Release Notes for iPlanet Portal Server 3.0

Service Pack 2

Updated February 12, 2001

These release notes contain important information available at the time of the release of iPlanet Portal Server 3.0™ Service Pack 2. Installing this product will update the iPlanet Portal Server 3.0 software to include both Service Pack 1 and Service Pack 2. New features and enhancements, installation notes, known problems, and other late-breaking issues are addressed here. Read this document before you begin using iPlanet Portal Server 3.0 with Service Pack 2.

An electronic version of these release notes can be found at the iPlanet documentation web site: `http://docs.iplanet.com/docs/manuals/`. Check the web site prior to installing and setting up the software and then periodically thereafter to view the most up-to-date release notes and manuals.

These release notes contain the following sections:

- Understanding the Typographic Conventions
- What's New in iPlanet Portal Server 3.0, Service Pack 1 and Service Pack 2
- Software and Hardware Requirements
- Service Pack 2 Installation Notes
- Bugs Fixed in Service Pack 1 and Service Pack 2
- Documentation Updates
- How to Report Problems
- For More Information

Understanding the Typographic Conventions

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

Table 0-1

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:port/login/`*`domain_name`* Where *`domain_name`* is a Portal domain name.

Shell Prompts in Command Line Interface Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

Table 0-2

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

What's New in iPlanet Portal Server 3.0, *Service Pack 1* and *Service Pack 2*

The following product enhancements to iPlanet Portal Server 3.0 are included in the Service Pack 2 software release:

- Open Portal Mode
- Configuring Multiple Instances of iPlanet Portal Server
- Configuring User Non-Root
- Configuring User Nobody
- Installing and Enabling Multiple Locale for a Domain
- Supporting SSL for Authentication in an Open Portal
- Anonymous Authentication
- Redirecting the User Using the goto Parameter
- Setting Persistent Cookies
- Extending Authentication
- Setting the Default URL
- Getting and Setting User Properties
- Using E-mail Address As User's Profile ID
- Login Channel
- JavaServer Page Provider
- Tabbed Desktop
- Changing Membership Login Password
- Reloading Templates with No Restart
- Enabling Anonymous Desktop
- Using Form Control
- Locking a Channel's Position
- Setting Up Full-width Channel

- Setting Up Frameless Channels
- Selecting the Locale
- URL Scraping with No Gateway Installed
- Forwarding Cookies
- Configuring Restart of the HTTP Proxy
- Enabling Access to HTTP Requests and Responses
- Gateway Logging
- Running Applications on a Non-iPlanet Portal Server

Open Portal Mode

If the portal does not contain sensitive information (deploying public information and allowing access to free applications), then by using the Open Portal mode (without a gateway), the portal server can respond faster to access requests by a large number of users than if a gateway is installed (Secure Portal mode).

The gateway, which provides encryption services and URL rewriting, is not required when the iPlanet Portal Server is operating in Open Portal mode.

Running iPlanet Portal Server without the gateway is referred to as Open Portal mode. The main difference between an open portal and a secure portal are the services presented by the open portal typically reside within the DMZ and not within the secured intranet.

NOTE Using the iPlanet Portal Server without the gateway (Open Portal mode) may improve the individual response of the portal for a large number of simultaneous users.

The Secure Portal

The iPlanet Portal Server 3.0 product was targeted towards customers deploying highly secure portals or remote access portals. These types of portals have a major emphasis on security and protection and privacy of intranet resources. The iPlanet Portal Server architecture is well suited to this type of portal. The URL Rewriting, URL Access Policy, and Netlet features of the gateway, allow users to securely access intranet resources from the Internet without exposing these resources to the public Internet. The gateway, residing in the DMZ, provides a single secure access point to all intranet URLs and applications. All other iPlanet Portal Server services such as Session,

Authentication, Desktop, Channels, and Profile database reside behind the DMZ in the secured intranet. Communication from the client browser to the gateway is encrypted using HTTP over SSL. Communication from the gateway to the server and intranet resources may be either `http` or `https`.

