Release Notes for iPlanet Portal Server 3.0, Service Pack 4

Service Pack 4

Updated October 10, 2002

The *Release Notes for iPlanet™ Portal Server, Version 3.0, Service Pack 4* document important information available at the time of release.

These release notes contain the following sections:

- What's New in Portal Server
- 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 4. For an online version of this and other Portal Server 3.0 documentation, see the iPlanet documentation Web site at:

`http://docs.iplanet.com/docs/manuals/`

After you install and start using iPlanet Portal Server 3.0, Service Pack 4, check this Web site periodically to view the most up-to-date documentation.

NOTE Installing this product updates the iPlanet Portal Server 3.0, Service Pack 4 software to include Service Pack 1, Service Pack 2, Service Pack 3, Service Pack 3a, and Service Pack 4. The information in this document includes documentation for previous service packs.

About This Document

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

- Typographic Conventions
- Sample Machine Names

Typographic Conventions

The following tables describes the typographic conventions used in this release note.

Table 1 Typographic Conventions

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

Sample Machine Names

The following table lists the machine names used in code examples and the types of iPlanet Portal Server components to which they correspond.

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 Portal Server

This section summarizes enhancements implemented in iPlanet Portal Server 3.0, Service Pack 1, Service Pack 2, and Service Pack 3a as well as in 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™ 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.

Mobile Access Pack Support 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 "Mobile Access Pack Support 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 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:

- JavaServer Pages Provider
- Reloading Templates without a Server Restart
- Tabbed Desktop
- Using Form Control
- Locking Channel Positions
- Setting Up Full-Width Channels

- Setting Up Frameless Channels
- Enabling Access to HTTP Requests and Responses
- Setting Session Time-out Units
- Running Desktop Applications on Macintosh Clients

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 4.

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

Using multiple cookies differing only in path or value is now supported. This is useful when managing non-iPlanet Portal Server cookies passed to other Web applications.

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.

The `HttpServletRequest` and `HttpServletResponses` objects passed to the new methods have the following indicated methods and return values:

Table 3 HttpServletRequest and HttpServletResponses

Methods	Returns
`getQueryString()`	`UnsupportedOperationException`
`getSession(boolean)`	Null
`isRequestedSessionIdFromCookie()`	False
`isRequestedSessionIdFromUrl()`	False
`isRequestedSessionIdValid()`	False
`getContentLength()`	-1
`getInputStream()`	`UnsupportedOperationException`
`getParameter(String)`	uses internal Map to return parameter
`getParameterNames()`	uses internal Map to return names
`getParameterValues(String)`	uses internal Map to return values
`getReader()`	`UnsupportedOperationException`
`encodeRedirectUrl(String)`	arg
`encodeUrl(String)`	arg
`sendError(int)`	`UnsupportedOperationException`
`sendError(int, String)`	`UnsupportedOperationException`
`sendRedirect(String)`	`UnsupportedOperationException`
`setStatus(int)`	`UnsupportedOperationException`
`setStatus(int, String)`	`UnsupportedOperationException`
`getOutputStream()`	`UnsupportedOperationException`
`getWriter()`	`UnsupportedOperationException`

Table 3 HttpServletRequest and HttpServletResponses *(Continued)*

Methods	Returns
`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 4 lists the minimum system requirements for running the Netlet, NetMail, and NetFile applications on Macintosh clients.

Table 4 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

Table 4 Minimum system requirements for running Portal Server applications on Macintosh clients

Component	Description
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:

- 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

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>
```

If the `Rewrite Applet/Object Parameter Values List` contains the following example entries, the corresponding URLs is rewritten as noted in Table 5.

Table 5 Rewrite Applet/Object Parameter Values List

Value	Description
`some.html iplanet.class *`	No parameter value is rewritten, because `object_of_applet/object_url` does not match the object of the request URL.
`/some_dir/some.html iplanet.class *`	`url1` and `url2` are rewritten. `url3` and `url4` are not rewritten because they are embedded within strings that do not appear to be URLs as they do not start with `/`, `http` or `https`.

Table 5 Rewrite Applet/Object Parameter Values List

Value	Description
`/some_dir/some.html iplanet2.class *`	No parameter value is rewritten because `iplanet2.class` does not match the value of the applet code attribute or the object `classid` attribute.
`* * server* *|*|*|`	`url3` is rewritten because `*|*|*|` matches `0|234|test|`.
`/some_dir/some.html clsid:D27CDB6E-AE6D \ movie`	`url6` is rewritten.
`/some_dir/some.html clsid:D27CDB6E-AE6D \ video **,*,**`	`url7` and `url8` are rewritten because the first `**` matches the position of `url7`, and the second `**` matches the position of `url8`.

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:

- A gateway 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 `platf ‘orm.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 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.

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.

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.

Mobile Access Pack Support Changes

This section provides details about changes in iPlanet Portal Server for supporting iPlanet™ Portal Server: Mobile Access Pack 3.0. It contains the following topics:

- File Lookup
- isPresentable() Method

File Lookup

A generic file path search API is now available for all data file types to support the iPlanet Portal Server: Mobile Access Pack architecture.

All components use the same API for file lookup, including desktop template lookup and JSP file lookup.

This file lookup API uses a combination of attributes to create a list of file paths to search. These attributes include:

- Desktop type
- Locale
- Component name
- Client path (optional)

TIP For information about the attributes, see "Appendix A" of the *iPlanet Portal Server: Mobile Access Pack Programmer's Guide*.

Example

This example of the file path search API asks for file name `foo.template` with these values:

- `Desktop type: myType`
- `Locale: en_US`
- `Component name: iwtMyChannel`
- `Client path: wml/Nokia/generic`
- `Filename: foo.template`

The File Lookup API searches the appropriate paths and returns the first file encountered, with its given file name.

isPresentable() Method

In the Mobile Access Pack architecture, each channel is responsible for identifying itself as able to present content for a particular client type. Each channel has access to the client type via the session, and is therefore capable of making the decision as to whether it supports the output format for this client type.

A channel determines if it is presentable by indexing the client data based on the client type stored in the iPlanet Portal Server 3.0, Service Pack 4 session. The channel can use any of the client data elements to determine whether it is presentable. For example, in the simplest case the channel may determine that it only supports clients where:

```
contentType=text/html
```

Each channel must be asked whether it supports the client type before output is gathered and returned to the user. So for each place in the desktop core where content is gathered, the channel generating the content must first be asked if it can produce this output format.

An iPlanet Portal Server 3.0, Service Pack 4 channel can generate content from two methods:

- `Provider.getContent()`
- `Provider.getEdit()`

The `Provider.getContent()` returns the main channel content. The `Provider.getEdit()` returns an edit page for the channel.

A channel is able to signal the desktop that it supports output of the main content or the edit page separately for different devices.

A new Provider API method answers whether the channel can return main channel content for the particular client:

```
public boolean isPresentable();
```

The `isPresentable()` method is part of the Provider interface and is implemented in the `ProviderAdapter`.

NetFile Changes

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

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

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:

- 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

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 6 describes netlet rules and provides their formats.

Table 6 Netlet Rules

Purpose	Type	Format
Rule for using a single pre-defined FTP server	Static	`ftp|null|false|30021|`*your_ftp_server*`.`*your_domain*`|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 6.
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.

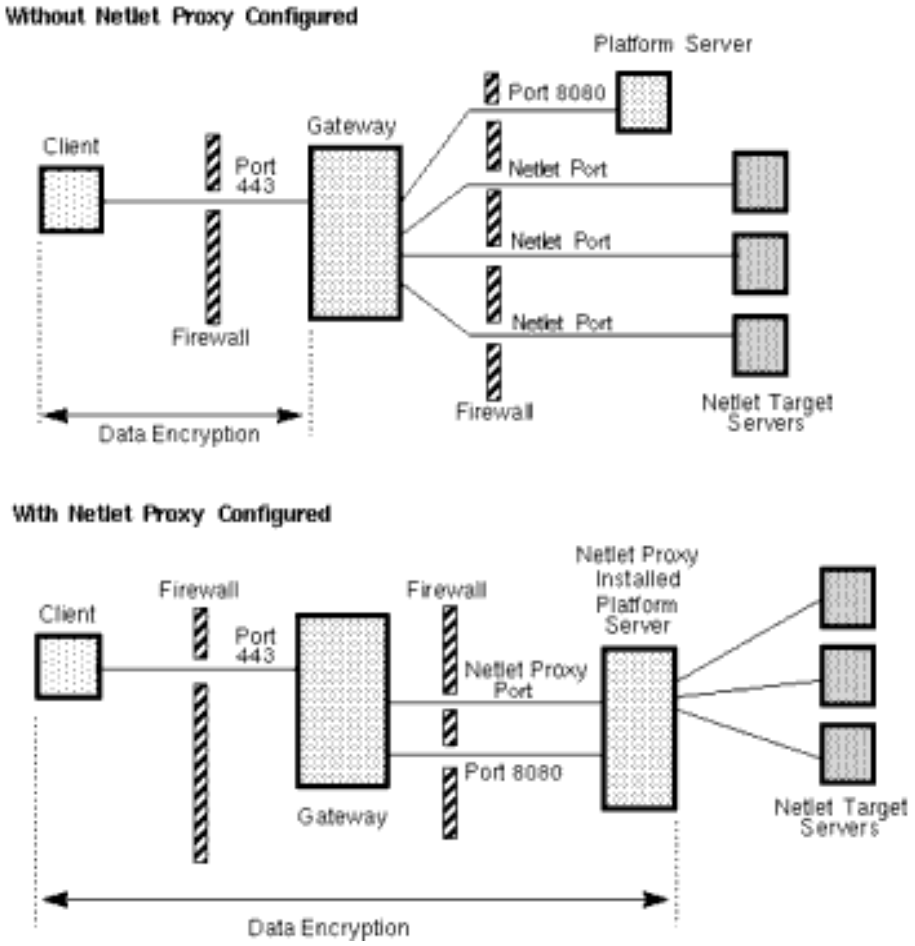

Figure 1 Netlet Proxy Implementation

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 3.0, Service Pack 4.

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\n\127.0.0.
```

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:

- 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

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 4 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 7 describes these parameters. These configuration files are located in the *install_directory*/netscape/server4/https-*server*/config file.

Table 7 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 JDK™ 1.2.2_09.
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.

Table 7 Web Server Performance Tuning Parameters *(Continued)*

Scope	Default	Recommended	Description
jvm.option			
jvm12.conf	-Xrunoii	-Xgenconfig:32m,32m,semispaces:32m,768m,markcompact	The parameters used in the genconfig option must be less than or equal to the values in the jvm.maxHeapSize and jvm.minHeapSize. For example: Given -Xgenconfig:min0, max0, semispaces:min1, max1, markcompact then max0 + max1 <= jvm.maxHeapSize and min0 + min1 <= jvm.minHeapSize
cache-init			
obj.conf	false	true	Add this line to obj.conf to disable the Web Server static page cache: Init fn="cache-init" disable="true"

Profile Service Changes

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

- Multi-Profile Server Support
- Getting and Setting User Properties

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 Portal Server instance are now directed to the profile server of that Portal Server. Each Portal Server 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 `pluggable auth` API 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 3.0, Service Pack 4 Service Pack 4 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 3.0, Service Pack 4 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-fontFace1]" 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 Component 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 Component 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 Component 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 Component 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.lbcooookie.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 3.0, Service Pack 4 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 3.0, Service Pack 4. Install it with the iPlanet Web Server. For information on installing a certificate, refer to the original *iPlanet Portal Server 3.0, Service Pack 4 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 3.0, Service Pack 4 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 3.0, Service Pack 4 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 Serveron different ports, after you install iPlanet Portal Server 3.0, Service Pack 4 Service Pack 4.

TIP For installation instructions, see “Service Pack 4 Installation Notes” in the *iPlanet Portal Server 3.0, Service Pack 4 Service Pack 4 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.iplanet.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

The following command options have been updated, and new commands have been added. The following examples assume that the commands are being run from the directory in which they reside:

`./ipsserver start`	Starts the original server only.
`./ipsserver startall`	Starts the original server and all created multiple instances.
`./ipsserver stop`	Stops the original server only.
`./ipsserver stopall`	Stops the original server and all created multiple instances.
`./ipsserver delete`	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 3.0, Service Pack 4. Install it with the iPlanet Web Server. For information on installing a certificate, refer to the original *iPlanet Portal Server 3.0, Service Pack 4 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/netscape/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 3.0, Service Pack 4 public APIs are supported only on Solaris™ operating systems.

