance1.sesta.com:
```

```
NOTE: Field entries cannot contain an = character.
      All Fields are mandatory, if left blank they
      will be filled by some default values
```

```
What is the fully-qualified DNS name of this host? [gwinstance2.sesta.com]
What is the name of your organization (ex: Company)? [] mycompany
What is the name of your organizational unit (ex: division)? [] mydivision
What is the name of your City or Locality? [] mycity
What is the name (no abbreviation please) of your State or Province? [] my
state
What is the two-letter country code for this unit? [] US
```

```
Token name is needed only if you are not using the default internal (software)
cryptographic module, for example, if you want to use a crypto card (Token
names
could be listed using: modutil -dbdir
/etc/opt/SUNWips/cert.gwinstance1.red.ipplanet.com -list);
Otherwise, just hit Return below.
```

```
Please enter the token name []  
  
Enter the name you like for this certificate: certificate2  
  
creating passphrase to be used for the certificate...  
IMPORTANT: Remember this passphrase, it may be needed later  
Enter passphrase []  
Verify (re-enter) passphrase []
```

After creating the instance, do the following to add the instance name and default portal domain for that instance:

1. Add the new gateway instance name to the Platform Gateway list.
 - a. Log on to the administration console as super administrator.
 - b. From the left frame select the Sever Management link.
 - c. Select Manage Server Profile.
 - d. Add the new gateway instances to the Gateway List. For example,
`gateway2.sesta.com`
2. Add the default portal domain for that instance.

This is the domain that the gateway instance will contact if one is not specified by the client. The domain is specified by adding the following to the Domain URLs list of that domain:

- a. From the left frame, select Manage Domains.
- b. Click on the Domain.
- c. Click on the Authentication Link.
- d. Add the gateway URLs to the Domain URLs list using the following format:

gateway_instance_name

gateway_instance_ame/portal_domain

gateway_instance_ipaddress

gateway_instance_ipaddress/portal_domain

Alternatively, use the `ipsadmin` command line utility to:

1. Update the Platform Gateway list by retrieving the `iwtPlatform` component profile.

2. Edit the `iwPlatform-gateways` attribute, and update the Domain URLs list by retrieving the domain profile and editing the `iwAuth-domainURL` attribute.

Using Wildcards In JavaScript Rewriter Rules

The JavaScript rewriting ability has been extended to include the ability to use wildcards for rules that can be added to the Rewrite JavaScript Variables in the URLs section of the Gateway Profile. This helps reduce the number of similar rules necessary to represent the same basic JavaScript content. It also allows the creation of rules to represent complex JavaScript content that makes proficient use of the JavaScript object model where arrays are used to access data values.

Previously, if the content looked like:

```
document.all["IMG"+img].src = "../../images/"
```

The only solution would be to change the code in a manner similar to the following:

```
up2dir = "../.." document.all["IMG"+img].src = up2dir+"images/"
```

and add `up2dir` to the Rewrite JavaScript Variables In URLs section of the Gateway Profile.

It is now possible to define a rule such as `document.all*.src` in the same section of the iPlanet Portal Server Gateway Profile.

Disabling Client-Side Caching of Redirected Content

A new entry has been added to the `/etc/opt/SUNWips/platform.conf` file called `allow.client.caching`. This controls the caching behavior of non-Desktop content redirected through the gateway.

Setting `allow.client.caching` value to **false** will result in a `pragma:no-cache` header being set for any content retrieved by the gateway. This ensures that no Portal content accessed by remote users will be cached on their local machine, regardless of their individual browser caching options if they are using at least an HTTP 1.0 compliant browser.

For example, if the iPlanet Portal Server has been deployed to take advantage of its authentication and secure remote access features, but not the Desktop itself, setting `allow.client.caching` to **false** will prevent whatever content is redirected after successful authentication from being cached on the user's local machine.

Limitations and Considerations

Setting `allow.client.caching` to **false**, will dramatically increase the load on the gateway component. Caching itself exists to eliminate unnecessary server requests for static content. However, in a secure environment, the performance ramifications of not allowing client caching of content may be outweighed by the added security of content not being permanently, even temporarily, stored on a remote machine. This might be the case when a remote employee is accessing sensitive corporate intellectual property from a public Internet kiosk.

Additionally, a Microsoft Internet Explorer 5.x limitation exists in which helper applications cannot load encrypted data with associated MIME types not handled internally by the browser if a “no-caching” header is set. The same is true for saving encrypted files to a different location on disk.

Internet Explorer has its own functionality for preventing the permanent caching of SSL pages. This functionality can be configured using an advanced browser setting called “Do Not Save Encrypted Pages To Disk.” When this option is not enabled, Internet Explorer first decrypts the SSL data, then caches it in the clear prior to handing the decrypted copy to a helper application like Word for `.doc` files. This functionality is not related to the iPlanet Portal Server itself, since it affects users accessing any SSL-enabled web server in the same way. When the “Do Not Save Encrypted Pages To Disk” option is enabled, the behavior appears to be exactly the same, except the browser cleans up after itself by removing the decrypted data from the cache directory once it is handed off to the helper application.

Therefore, the iPlanet Portal Server `allow.client.caching` option should not be set to false if Internet Explorer will be a supported client by the deployed portal, with end users downloading or saving files locally that are not registered to be handled internally by the browser itself.

Caching Alternatives

Many secure portal deployments need to work around the browser no-cache header limitation for SSL pages. Working around the browser no-cache header can be difficult if the browsers are not under corporate IT control. If the browsers are under IT control however, a custom Internet Explorer browser can be built using the Internet Explorer Administrator Kit (IEAK).

With the IEAK, the advanced browser option “Do Not Save Encrypted Pages to Disk” can be locked down in an enabled state. If the iPlanet Portal Server gateway is running https, no pages accessed by the client will be cached. This essentially works around the limitation of encrypted pages having to be decrypted and cached prior to being passed to a helper application. Such is the case when this browser option is not enabled. With the default iPlanet Portal Server `platform.conf` entry `allow.client.caching` set to true, Internet Explorer browsers can access any pages through the gateway regardless of whether they need helper applications to launch without caching any data.

To limit access and possible caching by other browsers, logic can be added to `/etc/opt/SUNWips/auth/[your_template_dir]/login_template.html` that disallows their login, and possibly usage.

For example:

```
<HEAD>
<TITLE>Login</TITLE>
<SCRIPT>
function checkBrowser() {
    if (navigator.userAgent.toLowerCase().indexOf("msie") > 0 ) {
        // NOP
    }
    else {
        document.location.href="/other_browser_error.html";
    }
}
</SCRIPT>
</HEAD>
<BODY BGCOLOR="#ffffff" onLoad="checkBrowser();"
onResize="this.history.go(-1);">
```

Alternately, multiple gateways may be used with a redirector in front basing its decision on the userAgent. This would enable `allow.client.caching` to be set to false on one iPlanet Portal Server gateway accessed by Netscape clients and set to true on a different gateway accessed by Internet Explorer clients (customized using IEAK or with a downloaded activeX plugin that would enforce the “Do Not Save Encrypted Pages To Disk” option enabled). Because SRAP licenses are based on the number of users instead of CPUs, having multiple gateway hardware boxes will not affect software costs for the same number of users.

Using the same psuedo-code as above for an Internet Explorer-only solution, the multi-browser solution might look as follows:

```
<HTML>
<HEAD>
<TITLE>http://portal.iplanet.com</TITLE>
<SCRIPT>
function checkBrowser() {
    if (navigator.userAgent.toLowerCase().indexOf("msie") > 0 ) {
        document.location.href="https://ie-portal.iplanet.com";
    }
    else {
        document.location.href="https://ns-portal.iplanet.com";
    }
}
</SCRIPT>
</HEAD>
<BODY BGCOLOR="#ffffff" onLoad="checkBrowser();"
SP;</BODY>
</HTML>
```

Advanced Rewriter Concepts

Two new Gateway Profile sections have been added. They are advanced configuration options and should be used only as a last resort for difficult rewriting problems that have no other workaround.

- Rewriting JavaScript Function Parameters in Fractured HTML
- Rewriting JavaScript Function Parameters Which Appear as JavaScript Or as A URL

To access these new Gateway Profile sections:

1. Log in to the Administration Console.
2. Select Gateway Management.
3. Select Manage Gateway Profile.
4. Scroll to the bottom of the frame and select Show Advanced Options.

The two new advanced Gateway Profile sections should be available for configuration.

Rewriting JavaScript Function Parameters in Fractured HTML

This Gateway Profile section is suitable for search, rewrite, and replace applications where JavaScript language dynamically creates HTML through multiple `document.write` function calls. For example:

```
...
    document.writeln('<FORM METHOD=GET');
    document.writeln('ACTION="../servlet/'+ name + '>');
...
```

In this particular case, the `FORM` tag is broken up by multiple `document.writeln()` function calls, and the rewriter is unable to determine that `ACTION` is an HTML tag attribute of the `FORM` tag. In order to rewrite correctly, the URL pattern `../servlet/` needs to be added to the Rewrite JavaScript Function Parameters in Fractured HTML section of the Gateway Profile.

Rewriting JavaScript Function Parameters Which Appear as JavaScript Or as A URL

Some JavaScript functions do not differentiate the context of what can be passed to the function as a parameter. This additional Gateway Profile section allows for some ambiguity in rewriting JavaScript function parameters. Specifically, this new Gateway Profile section allows the rewriting of JavaScript function parameters that are themselves either JavaScript or a URL. For example:

```
... Target("name", "javascript:top.location='http://www.yahoo.com'");
Target("name2", "http://www.google.com");
...
```

In this example, a function target has been created whose second function parameter can either be a URL or a JavaScript statement. To rewrite this correctly, **Target: ,y** would be added to Rewrite JavaScript Function Parameters in JavaScript or a URL, instead of Rewrite JavaScript Function Parameters.

NOTE There is a limitation to what is considered a valid URL for rules entered in this Gateway Profile section. Anything that starts with `http`, `https`, `..`, `./`, and `/` is considered a URL, and anything else is considered JavaScript. Therefore, URLs with no prepended path info will not be interpreted correctly and will not be rewritten as expected.

Redirecting URLs That Are Relative to the Server Root

URLs that are relative to the server root are resolved using the browser's URL field or may be constructed by using built-in scripting methods created from the browser's URL field. If the request to fetch the URL contains a Referer header (such as requests for embedded images) a redirection will be created so that the browser asks for the correct, rewritten, fully qualified URL.

If no Referer header exists, a 404 not found HTTP error will be returned instead. For example, the following message will be thrown in iwtGateway logs:

```
"Response
HTTP/1.0 404 Not Found
Date: Wed, 05 Feb 2003 20:00:50 PST
"

2/5/03 8:00:50 PM PST: Thread[Thread-198,5,main]
--> Session: Request:
GET HTTP/1.0
Host: null
Accept: */*
Referer:
http://showcase2.notes.net/mail/test123myname.nsf/($Inbox)/ED515AE20F1B
162885256CBF00BC4FC/?OpenDocument&PresetFields=s_ViewName;%28%24Inbox%29,s_Fr
om
Mail:1
```

```
Warning: Rewriter misconfigured for embedded URL /myweb/webpage.gif  
from Referer: <URLString here>
```

By turning on message level logging and testing the gateway access to internal content with Service Pack 5, it may now be possible to use the logs as a self-help mechanism for finding things that should be added to the Gateway profile.

Gateway Logging

Gateway logging is now disabled by default because logging traffic between the gateway and the server can affect portal performance.

Administrators can use the administration console to enable gateway logging.

To enable gateway logging, complete the following steps:

NOTE In the following instructions and examples, `/opt` is the default installation directory.

1. Log on to the administration console as super administrator.
2. From the left frame, select the Gateway Management link.
3. In the right frame, select the Manage Gateway Profile link to display the Component Profile: Gateway page.
4. At the bottom of the page, select Show Advanced Options.
5. Select the Logging Enabled check box.
6. Select Submit.
7. Select Continue when the console displays the Profile was successfully updated message.
8. Use these commands to stop and restart the gateway:

```
# /opt/SUNWips/bin/ipsgateway stop  
# /opt/SUNWips/bin/ipsgateway start
```

Rewriting JavaScript Variables in JavaScript

The entries in this list are the names of the JavaScript variables which are in turn expressed in JavaScript, and which is rewritten by the gateway.

The iPlanet Portal Server administration console's Gateway Profile page contains the Rewrite JavaScript Variables in JavaScript list.

If the list has the following entries:

- `jsvarjs1`
- `jsvarjs2`

and the rewriter's input is:

```
<html>

  <script language="JavaScript">

    var jsvarjs1 = "var1 = 'url1'; + some_var;
    var jsvarjs2 = "func2('url2');" + some_var;

  </script>

</html>
```

The gateway tries to rewrite the right-hand sides of both `jsvarjs1` and `jsvarjs2`.

- If there is an entry `var1` in Rewrite JavaScript Variables in URL, then `url1` is rewritten.
- If there is an entry `func2:y` in Rewrite JavaScript Function Parameters list, then `url2` is rewritten.

Rewriting JavaScript Functions with a Single Parameter

The gateway wraps the matched parameters with a function called `iplanet`, which does the actual rewriting when the browser interprets the page.

The iPlanet Portal Server administration console's Gateway Profile page contains the Rewrite JavaScript Function Parameters Function list. This is the syntax for entries in this list:

```
java_script_function_name: [y|], [y|], ...
```

Example

If the list has an entry:

```
func1:y
```

and the rewriter's input is:

```
<html>
  <script language="JavaScript">
    ...
    func1("http://" + some_func() + some_var);
  </script>
</html>
```

Then the output becomes:

```
<html>
  <script language="JavaScript">
    ...
    func1(iplanet("http://" + some_func() + some_var));
    function iplanet(url) {
      ...
    }
  </script>
</html>
```

Rewriting Javascript Functions with Multiple Parameters

The gateway rewrites JavaScript variables or JavaScript functions according to existing rules specific to that variable, or function, in the gateway profile.

The gateway tries to rewrite the matched parameters. A matched parameter in JavaScript is either in the form of a JavaScript variable or a JavaScript function.

The iPlanet Portal Server administration console's Gateway Profile page contains the Rewrite JavaScript Function Parameters list. Each entry in the list has the following syntax:

```
java_script_function_name: [y|], [y|], ...
```

If the list has an entry:

```
func1:y,,y
```

and the rewriter's input is:

```
<html>
  <script language="JavaScript">
    func1("func2('url2');", 500, var3='url3');
  </script>
</html>
```

The gateway tries to rewrite `func2` and `var3`.

- If there is an entry `var3` in Rewrite JavaScript Variables in URLs, then `url3` is rewritten.
- If there is an entry `func2:y` in Rewrite JavaScript Function Parameters list, then `url2` is rewritten

Editing Rewrite Applet/Object Parameter Values

Administrators can now use the administration console to edit the Rewrite Applet/Object Parameter Values list on the Gateway Profile page.

This is the syntax for entries in this list:

```
object_of_applet/object_url  applet_class/object_classid
applet/object_parameter_name  [url_pattern]
```

- If `url_pattern` is omitted, the value of the `applet/object` parameter is examined as a single URL, and the gateway rewrites accordingly.
- If `url_pattern` is included, the gateway rewrites according to the pattern matching.
 - The `url_pattern` consists of `*`, or `**`, plus the separation character used in the original parameter value to separate multiple fields. One wildcard (`*`) matches any field that is *not* to be rewritten. Two wildcards (`**`) match any field that *is* to be rewritten. The separation character could be `,` or `|`.
 - The last field to be rewritten does not have to be indicated by `**`. The `url_pattern` matches the start of the string in the parameter value, and the remainder of the value is considered a URL to be rewritten.

Example

If the gateway receives this request for the URL:

```
http://some_server/some_dir/some.html
```

And this is the response:

```
<html>
<applet archive=iplanet.jar code=iplanet.class>
<param name=server1 value="url1">
<param name=server2 value="url2">
<param name=server3 value="0|234|test|url3">
<param name=anotherParam value="yes,5,url4">
</applet>
<object classid="clsid:D27CDB6E-AE6D" codebase="url5"
<param name="movie" value="url6">
<param name="video" value="url7,2,url8">
</object>
</html>
```

Table 8 is a two column table that contains examples of entries for the Rewrite Applet/Object parameter Values List. The first column provides an example value that is entered in the list. The second column provides a description of how the URL is rewritten.

Table 8 Rewrite Applet/Object Parameter Values List

Value	Description
<code>some.html iplanet.class *</code>	No parameter value is rewritten, because <code>object_of_applet/object_url</code> does not match the object of the request URL.
<code>/some_dir/some.html iplanet.class *</code>	<code>url1</code> and <code>url2</code> are rewritten. <code>url3</code> and <code>url4</code> are not rewritten because they are embedded within strings that do not appear to be URLs as they do not start with <code>/,http</code> or <code>https</code> .
<code>/some_dir/some.html iplanet2.class *</code>	No parameter value is rewritten because <code>iplanet2.class</code> does not match the value of the applet code attribute or the object <code>classid</code> attribute.
<code>* * server* * * *</code>	<code>url3</code> is rewritten because <code>* * *</code> matches <code>0 234 test </code> .
<code>/some_dir/some.html clsid:D27CDB6E-AE6D \movie</code>	<code>url6</code> is rewritten.
<code>/some_dir/some.html clsid:D27CDB6E-AE6D \video **,*,**</code>	<code>url7</code> and <code>url8</code> are rewritten because the first <code>**</code> matches the position of <code>url7</code> , and the second <code>**</code> matches the position of <code>url8</code> .

Denying Unknown Certificate Authorities

A new attribute allows administrators to deny unknown certificate authorities (CAs). The `ips.gateway.trust_all_server_cert` attribute is in the `/etc/opt/SUNWips/platform.conf` file. It is used when the Portal Server gateway component uses SSL to communicate with:

- An HTTP proxy, on which a self-signed certificate is installed.
- An iPlanet Portal Server server, on which a self-signed certificate is installed.

TIP See [“Adding a Root CA Certificate”](#) for instructions on installing a Root CA certificate.

The default value of this attribute is `false`. Administrators should change the value to `true` to trust all CAs presenting signed certificates to the gateway component during an SSL handshake. For example:

```
ips.gateway.trust_all_server_certs=true
```

Typically, the Root CA certificate should be added to gateway certificate database so that the gateway component can identify the certificate presented. However, if a site presents a self-signed certificate, setting the `ips.gateway.trust_all_server_cert` attribute to `true` allows the iPlanet Portal Server gateway component to communicate with the site presenting the unknown certificate.

If the gateway does not recognize the certificate that is presented, and if the `ips.gateway.trust_all_server_cert` attribute is set to `false`, this error is generated:

```
03/22/00 4:24:42 PM PDT: Thread[main,5,main]
Cannot login to server
java.net.SocketException: writing to SSL socket (Peer's Certificate issuer is
not recognized.)
    at com.netscape.jss.ssl.SSLOutputStream.socketWrite(Native Method)
    at com.netscape.jss.ssl.SSLOutputStream.write(SSLOutputStream.java:68)
    at
java.io.BufferedOutputStream.flushBuffer(BufferedOutputStream.java:76)
    at java.io.BufferedOutputStream.flush(BufferedOutputStream.java:134)
    at com.iplanet.portalserver.gwutils.Login2.send(Login2.java:21)
    at com.iplanet.portalserver.gwutils.Login2.login(Login2.java:69)
    at com.iplanet.portalserver.gateway.eprox.EProxy.<clinit>(EProxy.java:
```

Setting the Number of Socket Connection Retries

A new parameter now allows administrators to specify the number of times the iPlanet Portal Server gateway tries to make a socket connection to a destination server should the first attempt fail. The `ips.gateway.sockretries` parameter is in the `platform.conf` file.

To specify the number of times the gateway tries to make a socket connection, edit the `platform.conf` file in `/etc/opt/SUNWips` and change the `ips.gateway.sockretries` definition. For example:

```
ips.gateway.sockretries=2
```

Using Outlook Web Access 2000

The Outlook Web Access (OWA) 2000 application can now be used with the iPlanet Portal Server gateway component. To do so, enable basic authentication for your server.

NTLM authentication is not supported.

Inactive Attributes

These attribute settings in the iPlanet Portal Server administration console are no longer used:

- IP Address Validation Enabled
- Trust Server SSL Certificate List
- ReverseProxy Maximum Socket Connections

These settings appear in administration console on the Manage Gateway Profile page, but they do not function. The information in the “IP address validation” section in Chapter 8 “Configuring the Gateway” of the *iPlanet Portal Server 3.0 Administration Guide* no longer applies.

Localization Changes

This section provides details about localization changes in iPlanet Portal Server. It contains the following topics:

- Installing and Enabling Multiple Locales for a Domain
- Selecting Locale
- Choice Property Keys
- Localizing JSP Provider Titles and Descriptions
- Sample JSP Provider Property File for Locales

Installing and Enabling Multiple Locales for a Domain

The administrator can now specify the locale for domains, roles, and users. A single Portal Server installation with three locale packages installed, for example, allows the administrator to set up three domains, one for each locale. Users registering in domain1 use locale 1. Users registering in domain2 use locale2 and so on.

When you install a new locale, you must run the `ipsadmin` command to update the `iwtPlatform` attribute. The `iwtPlatform-availableLocales` attribute lists all the locales available for the user. For example:

```
Attribute for available locales:
<iwt:Att name="iwtPlatform-availableLocales"
  type="stringlist"
  desc="Available Locale"
  idx="X-x7"
  userConfigurable="True">
  <Val>en_US</Val>
  <Rperm>ADMIN</Rperm><Rperm>OWNER</Rperm>
  <Wperm>ADMIN</Wperm>
</iwt:Att>
```

Although values for this attribute are `en_US` or `ja_JA`, for example, users see only the common name of the available locale — English or Japanese.

To specify the locale for domains, complete the following steps:

1. Log in to the administration console and select Manage Domains.
2. Select the domain that you are administering.
3. Select Platform and Show Advanced Options.
4. Specify the languages you wish to make available for this domain.

Selecting Locale

Users can now select their own locale from a list of locales available.

The provider displays the list of languages to the user. After the user makes a selection, it stores the selection in the user profile. The user must then log in again to get the new locale.

To select locale, users complete the following steps:

1. Log in to the Desktop.
2. Select Edit to display the Edit User Information page.
3. From the list of available languages pull-down menu, select the language.

Choice Property Keys

This feature allows the user to see the changes in the locale of choice.

When editing the profile, for channels created with the channel wizard in a non-English locale, the administrator now sees the choices translated in the chosen language of the locale.

Localizing JSP Provider Titles and Descriptions

A new properties file was added to localize the default Desktop's JSP Provider's title and description. The file, `iwtSampleJSP.properties`, is in `/opt/SUNWips/locale`.

This change is visible in the Desktop content provider list as the title and description and also on the Desktop channel title bar as the title.

To change the values of the JSP channel title and description, edit the `iwtSampleJSP.properties` file and change the `description` and `title` entries to display the desired text. For example:

```
description=My JSP Channel
```

```
title=My JSP
```

Other entries in the file are used in the administration console for this provider. They are not displayed for the end user. These values align with the `idx` values in the attributes of the XML files.

NOTE	<p>Titles of Desktop channels are a special case. A title attribute exists in the Domain Attributes page of the administration console. The title entry in the property file takes precedence over the profile entry listed in the administration console.</p> <p>Changing the title in the administration console has no affect, therefore, unless you also remove the entry for the title from that channel's properties file.</p>
-------------	--

Sample JSP Provider Property File for Locales

A copy of the JSP Provider properties file is created specifically so that you can create your own JSP property file for different localizations. In the file, locale specifiers are used as suffixes for locale-specific files. For example:

- The Egypt-Arabic localization file would be called `iwtSampleJSP_ar.properties`.
- The France-French localization file would be called `iwtSampleJSP_fr_FR.properties`.
- The U.S. English localization is called `iwtSampleJSP_en_US.properties`, but the default localization is `en_US`.

When a user creates a JSP Channel using the Channel Wizard, no properties file is created for that channel. The default property file for a newly created JSP channel is the `iwtJSPProvider.properties` file, but this file cannot be customized.

To customize or localize the title and description of the newly created JSP channel, complete the following steps:

1. As root, make a copy of the `iwtSampleJSP.properties` file in the *base_dir*/SUNWips/locale directory with the component name of your channel:

```
# cp iwtSampleJSP.properties domaintestjspchannel2.properties
```

2. Give the file write permissions.