The Open Portal

The release of iPlanet Portal Server 3.0 Service Pack 1 enables the features necessary for iPlanet Portal Server to be deployed without the services of the gateway.

Configuring iPlanet Portal Server 3.0 to Run SSL in Open Portal Mode

The typical public portal runs in the clear or using `http`. It may however be desirable to deploy a portal using HTTP over SSL (`https`). The Portal server may be configured to run `https` services during installation or manually changed from `http` to `https` after installation.

See the *iPlanet Portal Server 3.0 Administration Guide* for more information on using SSL.

NOTE This type of open portal does **not** require the services of the gateway.

Users access the server directly as if the server was configured for `http`, but use `https://server.domain` instead of `http://server.domain`.

The following features are **not available** when running without the gateway or in Open Portal mode:

Netlet	This feature is **not available** without the gateway. The netlet provides a secure encrypted tunnel for TCP/IP applications from the browser through the gateway to the backend service.
URL Access Policy Enforcement	Generic URL access validation is **not available** without the gateway. One of the many functions of the gateway is to ensure 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. For example, if a user is restricted from either running the desktop or adding specific channels within the desktop, this type of policy is still enforced.

URL Rewriting	There will be **no rewriting** services as there will be no gateway installed in Open Portal mode This means 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	This feature is **not available** in Open Portal. The gateway provides a single sign on service for HTTP Basic Authentication. When a user requests a web page that is password protected, web servers will return an *HTTP Basic Auth* request for the username and password. The user types in the username and password and the page is returned by the web server. The gateway listens for this interaction and stores the username and password in the user profile so the next time the user does not have to enter the information. The gateway responds on behalf of the user.

One iPlanet Portal Server installation may be configured to support both open and secure portal.

For example, a company may want to create a portal which resides within the intranet:

- When users access the portal from the intranet, log in to the server directly using `http`
- When accessing the portal from the internet use `https` through the gateway

Configuring Open Portal Mode

1. Install iPlanet Portal Server 3.0 software on the portal server.

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

When prompted for *Gateway Name*, use the name of the *portal server*.

NOTE iPlanet Portal Server 3.0 Gateway software is not installed for Open Portal mode.

---

2. Apply iPlanet Portal Server 3.0 Service Pack 2 on the portal server.
3. Stop and restart the portal Server:

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

Updating an Existing Gateway/Server Installation to Open Portal Mode

Install iPlanet Portal Server 3.0 Service Pack 2 on the portal server, then do the following:

- To completely remove the gateway on a different computer from the portal server, remove the `SUNWwtgwd` and `SUNWwtsd` packages.
- To completely remove the gateway, and the gateway and portal server are on the same machine, only remove the `SUNWwtgwd` package.
- To shut down the gateway only, run the `ipsgateway stop` script:

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

Logging Into the Open Portal

To log in to the Open Portal use the following rules:

NOTE Users should always use the fully qualified name of the server.

- If the server name is `my.sun.com` and the server is running *http* use the following URL:

  `http://my.sun.com:port`

or

  `http://my.sun.com` if port 80 is configured.

- If the server name is `my.sun.com` and the server is running *https* use the following URL:

  `https://my.sun.com:port`

or

  `https://my.sun.com` if port 443 is used.

Multi-hosting in Open Portal Mode

Service Pack 2 adds functionality which allows the server to access multiple DNS and IP addresses from a single server installation.

Access to the iPlanet Portal Server is through either:

- `http://server:port`
- `https://server:port` (if the server was configured to HTTPS)

  Where `server` is the Portal server name, and `port` is the Portal server port.

To log in to a different domain on the Portal, use the following URL:

`http://server:port/login/domain_name`

Where `domain_name` is a Portal domain name.

URL to Domain Mapping

If the existing installation of portal server contains multiple servers and multiple domains, a *URL to domain mapping* allows the portal server to find the domain automatically without the need to provide the domain name in the URL.