Software supported include:

- JDK software/Java™ runtime environment 1.2.2_09
- iPlanet Web Server 4.1 SP9a
- Solaris Operating Environment (SPARC™ Platform Edition) 2.6
- Solaris Operating Environment (SPARC Platform Edition) 7
- Solaris Operating Environment (SPARC Platform Edition) 8

Setting Up a Non-iPlanet Portal Server 3.0, Service Pack 4 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/notificationservice
   ```

4. Copy the following files from `/opt/SUNWips/lib` to the same location on the server host:
   - `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/jvm12.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.iplanet.portalserver.pll.client.PLLNotif
   icationServlet
   ```

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 3.0, Service Pack 4 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/SUNWips
```

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 3.0, Service Pack 4 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 `.msc` 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 4. Details are provided in the following areas:

- Authentication
- Administration
- Desktop
- Gateway
- Installation
- ipsadmin
- ipsserver
- Logging
- Mobile Access Pack
- 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

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*)

Workaround:
Log in to the iPlanet Portal Server product through the gateway.

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 3.0, Service Pack 4, 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 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.

   The locale is a language and country combination. For example: `en_US`

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 `X`s are hexidecimal digits.

   Files in this encoding can be created from files in a variety of native encoding using the `java native2ascii` program.

   NOTE A separate `.properties` 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.

External bookmark URLs are not redirected. (*4324617*)

Workaround:
Create a second bookmark channel to handle external sites.

The bookmark provider can not be used for URLs referencing Internet URLs that the gateway cannot or should not fetch.

To prevent this, remove `openURL` from the gateway profile rewrite JavaScript function parameters.

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

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

Logging in to simulators using LDAP and UNIX modules is not possible. (*4530516*)

Workaround:
A hot patch for using Service Pack 4 with Mobile Access Pack is needed. See the iPlanet Web site for information on this hot patch.

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

When attempting to upgrade individual platform servers from a multi-profile environment to a Service Pack 4 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}/bin/java -classpath ${CLASSPATH}
com.iplanet.portalserver.ipsadmin.ImportComponent $*
```