```
# chmod 600 domaintestjspchannel2.properties
```

3. Edit the values for the `title` and `description` entries, which appear as the channel title in its title bar, and the title and description on the Desktop content page.
4. Restart the server for the changes to take effect.

The entries other than `title` and `description` in this file are unused, because newly created JSP channels get their admin strings from the `iwtJSPProvider.properties` file. They all share the same strings and would all be edited or localized at once.

NetFile Changes

This section provides details about NetFile changes in iPlanet Portal Server. It contains the following topics:

- NetFile Internationalization and Usability Enhancements
- Using NetWare File Systems
- Defining Systems and Shares
- Defining Hidden Shares
- Alphabetized Shares on Windows NT Systems
- NetFile Usability

NetFile Internationalization and Usability Enhancements

NetFile enhancements include Internationalization compliance and features enabling broader support of FTP servers and usability enhancements. Internationalization compliance is achieved through a combination of internal modifications, and an additional modification to the end user interface. When creating a new share, there is now an option to select the system encoding type. In order to establish a successful connection, the encoding type selected by the end user must match the encoding type of the FTP server.

By applying this service pack, 15 encoding types are added to the NetFile properties files. For more information about the exact properties files entries refer to the section titled “[Template Modifications](#).” The default encoding type is ISO-8859-1, and will be associated with a system and consecutive shares if another encoding type is not explicitly selected from the drop-down menu prior to selecting OK.

The following usability enhancements have been added to make NetFile easier and more intuitive to use:

- WU-FTP and MSFTP support
- Novell 5.1 Support (when Novell is explicitly selected)
- Users are no longer able to add non-existent shares
- The use of the tab and return keys are normalized across the Netfile Java interface
- NetFile now shows hidden files (files beginning with a “.”)
- NetFile responses more accurately reflect successful or failed actions
- When multiple files are selected for download, all of the file names are now displayed correctly in the pop-up confirmation window
- NetFile saves selected filenames correctly on Macintosh platforms (instead of saving each as NetFileServlet)
- If the incorrect username is supplied when creating a share, the user will have the opportunity to re-enter it instead of only re-entering the password
- Directory names are shown in the chosen locale

NOTE NetFile I18N compliance has forced the deprecation of Internet Explorer 5.0 running on the Macintosh platform. To prevent a browser hang and possible client system crash when accessing NetFile with this browser and platform combination, NetFile will instead inform the user to upgrade their browser.

Using NetWare File Systems

File Transfer Protocol (FTP) support for NetWare File Systems through the NetFile and NetFile Lite applications is now available.

Adding a NetWare File System to NetFile

The administrator uses the administration console to add a NetWare File System to NetFile applications. This allows users to use NetFile in the same way they do for any other host type.

To add a NetWare File System, complete the following steps:

1. Select the NetFile link in the Desktop's Applications channel to start NetFile.
2. Select File and then select Add System.
3. Enter the fully qualified system name.
4. Select AUTO DETECT or NETWARE as the system type, and select OK.
5. Double click on the system in the Network Neighborhood to add a share.
6. Enter your Netware user name and password and select a directory to mount.
7. Double click on the share under the system name in the Network Neighborhood to browse the directory.

NOTE	Because Netware adheres to an 8.3 file naming convention, you may have to modify file names to upload them to a Netware host using NetFile. This may also be necessary to compress a file with a file extension on the Novell file system.
-------------	--

Adding a Novell File System to NetFile Lite

The administrator uses the administration console to add a Novell file system to NetFile Lite applications. This allows users to perform NetFile functions by using the check boxes next to the file names and selecting an action using a button at the bottom of the page.

To add a Novell file system, complete the following steps:

1. Select the NetFile Lite link in the Desktop's Applications channel to start NetFile Lite.
2. Fill in the form field for System Name and select the Machine Type as AUTODETECT or NETWARE.
3. Fill in the next form fields for User Name, Password, Directory to mount, and select Enter.
4. Select the View Systems link.

5. Select the host name from the list and select Enter.

Defining Systems and Shares

Administrators can now define Systems and Shares for NetFile and NetFile Lite at the domain, role and user levels. By setting common host data attributes, administrators can define systems and shares to be displayed in the end user's Network Neighborhood.

These NetFile profile attributes changes were made to allow this:

- The `iwtNetFile-hostlist` attribute can no longer be edited from the administration console.
- The `iwtNetFile-commonhostdata` attribute was created for NetFile to allow administrators to predefine systems and shares for the user.

Defining Systems and Shares at the Domain Level

To define Systems and Share at the domain level, complete the following steps:

1. Log on to the administration console as super administrator.
2. Select Manage Domains.
3. In the Portal Server Domains page, select the desired domain.
4. Expand the key next to Applications.
5. Select NetFile.
6. In the prepopulated Host list/type and share information field, modify the common host data attribute.

TIP Use the following format to enter (in one string with no spaces) the name, domain, type, and share information:

`name=name | domain=domain | type=type | share=directory`

Replace *name* with the fully qualified host name, *domain* with the name of the Windows NT domain (or NULL, if applicable), *type* with NT, WIN, NFS, FTP or NETWARE, and *directory* with hostdata shares or directories.

For example:

`name=xyz.sesta.com | domain=workgroup | type=NT | share=tempshare | share=C$`

7. For each entry, select Add to add the host and share to the list.
8. Select the Apply changes to all subRoles check box prior to selecting Submit to apply changes to subroles.

NOTE Applying changes to subroles may overwrite customizations done further down the tree, for example, at the user level.

9. Select Submit from the bottom of the page.

To view the defined systems or shares in NetFile, the end user must complete the following steps:

1. Log in to the iPlanet Portal Server Desktop.
2. Start NetFile or NetFile Lite application.
3. Select desired host and select Edit Host Info.
4. Enter user name and password for the required host or share.

Defining Systems and Shares at the Role Level

To define Systems and Share at the role level, complete the following steps:

1. Log on to the administration console as super administrator.
2. Select Manage Domains.
3. In the Portal Server Domains page, select the desired domain.
4. Select the desired role.
5. Expand the key next to Applications.
6. Select NetFile.
7. In the prepopulated Host list/type and share information field, modify the common host data attribute.

TIP Use the following format to enter (in one string with no spaces) the name, domain, type, and share information:

`name=name | domain=domain | type=type | share=directory`

Replace *name* with the remote host name, *domain* with the name of the Windows NT domain (or NULL), *type* with NT, WIN, NFS, FTP or NETWARE, and *directory* with hostdata shares or directories.

For example:

`name=pqr.sesta.com | type=FTP | share=/myshare`

8. For each entry, select Add to add the system and share to the list.
9. Select Submit.

NOTE End users cannot delete defined hosts and shares, even if they remove them and choose to save their session upon exit.

To view the defined systems or shares in NetFile, the end user must complete the following steps:

1. Log in to the iPlanet Portal Server Desktop.
2. Start NetFile or NetFile Lite application.
3. Select desired host and select Edit Host Info.
4. Enter user name and password for the required host or share.

Defining Systems and Shares at the User Level

To define Systems and Share at the user level, complete the following steps:

1. Log in to the iPlanet Portal Server administration console.
2. Select Manage Domains.
3. Select the desired domain.
4. Select the desired role.
5. Select Users.
6. Select the desired user name.
7. Expand the key next to Applications and select NetFile.

8. In the prepopulated Host list/type and share information field, modify the common host data attribute.

TIP Use the following format to enter (in one string with no spaces) the name, domain, type, and share information:

`name=name | domain=domain | type=type | share=directory`

Replace *name* with the remote host name, *domain* with the name of the Windows NT domain (or NULL), *type* with NT, WIN, NFS, FTP or NETWARE, and *directory* with hostdata shares or directories.

For example:

`name=abcedf | domain=NULL | type=WIN | share=WINDOWS | share=DESKTOP | share=TEMP`

9. For each entry, select Add to add the system and share to the list.
10. Select Submit.

NOTE End users cannot delete defined hosts and shares, even if they remove them and choose to save their session upon exit.

To view the defined systems or shares in NetFile, the end-user must complete the following steps:

1. Log in to the iPlanet Portal Server Desktop.
2. Start NetFile or NetFile Lite application.
3. Select desired host and select Edit Host Info.
4. Enter user name and password for the required host or share.

Defining Hidden Shares

Administrators and Desktop users can now define NT hidden shares for use in NetFile. The Common Host Data attribute allows administrators to define NT hidden shares through the administration console.

The procedure for defining hidden shares through the administration console is the same as that for defining regular shares. Desktop users can add hidden NT shares the same way they would add a regular share, as long as they use the correct user name and password for the hidden share.

For administrators and user instructions, see [“Defining Systems and Shares at the Domain Level.”](#)

Alphabetized Shares on Windows NT Systems

Windows NT shares in NetFile are now alphabetized. Because all shares on a Windows NT system are automatically displayed when a user selects a system name, alphabetizing the list of shares makes locating the desired share easier.

NetFile Usability

Several NetFile enhancements now make NetFile easier to use. These include the following:

- User can open NetFile files by double-clicking the file name.
- User can select multiple files for download.
- The maximum file size for uploading files with the NetFile application has increased to 500MB. NetFile Lite still has a maximum file size of less than 5 MB.

Netlet Changes

This section provides details about Netlet changes in iPlanet Portal Server. It contains the following topics:

- Automatic Proxy Configuration for Netlet Connections
- Controlling Server Session Timeout When Using the Netlet
- Unlimited Netlet Connections
- Enabling Secure FTP Using A Netlet Connection
- Using the Netlet Proxy
- Netlet Windows
- Using Automatic Proxy Configuration
- Configuring Internet Explorer INS Files

Automatic Proxy Configuration for Netlet Connections

The Netlet can now make use of the browser's Automatic Proxy Configuration file. This feature is supported in Netscape and in Internet Explorer with the Automatically Detect Proxy Settings option deselected. A valid PAC file must be specified in the configuration URL for either browser.

Setting the PAC File Location

In Netscape, the PAC file location can be set by doing the following:

1. Go to Edit | Preferences | Advanced | Proxies.
2. Enable Automatic proxy configuration by selecting the radio button.
3. Enter a URL to an automatic proxy file.
4. Click OK to save the new preferences.

In Internet Explorer, the PAC file location can be set by using one of the following procedures.

If you are using a dial-up connection:

1. Go to Tools | Internet Options | Connections.
2. Select the correct connection name.
3. Choose Settings.
4. Check Use Automatic Configuration Script.
5. Fill in the URL of the PAC file.
6. Select OK.

If you are using a LAN connection:

1. Go to Tools | Internet Options | Connections.
2. Select Lan Settings.
3. Select the option to Use Automatic Configuration Script.
4. Fill in the URL of the PAC file.
5. Select OK.

Internet Explorer can also make use of an auto configuration file. If end users are using INS files for autoproxy purposes, it must contain an entry for `AutoConfigJSURL` for the Netlet to read the proxy settings correctly. An example INS file section might look like:


```
[URL]
AutoConfig=1
AutoDetect=0
AutoConfigJSURL=http://server.com/corp.pac
AutoConfigURL=http://server.com/corp.ins
[Proxy]
HTTP_Proxy_Server=
FTP_Proxy_Server=
Gopher_Proxy_Server=
Secure_Proxy_Server=
Socks_Proxy_Server=
Use_Same_Proxy=1
Proxy_Enable=0
Proxy_Override=
```

Automatic Proxy Configuration File

An automatic proxy configuration file is written in JavaScript and defines a single function called `FindProxyForURL` that determines which proxy server, if any, the browser should use for each URL. Since the Netlet only needs a communication path back to the iPlanet Portal Server gateway, this decision needs to be made only once. The simplest PAC file is the one that only returns `DIRECT` (meaning no proxy should be used). The easiest way to test whether the Netlet is configured correctly to use PAC files is to create a simple PAC file and test it on one of the default dynamic Netlet rules, such as telnet.

Example of a simple PAC file:

```
// sample proxy pac file
function FindProxyForURL(url, host)
{
    // strings to return -- substitute actual proxy server address
    var proxy_yes = "PROXY myproxy.subdomain.domain.com:8080";
    var proxy_no = "DIRECT";

    // ...etc.
    // Proxy everything else
    return proxy_no;
}
```

This PAC file can be placed on a WebServer that is configured to send a MIME type of `application/x-ns-proxy-autoconfig` for the file extension `pac`.

Once that is done, the URL to the PAC file can be configured in the browser by using one of the procedures in [“Setting the PAC File Location.”](#) and the telnet Netlet rule can be launched from the Netlet Provider. The Proxy Server used is displayed in the Java console.

```
Netlet config: https://gateway.subdomain.domain:443/
http://server.subdomain.domain:8080/NetletConfig?func=loadResources
http://webserver.subdomain.domain/example.pac

https://gateway.subdomain.domain:443/http://server.subdomain.domain:8080/NetletConfig
DIRECT
Netlet not using proxy (Netscape)
```

NOTE The JavaScript programming language used in a PAC file must be limited to the domain necessary for Automatic Proxy. Arbitrary functions present in the PAC file will cause the Netlet Connection to fail. For more information about Proxies and automatic proxy configuration files, check the Netscape Developer web site.

Controlling Server Session Timeout When Using the Netlet

The session timeout value can be set to determine session time outs in one of the following ways:

- By considering Netlet traffic when determining whether a Portal Desktop user session is active
- By letting the Portal session timeout after the idle time has been exceeded even if a Netlet session is active

An entry called `netlet.session.extension` has been added to the `platform.conf` file. The `netlet.session.extension` entry can take a value of **true** or **false**.

- A value of **true** keeps the Desktop session alive if the Netlet is running.
- A value of **false** results in the termination of the Netlet session upon Desktop idle timeout.

Because of the inherent client/server relationship in most Netlet tunnels, an additional enhancement has been added that enables administrators to configure whether client-bound traffic should be considered when extending the portal session if the `netlet.session.extension` value is set to **true**. This option was previously located in the `platform.conf` file, where it was specified in an earlier patch as `netlet.session.extension.for.clientbound.traffic`. This option has moved to an Advanced Option in the Portal Server console Gateway Management screen.

Extending Portal Session for Client bound Netlet Traffic

The option can be changed as follows:

1. Log in to the iPlanet Portal Server Administration Console.
2. Click Gateway Management.
3. Click Manage Gateway Profile.
4. Click the Show Advanced Options button at the bottom of the frame.
5. Deselect or Select the checkbox next to Extend Portal Session for Client bound Netlet Traffic.

Enabling this option updates the iPlanet Portal Server Desktop idle timer even if the traffic is only initiated by the Netlet client's own server. Disabling this option updates the Portal Desktop idle timer only if there is activity initiated by the Netlet client itself. The implementation of this particular option depends on the definition of an Active Netlet User for any given portal deployment. As a rough guideline, here are two examples:

- Active Netlet user is defined as a real person interacting in real time with the Netlet client application.
- Active Netlet user is defined as a real person interpreting Netlet client data pushed from a server application.

If the active Netlet user is defined as a real person acting in real time with the Netlet client, the Extend Portal Session for Clientbound Netlet Traffic option should be disabled. This prevents the Portal Session from being extended in the end-user's absence if the server continues to send updates or other notification to the client application.

Conversely, if an active Netlet user is defined as a real person interpreting Netlet client data pushed from a server application, the Extend Portal Session for Clientbound Netlet Traffic option should be enabled. With this definition, an end user interpreting data streamed or pushed to the Netlet client does not suddenly and unexpectedly have their Netlet session terminated as a result of the Portal Desktop idle timeout.

Advanced Configuration of the Netlet Session Extension

The new attribute's associated XML looks like:

```
<iwt:Att name="iwtGateway-ThirdPrtySessExt"
  type="boolean"
  desc="Extend Portal Session for Clientbound Netlet Traffic"
  idx="X-x18"
  userConfigurable="false"
>
<Val>true</Val>
<Wperm>ADMIN</Wperm>
```

```
<Rperm>ADMIN</Rperm>
<Rperm>OWNER</Rperm>
</iwt:Att>
```

Unlimited Netlet Connections

The Netlet now supports an unlimited number of connections per Netlet. This rule change is beneficial if an application running through the Netlet requires many connections per Netlet.

NOTE Not all client operating systems can handle unlimited connections. The client operating system might have a connection limit based on its own resources. Limitations include JVM size and file descriptor limits.

Enabling Secure FTP Using A Netlet Connection

Secure remote FTP transfers from an end user system to an FTP server are now provided through a Netlet connection. Without a user name, an FTP URL is interpreted as an anonymous FTP connection.

Administrators can use static or dynamic Netlet rules to set up FTP service to a single FTP server. Static rules define the FTP server that is used to transfer files. Dynamic rules allow the user to specify the FTP server.

Table 9 is a three column table that describes netlet rules and provides their formats. The first column describes the purpose of the Netlet rule. The second column states what type of rule it is. The third column provides the format for writing the rule.

Table 9 Netlet Rules

Purpose	Type	Format
Rule for using a single pre-defined FTP server	Static	ftp null false 30021 <i>your_ftp_server.your_domain</i> 21
Rule in which the user logs in to the FTP server as an anonymous user	Dynamic	Ftp ftp://localhost:30021 false 30021 TARGET 21
Rule in which the user logs in to the FTP server with a user ID	Dynamic	Ftp ftp://user@localhost:30021 false 30021 TARGET 21

This Netlet enhancement requires creating a Netlet rule that listens for FTP requests. To create a static FTP Netlet rule for the Default Role, complete the following steps:

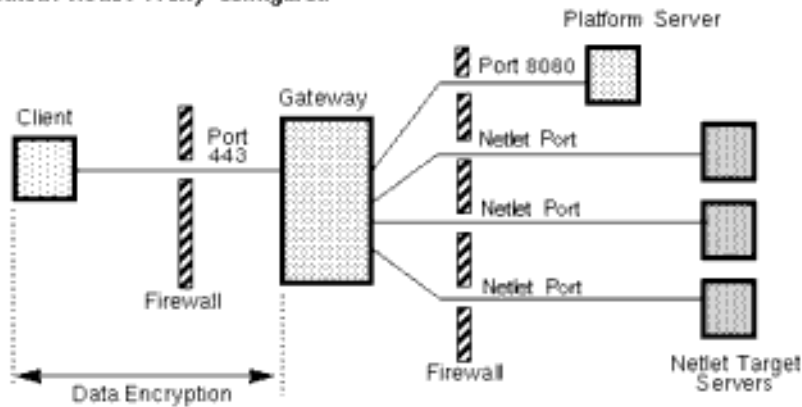
1. As root, log in to the administration console at `http://server.domain.subdomain:port/console`
2. Select Manage Domains.
3. Select the domain where you want to set the Netlet rule.
4. Select DefaultRole.
5. Expand the key next to Applications and select Netlet.
6. Select the form field below the Netlet Rules text area and add a Netlet rule similar to one in Table 9.
7. Select Add and then Submit.
8. Log out from the administration console.

Using the Netlet Proxy

The Netlet proxy is used for these reasons:

- To minimize the use of extra IP addresses and ports from the gateway through an internal firewall in a significantly sized deployment environment.
- To provide encryption for each transaction through the Netlet to iPlanet Portal Server from the gateway to the platform server. The Netlet proxy offers improved security benefits through data encryption but may increase the use of system resources.

Without Netlet Proxy Configured



With Netlet Proxy Configured

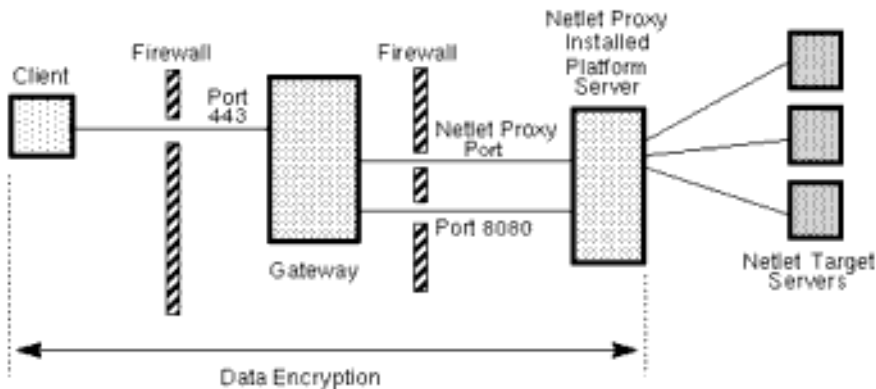


Figure 1 Netlet Proxy Implementation

Configuring the Netlet Proxy

To configure the Netlet proxy, complete the following steps:

1. Log in as root to the iPlanet Portal Server administration console.
2. From the left frame, select the Gateway Management link.
3. Select the Manage Gateway Profile link to display the Component Profile: Gateway page.

4. Scroll to the end of the page and select Show Advanced Options.
5. Select the Netlet Proxy Enabled check box to enable the netlet proxy.
6. In the Netlet Proxy Port text field, enter the available port number.

TIP To determine whether the port desired is available and unused, enter this command from the command line:

```
netstat -a | grep port_number | wc -l
```

7. Select Submit at the bottom of the page to commit these changes to the profile server.
8. On the Profile Successfully Update page, select Continue.

Configuring Restart of the Netlet Proxy

Administrators can use the command line interface to configure an automatic restart of the Netlet proxy whenever the system server is rebooted.

NOTE If you are using more than one Portal Server, repeat these steps for each server.

Configure the Netlet Proxy in the iPlanet Portal Server administration console before you start Portal Server and the gateway.

To start the netlet proxy automatically when the machine is rebooted, execute these commands as root:

```
# cd /opt/SUNWips/bin
# cp ipsnetletd /etc/rc3.d/K55ipsnetletd
# cp ipsnetletd /etc/rc3.d/S55ipsnetletd
# chmod 500 /etc/rc3.d/K55ipsnetletd
# chmod 500 /etc/rc3.d/S55ipsnetletd
```

NOTE These steps do not automatically start the netlet proxy when you use `ipsserver start` to restart iPlanet Portal Server.

Netlet Windows

Administrators can now change the contents of Netlet windows by editing the files that store the values for these messages.

To change the message displayed in the interim status window that lets the user know when the Netlet has finished loading, modify the `nc3` value in the `install_dir/SUNWips/locale/iwtNetletServlet.properties` file. For example:

```
nc3=<h2>Netlet is loading.</h2><p>The Netlet is still loading. Once the Netlet
has completed loading, click this button to continue with your Netlet session.
```

To change the message displayed in the status window when a static rule has been defined for the current user, modify the `Netlet-Provider-wait` value in the `iwtNetletProvider.properties` file. For example:

```
NetletProvider-wait=Wait until the Netlet popup initializes before using any
Netlet operations.\n
```

To change the messages displayed when a Macintosh client attempts to use an automatic proxy configuration file, or when the Netlet cannot determine the Macintosh browser's proxy settings, modify values in the `iwtNetletApplet.properties` file. For example:

```
ppd.1=Netlet Proxy Port
ppd.2=Netlet was unable to determine your browser proxy port setting.
ppd.3=Please enter your browser Proxy Port setting below:
ppd.4=OK
ppd.5=Cancel

pwarn.3mac=Netlet was unable configure your browser proxy settings. In your
browser's Preferences->Network->Proxies section:\n\n - add these entries to
the 'List of sites that you want to connect to
directly':\nlocalhost\n127.0.0.
```

To change the message displayed when the Netlet is started from a link within the Netlet channel itself rather than being launched following a successful login, modify the `iwtNetletServlet.properties` file. For example:

```
ntitle2=<HEAD><TITLE>Netlet Loading</TITLE></HEAD>

nc4=<h2>Netlet is loading.</h2><p>Please wait while the Netlet finishes
loading. This message should change once loading is complete.

contButton=Continue
```

The `nc4` value and the `contButton` value are displayed in the intermediate status window.

Using Automatic Proxy Configuration

The Netlet applet can be used with Web browsers that are configured to use automatic proxy configuration (PAC) files. The automatic proxy configuration feature is supported in the Netscape Navigator and Internet Explorer browsers.

Configuring Internet Explorer INS Files

In addition to using automatic proxy configuration (PAC) files, Internet Explorer can also use an `.ins` automatic configuration file for automatic proxy services.

If end users are using `.ins` files for automatic proxy purposes, the `.ins` file must contain an entry for `AutoConfigJSURL` so that the Netlet can read proxy settings correctly. The value for the `AutoConfigJSURL` is a URL that points to a valid PAC file. For example:

`AutoConfigJSURL=http://sesta.com/corp.pac`

Performance and Tuning Changes

This section provides details about performance and tuning changes in iPlanet Portal Server. It contains the following topics:

- Tuning the Gateway for Optimal Performance
- Support of Netscape Security Service (NSS)
- Maximum Thread Pool Size Parameter
- Loading Multiple Attributes in One Profile Request
- Short-Circuiting for Session and Logging Requests
- Web Server Performance

Tuning the Gateway for Optimal Performance

Tunable parameters and internal changes have been added to improve the overall performance of the iPlanet Portal Server gateway component. For detailed Bug IDs and descriptions of specific problems addressed by this service pack see the “[Bugs Fixed](#)” section.

The following changes are designed to improve performance:

- Elimination of iPlanet Portal Server gateway restarts as a result of the iPlanet Portal Server gateway not being able to immediately validate its own session
- Reduction of socket depletion by reallocating it to the connection pool as soon as it is no longer being used
- Increase in the JVM heap size
- Removal of verbose Garbage Collection logging
- Creation of tunable memory management options to control forced Garbage Collection
- Reduction of 502 errors returned by the gateway for remote sites that are under heavy load
- Fixed stack overflow when HTTP Proxy is enabled

Tuning the Gateway JVM Heap Space

The minimum and maximum JVM heap size for the gateway process is now 512MB and 768MB, respectively.

NOTE	Because the minimum heap size has been increased substantially from the default value of 32MB, the iPlanet Portal Server gateway process may not start if the machine does not meet or exceed the minimum hardware recommendations.
-------------	---

Tuning the Gateway JVM Forced Garbage Collection

Three new `/etc/opt/SUNWips/platform.conf` entries have been added to control the behavior of forced Garbage Collection of the JVM heap by the gateway process.

Table 10 is a three column table that lists and describes the new `platform.conf` entries. The first column provides the name of the `platform.conf` entry. The second column lists the default value. The third column gives a description of the new entry.

Table 10 Platform.conf Entries for Tuning Gateway JVM Forced Garbage Collection

platform.conf entry	Default Value	Description
ips.gateway.mem_management_option	false	The new memory management option is not enabled. Change the value to true in order for the other two platform.conf options to take effect.

Table 10 Platform.conf Entries for Tuning Gateway JVM Forced Garbage Collection

platform.conf entry	Default Value	Description
ips.gateway.mem_management_interval	30	This value determines the frequency of the forced Garbage Collection. The value is specified in seconds, and represents how often the iPlanet Portal Server gateway determines if the memory is remaining below the specified threshold.
ips.gateway.mem_threshold	70	This value represents the total percentage of free memory remaining in the heap. If the memory usage exceeds this threshold after reaching the specified interval, garbage collection will be forced.

NOTE Garbage collection is very CPU-intensive. Explicit tuning of garbage collection frequency should be done with the utmost care and understanding of the tuning implications. In addition, the explicit garbage collection tuning will not greatly impact larger portal configurations because it is unlikely that garbage collection will need to be explicitly called.

Tuning Gateway Socket Reconnection for Remote Websites Under Heavy Load

When the gateway component makes a call to retrieve data from a remote site, the socket may fail to open or the request may not be handled because the remote site is under heavy load. Previously, the gateway would report a 502 error and not attempt to reconnect. An additional entry has now been added to the `/etc/opt/SUNWips/platform.conf` file to specify a number of retries for socket reconnection. The retry interval is fixed at three seconds, but the number of retries can be changed by setting the value of `ips.gateway.sockretries`, which has a default value of 3.

Support of Netscape Security Service (NSS)

Netscape™ Security Service (JSS) version 2.8.4 to version 2.8.6 is now supported on the gateway component. This increases the number of HTTPS operations that the gateway component can sustain.

Certificates installed for the previous SSL library are automatically converted to the format required by NSS when Service Pack 5 is installed. However, certificate management for the gateway component is different from previous releases of the iPlanet Portal Server software. For more information on gateway certificate management see, “[Web Server Performance](#).”

Maximum Thread Pool Size Parameter

For better performance under load, administrators can increase the value of the Maximum Thread Pool Size parameter to 500. The default value is 200.

To increase this value, complete the following steps:

1. Log in to the administration console.
2. Select Gateway Management.
3. Select Manage Gateway Profile.
4. Select Show Advanced Options.
5. Change the value in the field for Maximum Thread Pool Size to 500.
6. Select Submit.
7. Restart the gateway for the changes to take effect.

Loading Multiple Attributes in One Profile Request

A new method called `Profile.loadAttributes` for loading multiple attributes in one profile request is now available. It is used to pass a set of attribute names that can contain wildcards for multiple profile components.

The parameter name is `attributeNames`. The value is a set of attribute names that can contain wildcard characters.

```
public void loadAttributes(Set attributeNames)
                        throws ProfileException
```

The returned attribute values are cached in the profile object. This allows a subsequent call to retrieve these attributes faster, thereby improving overall Portal Server performance.

Short-Circuiting for Session and Logging Requests

Short-circuiting for session and logging requests reduces the number of HTTP requests for logging and session services and eliminates XML parsing for these requests. This improves the overall performance of iPlanet Portal Server.

If the logging client and the logging server are in the same JVM, the HTTP connection is bypassed during client and server communication.

Likewise, if the session client and the session server are in the same JVM, no HTTP connection is needed for them to communicate.

Web Server Performance

Adjusting iPlanet Web Server parameter settings can improve the performance of the gateway component. Table 11 is a four column table that describes these parameters. The first column lists the parameter and the associated configuration file. The second column lists the default value. The third column lists the recommended value. The fourth column provides a description of the parameter.

These configuration files are located in the *install_directory*/netscape/server4/https-*server*/config file.

Table 11 Web Server Performance Tuning Parameters

Scope	Default	Recommended	Description
RqThrottle			
magnus.conf	1024	128	With iPlanet Web Server, Enterprise Edition 4.1, SP9, the maximum number of active Web Server threads is calculated using the formula $RqThrottle + MaxKeepAliveConnections$. The Portal Administrator can modify slightly the ratio between RqThrottle and MaxKeepAliveConnections but must keep the sum of the two parameters around 200 in scale properly.
MaxKeepAliveConnections			
magnus.conf	200	72	
jvm.minHeapSize			
jvm12.conf	327680000	32768000	For heavily accessed sites, set the minimum JVM heap size to 32 MB or higher to provide better performance and scalability with the genconfig options in the Java™ Development Kit (JDK™) 1.2.2_16-er-20030716.

Table 11 Web Server Performance Tuning Parameters *(Continued)*

Scope	Default	Recommended	Description
jvm.maxHeapSize			
jvm12.conf	131072000	805306368	For heavily accessed sites, set the maximum JVM heap size to 768 MB to avoid a JVM abort problem due to a lack of memory.
jvm.option			
jvm12.conf	-Xrunoii	-Xgenconfig:32m,32m,semispaces:32m,768m,markcompact	<p>The parameters used in the <code>genconfig</code> option must be less than or equal to the values in the <code>jvm.maxHeapSize</code> and <code>jvm.minHeapSize</code>.</p> <p>For example:</p> <p>Given <code>-Xgenconfig:min0, max0, semispaces:min1, max1, markcompact</code></p> <p>then <code>max0 + max1 <= jvm.maxHeapSize</code> and <code>min0 + min1 <= jvm.minHeapSize</code></p>
cache-init			
obj.conf	false	true	<p>Add this line to <code>obj.conf</code> to disable the Web Server static page cache:</p> <p><code>Init fn="cache-init" disable="true"</code></p>

Profile Service Changes

This section provides details about profile service changes in iPlanet Portal Server. It contains the following topics:

- Disabling Synchronization of User Profile Changes
- Multi-Profile Server Support
- Getting and Setting User Properties

Disabling Synchronization of User Profile Changes

By default, changes that users make to their profiles are distributed to other platform server instances using synchronization requests sent over HTTP. This ensures that any instance that has a cached copy of that user's profile updates its cache with those changes before it needs to handle a request for that user again.

However, many large sites use load balancers in front of their platform servers that maintain sticky sessions. This ensures that the same platform server instance handles all the portal requests made during a single user session. Under these circumstances, distribution of user profile changes to other instances represents an unnecessary burden on the network.

Therefore, it is now possible to disable synchronization of user profile changes by adding the following entry to the `/etc/opt/SUNWips/properties.file` on each platform server:

```
sync.user.profiles=false
```

This should only be used when load balancers that maintain sticky sessions are in use. A side-effect of this option is that an additional LDAP read of the user's profile is needed at each login to ensure cached copies are updated with changes made during sessions on other instances.

Multi-Profile Server Support

A separate profile service is now used for each Portal Server instance. The profile services are synchronized with each other to keep all modified profile data current. Previously, all Portal Server instances in a deployment used a single profile service. This was a potential single point of failure.

Profile requests originating at any Product_Name instance are now directed to the profile server of that Portal Server. Each Product_Name instance communicates directly with the Directory Server. Performance and scalability for simultaneous logins are improved because all profile requests go directly to LDAP without XML-to-LDAP overhead.

Multiple directory servers are not supported at this time.

The LDAPMonitor object now checks for LDAP connectivity. If it finds a lost connection, it removes all connections from its LDAP connection pool and lets the profile service create the LDAP connection as needed. The first profile service requesting an LDAP connection would then refill the connection pool.

Administrators can use `directory.monitor.sleeptime`, a new parameter in the `/etc/opt/SUNWips/properties.file`, to define the length of the sleep interval, which is 30 seconds by default.

TIP

This is the format of the parameter:

`directory.monitor.sleepTime=sleepTime_in_milliseconds`

To set the interval to 40 seconds, for example:

`directory.monitor.sleepTime= 40000`

Getting and Setting User Properties

Two new methods called `setUserSessionProperty` and `getUserSessionProperty` in the `pluggableAuthAPI` enable authentication modules to get and set properties in the user session. They allow authentication modules to communicate with channels, applications, or other authentication modules by setting session properties.

Example

A custom authentication module may add the user password to the session, so that an application can retrieve this property, for single sign-on at a later time.

The parameter name is the property name, and the parameter value is the property value in this example:

```
public void setUserSessionProperty(java.lang.String name,  
                                   java.lang.String value)  
    throws LoginException
```

The parameter name is the property name and this returns the property value in this example:

```
public java.lang.String getUserSessionProperty(java.lang.String name)  
    throws LoginException
```

Server Changes

This section provides details about server changes in iPlanet Portal Server. It contains the following topics:

- Using Open Portal Mode
- Configuring Multiple Server Instances
- Multi-hosting

Using Open Portal Mode

iPlanet Portal Server can now be deployed without the services of the gateway. Running without the gateway is referred to as open portal mode. One iPlanet Portal Server installation can be configured to support both open and secure portal modes.

The services presented by the open portal typically reside within the DMZ, not within the secured intranet. If a portal provides public information and allows access to free applications, using open portal mode allows Portal Server to respond faster to access requests.

TIP	Using the iPlanet Portal Server in open portal mode may improve the individual response of the portal for a large number of simultaneous users.
------------	---

The following Portal Server features are provided by the gateway component and are thus not available when running in open portal mode:

- Netlet, which provides a secure encrypted tunnel for TCP/IP applications from the browser through the gateway to the backend service.
- URL access policy enforcement, which ensures that any request for a URL is validated against the requesting user's policy. It is important to note that this does not mean there is no user policy. All iPlanet Portal Server services such as the Desktop are protected by the iPlanet Portal Server Policy server.

If a user is restricted from either running the Desktop or adding specific channels within the Desktop, for example, this type of policy is still enforced.

- URL rewriting, requiring that all URLs accessed from the Desktop must be resolvable and reachable by either the client host or the web proxy the client is configured to use.

- HTTP basic authentication, which provides a single sign-on service. The gateway listens for interaction between the user and the Web Server and stores the user name and password in the user profile so that the next time the user does not have to enter the information. The gateway responds on behalf of the user.

NOTE For instructions on installing the iPlanet Portal Server software in open portal mode, see Chapter 4, “Clean Installation,” in the *iPlanet Portal Server Installation Guide*.

Configuring Open Portal Mode

The typical public portal uses HTTP. You can now deploy a portal using HTTP over SSL (HTTPS). You can configure Portal Server to run HTTPS services during installation, or you can manually change from HTTP to HTTPS after installation.

See the *iPlanet Portal Server Administration Guide* for more information on using SSL.

The user accesses the server directly as though the server is configured for HTTP, but uses the URL `https://server.domain` instead of `http://server.domain`.

To update Portal Server to open portal mode following installation, complete the following steps:

1. Use the `ipsgateway stop` command to shut down the gateway.