The following example describes how to map a URL to a specific domain:

If the iPlanet Portal Server installation has one server (server1), and two domains (domain1 and domain2), the following URL to domain mapping is needed:

- http://server1:port/domain1 ---> go to domain1
- http://server1:port/domain2 ---> go to domain2

To map a URL to a domain, do the following in the Administration console:

1. Logon as Super Administrator.
2. Select the *Manage Domains* link from the left frame.
3. In the *Portal Server Domains* page, do the following:
   - Select one of the domains.
4. In the *Domain, Role and Users* page:
   a. Expand *Profiles* link.
   b. Select *Authentication* link.
   c. Scroll to the *Domain URLs* field, add the URLs for that domain.

      See the Domain URL Mapping List.

d. Select *Add*.

e. Select *Submit*.

Repeat these steps for the second domain.

Domain URL Mapping List

The domain URL list for domain1 must contain the following URLs:

- `/domain1`
- `server1/domain1`
- `server1 IP address/domain1`
- `/domain2`
- `server1/domain2`
- `server1 IP address/domain2`

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

1. Add the following two lines to `obj.conf` (as shown in bold text in the following example).

The `obj.conf` is located at:

`/opt/netscape/server4/https-`*`server1`*`/config/obj.conf`

Where *`domain 1`* and *`domain 2`* are the iPlanet Portal Server domain names.

```
Init fn=flex-init
access="/opt/netscape/server4/https-smyrna.iplanet.com/logs/access"
format.access="%Ses->client.ip% - %Req->vars.auth-user% [%SYSDATE%] '
%Req->reqpb.clf-request%' %Req->srvhdrs.clf-status%
%Req->srvhdrs.content-length%"
Init fn=load-types mime-types=mime.types
Init fn="load-modules"
shlib="/opt/netscape/server4/bin/https/lib/libNSServletPlugin.so"
funcs="NSServletEarlyInit,NSServletLateInit,NSServletNameTrans,NSServletService
" shlib_flags="(global|now)"
Init fn="NSServletEarlyInit" EarlyInit=yes
Init fn="NSServletLateInit"  LateInit=yes

<Object name=default>
NameTrans fn="NSServletNameTrans" name="servlet"
```

```
NameTrans fn="pfx2dir" from="/servlet" dir="/opt/SUNWips/servlets"
name="Servlet ByExt"
NameTrans fn="pfx2dir" from="/jsp.092" dir="/opt/SUNWips/public_html/jsp.092"
name="jsp092"
NameTrans fn=pfx2dir from=/ns-icons dir="/opt/netscape/server4/ns-icons"
name="es-internal"
NameTrans fn=pfx2dir from=/mc-icons dir="/opt/netscape/server4/ns-icons"
name="es-internal"
NameTrans fn="pfx2dir" from="/help" dir="/opt/netscape/server4/manual/https/ug"
name="es-internal"
NameTrans fn="pfx2dir" from="/manual" dir="/opt/netscape/server4/manual/https"
name="es-internal"
NameTrans fn="pfx2dir" from="/cgi-bin" dir="/opt/SUNWips/cgi-bin" name="cgi"
NameTrans fn="pfx2dir" from="/NetMail" dir="/opt/SUNWips/public_html/NetMail"
NameTrans fn="pfx2dir" from="apps" dir="/opt/SUNWips/public_html/"
NameTrans fn="pfx2dir" from="/content" dir="/opt/SUNWips/public_html/content"
NameTrans fn="pfx2dir" from="/locale" dir="/opt/SUNWips/locale"
NameTrans fn=document-root root="/opt/SUNWips/public_html"
NameTrans fn="redirect" from="/domain1" url="/login/domain1"
NameTrans fn="redirect" from="/domain2" url="/login/domain2"
PathCheck fn=unix-uri-clean
PathCheck fn="check-acl" acl="default"
PathCheck fn=find-pathinfo
PathCheck fn=find-index index-names="index.html,home.html"
ObjectType fn=type-by-extension
ObjectType fn=force-type type=text/plain
Service type="magnus-internal/jsp" fn="NSServletService"
Service method=(GET|HEAD) type=magnus-internal/imagemap fn=imagemap
Service method=(GET|HEAD) type=magnus-internal/directory fn=index-common
Service method=(GET|HEAD|POST) type=*~magnus-internal/* fn=send-file
AddLog fn=flex-log name="access"
</Object>
```