To the line below:

```
${JAVA_HOME}/bin/java -ms 128m -mx256m -classpath ${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 release of iPlanet Portal Server includes enhancements and fixes to the following known problems:

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
Administration Console		
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 (`CVal`) key value pairs in the `iwtAuthCert.properties` file, and spaces in the keys in the `iwtAuthCert.properties` 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 `.properties` 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		
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

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
4343671	`authd` did not support open Portal Server login.	SP1
Desktop		
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 `sn` and `givenname` 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	`URLScraperProvider` 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 `TimeZone` are not effective until user logs in again.	SP3
4412806	Relative URL redirects from JSPProvider `processEdit` fail.	SP3
4426023	SunBlue templates do not work with SP2.	SP3
4448938	Changing to layout Option Four causes wide channels to be removed.	SP3
4450801	Selecting Open all pages in the desktop when editing bookmarks causes the javaScript function `openURL` to call the server twice in the URL.	SP3

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
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		
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

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
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
4344066	Referer headers must be forwarded so servers can track the user's URL.	SP3
4350023	The `ipshttpd` script does not set the maximum number of file descriptors to a high enough value for the gateway proxy process, causing the `ipshttpd` process to run out of file descriptors. When that happens, `ipshttpd` stops responding.	SP3
4352555	The JavaScript rewriter mishandles escaped double quote.	SP3
4354655	Users cannot authenticate with Internet Explorer, if `hostname` contains capital letters.	SP3
4358856	If the server and the gateway are installed on two different machines, the `iwtGateway.properties` file is not installed in *basedir*`/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	Gateway ceases to resolve DNS hostnames intermittently.	SP3
4380531	Rewriter misplaces `iplanet()` function.	SP3
4381501	The URL rewriter incorrectly rewrites relative URLs by using the document's URL instead of its instead of its base URL (indicated by the BASE tag).	SP3
4389707	In some cases the gateway or gateway proxy would not respond due to `CLOSE_WAIT` sockets accumulating, and not getting closed.	SP3
4396142	If an applet is between `<OBJECT>` and `</OBJECT>`, 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

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
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 `http://` 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
Install		
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		
4363059	Importing privileges after accessing the Policy page requires relogging to view.	SP3
4350031	`ipsadmin -import` 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	`ipsadmin` did not work if server was running on SSL mode.	SP1

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
4337917	`ipsadmin` 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	`ipsserver stop` 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 `ipsserver stop` command should stop only relevant processes.	SP2
Japanese Language Version		
4402583	Incorrect country code for Japan in the `iwtUser.properties` file.	SP3
4336096	On Japanese localization, NetFile Java did not work on Solaris and Windows NT.	SP1
Logging		
4343010	When logging is disabled, the log client still sends the log message.	SP3
4401461	Oracle `jdbc` 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		
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
NetFile		
4381166	Mail form field values in NetFile are not checked uniformly.	SP4
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 `PORT` command uses the wrong IP address when sending data back to the client.	SP4

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
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 `isAllowed` 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 `ipsadmin` 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 `LANG` setting specifies Japanese or Chinese locale, NetFile download functions for image, HTML, and executable files do not work.	SP3
4371647	If the server's `LANG` setting specifies Japanese or Chinese locale, NetFile upload functions for image, HTML, and executable files do not work.	SP3
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		
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

Table 8 Fixed Bug List

Bug ID	Bug Description	Fixed In
4461255	Dynamic rules should be supported when using FTP through a Netlet connection.	SP4
4500165	The port number is not stripped from the host name when evaluating a PAC file.	SP4
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 *iPlanet Portal Server 3.0, Service Pack 4 Installation Guide*.	SP4
4332715	Applet download rule section is broken.	SP3
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
Profile		
4352059	The profile `isAllowed` method does not do wildcard matching.	SP3
4394184	A certificate error occurs when using an HTTPS connection when the VIP name does not match the server name.	SP3
4424086	Profile server should be able to reconnect to the LDAP server.	
4399031	`ipsadmin` has wrong content type for `UpdateProfileCache` request.	SP3
4412089	Profile server enters busy wait loop.	SP3
4340128	Profile API returns valid profile object for non existing profiles.	SP2
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 *iPlanet Portal Server 3.0 Administration Guide*. For correct instructions, see "Adding a Gateway After Installation" in this document.	SP4
4332242	Document required disk space for `/var; /etc; /opt`; and `installation directory`.	SP3
4373115	Portal Server and gateway components on a single computer must use the same `install` directory.	SP3
4402209	Correct instructions for adding `iwtTabProvider` in selected channels.	SP2
4343016	Incorrect URL for documentation.	SP1

Documentation Updates

This section provides information that supplements the *iPlanet Portal Server 3.0, Service Pack 4 Administration Guide*. Topics include:

- Certificate Management for the Gateway
- Adding a Gateway After Installation

Documentation for iPlanet Portal Server 3.0, Service Pack 4 is at this Web site:

`http://docs.iplanet.com/docs/manuals/portal.html`

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 Server3.0 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*`/netscape/server4/alias`. If necessary, they can be shared between the iPlanet Portal Server server and gateway components or the gateway 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/ispgateway 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/ispgateway 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, compete 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 9 displays all public certificate authorities included in the certificate database by default. Their trust attributes are also provided.

Table 9 Public Certificate Authorities

Certificate Authority Name	Trust Attributes
ABAecom (sub., Am. Bankers Assn.) Root CA	CG,C,C
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

Table 9 Public Certificate Authorities *(Continued)*

Certificate Authority Name	Trust Attributes
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
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

Table 9 Public Certificate Authorities *(Continued)*

Certificate Authority Name	Trust Attributes
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
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.

The possible attribute values and the meaning of each value are listed in Table 10.

Table 10 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 3.0, Service Pack 4 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 3.0, Service Pack 4 Service Pack 4, 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

Useful iPlanet information can be found at the following Internet locations:

- iPlanet release notes and other documentation --- `http://docs.iplanet.com/docs/manuals/`
- iPlanet product status --- `http://www.iplanet.com/support/technical_resources/`
- iPlanet developer information --- `http://developer.iplanet.com/`
- iPlanet learning solutions --- `http://www.iplanet.com/learning/index.html`
- iPlanet product data sheets --- `http://www.iplanet.com/products/index.html`