```
# /opt/SUNWips/bin/ipsgateway stop
```

2. Use the `pkgrm` command to remove the gateway.

TIP When the gateway and Portal Server are on different machines, remove the `SUNWwtgwd` and `SUNWwtsd` packages.

When the gateway and Portal Server are on the same machine, remove only the `SUNWwtgwd` package.

Logging In

The rules for logging in to the open Portal Server include the following:

- If the server is running HTTP and is using the default HTTP port 80, use the following URL:

`http://server.domain`

- If the server is running HTTP and is using a non-default port number, use the following URL:
`http://server.domain:port`
- If the server is running HTTPS and is using the default HTTPS port 443, use the following URL:
`https://server.domain`
- If the server is running HTTPS and is using a non-default HTTPS port number, use the following URL:
`https://server.domain:port`

NOTE Use the fully qualified name of the server.

Supporting SSL Login

In a portal setup without the gateway, this feature provides support for SSL (HTTPS) server for user registration although the sites run without SSL (HTTP).

All registrations and logins now can be directed to an HTTPS server, while all Desktop redirects are sent to an HTTP server. The iPlanet Portal Server supports this configuration by running two instances of iPlanet Portal Server. One instance runs HTTP, and the other instance runs HTTPS.

After you set up the server instances, you convert the second instance of the server to SSL. After configuring the second instance, you update user profiles to redirect users to the non-SSL server after authentication. See “Multi-Profile Server Support” for detailed information on setting up two instances of iPlanet Portal Server.

To ensure that all unauthenticated sessions on the non-SSL server are redirected to the SSL server, you must edit the `platform.conf` file in `/etc/opt/SUNWips/` directory and then set the user profile to point to the non-SSL port on the open portal.

To do this, complete the following steps:

1. Become `root` and change directory to `/etc/opt/SUNWips`.
2. In the appropriate `platform.conf` files, change the value for `ips.nosession.url` setting to this:

```
ips.nosession.url=https://server.domain:port/login
```

TIP Replace *server* with the host name of the SSL server and *port* with the port number where the server is running. For example:

```
ips.nosession.url=https://server1.sesta.com:8081/login
```

If you have multiple iPlanet Portal Server server instances, you must edit the `platform.conf` file associated with each instance.

3. Add the following to the

`/etc/opt/SUNWips/desktop/customized_template/iwtLoginProvider/display.html` file:

```
<FORM ACTION="https://server1.sesta.com:8081/login/Membership"
onSubmit="return checkBlank()" MET
HOD=GET NAME="userid_form" ENCTYPE="application/x-www-form-urlencoded">
```

and

```
<FONT FACE="[tag:iwtDesktop-fontFacel]" SIZE="-1"><A
HREF="https://server1.sesta.com:8081/login/Membership?arg
=newsession&page=1&Submit=New%20User">Sign Me Up</A></FONT>
```

4. Log in to the administration console and select Manage Domains.

5. Select your domain and under Profiles, select User.

6. Select Show Advanced Options.

7. Change User's Default URL from `/DesktopServlet` to:

```
http://server.domain:port/DesktopServlet
```

8. Select Submit at the bottom of the page, and save the changes.

9. On the Profile Successfully Updated page, select Continue.

NOTE For information about changing multiple instance servers to SSL in open portal mode, see [“Changing Created Multiple Instance Servers to SSL.”](#)

URL Scraping

Some rewriting facilities that were only in the gateway profile are now available with the server. This allows administrators to configure parameters for URL scraping in open portal mode. These parameters include:

- Rewrite HTML attributes

- Rewrite HTML attributes containing JavaScript
- Rewrite JavaScript function parameters
- Rewrite JavaScript variables in URLs
- Rewrite JavaScript variables functions
- Rewrite JavaScript function parameters in HTML
- Rewrite JavaScript variables in HTML
- Rewrite Applet parameter values list

When the open portal mode is installed, the selections on the Gateway Profile page are not disabled even though most selections are disabled because no gateway is running.

To view this and observe the impact, in the administration console, do the following to access the Gateway Profile page:

1. Log on to the administration console as super administrator.
2. From the left frame, select Gateway Management.
3. Select the Manage Gateway Profile link.
4. Select the Gateway Profile page.

Using a Load Balancer

iPlanet Portal Server now supports using a load balancer in open portal mode. The load balancer must support persistent connections, sometimes referred to as sticky sessions based on cookies. If the load balancer supports persistence based on a cookie name and value, this feature must be enabled.

If the Portal Server environment includes a load balancer, and a URL scraper channel that references material from a server other than the iPlanet Portal Server, that material is looked up from the server on which it sits. For example, server names in an image's URL are visible in the browser's page information window, and the browser accesses those images without using the load balancer.

The load balancer must be able to recognize the cookie on the first reply from portal. It should then continue to send all requests with that cookie name and value to that same server. Cookie persistence algorithms that do not recognize the cookie on the reply do not work, because the first and second request can end up on different servers.

If the load balancer does not support this type of cookie persistence algorithm, but it supports load balancing to specific servers based on the presence of a cookie name and value, the administrator can edit the appropriate `platform.conf` file to configure cookie values on each server.

Each server defines a special cookie that the load balancer is configured to recognize and always forwards requests with that cookie to that specific server. Each Portal Server instance sets this cookie along with the usual portal session cookie.

Cookies can be used to establish session persistence between some load balancers and servers in an iPlanet Portal Server installation.

To use a load balancer in open portal mode, complete the following steps:

1. Set up a load balancer to the servers.
2. As root, add the following lines to the `platform.conf` file:

```
ips.lbcookie.name=IPSLbCookie  
ips.lbcookie.value=some_unique_server_string
```

TIP

This step is required only if the load balancer used supports load balancing to specific servers based on the presence of a cookie name and value. Refer to the documentation shipped with the load balancer to determine if this step is required.

Resonate is an example of a load balancer that requires administrators to edit the `platform.conf` file. When Resonate's administration console is used to create the cookie persistence rule for each server instance, the same

`ips.lbcookie.name` value assigned here must be used there.

3. Log in to the administration console as the super administrator.
4. Select Server Management and select Manage Profile Server.
5. Add the load balancer domain name to the Cookie Domain List and select Add.

TIP

Use this format to add the domain name:

`.domain_name.com`

Note the `.` that precedes the name.

For example:

`.sesta.com`

6. Select Add.
7. Select Submit.
8. Add the load balancer name to Domain URLs list.
9. In the administration console, select the desired domain.
10. Select Authentication.
11. Add the load balancer name three times to Domain URLs list.

TIP

You can use these formats to add the load balancer domain name:

`www.domain.com` (for example: `www.sesta.com`)

`www.domain.com/default_domain.com` (for example: `www.sesta.com/sesta.com`)

`www.domian.com/login` (for example: `www.sesta.com/login`)

12. Edit the URL for channels that reference their content from the iPlanet Portal Server server.

NOTE

This step is not for channels that point to external content. It is useful for portal-related content that is displayed in channels.

13. In the administration console, select the desired domain.
14. Click the key next to Applications to expand the list choices, and select Desktop.
15. Edit the URL scraper channels that reference their content from the server. Change the attribute to a relative URL by removing the protocol, server and port number from the URL.

TIP

For example, change this URL scraper channel value:

`http://server1.sesta.com:8080/ipinfo.html`

to:

`/ipinfo.html`

16. Select Submit.

Changing the Primary Profile Server to SSL

The profile server's protocol can be changed to HTTPS. This is the server that has the profile service running on it. See the following instructions.

NOTE In the following instructions and examples, `/opt` is the default installation directory.

NOTE Obtain a certificate from any of the certificate authorities supported by iPlanet Portal Server. Install it with the iPlanet Web Server. For information on installing a certificate, refer to the original *iPlanet Portal Server Installation Guide*. See “To Generate a Certificate for the Server Component of the Portal Server Product” steps 1 through 17. Do not change the encryption on/off option.

1. As root, use this command to start Portal Server:

```
# /opt/SUNWips/bin/ipsserver start
```

2. Log in to the administration console as super administrator.
3. From the left frame, select the Server Management link.
4. Select the Manage Server Profile link.
5. Change the Platform Server List attribute to HTTPS. For example:
`https://ipsserver.siroe.iplanet.com:8080`
6. Select Submit to save the changes.
7. Select Continue on the Profile Successfully Updated page.
8. From the left frame, select Server Management link.
9. Select Manage Naming profile.
10. In Profile URL, change the protocol to HTTPS. For example:

```
https://server1.server2.sesta.com@8080/profileservice
```

NOTE The profile URL would be changed to HTTPS if the original server is running the profile service as well. If the profile service is running on a different machine, the protocol should be the same as the server running the profile service.

11. In Logging URL, change the protocol to HTTPS. For example:

https://server1.server2.sesta.com:8080/loggingservice

12. Select Submit to commit these changes to the profile server.

13. Select Continue on the Profile Successfully Updated page.

14. In a terminal window, go to the `/etc/opt/SUNWips` directory.

TIP This directory contains `platform.conf` files of the type:

`/etc/opt/SUNWips/platform.conf.server.domain`

`/etc/opt/SUNWips/platform.conf.server.domain@8081`

`/etc/opt/SUNWips/platform.conf.server.domain@8082`

15. In the `platform.conf` file for the primary server, which is `/etc/opt/SUNWips/platform.conf.server.domain`, change HTTP to HTTPS in these definitions:

`ips.server.protocol` (for example, `ips.server.protocol=https`)

`ips.naming.url` (for example, `ips.naming.url=https`)

`ips.notification.url` (for example, `ips.notification.url=https`)

16. In the `platform.conf` file for the second server, which is `/etc/opt/SUNWips/platform.conf.server.domain@8081`, change HTTP to HTTPS in this definition:

`ips.naming.url` (for example, `ips.naming.url=https`)

17. In the `platform.conf` file for the third server, which is `/etc/opt/SUNWips/platform.conf.server.domain@8082`, change HTTP to HTTPS in this definition:

`ips.naming.url` (for example, `ips.notification.url=https`)

18. Use a text editor to edit the `/opt/netscape/server4/https-server1/config/magnus.conf` file to turn on the Security option. For example:

```
Security on
```

19. Use this command to stop and restart all Portal Server instances:

```
# /opt/SUNWips/bin/ipsserver startall
```

Configuring Multiple Server Instances

You can now run multiple instances of the iPlanet Portal Server on different ports. Running multiple instances of Portal Server, each with its own copy of iPlanet Web Server on the same physical machine, changes the context of iPlanet Portal Server to have multiple web servers and JVMs on the same machine.

It is possible to configure the various instances to implement SSL, giving a user the flexibility of switching to SSL mode for security on any of the iPlanet Portal Server instances. So when running in open portal mode, iPlanet Portal Server instances can talk over SSL.

NOTE Using the `create` command only configures new iPlanet Portal Server instances using the HTTP protocol.

Installing Multiple Server Instances

You can create multiple instances of the iPlanet Portal Server on different ports, after you install iPlanet Portal Server.

TIP For installation instructions, see “Service Pack 5 Installation Notes” in the *iPlanet Portal Server Installation Guide*.

To configure multiple server instances, complete the following steps:

NOTE In the following instructions and examples, `/opt` is the default installation directory.

1. As root, enter the following commands:

```
# cd /opt/SUNWips/bin
# ./ipsserver create
```

This option is interactive. The administrator can continue to enter unique port numbers, not already in use, where multiple instances are to be created. Select Return after your last entry.

TIP To determine whether the desired port is available and unused, enter this command from the command line:

```
netstat -a | grep port | wc -l
```

This process takes approximately 5 minutes, depending on the machine architecture. Here is an example of what the script output and user input looks like:

```
The installation directory is found to be /opt using the same
Enter a blank line when finished!
What is the port number where the Portal Server Server will run? 8081
What is the port number where the Portal Server Server will run? 8082
Do you want to overwrite this ? y/[n] Y
```

Should any instances entered already exist, the following message is displayed before you are prompted to overwrite:

```
Warning:: server instance already exists:server1.sesta.com-8081
```

2. Select Return when the menu is completed.
3. Use this command to stop and restart all the Portal Server instances:

```
# /opt/SUNWips/bin/ipsserver startall
```

TIP To start the different server instances separately, use the individual `ipsserver` scripts in the `/opt/SUNWips/bin` directory.

To start the server instance running on 8081, for example, use:

```
/opt/SUNWips/bin/ipsserver.server1.sesta.com@8081 start
```

You can still start the original server using:

```
/opt/SUNWips/bin/ipsserver start
```

4. Log on to the administration console as super administrator.
5. From the left frame, select the Server Management link.
6. Select the Manage Server Profile link.
7. Add the new server instances to the Server List. For example:

```
http://ipsserver.server1.sesta.com:8081
```

```
http://ipsserver.server1.sesta.com:8082
```
8. Select Submit and save the changes.
9. On the Profile Successfully Updated page, select Continue.
10. Use this command to stop and restart all the Portal Server instances:

```
# /opt/SUNWips/bin/ipsserver startall
```

These instances can be directly accessed through the web browser. For example:

```
http://server1.sesta.com:8080
```

```
http://server1.sesta.com:8081
```

```
http://server1.sesta.com:8082
```

If the machine name is `siroe.ipplanet.com`, and two port numbers 8081 and 8082 were configured as shown in the Step 1, and the install directory was `/opt`, the following files are listed:

```
/opt/SUNWips/bin/ipsserver.server1.sesta.com@8080
```

```
/opt/SUNWips/bin/ipsserver.server1.sesta.com@8081
```

```
/opt/SUNWips/bin/ipsserver.server1.sesta.com@8082
```

Updated Command Options

Table 12 lists new ipsserver commands and the command options that have been updated. The first column contains the command name and option. The second column contains a description of the command option.

The following examples assume that the commands are being run from the directory in which they reside.

Table 12 New ipsserver command Options

Command	Description
<code>./ipsserver start</code>	Starts the original server only.
<code>./ipsserver startall</code>	Starts the original server and all created multiple instances.
<code>./ipsserver stop</code>	Stops the original server only.
<code>./ipsserver stopall</code>	Stops the original server and all created multiple instances.
<code>./ipsserver delete</code>	Deletes all created multiple instances, but leaves the original server.

Changing Created Multiple Instance Servers to SSL

In open portal mode, you can change the protocol to HTTPS of any of the other created multiple instances. Make these changes for the server where SSL is required. Make sure that the key pair file password and the trust database password entered for any of the certificate installation is the same between all the iPlanet Portal Server created multiple servers which are being configured to talk over SSL and that password *must* be the SSL passphrase entered during the iPlanet Portal Server installation.

NOTE In the following instructions and examples, `/opt` is the default installation directory.

NOTE Obtain a certificate from any of the certificate authorities supported by the iPlanet Portal Server. Install it with the iPlanet Web Server. For information on installing a certificate, refer to the original *iPlanet Portal Server Installation Guide*. See “To Generate a Certificate for the Server Component of the Portal Server Product” steps 1 through 17. Do *not* change the encryption on/off option.

If the instance running on port 8081 is to be secure, for example, complete the following steps:

1. Stop and restart all Portal Server instances:

```
# /opt/SUNWips/bin/ipsserver startall
```

2. Log on to the administration console as super administrator.
3. Select the Server Management link from the left frame.
4. Select the Manage Server Profile link in the right frame.
5. Change the Platform Server List attribute to https. For example:
`https://ipsserver.server1.sesta.com:8081`
6. Select Submit.
7. Select Continue on the Profile Successfully Updated page.
8. Open the `platform.conf` file of the server that is configured for SSL, in the `/etc/opt/SUNWips` directory.
9. Find the `ips.server.protocol` setting and change it to the following:
`ips.server.protocol=https`
10. Find the `ips.notification.url` setting and change it to the following
`ips.notification.url=https`
11. Open the `/opt/netcape/server4/https-server1.domain@port/config/magnus.conf` file.
12. Find the Security setting and change it to the following:
`Security on`
13. Use this command to `s top` and restart all Portal Servers:

```
# /opt/SUNWips/bin/ipsserver startall
```

14. To confirm that the configured server is talking SSL protocol, enter its URL in a browser. For example:
`https://server1.sesta.com:8081`

Multi-hosting

The server can now access multiple instances of iPlanet Portal Server from a single server installation. Access to Portal Server is through one of these:

- `http://server.domain:port`
- `https://server.domain:port` (if the server is configured to use HTTPS)

To log in to a different domain on Portal Server, use this URL:

`http://server.domain:port/login/domain`

Mapping URLs to Domains

If the existing installation of Portal Server contains multiple servers and multiple domains, a URL-to-domain mapping setting allows Portal Server to find the domain automatically. The domain name does not need to be provided in the URL.

If the Portal Server installation has one server and two domains (`domain1` and `domain2`), the following URL-to-domain mapping is needed:

- `http://server.domain:port/domain1` to go to `domain1`
- `http://server.domain:port/domain2` to go to `domain2`

To map a URL to a domain, complete the following steps:

1. Log in to the administration console as super administrator.
2. From the left frame, select the Manage Domains link to display the Portal Server Domains page.
3. Select one of the domains to display the Domain, Role and Users page.
4. Expand the Profiles link and select the Authentication link.
5. In the Domain URLs field, add the URLs for that domain.
6. Select Add.
7. Select Submit.

NOTE You must repeat these steps for each domain.

Domain URL Mapping List

The domain URL list for `domain1` must contain the following URLs:

- `/domain1`

- server1.domain/domain1
- server1 IP address/domain1
- /domain2
- server1.domain/domain2
- server1 IP address/domain2

NOTE In the following instructions and examples, /opt is the default installation directory.

1. Add the following two lines to the obj.conf file in the /opt/netscape/server4/https-**server1**/config/ directory:

```
NameTrans fn="redirect" from="/domain1" url="/login/domain1"
```

```
NameTrans fn="redirect" from="/domain2" url="/login/domain2"
```

Replace domain 1 and domain 2 with iPlanet Portal Server domain names.

2. Use this command to stop and restart the server:

```
# /opt/SUNWips/bin/ipsserver start
```

Example 2

If there are three servers (server1, server2, and server3) and two domains (domain1 and domain2), the following are the URL to domain mappings:

```
http://server1.domain:port ---> go to domain 1
```

```
http://server2.domain:port ---> go to domain 2
```

```
http://server3.domain:port ---> go to domain 2
```

To map a URL to a domain, complete the following steps:

1. Log in to the administration console as super administrator.
2. From the left frame, select the Manage Domains link.
3. In the Portal Server Domains page, select one of the domains.
4. In the Domain, Role and Users page, expand Profiles link and select the Authentication link.

5. Scroll to the Domain URLs field, add the URLs for that domain. (See the “[Domain URL Mapping List for Example 2](#)” section.)
6. Select Add.
7. Select Submit.
8. Repeat these steps for the second domain.

Domain URL Mapping List for Example 2

The domain URL list for `domain1` must contain the following URLs:

- `server1.domain`
- `server1.domain IP address`
- `server1.domain/domain1`
- `server1.domain IP address/domain1`
- `.domain/domain1`
- `server1.domain/login`
- `server1.domain IP address/login`

The domain URL list for `domain2` must contain the following URLs:

- `server2.domain`
- `server2.domain IP address`
- `server2.domain/domain2`
- `server2.domain IP address/domain2`
- `.domain/domain2`
- `server2.domain/login`
- `server2.domain IP address/login`
- `server3.domain`
- `server3.domain IP address`
- `server3.domain/domain2`
- `server3.domain IP address/domain2`
- `server3.domain/login`
- `server3.domain IP address/login`

Running Applications on a Non-iPlanet Portal Server

If you write applications using iPlanet Portal Server APIs, you can run them on a server host that is not iPlanet Portal Server. The applications can be either standalone Java applications (with some limitations) or a servlet application running on iPlanet Web Server.

NOTE iPlanet Portal Server public APIs are supported only on Solaris™ operating systems.

Software supported include:

- JDK software/Java™ runtime environment 1.2.2_16-er-20030716
- Sun ONE Web Server 4.1 SP12
- Solaris™ 2.6 Operating System (SPARC™ Platform Edition)
- Solaris™ 7 Operating System (SPARC Platform Edition)
- Solaris™ 8 Operating System (SPARC Platform Edition)

Setting Up a Non-iPlanet Portal Server Server

NOTE In the following instructions and examples, `/opt` is the default installation directory.

To set up a non-Portal Server, complete the following steps:

1. Create the following directories on the server host.

```
/opt/SUNWips
/opt/SUNWips/lib
/opt/SUNWips/locale
/etc/opt/SUNWips
```

2. Copy the `/etc/opt/SUNWips/platform.conf` file to the same location on the server host.
3. Modify the `ips.notification.url` parameter in the `platform.conf` file to be the fully qualified domain name of the server the application will run on. For example:

```
ips.notification.url=http://server1.sesta.com:8080/notificationsevice
```

4. Copy the following files from `/opt/SUNWips/lib` to the same location on the server host:

```
o ips_sdk.jar
```

- xml.jar
 - jndi.jar
5. Copy the following files from /opt/SUNWips/locale to the same location on the server host:
 - iwtPll.properties
 - iwtProfile.properties
 - iwtSession.properties
 - iwtLogging.properties
 - iwtNaming.properties
 6. If the client application will run under iPlanet Web Server, update the classpath on the iPlanet Web Server:


```
iws_server_root/https-your_server/config/jvml2.conf
```

In the classpath, include:

 - /opt/SUNWips/locale
 - ips_sdk.jar
 - xml.jar
 - jndi.jar
 7. Add the following line to the iPlanet Web Server file *iws_server_root/https-your_server/config/rules.properties*:


```
/notificationService=notificationService
```
 8. Add the following line to the iPlanet Web Server file *iws_server_root/https-your_server/config/servlets.properties*

```
servlet.notificationService.code=com.ipplanet.portalserver.pll.client.PLLNotificationServlet
```
 9. Restart the iPlanet Web Server server after updating these files.

Applications Not Running Under iPlanet Web Server

A notification feature of the iPlanet Portal Server session and profile APIs allows applications to listen for profile and session state changes. If an application runs as a standalone application:

- The application cannot receive session or profile notifications.
- The client side cache is not updated when attributes change in the profile. The application sees the changes only after the user logs out and logs back in.

- After the user session times out on the iPlanet Portal Server session server, the user still has a valid session until the cache refresh timer is reached.

TIP Use the administration console to reduce the cache seconds attribute in the session profile.

Running Client Applications Using SSL

If the iPlanet Portal Server server is configured to use SSL, the iPlanet Portal Server APIs also use SSL. The application must also use SSL to communicate with the iPlanet Portal Server services.

The iPlanet Web Server, when installed, is not properly configured to support outgoing SSL connections by servlets.

NOTE In the following instructions and examples, `/opt` is the default installation directory.

To enable SSL connections by servlets, complete the following steps:

1. Copy the following files from the `/opt/SUNWips/lib` directory to the same location on the server host:
 - `ssl.jar`
 - `x509v1.jar`
2. include the following files in the classpath in the iPlanet Web Server `iws_server_root/https-your_server/config/jvm12.conf` file:
 - `ssl.jar`
 - `x509v1.jar`
3. Copy the `/opt/SUNWips/lib/solaris/sparc/libjssl.so` file to the `iws_server_root/bin/https/lib` directory.
4. Restart the iPlanet Web Server after updating these files.

Running Applications Through the Gateway

To run applications using the iPlanet Portal Server gateway, you must configure the gateway to forward iPlanet Portal Server cookies to the application host. By default the gateway forwards cookies only to the iPlanet Portal Server.

If the URL of the server the application is running on is not added to this attribute, the iPlanet Portal Server cookie is not forwarded, and the application has an invalid user session.

NOTE In the following instructions and examples, `/opt` is the default installation directory.

To configure the gateway to forward cookies, complete the following steps:

1. Log on to the administration console as super administrator.
2. From the left frame, select the Gateway Management link.
3. In the right frame, select the Manage Gateway Profile link.
4. Select the Manage Gateway Profile link in the right frame.
5. Scroll down to the Forward Cookie URL List attribute.
6. Enter the URL of the server the application is running on in this field. For example:
`http://auth.sesta.com:8080`
7. Select the Submit button at the bottom of the page to commit these changes to the profile server.
8. Select the Continue button on the Profile Successfully Updated page.
9. Use this command to restart the gateway:

```
# /opt/SUNWips/bin/ipsgateway start
```

Running Applications Without the Gateway

To run applications without the gateway, access the application using a fully qualified domain name (FQDN).

If a fully qualified domain name is not used, the iPlanet Portal Server cookie is not forwarded to the application, and the user session is invalid.

Third-Party Software Changes

This section provides details about updating the `smbclient` command in iPlanet Portal Server.

Adding smb.conf Parameter to smbclient

The `smb.conf` parameter has been added to the `smbclient` command to allow NetFile to display ISO8859-1 character sets in file names.

This new parameter also provides a way for administrators to configure the NetFile application to take advantage of other `smbclient` features.

Example

Here is an example of an `smb.conf` file that could be used to see the choices translated in a locale's chosen language:

```
# Samba config file created using SWAT
# from foo.sesta.com (1.2.3.4)
# Date: 2002/01/16 18:16:51

# Global parameters
[global]
    path=/
    workgroup = MYWORKGROUP
    security = user
    hosts allow = localhost 1.2.
    username map = /opt/samba/lib/users.map
    encrypt passwords = yes

[tmp]
    comment = temporary files
    path = /tmp
    read only = yes
    user = root

[homes]
    comment = Users' home directories
    path = /u/%S
    writeable = Yes

[printers]
    path = /tmp
    guest ok = Yes
    printable = Yes

[CTEServer]
    comment = site of web server
    path = /opt/netscape/server4

[iPortal]
    comment = top directory for iPortal files
    path = /opt/SUNWwips
```

An accompanying map file in `/opt/samba/lib/users.map` might look like this:

```
root = admin administrator
```

For more information about Samba-specific configurations, refer to the samba Web site at:

<http://samba.org/samba>

Webmail Changes

This section provides details about enabling Webmail applications in iPlanet Portal Server.

Enabling Webmail Applications in Portal Server

Portal Server can now deliver Webmail applications.

A connection handling problem between the Internet Explorer 5.5 browser and iPlanet Portal Server may result in `Page not Found` errors when Webmail is used. The administrator can avoid this problem by editing the Messaging Server's `main.js` file.

To change the `main.js` file on the Messaging Server, complete the following steps:

1. As root, edit the `/msg_install_dir/msg*/html/main.js` file.
2. Find the following line:

```
// \5c -> \
```

3. Change this line to:

```
// \5c -> backslash
```

4. Find all instances of `.msg` entries and change each `msgHREF` to `srcHREF` to get the rewritten URL.

Deprecated Features

The following features and products might not be supported in future releases of the iPlanet Portal Server product:

- Firewall software that is currently included with the iPlanet Portal Server product
- NetFile Lite
- GraphOn server and client (client still available for download)
- Citrix (available for download)
- PCAnywhere Java client (available for download)
- Mail check channel (replaced by mail channel)

Although the GraphOn client, Citrix software, and PCAnywhere Java client will no longer be included as third-party software with the iPlanet Portal Server product, they will continue to work with the iPlanet Portal Server product and are available from their respective websites.

Known Problems and Limitations

This section lists known problems with iPlanet Portal Server 3.0, Service Pack 5. Details are provided in the following areas:

- Authentication
- Administration
- Desktop
- Gateway
- Installation
- ipsadmin
- ipsserver
- Logging
- NetFile

- NetMail
- Sample Providers
- Upgrade

Authentication

The LDAP authentication module does not allow the administrator to specify a search filter when configuring the server for user lookup in the directory. (4599553)

The text field, search filter for `userId`, refers to the attribute (by default, the `uid` attribute) to use in searching the directory. Then the attribute specified in the search filter for `userId` is used to create the search filter used in the lookup.

For example, if you did not specify an attribute in the search filter for `userId` text field and left it blank, the default is `uid`. So, the search filter becomes `(uid=jim)`, where `jim` is the user name that the user entered. If the search filter for `userId` field contained the value `surname` or `sn`, then the search filter would become `surname=jim`.

Workaround:

None.

Administration

Inherited value is not reflected once the change has been submitted. (4825404)

If the Make Inherited option is selected for a field in the Administration console, the inherited value is not reflected after the change has been submitted. However the change is written back to the profile server, and will be reflected when the profile is next refreshed.

If an end user has customized the Desktop, new channels cannot be pushed to the Desktop. (4500010)

Currently, if an end user personalizes the Desktop and the administrator creates a new channel, there is no way for the channel to automatically appear on the Desktop.

Workaround

Each user needs to add the new channel manually.

Adding channels using a platform server that does not have the profile server installed causes an error. (4521342)

Although the channel wizard is present in the administration console, if a platform server does not have the profile server installed, an error occurs and channels will not be added to the Desktop.

Workaround

To add channels, the administrator must be logged onto the primary server (first installed server), or original profile server.

The Desktop is blank if no channels are selected in the administration console and in the Desktop. (4375670)

Workaround:

None.

The setDomain method should attempt to retrieve a domain profile before setting the domain. (4378030)

Workaround:

None.

The administration console allows duplicate tab names if one attribute is different. (4376634)

Workaround:

Verify that tab names are not duplicated.

The Valid Session number in the Manage User Session page provides an inaccurate number of valid sessions. (4381586)

When you log in to the administration console (either as super user or any user) and select Manage User Session, the Valid Session number is shown as 1. When you log in again from another browser, the Valid Session number does not increment to 2 to show that two valid sessions are in progress.

Workaround:

None.

Contents of profilestyle.css can become visible in the administration console when adding a new user to a newly created domain. (4379326)

Workaround:

None.

After the server is restarted, the gateway cannot be restarted from the administration console. (4531433)

After the server is restarted, the gateway's session becomes invalid. The next connection will cause the gateway to restart itself.

Workaround:

Manually restart the gateway and then click on the Gateway Management link again in the admin console.

NOTE Just hitting the browser reload button will not work.

The gateway cannot be restarted from the administration console if a case mismatch for the gateway name occurs during installation. (4521387)

During installation of the gateway and the profile server, the fully qualified name of the gateway given should match the profile server name. For example, if `gateway.sesta.com` is the fully qualified name provided during the gateway installation, during the profile server installation, the gateway name must be entered as `gateway.sesta.com` (not `gateway.SESTA.COM`, for example) during the profile server installation.

Workaround:

if there is a case mismatch problem occurs, edit the `/etc/opt/SUNWips/platform.conf` file to change the `ips.gateway.host` value to match the entry in the server configuration. For example, change the value to `ips.gateway.host=gateway.sesta.com`. Then restart the gateway.

Workaround:

When accessing the administration console through the gateway, the URL in the browser's address field reflects the name of the server that the gateway is connecting to. The server name must be that of the primary server. If more than one instance is running on the primary server, the URL must also contain the port number for the primary instance.

The URL should be similar to the following:

`https://server1.sesta.com:333/https://primary_server.sesta.com:primary_instance_port/`

1. Verify that the gateway is connecting to the primary server and the primary iPlanet Portal Server instance. If necessary:
 - Replace the server name in the URL so that it contains the name of the primary server.
 - Replace port number in the URL so that it contains the port number of the primary iPlanet Portal Server instance.
2. Select Enter.

Desktop

Disabling the Netlet provider in the Administration console for a user causes "Document contained no data" error message. (4319604)

Workaround:

Remove the provider from the channel list in the Administration console.

When using Internet Explorer 5x on Windows 98, closing the Netlet window crashes the web browser. (4355280)

Workaround:

None.

Using bookmark provider with Internet Explorer 4.x client on open portal gets a script error (4358738)

Workaround:

None. This Internet Explorer 4.x bug is not reproducible with Internet Explorer 5.x or Netscape browsers.

delAttribute permits deletion of a profile attribute without write permission. (4447005)

Workaround:

None.

Administrators can delete their own accounts. (4454833)

Workaround:

1. Log on as root.
2. At the prompt, enter this string:

```
# echo '<iwt:Att  
name="iwtUser-role"><Val>/$DOMAIN/AdminRole</Val></iwt:Att>' |  
/opt/SUNWips/bin/ipsadmin create user /$DOMAIN/root/dev/stdin
```

`$DOMAIN` is the default domain and `AdminRole` is the administrator's role.

3. Select Return.

Descriptions for channels created with channel wizard cannot be localized. (4457299)

Workaround:

To localize the description and title for a channel created with the channel wizard, complete the following steps:

1. On each iPlanet Portal Server, create a file called
`/opt/SUNWips/locale/channel_locale.properties` where *channel* is the fully qualified name of the channel and *locale* is the name of the locale to be supported.

TIP	<p>The fully qualified name of the channel is printed on the last page of the channel wizard, and it is also shown in the available channels list in the Desktop profile.</p> <p>The locale is a language and country combination. For example: <code>en_US</code></p>
------------	--

2. In this file, create these entries for the description and title:

```
description=This is the description
```

```
title=This is the title
```

The `.properties` file must use Java Unicode encoding, where multi-byte characters are represented as `xxxx` where the `xs` are hexadecimal digits.

Files in this encoding can be created from files in a variety of native encoding using the `java native2ascii` program.

NOTE	A separate <code>.properties</code> file is necessary for each locale to be supported.
-------------	--

The user's default HTML character set is overridden, which causes problems in an iPlanet Portal Server environment that uses multiple locales. (4481045)

Workaround:

Specify the user's character set in the profile and in the `.properties` file. To do so, complete the following steps:

1. Log in to the administration console.
2. Select Manage Domains.
3. Select the domain for which you want to specify the locale and character set.
4. Select User in the Profiles list.
5. Enter the locale information in User's Default Locale. To specify the Japanese locale, for example, enter `ja_JP`
6. In the User's Default HTML charset field, enter the character set information.
7. Select Submit at the bottom of the page.
8. Select Continue on the Profile Successfully Updated page.
9. As root, create a property file for the locale, if one does not already exist, in `/opt/SUNWips/locale`.

10. Rename the file, by adding the locale specifier. For example, to create a property file for the Japanese locale:

```
# cp /opt/SUNWips/locale/iwtUser.properties iwtUser_ja_JP.properties
```

11. Edit the property file to specify the character set. For example, to specify the Japanese locale:
charset=EUC-JP

NOTE This workaround applies for the NetMail character set and the `iwtNetMailServlet.properties` file. Perform this procedure for creating and editing the `iwtNetMailServlet.properties` file.

Reconnecting to a Netmail Java session causes Internet Explorer 5.0 or Internet Explorer 5.5 browsers to close when running on a Windows 2000 client machine when using Microsoft Virtual Machine (VM) for Java, 5.0 Release 5.0.0.3234. (4525913)

Workaround:

Install Microsoft VM for Java, 5.0 Release 5.0.0.3802.

Users logged in as anonymous cannot access other authentication mechanisms with the same iPlanet Portal Server session. (4525900)

This problem requires the user to exit the browser because the anonymous user Desktop page does not have a means for logging out of the session.

Workaround:

None.

Gateway

When the Non Portal Server Cookie Management option is enabled, the gateway rewrites cookies using the domain name of the gateway. Internet Explorer does not accept these cookies when domain names contain upper case letters. (4647934)

Workaround:

Use lower case letters when setting domain names during installation and when referring to domain names.

Installation

Installing the iPlanet Portal Server product over a previous installation that did not install correctly causes the installation log file to get very large. (4448387)

Workaround:

After installation, remove the installation log file

```
/var/sadm/install/logs/ipsinstall.process_id/install.log.
```

Solaris 8 patch causes patchadd -p command called from install script to fail due to large output. (4638284)

Workaround:

Change the variable assignment for AWK from `usr/bin/awk` to `usr/bin/nawk` in `ipsinstall`. The approximate location for this change is at line 10 in the script.

ipsadmin

When using an `ipsadmin` command line option to add, delete, or change a `userid` that contains special characters, the special characters are treated as delimiters and the `ipsadmin` utility gives an error. (4640045)

Workaround:

Place single or double quotation marks around the string that contains the special character to identify it as a single token.

The command `ipsadmin` does not check for the syntax of boolean flags. (4319514)

Workaround:

When you create an XML file, if the attribute type is boolean, add a true or false statement. For example:

```
<iwt:Att name="iwtUser-trustProxyEnabled"
  desc="Trust Proxy Feature"
  type="boolean"
  idx="X-x1"
  userConfigurable="TRUE">
  <Val>false</Val>
  <Rperm>ADMIN</Rperm><Rperm>OWNER</Rperm>
  <Wperm>ADMIN</Wperm>
</iwt:Att>
```

If the iPlanet Portal Server software is in a non-English locale, any input provided to the `ipsadmin` command should be in UTF-8 character encoding when using the certain options with an xml file. **(4614401)**

These options include the following:

- `ipsadmin change`
- `ipsadmin create`
- `ipsadmin import`

Workaround:

XML files should not use Java Unicode encoding as produced by `native2ascii`. To change the character set encoding in an XML file, do one of the following:

- Set the encoding header at the top of the XML file to the correct character set.
- Convert the file to UTF8 and set the encoding in the XML file to UTF.

An example of an encoding header using the Thai character set would be:

```
<?xml version="1.0" encoding="TIS620"?>
```

An example of an encoding header set to UTF8 would be:

```
<?xml version="1.0" encoding="UTF8"?>
```

To convert an XML file to UTF8 do the following:

1. Extract `getdomain.xml` using the `ipsadmin` utility.

```
# ipsadmin get domain sun.com > getdomain.xml
```

2. Use `native2ascii` to convert it to `ascii` mode.

```
# native2ascii -encoding character_encoding getdomain.xml getdomain-ascii.xml
```

For example, if using Thai character set encoding, the command would look like:

```
# native2ascii -encoding TIS620 getdomain.xml getdomain-ascii.xml
```


3. Use `native2ascii` to convert it to UTF mode.

```
# native2ascii -encoding UTF8 -reverse getdomain-ascii.xml\  
getdomain-utf8.xml
```

4. Get the XML file back using the `ipsadmin` utility.

```
# ipsadmin change domain sun.com getdomain-utf8.xml
```

ipsserver

The `ipsserver start` command requires additional arguments if the server is running multiple instances. (4379242)

For more information, see [“Configuring Multiple Server Instances.”](#)

Workaround:

To start all processes for all instances, use the `ipsserver startall` command:

```
# ipsserver startall
```

To start the processes for a specific instance, use the `ipsserver start` command and the server-specific `ipsserver` file:

```
# /opt/SUNWips/bin/ipsserver.servername.sesta.com@port start
```

Heavy loads for an extended duration cause components in the operating system to fail. (4472975)

Workaround:

None.

Logging

Log records should be written using iwtPlatform-locale not iwtUser-locale. (4376995)

Workaround:

None.

Mobile Access Pack

The iPlanet Portal Server: Mobile Access Pack software is not supported in Service Pack 5.

NetFile

The hour glass occasionally keeps running after attempting to add a share in NetFile Java. (4342453)

Workaround:

Select some other part of NetFile to clear up the hour glass.

NetFile Lite does not check the size of a file before attempting to upload. If the file is greater than 5 MB, the upload fails. (4293370)

Workaround:

None.

Uploading tar files greater than the 5 MB limit in NetFile Lite, and tar files greater than the 500 MB limit in NetFile generates an incorrect error message. (4372826)

Workaround:

None.

The NetFile application allows users to access denied hosts if those hosts were added to the Desktop before a deny rule was added in the iPlanet Portal Server administration console. (4463515)

Workaround:

None.

if Portal Server and the FTP server are on different subnets, the FTP server is tried on all the IP addresses of the interfaces. (4486094)

It is expected that the interface's IP address and the IP address of the FTP Server are on the same subnet. The solution does not work with IPv6 to IPv4 tunneling. The solution does not work with tunnelled source and destination, even if the source and destination addresses are IPv4. The solution works with multiple homes created for separating two different networks.

In the case an appropriate IP address/interface cannot be determined, the FTP server is tried for on all IP addresses of the interfaces. In this case the request can time out and NetFile would show the contents to be blank.

NetMail

A race condition occurs if when replying to a message, selecting send and then immediately deleting the message. (4321516)

Workaround:

Wait for the reply flag to be set (slow down) or delete the message again.

IMAP password is displayed in clear text in source of edit. (4307367)

Workaround:

None

Sample Providers

The editType attribute is missing in the iwtHelloWorld3Provider.xml file and the iwtQuotationProvider.xml file. (4389071)

Workaround:

Add the following code inside the component tags of iwtHelloWorld3Provider.xml:

```
<iwt:Att name="iwtHelloWorld3Provider-editType"
  desc="Edit Form Type"
  type="singlechoice"
  idx=" "
  userConfigurable="TRUE">
  <Val>edit_subset</Val>
  <CVal>edit_subset</CVal>
  <CVal>edit_complete</CVal>
```

```
<Rperm>ADMIN</Rperm><Rperm>OWNER</Rperm>
<Wperm>ADMIN</Wperm>
</iwt:Att>
```

Add the following code inside the component tags of `iwtQuotationProvider.xml`:

```
<iwt:Att name="iwtQuotationProvider-editType"
  desc="Edit Form Type"
  type="singlechoice"
  idx=" "
  userConfigurable="TRUE">
  <Val>edit_subset</Val>
<CVal>edit_subset</CVal>
<CVal>edit_complete</CVal>
  <Rperm>ADMIN</Rperm><Rperm>OWNER</Rperm>
  <Wperm>ADMIN</Wperm>
</iwt:Att>
```

Upgrade

Custom-added attributes are lost after upgrade is complete. (4766377)

During an upgrade, any custom-added attributes will be lost. This is because, if `ipsadmin` utility is used to add the new attributes, the utility will only add the attribute in the directory.

Workaround

In order for custom-added attributes to be carried over after an upgrade, the administrator must manually add the new attributes in the associated xml file.

When attempting to upgrade individual platform servers from a multi-profile environment to a Service Pack 5 multi-profile environment, the installer assumes that Directory Server is installed locally and attempts to re-install it. (4714378)

Workaround:

Temporarily change the `ips.profile.host` entry in the `platform.conf` file from the `localhost` to the “real” profile FQD.

When attempting to upgrade from a highly-customized Portal Server with many new components or channels, a tuned `ipsadmin` script is replaced by a default script and heap space allocated for successive component imports is inadequate.

Workaround:

Modify the `ipsinstall` script to stop for intervention right after the `SUNWwtds` package has been installed. The approximate location for this change is at line 3353 in the script. Change the following lines:

```
if [ "$PS_HOST" = "$LOCAL_HOST" ]; then
    SaveAttributes $TMP_DIR/attributes

    ProcessAttributes $TMP_DIR/attributes-preSP4
    $TMP_DIR/attributes$WORK_DIR/attributes-install

    InstallAttributes $WORK_DIR/attributes-install
fi
```

To the lines below:

```
if [ "$PS_HOST" = "$LOCAL_HOST" ]; then
    /usr/bin/echo "pkgadd complete..."
    /usr/bin/echo "make required changes in a different shell and press 'c' to
continue..."
    /usr/bin/echo "  \n\t[C]ontinue"
    read ans
    if [ $ans = 'c' ] || [ $ans = 'C' ]; then
        /usr/bin/echo ""
    else
        while [ $ans ]
        do
            /usr/bin/echo "Answer not understood"
            /usr/bin/echo "  \n\t[C]ontinue"
            read ans
            if [ $ans = 'c' ] || [ $ans = 'C' ]; then
                break
            fi
        done
    fi

    SaveAttributes $TMP_DIR/attributes

    ProcessAttributes $TMP_DIR/attributes-preSP4 $TMP_DIR/attributes
    $WORK_DIR/attributes-install

    InstallAttributes $WORK_DIR/attributes-install
fi
```

Once the installer prompts you to continue, edit *install_dir*/SUNWips/bin/ipsadmin. The approximate location for this change is at line 34 in the script. Change the following line:

```
{
  JAVA_HOME=/usr/java/j2sdk1.4.2_01
  CLASSPATH=com.iplanet.portalserver.ipsadmin.ImportComponent $*
}
```

To the line below:

```
{
  JAVA_HOME=/usr/java/j2sdk1.4.2_01
  CLASSPATH=com.iplanet.portalserver.ipsadmin.ImportComponent $*
}
```

Upgrade may take a long time because custom components are imported twice, regardless of whether they differ from their XML counterparts.

Workaround:

Edit the *ipsinstall* and *ipsadmin* scripts as noted previously in this Upgrade section. In addition, once the installer prompts you to continue, remove the XML files from */etc/opt/SUNWips/xml* that do not differ from values stored in LDAP.

Bugs Fixed

This section lists the fixes to the known problems associated with previous iPlanet Portal Server product releases.

Table 13 is a three column table that describes the bugs that have been fixed in this release. The first column contains the Bug ID and the component with which the bug is associated. The second column provides a description of the bug. The third column lists the Service Pack number that contains the bug fix.

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
Administration Console		

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4402762	The authentication component does not use the <code>iwUser-defaultURL</code> attribute value from a user's profile if the domain profile contains this attribute value.	SP5
4487666	Changes to External LDAP mappings made using <code>ipsadmin</code> command utility do not take effect. If new values are added to ExtLdap mapping using the <code>ipsadmin</code> command, the values get changed but the remote flags are not set therefore the changes do not take affect.	SP5
4507848	If Certificate authentication and SSL between the gateway and the iPlanet Portal Server are enabled at the same time, users are unable to login.	SP5
4688619	The iPlanet Portal Server returns a 502 gateway error when the administrator chooses Server Name under Session Servers.	SP5
4692953	Clicking on a server link on the Logging Servers page gives an iPlanet Portal Server gateway Error.	SP5
4489554	The attribute in LDAP to use for Profile ID field in Cert Authentication is a password field.	SP4
4490575	Administration console allows roles and users to be entered with non-ASCII characters, and generates an unclear warning message.	SP4
4490573	The Users First Name field in Membership Authentication is a password field.	SP4
4500644	The Service Pack 3 and Service Pack 3a versions limit the number of entries in the Cookie Domain List field to four. If more than four entries are used, the gateway component does not start.	SP4
4365124	Missing choice value (<code>cVal</code>) key value pairs in the <code>iwAuthCert.properties</code> file, and spaces in the keys in the <code>iwAuthCert.properties</code> file prevent some translated strings from being displayed in the administration console. Instead, the strings are displayed in the default language, which is English.	SP3
4387384	The keys in the xml files and the <code>.properties</code> files do not match, so some translated strings are not displayed in the administration console. Instead, the administration console displays the strings in the default language, which is English.	SP3
4374777	Domain Admin Roles page shows incorrect listing of domain administration roles.	SP2
4343322	Server restart from administration console did not work.	SP1
Authentication		
4496631	Wrong value is inserted upon creation of CSR if a blank field exists.	SP5
4525919	Problem with SSL authentication.	SP5
4621113	The LDAP authentication module fails when iDAR is interposed between the iPlanet Portal Server and the LDAP server.	SP5

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4639482	If the user logs in as anonymous, then uses the Login provider to login in, the user will not be able to use the Netlet. The Netlet loads, but the following error message is displayed: "Unable to connect to Gateway: default:443."	SP5
4658803	A series of rapid logins and logouts (100 users at 3 minutes per user session), cause the authentication servlet to fail to read the domain profile. This eventually results in an HTTP 500 server error and a fairly large memory leak.	SP5
4691500	Authentication fails when the AuthCert module cannot find the CN in an issuer name.	SP5
4417697	Authentication time out returns the error message document contains no data instead of a message stating that the session timed out.	SP4
4440245	Login channel causes passwords to show up in Web Server's access log. For more information, see "Default Login Channel Templates Changes" in this document.	SP4
4475149	Authentication chaining fails when SecureID is the second authentication module.	SP4
4362849	Certificate without cn causes a Java IO exception.	SP3
4378157	Authentication fails when platform server is configured to use HTTPS.	SP3
4412431	certadmin self-signed certificate validity defaults to 90 days.	SP3
4339793	UNIX authentication fails when the server and the doUnix helper are out of sync.	SP2
4346955	The verbose option for doSecureID does not allow logins.	SP2
4357503	The option to match the certificate in LDAP does not work if the certificate in the LDAP directory is stored as binary.	SP2
4343671	authd did not support open Portal Server login.	SP1
Desktop		
4467958	The Bookmark channel should be able to take a ' ' symbol in the title field. Currently, the ' ' symbol is used as dilimiter and does not recognize it as a regular character. The solution is to replace ' ' symbol with '-' and store the title accordingly.	SP5
4481400	The JSPProvider channel can not set a cookie at the browser.	SP5
4498354	The current implementation of the JavaScript in the bookmarks channel causes saved bookmarks to be sent through the gateway by using the <code>"/redirect"</code> scheme even when unnecessary.	SP5
4507845	The URLScraper does not pass cookies to the client.	SP5

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4508826	Internet Explorer caches Desktop content. If the user logs out and then selects the back button the Desktop is displayed. The links will not work, but the contents are visible.	SP5
4523437	If a bookmark is added with the same title and same URL as an existing one, it causes a server error.	SP5
4524840	The Tab edit button is displayed on the Desktop even when the Tab Provider is not editable.	SP5
4530205	Time zones on summer time should be indicated with an asterisk (*). According to the description of time zones on the User Information Channel, summer time is indicated with an asterisk (*), however, none of the time zones using summer time have asterisks.	SP5
4532494	The URLScraper channel does not pass the User-Agent information to the server from which it is making the request. In some cases, this header is needed to fulfill the request.	SP5
4624637	After the multi-profile fix, if the user changed the Layout Provider, many sync requests were generated. The amount of these requests causes a delayed response.	SP5
4631722	Internet Explorer caches content when the user sets the browser setting "Check for Newer Versions of stored pages" to "Never." This is because the Login Servlet does not set required Internet Explorer headers.	SP5
4641416	Cell padding around Tab Provider cannot be specified because of hard coded HTML in DesktopServlet.	SP5
4641424	Cell spacing cannot be specified in the main block of channels and providers.	SP5
4641439	Background color cannot be specified for main block of channels.	SP5
4661902	The iPlanet Portal Server 3.0 software does not provide the ability to maximize a provider. A provider can be minimized or restored, but cannot occupy the entire width of the Desktop without the presence of other providers.	SP5
4667201	A user who belongs to a non-default domain is taken back to the default domain's login page after a session timeout.	SP5
4731180	The Web server goes to sleep when the URLScraper is used to get SSL content.	SP5
4741188	Desktop caching is currently not allowed.	SP5
4743921	The time zone setting in the User Information Provider cannot be updated.	SP5
4804607	High level caches are not updated when profile data changes, so changes in Desktop configuration are not synchronized across instances.	SP5

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4804617	A multi-instance portal environment in which request handling is distributed by a load balancer that is not using sticky sessions causes changes in displayed channels to be undone by other instances.	SP5
4460159	Maximized channel with no content should display the message Content not available.	SP4
4481973	Edit Page of Netlet and Bookmark Provider can not be accessed after any one of the fields is deleted.	SP4
4483942	Entries with multiple <code>sn</code> and <code>givenname</code> do not display correctly in the User Info channel.	SP4
4489005	A URL scraped channel does not display JPEG files with a non-relative path.	SP4
4512981	The tab provider displays tabs in only right-to-left alignment. For more information, see “Tabbed Desktop” in this document.	SP4
4513037	The JSP provider cannot localize title or description. For information on the JSP Provider sample properties file, see “Localizing JSP Provider Titles and Descriptions” in this document.	SP4
4549142	HTTPS to HTTP changeover did not happen in Service Pack 3a.	SP4
4387813	Occasionally, the Desktop is displayed only after the entire timeout — the default timeout is 30 seconds.	SP3
4394315	Detaching all channels on the Desktop causes an unrecoverable error that makes the Desktop unusable.	SP3
4396908	Desktop provider does not catch throwable, resulting in a Desktop error page with the message A fatal error has occurred displayed in the channel window.	SP3
4394038	Some attribute strings for Desktop tabs are displayed in English for other locales.	SP3
4397293	Desktop logs expired or invalid sessions as an errors instead of warnings in the debug log files. This can debug files to grow unnecessarily large.	SP3
4401121	<code>URLScrapperProvider</code> does not preserve backward compatibility.	SP3
4401145	Date formatting does not work properly in Japanese locale.	SP3
4403468	Channel titles are always displayed in the language stored in the profile service.	SP3
4412336	Changes to <code>TimeZone</code> are not effective until user logs in again.	SP3
4412806	Relative URL redirects from <code>JSPProvider processEdit</code> fail.	SP3
4426023	SunBlue templates do not work with SP2.	SP3
4448938	Changing to layout Option Four causes wide channels to be removed.	SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4450801	Selecting Open all pages in the Desktop when editing bookmarks causes the javaScript function <code>openURL</code> to call the server twice in the URL.	SP3
4349181	The Channel Wizard works incorrectly when an in-line channel is created if the iSyndicate connector is installed.	SP2
4353071	Weather provider templates should not be installed. The product does not contain a weather provider.	SP3
4365483	Content provider should check for null provider in content provider edit page creation.	SP2
4330685	The URL scraper failed when it tried to fetch a URL that resulted in a redirect.	SP1
4335174	URL rewriting did not work for relative URLs in URL scraper.	SP1
4338083	Removing a channel with thin-thick-thin layout caused null pointer.	SP1
4343673	URL scraper provider did not handle redirects.	SP1
4343674	RSS and URLscraper providers did not support using a proxy.	SP1
Gateway		
4361400	The iPlanet Portal Server gateway POST request forwarding performance inefficient.	SP5
4389707	In some cases, <code>CLOSE_WAIT</code> sockets accumulate and never get closed.	SP5
4476255	If an HTML form action is inside <code>document.write</code> function and is broken into two or more statements, gateway doesn't understand it as a single tag and therefore doesn't rewrite it.	SP5
4485983	gateway prints debug messages to console for short connections because exception messages are printed to standard out and standard err, rather than using the Debug class.	SP5
4498349	The Gateway redirect option does not base its decision on gateway profile. The gateway attempts to fetch the response for a URL request without first checking to see if the gateway scheme is "redirect."	SP5
4503622	When the iPlanet Portal Server http proxy is enabled, and the gateway is used under heavy load with HTML pages containing a large number of images, it starts giving StackOverflow Error and stops responding.	SP5
4504371	Wildcard support for JavaScript variables does not exist. For URLs and variables which may be dynamically generated, it is not possible to define a rule that applies to them all without being able to specify a wildcard for the entry in the Gateway Profile.	SP5
4508190	Rewriter was case sensitive for CSS function.	SP5

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4512581	The rewriter ignores content between nested SPAN tags. Service Pack 3 Hot Patch 1 broke the rewriting functionality of content between the SPAN tags in order for Microsoft Exchange to work through the gateway.	SP5
4512672	URLs are not rewritten inside JavaScript while adding a menu item. If javascript variables like <code>top.location</code> were added to the Rewrite javascript variables in urls section, they do not get rewritten correctly because of the presence of location in the Rewrite Javascript variables function section.	SP5
4513379	If the domain, and path are not explicitly set, they are not prepended to the cookie name when the gateway wraps the header up and sends it to the client. In some cases this causes problems maintaining uniqueness.	SP5
4514053	The gateway blindly rewrites source tags even if they are empty. An empty source tag can cause an error 404 to occur. Once a 404 error has been reported in the frame, it is no longer accessible to JavaScript functions.	SP5
4516049	The gateway incorrectly handles multiple Content-Length headers. The first value is rewritten with the new length after translation and appended to the end of the request. However, the Internet Explorer browser uses the first content-length header it encounters which would be smaller than the translated length, which causes the page sent back to the client to be truncated.	SP5
4516836	Pages redirected through the gateway should have the option not to be cached. When surfing pages through the bookmark provider or by specifying the redirected URL in the location field of the browser, the content can be cached on a local system.	SP5
4526286	Relative URLs with no prepended path information embedded in remote JavaScript are not rewritten correctly on import.	SP5
4528139	The option to disable client-bound Netlet traffic from extending iPlanet Portal Server session is needed.	SP5
4530009	If an HTML page is written in different parts using the <code>document.write</code> function, the rewriter may not understand all the attributes and tags correctly because of the quotation marks.	SP5
4587433	Cookies are not set while using http-proxy, if the domain is not the iPlanet Portal Server's domain.	SP5
4617479	If an applet archive tag has multiple jar files separated by commas, only the first archive tag is rewritten.	SP5
4620125	The iPlanet Portal Server gateway has a problem re-writing URLs when it sees a codebase directive with an applet tag. The gateway does not translate any other <code><a href</code> directive correctly within the HTML file even though the codebase should only be in scope until the closing APPLET tag.	SP5

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4622383	The rewriter should not automatically rewrite SRC tags the iPlanet Portal Server gateway does not understand.	SP5
4623720	The iPlanet Portal Server gateway passes different Content-Length: size in the HTTP header than the actual size. This happens only when the iPlanet Portal Server gateway sends HTTP/1.0 302 Moved Temporarily. The difference is one byte (the actual payload is bigger).	SP5
4624513	In some cases the iPlanet Portal Server gateway hangs under load. The java process does not die, and new connections are accepted, but no response is returned.	SP5
4631945	The applet getCodeBase call fails through the iPlanet Portal Server gateway if BASE HREF is commented out.	SP5
4636629	The iplanet function causes an error when rewriting JavaScript variables.	SP5
4641833	The rewriter has no option for specifying a JavaScript function parameter that is either a URL or JavaScript.	SP5
4645591	The iPlanet Portal Server gateway incorrectly rewrites JavaScript programming language containing the style tag.	SP5
4647942	Rules containing dotted separators cannot be used in the specified iPlanet Portal Server gateway profile section "rewrite javascript variables function."	SP5
4649735	Gateway rewriter cannot understand charset UTF8 only UTF-8.	SP5
4659553	If the URL specifies the protocol in upper case, the rewriter will not rewrite the URL. For example, only URLs starting with http are rewritten, and URLs starting with Http: or HTTP are not rewritten.	SP5
4667660	Using Outlook Web Access and Internet Explorer in combination, causes errors when the inbox is opened through the iPlanet Portal Server gateway.	SP5
4668058	Sometimes under load, the content character set is forced to be converted into other character set than one specified in header of the HTML.	SP5
4681424	Relative URLs are not rewritten correctly if the absolute URL used for the BASE HREF value does not contain any path information.	SP5
4682364	A defect in the logging service causes the iPlanet Portal Server gateway to hangs on DNS lookup.	SP5
4689262	The iPlanet Portal Server gateway encounters an error when the location header is all lower case.	SP5
4691715	The last scraped page's iplanet function will take precedence, and all other URLs in other scraped pages will use its requestPHP variable value to be rewritten.	SP5
4696780	Pages are not displayed correctly through the gateway. BASE tags containing a target attribute are commented out.	SP5

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4704765	Unencoded Korean characters in the request URL are not handled properly when the <code>LANG</code> setting for the iPlanet Portal Server gateway is “Ko.”	SP5
4710385	Requests to single or double level domain are not adhering to the HTTP proxy rules.	SP5
4721347	URL rewriting fails for JavaScript strings that extend across several lines.	SP5
4721367	The iPlanet Portal Server gateway does not correctly rewrite the <code>META</code> tag when putting the URL in quotation marks.	SP5
4722723	The iPlanet Portal Server gateway does not store basic authentication credentials when using <code>httpproxy</code> .	SP5
4731947	Applet Parameters are not rewritten if the code contains a line break.	SP5
4732184	The URLrewriter cannot rewrite cookie paths that contain an underscore (<code>_</code>).	SP5
4746213	When the rewriter needs to add the <code>iplanet</code> function to “Rewrite JavaScript Variable Function” and there is no <code><head></code> tag, the <code>iplanet</code> function is placed in the middle of the HTML code.	SP5
4749854	The <code>iplanet</code> function has the variable <code>requrl</code> , which is not defined. If the <code>iplanet</code> function is called with an already rewritten URL, it produces JavaScript error.	SP5
4749859	The iPlanet Portal Server gateway moves a server into the unavailable list when it is unable to make a single socket connection to that server. The gateway does not retry to make the connection.	SP5
4754230	Cookies are not rewritten correctly for an iPlanet Portal Server gateway that is installed in a top level domain.	SP5
4775165	The server certificate cannot be renewed on the gateway.	SP5
4777957	The <code>iplanet</code> function does not check to see if variables are null. This affects the rewriting of variables in imported JavaScript in the Exchange interface.	SP5
Still open		
4777962	The gateway automatically forwards requests for nonexistent domains, creating a unnecessary traffic and putting undue load on the Gateway.	SP5
4777964	If the gateway socket timeout is not set for the <code>erproxy</code> , denial of service attacks can occur.	SP5
4778676	The gateway translates special characters when rewriting XML, causing incorrect XML syntax.	SP5
4780863	The gateway strips off XML declaration tag.	SP5
4782435	When a style attribute is followed by a boolean attribute and a <code>DOMstring</code> attribute, the rewriter throws a string out of bounds exception.	SP5

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4782512	The gateway does not handle implied tags. The rewriter inserts <HEAD></HEAD> tag in the wrong place if a pair does not already exist.	SP5
4788050	The rewriter does not ignore comments that occur prior to opening XSL tag, which breaks the message multi-view functionality in Microsoft Exchange.	SP5
4801591	img src tags with absolute http URLs are rewritten.	SP5
4801644	The gateway does not distinguish between base href internal and external URLs.	SP5
4343352	Outlook Web Access 2000 does not work out-of-the-box. See “Using Outlook Web Access 2000” in this document.	SP4
4413804	The gateway cannot handle cookies differing only in path. For more information, see “Desktop and Provider Changes” in this document.	SP4
4415017	JavaScript window.location.path value is not rewritten correctly.	SP4
4418714	The gateway component does not rewrite JavaScript variables that contain escaped double quotes.	SP4
4468740	Internal applications cannot be accessed because cookie domain rewriting does not use gateway domain or cookie domains list.	SP4
4470387	Internal applications that use URLs in which the file path starts with the word login cannot be accessed when using personal digital certificates (PDCs). iPlanet Portal Server redirects these URLs to the Desktop.	SP4
4474989	The gateway does not rewrite cookies correctly when used with the HTTP Proxy.	SP4
4481171	Re-submitted HTTP posts to foreign hosts by the gateway contain no data.	SP4
4483894	The gateway component does not handle pages correctly when lines end with line feed only.	SP4
4488953	The HTTP proxy does not work when the server is using SSL.	SP4
4492127	iPlanet Portal Server 3.0, Service Pack 3 does not work with iPlanet Messaging Server 5.1.	SP4
4493116	The gateway component should not add default port number to re-written links.	SP4
4496453	The gateway rewrites src= tags when it is an SSL site and the site is not in the rewrite domain/subdomain list.	SP4
4501739	The gateway does not display a URL correctly unless / follows the hostname.	SP4
4502199	If the socket connection cannot be created, the gateway sends a 502 HTTP error code to the client indicating that the server is unavailable. For information about the addition of the isp.gateway.sockretries parameter, see “Setting the Number of Socket Connection Retries” in this document.	SP4
4342774	HTTP basic auth caching (SSO) fails when using server HTTP proxy.	SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4344066	Referer headers must be forwarded so servers can track the user's URL.	SP3
4350023	The <code>ipshttpd</code> script does not set the maximum number of file descriptors to a high enough value for the HTTP proxy process, causing the <code>ipshttpd</code> process to run out of file descriptors. When that happens, <code>ipshttpd</code> stops responding.	SP3
4352555	The JavaScript rewriter mishandles escaped double quote.	SP3
4354655	Users cannot authenticate with Internet Explorer, if <code>hostname</code> contains capital letters.	SP3
4358856	If the server and the gateway are installed on two different machines, the <code>iwtGateway.properties</code> file is not installed in <i>basedir</i> /SUNWips/locale directory of the server machine. The gateway-related strings are displayed in the default language, English, for foreign languages on the server machine.	SP3
4375934	The gateway ceases to resolve DNS hostnames intermittently.	SP3
4380531	Rewriter misplaces <code>iplanet()</code> function.	SP3
4381501	The URL rewriter incorrectly rewrites relative URLs by using the document's URL instead of its base URL (indicated by the BASE tag).	SP3
4389707	In some cases the gateway or HTTP proxy would not respond due to <code>CLOSE_WAIT</code> sockets accumulating, and not getting closed.	SP3
4396142	If an applet is between <code><OBJECT></code> and <code></OBJECT></code> , the URL rewriter does not rewrite the URL.	SP3
4396151	The URL rewriter does not rewrite the applet parameter value if there is space between an HTML tag's parameter name and value.	SP3
4407007	URL Scraper and RSS channel providers fail when load balancing is active.	SP3
4416215	URLscraper does not handle the character set from Content-Type.	SP3
4430846	Internet Explorer 5.5 cannot display Webmail application when used with the gateway.	SP3
4388783	The gateway component should use JSS for talking to the platform server in HTTPS mode.	SP3
4342320	Gateway boot process hangs if the server is not started first.	SP2
4330036	Rewriter did not work if a URL had no leading <code>http://</code> and no port number specified.	SP1
4335199	Rewriter for applet tags could rewrite only limited number of URLs in a parameter.	SP1
4338888	Membership Module allowed a blank password to authenticate.	SP1
4340633	Gateway did not re-authenticate when its session died.	SP1

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
Install		
4655732	Upgrade script does not give executable permissions to the web server stop script.	SP5
*not fixed		
4661638	The ipinstall script displays false error messages about missing patches.	SP5
4729301	When using iPlanet Portal Server with iPlanet Web Server 4.1 Service Pack 11, an improperly formed request using chunked transfer encoding is received by the web server it can cause a buffer overflow.	SP5
4521473	BaseDir was restricted to less than 21 characters.	SP4
4226991	Confirmation message when user is removing components.	SP3
4240879	Wrong install script name in error message.	SP3
4335044	Install needs to check disk space for installing Java packages. If Java packages don't get installed, the install script fails.	SP3
4341308	Stop script stops all slapd processes and all external LDAP server processes.	SP3
4350541	The installation script requires a fully qualified domain name (FQDN) with three parts (separated by two dots). It does not accept an FQDN with only one dot.	SP3
4437706	Installing gateway with profile server, using non-default port for SSL, sets port to 443.	SP3
4380586	Gateway does not start when server and gateway use SSL.	SP3
4418223	Mismatched version string.	SP3
4423962	Install script asks for patches not in the image.	SP3
4424472	pkginfo files should be updated after installation.	SP3
4429042	Service Pack 3 image should not include jdk1.2.2_05 patches.	SP3
4448611	Installing profile server with a web proxy causes ipsserver to fail.	SP3
ipsadmin		
4460785	The command line utility ipsadmin returns invalid XML if the attributes value contains special characters. If the administrator tries to use this XML file it gives SAXParserException.	SP5
4506829	Unable to change user attribute values to null using ipsadmin.	SP5
4518297	After installing iPlanet Portal Server Service Pack 4, unnecessary messages were displayed on console when using ipsadmin for any profile changes.	SP5
4363059	Importing privileges after accessing the Policy page requires relogging to view.	SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4350031	<code>ipsadmin -import</code> converts new attributes in previously existing components to lower case and reports all attributes of new components as already existing. This bug is fixed in the iPlanet Directory Server 4.12 release.	SP2
4336880	<code>ipsadmin</code> did not work if server was running on SSL mode.	SP1
4337917	<code>ipsadmin</code> did not encrypt “protected” attributes.	SP1
ipsserver		
4389604	Stop script does not always stop the Directory Server.	SP3
4396039	Portal Server hangs if restarted under load.	SP3
4344376	<code>ipsserver stop</code> script kills all HTTPD processes running on the server. In doing so, it may also kill some external iPlanet Web Servers running on the server. The <code>ipsserver stop</code> command should stop only relevant processes.	SP2
Japanese Language Version		
4402583	Incorrect country code for Japan in the <code>iwtUser.properties</code> file.	SP3
4336096	On Japanese localization, NetFile Java did not work on Solaris and Windows NT.	SP1
Logging		
4526036	With the release of the iPlanet Portal Server Service Pack 3 software, log records written using the Logging API were logging userID as authentication. This makes logging useless because there is no way to associate any entry with any user.	SP5
4660535	The LogManager class has a memory leak.	SP5
4343010	When logging is disabled, the log client still sends the log message.	SP3
4401461	Oracle <code>jdbc</code> driver does not re-initialize when the database cycles off and on.	SP3
4343009	When logging was disabled, client API threw exceptions.	SP1
4352291	Ability to turn gateway logging on or off.	SP1
NetMail		
4616323	NetMail sessions are not released when the user logs only out of the iPlanet Portal Server Desktop.	SP5
4633290	Installing NetMail locally on a Macintosh client will break on Macintosh clients running Internet Explorer.	SP5
4378936	Double-byte folder names are not supported in NetMail Lite.	SP3
4378943	Double-byte nickname entries in NetMail Lite address book are not supported.	SP3
4340200	Session timed out when running NetMail without the gateway.	SP1

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
NetFile		