2. Stop and restart the server:

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

The following is another example:

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:port ---> go to domain 1

http://server2:port ---> go to domain 2

http://server3:port ---> go to domain 2

To map a URL to a domain, do the following in the Administration console:

1. Logon as Super Administrator.
2. Select the *Manage Domains* link from the left frame.
3. In the *Portal Server Domains* page, do the following:
   - Select one of the domains.
4. In the *Domain, Role and Users* page:
   a. Expand *Profiles* link.
   b. Select *Authentication* link.
   c. Scroll to the *Domain URLs* field, add the URLs for that domain.

      See the *Domain URL Mapping List* section below.
   d. Select *Add*.
   e. Select *Submit*.

      Repeat these steps for the second domain.

Domain URL Mapping List

The domain URL list for domain1 must contain the following URLs:

- server1
- server1 IP address
- server1/domain1
- server1 IP address/domain1
- /domain1
- server1/login
- server1 IP address/login

The domain URL list for domain2 must contain the following URLs:

- server2
- server2 IP address
- server2/domain2
- server2 IP address/domain2
- /domain2
- server2/login
- server2 IP address/login
- server3
- server3 IP address
- server3/domain2
- server3 IP address/domain2
- server3/login
- server3 IP address/login

Configuring Multiple Instances of iPlanet Portal Server

This configuration supports running multiple instances of the iPlanet Portal Server 3.0 on different ports, giving the user just one virtual server to interact with.

Running multiple instances of iPlanet Portal Server 3.0 servers, each with its own copy of iPlanet Web Server on the same physical machine, changes the context of iPlanet Portal Server 3.0 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 will only configure *new* iPlanet Portal Server instances using the *http* protocol.

Installing Multiple Server Instances

To create multiple instances of the iPlanet Portal Server installation on different ports, do the following:

1. Install iPlanet Portal Server 3.0 Service Pack 2 on the Portal server, then do the following steps.

   See the Service Pack 2 Installation Notes in this document.

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

2. As root, in a terminal window enter the following commands:

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

This is an interactive option where the administrator can continue to enter unique port numbers, not already in use, where the multiple instances are to be created. Enter a blank line (*Return*) when finished.

TIP From the command line, type:

`netstat -a`

This will print out all ports currently assigned and in use.

This process takes approximately 5 minutes depending on the machine architecture. The script output looks like the following example. (Where the bold text is user input).

```
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
```

If any of the above instances already exist then the following message will be displayed before being prompted to overwrite:

```
Warning:: server instance already exists:smyrna.red.iplanet.com-8081
```

3. Select *Return* when menu is completed.
4. Stop and restart all the Portal Servers:

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

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:

```
/opt/SUNWips/bin/ipsserver.smyrna.red.iplanet.com@8081 start
```

The original server can still be started by:

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

5. In the iPlanet Portal Server Administration Console, do the following:
   a. Logon as Super Administrator.
   b. Select the *Server Management* link from the left frame.
   c. Select the *Manage Server Profile* link in the right frame.
   d. Change the *Server List* attribute.

      Add the new server instances to the *Server List:*

      `http://ipsserver.smyrna.red.iplanet.com@8081`

      `http://ipsserver.smyrna.red.iplanet.com@8082`
   e. Select the *Submit* button, at the bottom of the page, and save the changes.
   f. Select the *Continue* button on the *Profile Successfully Updated* page.
6. Stop and restart all the Portal Servers:

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

This will start all the portal server instances, including the original installation.

These instances can be directly accessed through the web browser, as follows:

```
http://servername:port1
http://servername:port2
```

If the machine name is `smyrna.red.iplanet.com`, and two port numbers `8081` and `8082` were configured as shown in the Step 2 example, and the install directory was `/opt`, the following files will be listed:

```
/opt/SUNWips/bin/ipsserver.smyrna.red.iplanet.com
/opt/SUNWips/bin/ipsserver.smyrna.red.iplanet.com@8081
/opt/SUNWips/bin/ipsserver.smyrna.red.iplanet.com@8082
```

Updated Command Options

The following command options have been updated, and new commands added:

`./ipsserver start`	Starts the original server only.
`./ipsserver startall`	Starts the original server and all the created multiple instances.
`./ipsserver stop`	Stops the original server only.
`./ipsserver stopall`	Stops the original server and all the created multiple instances.
`./ipsserver delete`	Deletes all the created multiple instances, but leaves the original server.

Changing the Profile Server to SSL in an Open Portal Environment

This section discuses how to change the profile server's protocol to HTTPS. This is also the server which has the profile service running on it. See the following instructions.

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

NOTE Obtain a certificate from any of the certificate authorities supported by the iPlanet Portal Server 3.0. Install it with the iPlanet Web Server. For information on installing a certificate, refer to the *iPlanet Portal Server 3.0 Installation Guide, 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. In a terminal window, become root, and type the following command:

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

2. In the iPlanet Portal Server Administration Console, do the following:
   a. Logon as Super Administrator.
   b. Select the *Server Management* link from the left frame.
   c. Select the *Manage Server Profile* link in the right frame.
   d. Change the *Platform Server List* attribute.

      Change the protocol of the URL for the original server to be *https*.

      https://ipsserver.smyrna.red.iplanet.com@8080
   e. Select the *Submit* button, at the bottom of the page, and save the changes.
   f. Select the *Continue* button on the *Profile Successfully Updated* page.
3. From the admin console, select *Server Management*.
   a. Select *Manage Naming profile*.
   b. In the *Profile URL*, change the protocol to *https*.

      https://ipsserver.smyrna.red.iplanet.com@8080/profileservice

      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.
   c. In the *Logging URL*, change the protocol to *https*.

      https://ipsserver.smyrna.red.iplanet.com@8080/loggingservice

d. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.

e. Select the *Continue* button on the *Profile Successfully Updated* page.

4. In a terminal window, open the `/etc/opt/SUNWips` directory.

The directory will contain `platform.conf` files of the type:

`/etc/opt/SUNWips/platform.conf.smyrna.red.iplanet.com`

`/etc/opt/SUNWips/platform.conf.smyrna.red.iplanet.com@8081`

`/etc/opt/SUNWips/platform.conf.smyrna.red.iplanet.com@8082`

5. Make the following changes to the `platform.conf` file of the server that will be configured for SSL, The file maybe any of the files listed above.

In this example the original server will be configured for SSL,

From a terminal window, use a text editor to edit the `platform.conf` file:

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

Edit the following entries as shown in bold text in the following example:

- `ips.server.protocol=`**`https`**
- `ips.naming.url=`**`https`**
- `ips.notification.url=`**`https`**

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.29 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=https
ips.server.host=smyrna.red.iplanet.com
ips.server.port=8080
ips.profile.host=smyrna.red.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=smyrna.red.iplanet.com
ips.gateway.port=443
ips.virtualhost=smyrna.red.iplanet.com 192.101.107.10
ips.naming.url=https://smyrna.red.iplanet.com:8080/namingservice
ips.notification.url=https://smyrna.red.iplanet.com:8080/notificationser
vice
ips.daemons=securid radius safeword unix skey
securidHelper.port=8943
radiusHelper.port=8944
safewordHelper.port=8945
unixHelper.port=8946
skeyHelper.port=8947
```

```
#


ips.cookie.name=iPlanetPortalServer
ips.locale=en_US
ips.debug=error
ips.version=3.0
ips.basedir=/opt
ips.logdelimiter=&&
```

6. From a terminal window, use a text editor to edit the `magnus.conf` file:

`/opt/netscape/server4/https-`*`servername`*`/config/magnus.conf`

The Security option must be turned on, for the server to talk over SSL.

Edit the entry as shown in bold text:

```
#ServerRoot /opt/netscape/server4/https-smyrna.red.iplanet.com
ServerID https-smyrna.red.iplanet.com
ServerName smyrna.red.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-smyrna.red.iplanet.com/logs/pid
User root
MtaHost localhost
DNS off
Security on
Ciphers +rc4,+rc4export,+rc2,+rc2export,+des,+desede3
SSL3Ciphers
+rsa_rc4_128_md5,+rsa_3des_sha,+rsa_des_sha,+rsa_rc4_40_md5,+rsa_rc2
_40_md5,-rsa_null_md5,+rsa_des_56_sha,+rsa_rc4_56_sha
ACLFile
/opt/netscape/server4/httpacl/generated.https-smyrna.red.iplanet.com.a
cl
ClientLanguage en
AdminLanguage en
DefaultLanguage en
AcceptLanguage off
RqThrottle 1024
StackSize 131072
CGIWaitPid on
CGIWaitPid on
```

7. Stop and restart all the Portal Servers:

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

Changing the Created Multiple Instance Servers to SSL in an Open Portal Environment

The section discuses how to 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 server installation.

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

NOTE Obtain a certificate from any of the certificate authorities supported by the iPlanet Portal Server 3.0. Install it with the iPlanet Web Server. For information on installing a certificate, refer to the *iPlanet Portal Server 3.0 Installation Guide, 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, do the following:

1. Stop and restart all the Portal Servers:

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

2. In the iPlanet Portal Server Administration Console, do the following:
   a. Logon as Super Administrator.
   b. Select the *Server Management* link from the left frame.

c. Select the *Manage Server Profile* link in the right frame.

d. Change the *Platform Server List* attribute.

Change the protocol of the URL for the instance server to be *https*.

https://ipsserver.smyrna.red.iplanet.com@8081

e. Select the *Submit* button, at the bottom of the page, and save the changes.

f. Select the *Continue* button on the *Profile Successfully Updated* page.

3. In a terminal window, open the `/etc/opt/SUNWips` directory.

The directory will contain `platform.conf` files of the type:

```
/etc/opt/SUNWips/platform.conf.smyrna.red.iplanet.com
```

```
/etc/opt/SUNWips/platform.conf.smyrna.red.iplanet.com@8081
```

```
/etc/opt/SUNWips/platform.conf.smyrna.red.iplanet.com@8082
```

4. Make the following changes to the `platform.conf` file of the server that will be configured for SSL,

---

NOTE If the original server running the profile server has been changed to talk over SSL, then the protocol in `ips.naming.url` also needs to be changed to *https*.

From a terminal window, use a text editor to edit the `platform.conf` file for the instance server:

```
/etc/opt/SUNWips/platform.conf.smyrna.red.iplanet.com@8081
```

Edit the following entries, as shown in bold text, in the following example:

- `ips.server.protocol=`**`https`**
- `ips.notification.url=`**`https`**

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.29 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=https
ips.server.host=smyrna.red.iplanet.com
ips.server.port=8081
ips.profile.host=smyrna.red.iplanet.com
ips.gateway.protocol=https
```

```
#
ips.gateway.host=smyrna.red.iplanet.com
ips.gateway.port=443
ips.virtualhost=smyrna.red.iplanet.com 192.101.107.10
ips.naming.url=http://smyrna.red.iplanet.com:8081/namingservice
ips.notification.url=https://smyrna.red.iplanet.com:8081/notificationser
vice
ips.daemons=securid radius safeword unix skey
securidHelper.port=8943
radiusHelper.port=8944
safewordHelper.port=8945
unixHelper.port=8946
skeyHelper.port=8947


ips.cookie.name=iPlanetPortalServer
ips.locale=en_US
ips.debug=error
ips.version=3.0
ips.basedir=/opt
ips.logdelimiter=&&
```

5. The Security option must be turned on, for the server to talk over SSL.

From a terminal window, use a text editor to edit the `magnus.conf` file:

`/opt/netscape/server4/https-`*`servername@port`*`/config/magnus.conf`

Edit the following entries, as shown in bold text, in the following example:

```
#ServerRoot /opt/netscape/server4/https-smyrna.red.iplanet.com
ServerID https-smyrna.red.iplanet.com
ServerName smyrna.red.iplanet.com:8081
Port 8081
LoadObjects obj.conf
RootObject default
ErrorLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-smyrna.red.iplanet.com/logs/pid
User root
MtaHost localhost
DNS off
Security on
Ciphers +rc4,+rc4export,+rc2,+rc2export,+des,+desede3
SSL3Ciphers
+rsa_rc4_128_md5,+rsa_3des_sha,+rsa_des_sha,+rsa_rc4_40_md5,+rsa_rc2
_40_md5,-rsa_null_md5,+rsa_des_56_sha,+rsa_rc4_56_sha
ACLFile
/opt/netscape/server4/httpacl/generated.https-smyrna.red.iplanet.com.a
cl
ClientLanguage en
AdminLanguage en
```

```
DefaultLanguage en
AcceptLanguage off
RqThrottle 1024
StackSize 131072
CGIWaitPid on
CGIWaitPid on
```

6. Stop and restart all the Portal Servers:

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

7. To confirm that the configured server is talking SSL protocol, directly access it at:

```
https://smyrna.red.iplanet.com:8081
```

Configuring User Non-Root

This procedure configures User Non-Root on an iPlanet Portal Server 3.0 server. For the examples shown, the server and gateway are installed on the same system. If installing the gateway on a separate system, perform the same steps on the gateway computer, where appropriate.

NOTE A root-started gateway can run with a non-root user started server.

Installation Examples

When installing the iPlanet Portal Server 3.0 server, select a non-default install. If specifying a non-root userid, enter an unused port number above 1024 for the directory server (default is 389); these examples use port 8389, as all the other iPlanet Portal Server ports are in the 8000's. If a root password is not being implemented, change the super administrator's *userid* from the default *root*. If converting the gateway specify a different port, these examples use port 8443, instead of the default 443. Select a non-default install for the gateway to do this. A sample server and gateway install sessions appears below.

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

Installing iPlanet Portal Server Server

See the *iPlanet Portal Server 3.0 Installation Guide* for more information on installing the iPlanet Portal Server server software.

TIP Non-default entries are shown in bold text.

```
1) Server
2) Gateway
3) Exit

Choice? [3] 1
Installing the iPlanet Portal Server server...
Do you want to use the default settings? [y]/n n

What should the root of the role tree be named? [iplanet.com]
What directory do you want to install the server in? [/opt]

You must install one Profile Server for each
iPlanet Portal Server install group. Please select whether you'd like
to install the Profile server on this machine, or whether this
iPlanet Portal Server server should reference a Profile server
installed on another host.

Should the local machine be the profile server? [y]/n


What is the host name of the machine
where the Profile Server will run? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]
What port should the LDAP server use? [389] 8389
What is the Portal Server super admin user name? [root] Userid

Will/Do you have multiple servers in this install group? y/[n] n

Will/Do you have multiple gateways in this install group? y/[n] n

What is the host name of the machine
where the Gateway Server will run? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]
Should this/these gateway(s) use a web proxy? y/[n]
What port will the gateway encrypting proxy (eproxy) run on? [8443]

Do you want to run SSL between the iPlanet Portal Server
Gateway(s) and Server(s)? y/[n]

What is the Profile Server port? [8080]

What is the Admin Server port? [8888]
```

```
The iPlanet Portal Server admininistration password will be used to
manage and install certificates on the gateway and the server, to
configure the web and LDAP servers, and to allow secure
communication between the gateway(s) and server(s).

Please enter the same password for each server/gateway in this
iPlanet Portal Server install group.

iPlanet Portal Server admin password ( 8 chars minimum ) :
Re-enter iPlanet Portal Server admin password :

Do you want to start the iPlanet Portal Server Server
when installation is complete? y/[n] n

You have selected not to start the iPlanet Portal Server Server.
You will need to start it manually prior to accessing iPlanet Portal Server.


Currently selected settings:
        Portal Server Server       : http://smyrna.red.iplanet.com:8080
        Portal Server Gateway      : smyrna.red.iplanet.com:8443
        Profile Server             : http://smyrna.red.iplanet.com:8080
        LDAP Server                : smyrna.red.iplanet.com:8389
        Web Proxy                  : false
        Role Tree Root             : iplanet.com
        Installation Directory     : /opt
        Start Portal Server Server : n

Are all settings correct? [y]/n
```

Installing iPlanet Portal Server Gateway

See the *iPlanet Portal Server 3.0 Installation Guide* for more information on installing the iPlanet Portal Server gateway software.