4201106	In the NetFile application, the Return key should choose OK to avoid having to move the hand from the keyboard to the mouse.	SP5
4243052	An incorrect error is reported when creating an existing directory.	SP5
4381090	Users are able to add nonexistent shares. If a non existing share is added and you try to open the share, an error occurs and permission denied. If the share is not present, the user should not be allowed to add it.	SP5
4381171	Multiple files are mailed as copies of the same message with one attachment at a time. They should be mailed as multiple attachments.	SP5
4409910	Japanese files and folder names are not displayed correctly on NetFile and NetFile Lite, which makes the navigation and transfer of these directories or files impossible.	SP5
4414646	When mailing a file in NetFile using the Mail button, the From: address values are sourced and filled in incorrectly.	SP5
4451556	NetFile Truncates directory listings for subfolders if the number of listings is more than approximately 30.	SP5
4452946	File listing does not work for Windows NT FTP server host types. The file listing is not viewable although the file can be uploaded correctly.	SP5
4467076	When deleting a file with NetFile FTP, a messaging saying that the file has been Deleted is displayed, but the file is not actually deleted. This problem occurs if the user deleting the file is different from the file owner.	SP5
4494110	When saving a file from the NetFile applet on the Macintosh using Internet Explorer 5 or MRJ, the name <code>NetFileServlet</code> is used as the filename in the dialog box. The actual filename gets ignored.	SP5
4494943	When more than one user is specified in the To field, using a comma as a separator, mail is sent to only one user.	SP5
4496636	Mail sent from NetFile containing Japanese characters gets corrupted.	SP5
4500257	When downloading any files with Internet Explorer using NetFile, the file extension becomes <code>.NetFile</code> .	SP5
4503001	When a large number of files is selected and the Mail button is clicked, the Mail dialog opens and is displayed huge horizontally.	SP5
4748543	Internationalization: A warning message is displayed when uploading multi-byte files in Netfile.	SP5
4381166	Mail form field values in NetFile are not checked uniformly.	SP4

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4381168	File names are not displayed when mailing multiple files from the NetFile Java application. File names are now displayed as a comma separated list.	SP4
4417700	Sending a blank email reply with the NetFile application causes the browser to spin indefinitely.	SP4
4451563	The window for displaying files on right side is too small. The file name window has been changed to allow 11 additional characters.	SP4
4486094	NetFile FTP connection method does not work properly with server components using multiple network interfaces. The <code>PORT</code> command uses the wrong IP address when sending data back to the client.	SP4
4350500	The Print and Save functions don't work in Netscape Navigator for files sent by NetFile.	SP4
4335215	The NetFile Lite application incorrectly displays compressed file names when using Windows NT hosts.	SP3
4349633	NetFile Lite behavior, under certain circumstances, can compromise password security.	SP3
4352059	The profile <code>isAllowed</code> method does not do wildcard matching.	SP3
4357835	NetFile Lite can display only one share for Windows systems.	SP3
4357841	NetFile Lite does not save changes to host information upon exiting and saving the session.	SP3
4357844	NetFile has problems displaying hidden shares that have been defined by the administrator.	SP3
4357847	NetFile shares that have been defined through <code>ipsadmin</code> can be added again through the NetFile application resulting in duplicate shares.	SP3
4357856	Using the host info menu in NetFile to edit host information, such as user name and password, removes the shares associated with that host.	SP3
4361900	NetFile assumes that a system is valid without verifying that the system exists. If the system to which NetFile tries to connect does not exist, the NetFile application eventually times out.	SP3
4365921	NetFile applet occasionally does not pass the sessionid to the servlet during a servlet call, resulting in a session exception that causes the log files to get unnecessarily large.	SP3
4368446	If the server's <code>LANG</code> setting specifies Japanese or Chinese locale, NetFile download functions for image, HTML, and executable files do not work.	SP3
4371647	If the server's <code>LANG</code> setting specifies Japanese or Chinese locale, NetFile upload functions for image, HTML, and executable files do not work.	SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4431453	NetFile mail functionality can overwrite iPortal Web Server configuration files.	SP3
4340074	Session timed out when running NetFile without the gateway.	SP1
4342428	NetMail was unable to receive mail with attached text file sent from NetFile.	SP1
Netlet		
4371977	If a dynamic netlet rule with target listening on different ports is specified, it does not work properly and the target is set only for the first port.	SP5
4421884	Netlet does not work on a Macintosh machine because it cannot resolve localhost. It needs the value 127.0.0.1 instead.	SP5
4525103	The ability to increase the session time out when the user is working with the Netlet should be configurable.	SP5
4700642	The Netlet does not parse spaces in PAC files.	SP5
4717742	The Netlet cannot find a PAC file when it is specified using a file URL. For example: file://.	SP5
4727195	Large PAC files are truncated when content length is not explicitly set.	SP5
4756228	With Internet Explorer, the Netlet does not connect to the server after the user logs out and then logs in again.	SP5
4799502	Current idle time is constantly reset by the Netlet when the MaxCache time value has been exceeded.	SP5
4199840	Netlet does not support Netscape with PAC files. For more information, see “Installed Software Modules, Customizations, and Third-Party Products” in Chapter 2 of the <i>iPlanet Portal Server Installation Guide</i> .	SP4
4461255	Dynamic rules should be supported when using FTP through a Netlet connection.	SP4
4461264	Netlet does not support .ins files for Internet Explorer Configuration. For more information, see “ Configuring Internet Explorer INS Files ” in this document.	SP4
4492648	Netlet activity is not monitored and causes a session idle time out even when the Netlet is in use.	SP4
4500165	The port number is not stripped from the host name when evaluating a PAC file.	SP4
4526425	The autoproxy does not work when the autoconfig URL does not point directly to a file or redirect to a file. For instance, if http://domain_name:1001 is used an exception is thrown.	SP4
4527455	PAC files that contain evaluation entries based on the client IP address either fail or are evaluated incorrectly.	SP4
4332715	Applet download rule section is broken.	SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4377505	Netlet applet is hardcoded for a maximum of ten connections per rule.	SP3
4410474	The global encryption version of Netlet Applet incorrectly shipped with the domestic version of iPlanet Portal Server 3.0, Service Pack 3.	SP3
Platform		
4763552	The request XML document for any service gets corrupted under a heavy load. The <code>PLLRequestServlet</code> does not read the XML document correctly.	SP5
4804302	Sizes of PLL Session threadpool are not configurable, which causes the server to hang in some cases.	SP5
4394184	A certificate error occurs when using an HTTPS connection when the VIP name does not match the server name.	SP3
Profile		
4518877	After installing the iPlanet Portal Server Service Pack 3 Hot Patch 1 software, a <code>profileException</code> is thrown saying that attribute <code>iwtGateway-responsedelay</code> is not found.	SP5
4532733	After multi-server fix, if a suborole has modified content, and the administrator has changed the upper domain or role, the change is visible only on the server on which the change was made. The change is not visible on the other platform servers.	SP5
4619325	If the iPlanet Portal Server software is configured to run SSL in open portal mode on port 80, users are not able to see the Desktop on Internet Explorer. Netscape works fine.	SP5
4776292	A single write operation produces a large number of LDAP reads.	SP5
4780767	The Profile service issues excessive requests for the domain list.	SP5
4804521	Unnecessary LDAP reads occur if a request has no iPlanet Portal Server cookie.	SP5
4804531	A single Desktop reload causes multiple sessionservice requests.	SP5
4804541	Every time a user logs in to the portal, the profile server receives an LDAP request.	SP5
4805519	Every time a user with a profile that is not already cached logs in, two LDAP requests are issued for their profile in immediate succession. Since user profiles are cached, only one request should be necessary.	SP5
4424086	Profile server should be able to reconnect to the LDAP server.	SP4
4352059	The profile <code>isAllowed</code> method does not do wildcard matching.	SP3
4399031	<code>ipsadmin</code> has wrong content type for <code>UpdateProfileCache</code> request.	SP3
4412089	Profile server enters busy wait loop.	SP3
4340128	Profile API returns valid profile object for non existing profiles.	SP2

Table 13 Fixed Bug List

Bug ID	Bug Description	Fixed In
4339191	Domain search did not search for users mapped from external LDAP. The search limit for external LDAP users is 400 users only.	SP1
4341571	External LDAP attribute mappings did not work with binary type attributes.	SP1
Documentation		
4530195	The steps to add a gateway are documented incorrectly in the <i>iPlanet Portal Server 3.0 Administration Guide</i> . For correct instructions, see “ Adding a Gateway After Installation ” in this document.	SP4
4332242	Document required disk space for <code>/var;</code> <code>/etc;</code> <code>/opt;</code> and installation directory.	SP3
4373115	Portal Server and gateway components on a single computer must use the same <code>install</code> directory.	SP3
4402209	Correct instructions for adding <code>iwtTabProvider</code> in selected channels.	SP2
4343016	Incorrect URL for documentation.	SP1

Documentation Updates

This section provides information that supplements the *iPlanet Portal Server Administration Guide*. Topics include:

- Non-Portal Server Cookie Management
- Certificate Management for the Gateway
- Adding a Gateway After Installation

Documentation for iPlanet Portal Server is at this Web site:

<http://docs.iplanet.com/docs/manuals/portal.html>

Gateway Profile Attributes

Table 14 is a two column table that lists the gateway profile attributes. The first column contains the attribute name, and the second column provides a brief description of each attribute.

For more detailed information on configuring the gateway, see the iPlanet Portal Server Administrator’s Guide 3.0 at:

<http://docs.sun.com/>

For detailed information specifically related to rewriter configuration, see the *Sun™ONE Portal Server 3.0 Rewriter Configuration and Management Guide* at:

<http://www.sun.com/solutions/blueprints/>

Table 14 Gateway Profile Attributes

Attribute	Attribute Description
Allow 40 Bit Browser Connections	Allow connections to the gateway from browsers that only support weak (40 bit) encryption.
Rewrite Form Input Tags List	<p>List of FORM tag attributes that get rewritten. The FORM tag attribute ACTION gets rewritten out of the box. Other attributes that might need to be added are INPUT and SELECT.</p> <p>Syntax:</p> <p><i>object_of_url_with_form form_name input_or_option_name [url_pattern]</i></p>
Rewrite All URLs Enabled	<p>If this attribute is set to true, the Gateway will rewrite any URL without checking the URLs subdomains and domains against entries in DNS Domains and Subdomains list.</p> <p>If false, the DNS Domains and Subdomains list applies.</p>
PDC Enabled Gateway List	List of gateways that require authentication by Personal Digital Certificate.
IP Address Validation Enabled	No longer used
HTTP Basic Authentication Enabled	Web sites may be protected with HTTP Basic Authentication, requiring visitors to enter a username and password before viewing the site (the HTTP response code is 401 and WWW-authenticate: BASIC). Sun ONE Portal Server can save the username and password so that users need not re-enter their credentials when they revisit BASIC-protected web sites. These credentials are stored in the user profile on the Sun ONE Directory Server.
Forward Cookie URL List	<p>Sun ONE Portal Server utilizes a cookie to track user sessions. This cookie is forwarded to the server when the gateway makes HTTP requests to the server (for example, when the desktop servlet is called to generate the user's desktop page). Applications on the server use the cookie to validate and identify the user.</p> <p>The Portal Server's cookie is not forwarded to HTTP requests made to machines other than the server, unless URLs on those machines are specified in the Forward Cookie URL Lists. Adding URLs to this list therefore enables servlets and CGIs to receive the Portal Server's cookie and use the APIs to identify the user.</p>

Table 14 Gateway Profile Attributes

Attribute	Attribute Description
Non Portal Server Cookie Management	<p>Specifies whether cookies get rewritten and restored.</p> <p>If false, cookies are forwarded, but not rewritten or restored</p> <p>If true cookies are rewritten</p>
Use Intranet Web Proxy	<p>Specifies whether a Web Proxy is to be used. If a web proxy is specified in the DNS Domains and Subdomains list, the gateway checks this attribute.</p> <p>This checkbox can be used in conjunction with:</p> <ul style="list-style-type: none"> • Don't Use Web Proxy Enabled • Use Web Proxy Enabled <p>If this box is checked, the Don't Use Web Proxy Enabled list can be used to add URLs that do not get proxied, but are contacted directly.</p> <p>If the box is not checked, the Use Web Proxy Enabled list can be used to add URLs that do get proxied.</p>
Use Web Proxy Enabled	<p>List of URLs that get proxied when the Use Intranet Web Proxy attribute is set to false.</p> <p>Syntax:</p> <p>A URL</p> <p>* is a wild card that matches everything</p>
Don't Use Web Proxy Enabled	<p>List of URLs that do not get proxied when the Use Intranet Web Proxy attribute is set to true.</p> <p>Syntax:</p> <p>A URL</p> <p>* is a wild card that matches everything</p>
Rewrite HTML Attributes	<p>List of HTML attributes that contain URLs to be rewritten by the gateway. If an attribute in this list contains a URL, that URL will be rewritten.</p>

Table 14 Gateway Profile Attributes

Attribute	Attribute Description
DNS Domains and Subdomains	<p data-bbox="458 270 1165 326">These entries tell the gateway what web proxy (if any) to use when contacting specific subdomains in specific domains.</p> <p data-bbox="458 345 1222 460">If Use Intranet Web Proxy is enabled, and the requested URL is not listed in the Do Not Use Webproxy URLs list, the gateway connects to the destination host through the specified proxy. The proxy, if specified, is looked up from the Proxies for Domains and Subdomains list.</p> <p data-bbox="458 479 1165 562">If a web proxy is not indicated for the target URL through the DNS Domains and Subdomains list as described above, the gateway will connect to the destination host directly.</p> <p data-bbox="458 581 1172 637">If a web proxy is indicated, the gateway will check the attribute Use Intranet Web Proxy.</p> <p data-bbox="458 656 536 683">Syntax:</p> <p data-bbox="458 703 1093 730"><i>domain_name web_proxy1:port1 subdomain1 web_proxy2:port2 </i></p>
Rewrite Text data of XML document	<p data-bbox="458 749 1222 864">Rewrites PCDATA. Add the tag name to the Rewrite Text data of XML document section. If the PCDATA is dependent on the tag attribute values, both the tag name and the attribute definition need to be added to the Rewrite Text Data of XML Document profile section.</p> <p data-bbox="458 883 1222 939">Pre-populated with the entries required for Outlook Web Access 2000 to work through the gateway.</p> <p data-bbox="458 958 536 986">Syntax:</p> <p data-bbox="458 1005 548 1032"><i>tagName</i></p> <p data-bbox="458 1052 743 1079"><i>tagName, URLattribute=href</i></p>
Rewrite Attribute value of XML document	<p data-bbox="458 1098 1222 1154">Used to rewrite XML values that contain URLs. Add a rule that contains the attribute name.</p> <p data-bbox="458 1173 1222 1229">Pre-populated with the entries required for Outlook Web Access 2000 to work through the gateway.</p> <p data-bbox="458 1248 536 1275">Syntax:</p> <p data-bbox="458 1295 601 1322"><i>attributeName</i></p> <p data-bbox="458 1341 1222 1425">Note: To differentiate specific tag names containing the same attribute names from having their values rewritten, specify a rule with the syntax <i>attrName, tagName</i></p>

Table 14 Gateway Profile Attributes

Attribute	Attribute Description
Rewrite HTML Attributes Containing JavaScript	<p>Used for event handlers (HTML attributes that contain JavaScript whose values will attempt to be translated as URLs).</p> <p>Syntax:</p> <p><i>eventHandlerName</i></p>
Rewrite JavaScript Function Parameters	<p>List of JavaScript function parameters to be rewritten. Used to rewrite document object methods. If the URL is a raw URL, then the function name can be added to the Rewrite JavaScript Function Parameters section of the gateway profile.</p> <p>If the content is passed through the gateway that contains a call to a method, where the first parameter is not a raw URL, then the method would have to be moved from the default section of the gateway profile to the Rewrite JavaScript Function Parameters Function section.</p> <p>Syntax:</p> <p><i>java_script_function_name</i>: [y], [y], ...</p>
Rewrite JavaScript Variables In URLs	<p>List of JavaScript variables. The gateway rewrites the value of the URL that is assigned to the JavaScript variable. Used to rewrite document object properties.</p>
Rewrite JavaScript System Variables Function	<p>Used to rewrite built-in JavaScript variables for which a relative URL is required, rather than translating its value into an absolute URL. <i>location.pathname</i> for instance should only specify the path portion of a URL.</p> <p>Entries in this section of the gateway profile will likely be sparse, but this section can be useful if the content defines its own object rather than using the window object.</p> <p>Syntax:</p> <p><i>variable_url_name</i></p>
Rewrite JavaScript Variables Function	<p>Used to rewrite JavaScript variables. If a JavaScript variable is used instead of a raw URL, the Rewrite JavaScript Variables Function inserts a function called <i>iplanet</i> within the SCRIPT tag and changes the variable name on the right side of the variable assignment to <i>iplanet(variable_name)</i>.</p> <p>Syntax:</p> <p><i>document_object_name</i></p>

Table 14 Gateway Profile Attributes

Attribute	Attribute Description
Rewrite JavaScript Function Parameters Function	<p>Used to rewrite browser object methods that contain URLs. If the content is passed through the gateway that contains a call to a method, where the first parameter is not a raw URL, then the method would have to be moved from the default section of the gateway profile to the Rewrite JavaScript Function Parameters Function section.</p> <p>An iplanet function is defined and the variable, or parameter in this case, is then wrapped within an iplanet function call.</p> <p>Syntax:</p> <pre>java_script_function_name: [y], [y], ...</pre>
Rewrite JavaScript Function Parameters In HTML	<p>The gateway will rewrite the HTML in the parameters of the JavaScript function if there is a match.</p> <p>Syntax:</p> <pre>java_script_function_name:[y],[y],...</pre>
Rewrite JavaScript Function Parameters In JavaScript	<p>Used to rewrite URLs in nested JavaScript. Lets the rewriter know that the first parameter of the function call contains JavaScript content. So, the rule must be added to the Rewrite JavaScript Function Parameters in JavaScript section of the gateway profile.</p> <p>Used in conjunction with the Rewrite JavaScript Function Parameters section. The rule must be also be added to the Rewrite JavaScript Function Parameters section.</p>
Rewrite JavaScript Variables In HTML	<p>Used to rewrite dynamically created HTML blocks. If an attribute is created dynamically by the client rather than passing through the gateway, which would normally translate the attribute value (the JavaScript variable that contains HTML to be rewritten requires a rule in the Rewrite JavaScript Variables in HTML section).</p>
Rewrite JavaScript Variables In JavaScript	<p>Used when rewriting JavaScript content for statements whose right side contains variable initializations that could have a right side that is a URL string literal. For the URL to be rewritten correctly, a rule address needs to be added to the Rewrite JavaScript Variables in URLs section of the gateway profile,</p> <p>Syntax:</p> <pre>var address = 'http://www.domain_name.com'</pre>

Table 14 Gateway Profile Attributes

Attribute	Attribute Description
Rewrite Applet/Object Parameter Values List	<p>Used to rewrite Applet and Object attributes that contain URLs. The attributes ARCHIVE and CODEBASE are rewritten out-of-the-box.</p> <p>General syntax must include:</p> <ul style="list-style-type: none"> • Page or object identifier • Class name, including extension • Parameter name <p>Syntax:</p> <pre>object_of_applet/object_url applet_class/object_classid applet/object_parameter_name [url_pattern]</pre>
Advanced Attributes	
Gateway Timeout (milliseconds)	Specifies the time interval in milliseconds after which the gateway times out its connection with the browser.
Rewrite JavaScript Function Parameters In Fractured HTML	<p>This section is suitable for search, rewrite, and replace applications where JavaScript language dynamically creates HTML through multiple <code>document.write</code> function calls.</p> <p>The rule is in the form of a URL pattern.</p> <p>For more information see the section “Advanced Rewriter Concepts”</p>
ReverseProxy Maximum Socket Connections	No longer used
MIME Type Translator Class	Specifies the MIME type. This section extends the rewriter functionality to other MIME types.
Maximum Thread Pool Size	Specifies the maximum number of threads that can be pre-created in the gateway thread pool.
Rewrite JavaScript Function Parameters in JavaScript or a URL	<p>Used when JavaScript functions do not differentiate the context of what can be passed to the function as a parameter. This section allows for some ambiguity in rewriting JavaScript function parameters. Specifically, when rewriting JavaScript function parameters that are themselves either JavaScript or a URL.</p> <p>Syntax:</p> <pre>java_script_function_name: [Y], [Y], ...</pre> <p>For more information see the section, “Advanced Rewriter Concepts”</p>

Table 14 Gateway Profile Attributes

Attribute	Attribute Description
Extend Portal Session for Clientbound Netlet Traffic	If this is disabled, only client activity on netlet connections extend the portal session (stop it from timing out). This is to avoid server side applications that send regular hello packets from keeping the session active when the user has abandoned it. However, some administrators may wish server side data to extend the session so that they can access system management or monitoring applications for which user interaction is relatively minor.
Gateway Port	The port number on which all gateway instances registered against this profile server listen.
Gateway Protocol	The protocol (HTTP or HTTPS) that all gateway instances registered against this profile server use.
Non Authenticated URL Paths	Specifies that some URLs do not need any authentication. These are normally directories and folders that contain images.
Trust Server SSL Certificate List	List of hostnames with SSL certificates that are trusted, even if the certificate can not be verified.
HTTP Proxy Enabled	If the http proxy is enabled, the gateway will send HTTP requests to the HTTP proxy instead of directly to the destination host. The HTTP proxy will then send the request to destination server.
HTTP Proxy Port	The port number on which the HTTP Proxy (if enabled) listens
Netlet Proxy Enabled	Enable proxying by the platform server of netlet traffic from the gateway to the target system. This avoids the need for internal systems accessed by the netlet to be directly reachable from the gateway.
Netlet Proxy Port	The port number on which the Netlet Proxy (if enabled) listens.
Logging Enabled	Enable logging of connections made to the Gateway on the platform server via the logging service.

Non-Portal Server Cookie Management

The iPlanet Portal Server *Administration Guide 3.0* currently states the following:

Many web sites use cookies to track and manage user sessions. When the gateway proxies requests to web sites that set cookies in the HTTP header, the gateway will either discard or pass-through those cookies in the following manner:

- discard all cookies if this attribute is set 'false'
- pass-through all cookies to the user's browser and back to the appropriate web site(s) when the user makes subsequent visits to the web site(s) if this attribute is set 'true'

The actual behavior of the non-portal server cookie management feature is to allow or prevent cookies from being rewritten and restored. Cookies set by the application server are not discarded when the option is set to false.

The non-portal cookie management feature handles cookies in the following manner:

- Forward, but not rewrite or restore the cookie if this attribute is set to “false”
- Rewrite the cookie using the Gateway’s domain and forward the cookie if this attribute is set to “true”

This means that if the cookie is set from a different domain than that of the Gateway, and the non-portal server cookie management attribute is set to true, the Gateway will rewrite the cookie’s domain and the browser will accept it. When the cookie is returned to the application, the Gateway will restore the cookie’s original domain.

By setting this attribute to false, the Gateway does not rewrite the cookie. If the cookie is set from a different domain, the browser will not recognize it and will, therefore, reject the cookie. However, if the cookie is sent from the same domain as that of the Gateway, the browser will recognize the cookie as a valid cookie and will store it, even if the non-portal server cookie management attribute is set to false.

NOTE	If this feature is enabled and later disabled, a cookie that has been previously set will not be restored to its correct domain when it is sent back to the application server.
-------------	---

Certificate Management for the Gateway

SSL certificate management changes have changed information for SSL certificates for the gateway component presented in Chapter 11 of the *iPlanet Portal Server 3.0 Administration Guide* and Appendix A of the original *iPlanet Portal Server 3.0 Installation Guide*.

The following information replaces the existing documentation on SSL certificates for the gateway.

NOTE	Documentation about certificates for the iPlanet Portal Server server component still applies.
-------------	--

Understanding SSL Certificates

The `certadmin` script in `installation_directory/SUNWips/bin/` wraps around the `ipscertutil` command for convenience and consistency with previous certificate administration. The `certadmin` script should satisfy the conventional needs of certificate administration. For additional functions, use the `ipscertutil` command directly. For example, use `ipscertutil` to delete a certificate from the certificate database. The command `ipscertutil -H` lists use.

Certificate-related files are located in `/etc/opt/SUNWips/cert`. Three of the five certificate files, `cert7.db`, `key3.db`, and `secmod.db`, are binary files containing data for certificates, keys, and cryptographic modules. These files can be manipulated implicitly by using the `certadmin` script.

These binary files have the same formats as the database files used by iPlanet Web Server. They are located in `installation_directory/netcape/server4/alias`. If necessary, they can be shared between the iPlanet Portal Server server and gateway components or the HTTP proxy.

The other two certificate files are hidden text files: `.jsspass` and `.nickname`. The `.nickname` file stores the names of the token and certificate that gateway currently uses, in the form of `token_name:certificate_name`. If using the default token (the token on the default internal software encryption module), omit the token name. In most cases, only the certificate name is stored in `.nickname` file.

The `.jsspass` file contains the password for the encryption module that iPlanet Portal Server gateway currently uses. The default module is the internal software module.

During the installation of the iPlanet Portal Server gateway component, a self-signed SSL certificate is created and installed. If necessary, use the `certadmin` script to do additional certificate administration.

Generating a Self-Signed SSL Certificate for the Gateway Component

Administrators use the `certamin` script to generate a self-signed certificate for the gateway. To do this, complete the following steps:

1. As root, run the `certadmin` script. The following example assumes that `/opt` is the installation directory.

```
# /opt/SUNWips/bin/certadmin
```

2. Select 1 from the Certificate Administration menu to generate a self-signed certificate.
3. When Certificate Administration script asks if you want to keep the existing database files, select whether to keep the existing certificate database files.

TIP If you answer `y`, the script prompts you to enter organization-specific information, token name and certificate name.

The token name (default being empty) and certificate name is stored in the `.nickname` file under `/etc/opt/SUNWips/cert`.

If you answer `n`, the original certificate directory is backed up, and the scripts also asks for a passphrase. A passphrase needs to be set to create a new set of certificate, key and encryption module database files. The passphrase is stored in the `.jsspass` file under `/etc/opt/SUNWips/cert`.

4. When a self-signed certificate is generated and the prompt returns, use these commands to restart the gateway component for the certificate to take effect:

```
# /opt/SUNWips/bin/ipsgateway stop
# /opt/SUNWips/bin/ipsgateway start
```

Multiple certificates can be stored in the database files. The one that the gateway component uses is identified by the `.nickname` file. You can edit this file to switch to a different existing certificate.

Obtaining and Installing an SSL Certificate from a Certificate Authority

During installation of the gateway component of the Portal Server product, a self-signed certificate is created and installed. At any point after installation, you can install SSL certificates signed either by vendors who provide official certificate authority (CA) services or by your corporate CA.

Three main steps are involved in this task.

- Generating a Certificate Signing Request (CSR)
- Using the CSR to Order a Certificate from a CA
- Installing the Certificate from the CA

Generating a Certificate Signing Request (CSR)

To generate a certificate signing request, complete the following steps:

1. As root, run the `certadmin` script. The following example assumes that `/opt` is the installation directory.

```
# /opt/SUNWips/bin/certadmin
```

2. Select 2 from the Certificate Administration menu to generate a certificate signing request (CSR).
3. Provide the organization-specific information that the script asks for.

NOTE The webmaster's email and phone number are required.

A CSR is generated and stored in the file `/tmp/csr.hostname` and is printed to the screen so that you can copy and paste it.

Using the CSR to Order a Certificate from a CA

To use the certificate signing request to order a certificate from a certificate authority, complete the following steps:

1. Go to the Certificate Authority's Web site and order your certificate.
2. Provide the CSR from the last step, as requested by the CA.
3. Provide other information, if requested by the CA.
4. After you receive your certificate from the CA, save it in a file.

The following example omits the actual certificate data.

```
-----BEGIN CERTIFICATE-----
```

The certificate itself

```
-----END CERTIFICATE-----
```

NOTE Include both the `BEGIN CERTIFICATE` line and the `END CERTIFICATE` line with the certificate in the file.

Installing the Certificate from the CA

To install the certificate from the CA in your local database files in `/etc/opt/SUNWips/cert`, complete the following steps:

1. As root, run the `certadmin` script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

2. Select option 4 from the Certificate Administration menu to install your certificate from the CA.

The script asks you to enter certificate file name, certificate name and token name.

```
What is the name (including path) of file that contains the certificate?  
Please enter the token name you used when creating CSR for this certificate []
```

3. When the script asks you to enter certificate file name, certificate name and token name, provide this information.

TIP Once the certificate is installed in `/etc/opt/SUNWips/cert`, the screen prompt returns.

4. Use these commands to restart the gateway component so that the certificate takes effect:

```
# /opt/SUNWips/bin/ipsgateway stop  
# /opt/SUNWips/bin/ipsgateway start
```

Adding a Root CA Certificate

When the gateway is an SSL client, importing a root CA certification into the gateway's certificate database enables the gateway component to communicate with an Internet or an intranet HTTPS site. If the root certificate is not in the gateway's certificate database, the gateway component does not recognize the server's CA certificate, and the SSL handshake fails.

To import a root CA certificate into the gateway component’s certificate database, complete the following steps:

1. As root, run the `certadmin` script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

2. Select option 3 from the Certificate Administration menu to add the root CA certificate.
3. When the script asks for the name of the file that contains the root certificate, provide this information.

If the gateway component is set up to communicate with an HTTPS site that presents a self-signed certificate, allowing the gateway component to trust any unknown CAs can be useful. However, this approach must be used with caution. See “[Denying Unknown Certificate Authorities](#)” for more information on configuring the gateway component.

TIP

Most well-known public certificate authorities are already included in the certificate database.

Viewing the Public CA list

To view the list of Public CAs, complete the following steps:

1. As root, run the `certadmin` script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

2. Section option 6 from the certificate administration menu to display all root CA certificates.

Table 15 is a two column table that displays all public certificate authorities included in the certificate database by default. The first column contains the Certificate Authority name, and the second column lists heir trust attributes.

Table 15 Public Certificate Authorities

Certificate Authority Name	Trust Attributes
ABAEcom (sub., Am. Bankers Assn.) Root CA	CG,C,C

Table 15 Public Certificate Authorities *(Continued)*

Certificate Authority Name	Trust Attributes
American Express CA	C,C,
American Express Global CA	C,C,
Baltimore CyberTrust Code Signing Root	,C
Baltimore CyberTrust Mobile Commerce Root	CG,C,
Baltimore CyberTrust Root	CG,C,
BelSign Object Publishing CA	,C
BelSign Secure Server CA	,C,,
Deutsche Telekom AG Root CA	C,C,C
Digital Signature Trust Co. Global CA 1	CG,C,C
Digital Signature Trust Co. Global CA 2	CG,C,C
Digital Signature Trust Co. Global CA 3	CG,C,C
Digital Signature Trust Co. Global CA 4	CG,C,C
E-Certify Commerce ID	C,,
E-Certify Internet ID	,C,
Entrust.net Premium 2048 Secure Server CA	C,C,C
Entrust.net Secure Personal CA	C,C,C
Entrust.net Secure Server CA	C,C,C
Equifax Premium CA	C,C,C
Equifax Secure CA	C,C,C
Equifax Secure Global eBusiness CA	C,C,C
Equifax Secure eBusiness CA 1	C,C,C
Equifax Secure eBusiness CA 2	C,C,C
GTE CyberTrust Global Root	CG,C,C
GTE CyberTrust Japan Root CA	CG,C,C
GTE CyberTrust Japan Secure Server CA	CG,C,C
GTE CyberTrust Root 2	CG,C,C
GTE CyberTrust Root 3	CG,C,C
GTE CyberTrust Root 4	CG,C,C
GTE CyberTrust Root 5	CG,C,C

Table 15 Public Certificate Authorities *(Continued)*

Certificate Authority Name	Trust Attributes
GTE CyberTrust Root CA	CG,C,C
GlobalSign Partners CA	C,C,C
GlobalSign Primary Class 1 CA	C,C,C
GlobalSign Primary Class 2 CA	,C,
GlobalSign Primary Class 3 CA	,C,
GlobalSign Root CA	C,C,C
TC TrustCenter, Germany, Class 0 CA	Cw,C,C
TC TrustCenter, Germany, Class 1 CA	,C,
TC TrustCenter, Germany, Class 2 CA	C,C,C
TC TrustCenter, Germany, Class 3 CA	C,C,C
TC TrustCenter, Germany, Class 4 CA	C,C,C
Thawte Personal Basic CA	,C,C
Thawte Personal Freemail CA	,C,
Thawte Personal Premium CA	,C,C
Thawte Premium Server CA	CG,,C
Thawte Server CA	CG,,C
Thawte Universal CA Root	CG,C,C
ValiCert Class 1 VA	C,C,C
ValiCert Class 2 VA	C,C,C
ValiCert Class 3 VA	C,C,C
ValiCert OCSP Responder	C,C,C
VeriSign Class 4 Primary CA	CG,C,C
Verisign Class 1 Public Primary Certification Authority	,C,
Verisign Class 1 Public Primary Certification Authority - G2	,C,
Verisign Class 1 Public Primary Certification Authority - G3	,C,
Verisign Class 2 Public Primary Certification Authority	,C,C
Verisign Class 2 Public Primary Certification Authority - G2	,C,C
Verisign Class 2 Public Primary Certification Authority - G3	,C,C
Verisign Class 3 Public Primary Certification Authority	CG,C,C

Table 15 Public Certificate Authorities (*Continued*)

Certificate Authority Name	Trust Attributes
Verisign Class 3 Public Primary Certification Authority - G2	CG,C,C
Verisign Class 3 Public Primary Certification Authority - G3	CG,C,C
Verisign Class 4 Public Primary Certification Authority - G2	CG,C,C
Verisign Class 4 Public Primary Certification Authority - G3	CG,C,C
Verisign/RSA Commercial CA	C,C,
Verisign/RSA Secure Server CA	C,C,

For information on modifying the trust attributes of a public CA, see [“Modifying Trust Attributes of a Certificate.”](#)

Modifying Trust Attributes of a Certificate

The trust attributes of a certificate provide information about whether the certificate is a regular server certificate (also called user certificate) as opposed to a root certificate, and whether the certificate (in the case of a root certificate) can be trusted as the issuer of a server or client certificate.

Three trust categories are available for each certificate: SSL, email, and object signing. In the context of the gateway component, only the first category is useful. In each category position, zero or more attribute codes are used.

Table 16 is a two column table that lists the certificate trust attributes. The first column lists the possible attribute values, and the second column provides a description of that attribute.

Table 16 Certificate Trust Attributes

Attribute	Description
p	Valid peer
P	Trusted peer (implies p)
c	Valid CA
T	Trusted CA to issue client certificates (implies c)
C	Trusted CA to issue server certificates (SSL only) (implies c)
u	Certificate can be used for authentication or signing
w	Send warning (use with other attributes to include a warning when the certificate is used in that context)

Attribute codes for the categories are separated by commas, and the entire set of attributes is enclosed by quotation marks. For example, the self-signed certificate generated and installed during the gateway installation is marked `u,u,u` to designate that it is a server certificate (user certificate), as opposed to a root CA certificate.

Viewing Trust Attributes

You can use the certificate administration script to view all certificates and their corresponding trust attributes.

To view the trust attributes of a certificate, complete the following steps:

1. As root, run the `certadmin` script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

2. Select option 7 from the certificate administration menu to list all certificates.

Setting the Trust Attribute for a Certificate

The trust attributes of a certificate must be modified if client authentication is used with the gateway.

An example of client authentication is PDC (Personal Digital Certificate) as described in Chapter 6 of the *iPlanet Portal Server 3.0 Administration Guide*. The CA that issues the PDCs must be trusted by the gateway. For example, the CA certificate should thus be marked `T` for SSL.

To set the trust attribute for a certificate, complete the following steps:

1. As root, run the `certadmin` script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

2. Select option 5 from the certificate administration menu to change a certificate's trust attributes.
3. When the script asks for the name of the certificate, provide this information. For example:
`Thawte Personal Freemail CA.`
4. When the script asks for the certificate's trust attribute, provide this information. For example:
`CT,CT,CT` (in this case, this is the default new value, so you just need to select Enter)

Once the certificate trust attribute is changed, the gateway recognizes client certificates signed by that certificate authority.

Adding a Gateway After Installation

The first two steps in the procedure “To Add a Gateway After Installation” in the *iPlanet Portal Server Administration Guide* are incorrect. The correct procedure for adding a gateway after installation is described here.

To add a gateway after you install Portal Server, complete the following steps:

1. Select Server Management on the administration console menu.
2. Select Manage Server Profile.

The Component Profile: Platform page is displayed.

3. Scroll to the Gateway List attribute box.
4. Type the fully qualified host name of the new gateway in the field below the attribute box.
5. Select Add to add the gateway.

The new gateway uses the default platform values for gateway port number, name of platform profile, retry interval, and default domain.

6. If the added gateway is on a different domain from the iPlanet Portal Server, scroll to the Cookie Domain List field and enter the new gateway domain name in the field.

For example, if the new gateway host name is `host1.domain1.com` and the iPlanet Portal Server host name is `host2.domain2.com`, then `domain1.com` is added to the Cookie Domain List attribute.

7. Select Add.
8. Select Submit to create the new gateway. A message that the profile was successfully updated is displayed.
9. Select Continue.
10. Select Manage Domains to add new gateway URLs so that the user can log in from the gateway.
11. Select the domain desired to give access to the new gateway to open its Domain, Role and Users page.
12. Select the Authentication link.
13. Scroll to the Domain URLs List window attribute and type the gateway host name in the field.

14. Select Add. Additional forms of the URL are also added to this list as indicated by the following steps.
15. Type the IP address of the new gateway.
For example, if the IP address is 10.0.0.1, type this value.
16. Select Add.
17. Type the URL in the form of *gateway_ipaddress/gateway_domain*.
For example, from the above indicated values, type 10.0.0.1/sesta.com
18. Select Add.
19. Enter the URL in the form of */gateway_domain*.
For example, from the above indicated value, type /sesta.com
20. Select Add.
21. Select Submit. The Profile Successfully Updated message is displayed.
22. Select Continue and repeat Step 11 through Step 21 for any other domains that require access to the new gateway.
23. From the administration console home page, select the Server Management link from the left frame.
24. Select the server name associated with the added gateway and select Restart Servers. The prompt, Restart request had been sent to the servers, is displayed.
25. Select Continue to return to the Server Management page.

How to Report Problems

If you have problems with iPlanet Portal Server, contact iPlanet customer support using one of the following mechanisms:

- iPlanet online support Web site at <http://www.iplanet.com/support/online/>
From this location, the CaseTracker and CaseView tools are available for logging problems.
- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when contacting customer support:

- Description of the problem, including the situation where the problem occurs and its impact on the operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods used to reproduce the problem
- Any error logs or core dumps

Where to Find More Information

- **iPlanet Portal Server release notes and other documentation** — <http://docs.sun.com/db/prod/sunone>
- **Product status** — <http://www.sun.com/service/sunone/software/index.html>
- **Products and Services information** — <http://www.sun.com/service/sunps/sunone/index.html>
- **Developer information** — <http://developer.iplanet.com/>
- **Learning solutions** — <http://www.sun.com/software/training/>
- **Product data sheets** — <http://www.sun.com/software/>

Use of iPlanet Portal Server is subject to the terms described in the license agreement accompanying it.

Copyright © 2003 Sun Microsystems, Inc. All rights reserved.

Sun, Sun Microsystems, the Sun logo, iPlanet, the iPlanet logo, Java, Java Development Kit, JKD, JavaServer Pages, JSP, Java Virtual Machine, JVM, Javadoc, JavaScript, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Netscape, the Netscape logo, and Netscape Navigator is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

Federal Acquisitions: Commercial Software -- Government Users Subject to Standard License Terms and Conditions The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of the product or this document may be reproduced in any form by any means without prior written

authorization of Sun Microsystems, Inc. and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright © 2003 Sun Microsystems, Inc. Tous droits réservés.

Sun, Sun Microsystems, le logo Sun, iPlanet, et le logo iPlanet, Java, Java Development Kit, JKD, JavaServer Pages, JSP, Java Virtual Machine, JVM, Javadoc, JavaScript, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et d'autre pays. Netscape, le logo Netscape N, et Netscape Navigator sont marques de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays. UNIX est une marque enregistrée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company Ltd.

Toutes les marques SPARC, utilisées sous licence, sont des marques déposées ou enregistrées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Le produit décrit dans ce document est distribué selon des conditions de licence qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ni de ce document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable de Sun Microsystems, Inc., le cas échéant, de ses bailleurs de licence.

CETTE DOCUMENTATION EST FOURNIE "EN L'ÉTAT", ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.