TIP Non-default entries are shown in bold text.

```
1) Server
2) Gateway
3) Exit

Choice? [3] 2
Installing the iPlanet Portal Server gateway ...
Install the firewall on this system? [y]/n n

Do you want to use the default settings? [y]/n n
What directory do you want to install the gateway in? [/opt]
```

```
What is the host name of the machine
where the Gateway Server will run? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]
What port will the gateway encrypting proxy (eproxy) run on? [8443]

What is the host name of the machine
where the Profile Server is running? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]

Do you want to run SSL between the iPlanet Portal Server
Gateway(s) and Server(s)? y/[n]

What is the Profile Server port? [8080]
The iPlanet Portal Server admininistration password will be used to
manage and install certificates on the gateway and the server, to
configure the web and LDAP servers, and to allow secure
communication between the gateway(s) and server(s).

Please enter the same password for each server/gateway in this
iPlanet Portal Server install group.

iPlanet Portal Server admin password ( 8 chars minimum ) :
Re-enter iPlanet Portal Server admin password :

IMPORTANT: You must have a self-signed certificate for the SSL server.

This certificate will be used for the SSL connections. You can
generate a request for a certificate from a Certificate Authority (CA)
and install CA certificates after this installation using the
'/opt/SUNWips/bin/certadmin' script.

No certificate was found on this server.
Creating new self-signed certificate...
NOTE: Certificate field entries cannot contain an = character.

What is the name of your organization (ex: Company)? [] iPlanet
What is the name of your organizational unit (ex: division)? [] Eng
What is the name of your City or Locality? [] Santa Clara
What is the name of your State or Province? [] CA
What is the two-letter country code for this unit? [] US


Do you want to start the iPlanet Portal Server Gateway
when installation is complete? y/[n] n

You have selected not to start the iPlanet Portal Server Gateway.
You will need to start it manually prior to accessing iPlanet Portal Server.

Currently selected settings:
        Profile Server              : http://smyrna.red.iplanet.com:80
        Installation Directory      : /opt
        Portal Server Gateway       : smyrna.red.iplanet.com:8443
        Start Portal Server Gateway : n
        Install Firewall            : n
```

```
Are all settings correct? [y]/n

Installing packages
    SUNWwtgwd...

Firewall was not installed. Please make sure the port you
configure this gateway to use (during Server install) is open.

iPlanet Portal Server Gateway has been successfully installed.
done.

Select which component to install:

1) Server
2) Gateway
3) Exit

Choice? [3] 3
```

Configuring User Non-Root on the Server

Perform all steps as root, except as noted.

NOTE Install the iPlanet Portal Server 3.0 server, the gateway, the third-party products, and Service Pack 2 before starting execution of the procedure described below. Failure to do this will result in having to redo some of the install steps.

See the *Installation Instructions* for more information on installing Service Pack 2.

After installing the iPlanet Portal Server software do the following:

1. As root, in a terminal window:

```
# chmod 666 /dev/random
```

NOTE In the following examples for non-root user, substitute *userid* for the *qualified name* of a user.

2. Edit the following file:

`/opt/netscape/server4/http-`*`Servername`*`/config/magnus.conf`.

Change the user `root` to the name of the user login name (`Userid`), as shown in bold text.

```
ServerID https-smyrna.red.iplanet.com
ServerName smyrna.red.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/errors
PidLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/pid
User Userid
MtaHost localhost
DNS off
Security off
Ciphers +rc4,+rc4export,+rc2,+rc2export,+des,+desede3
SSL3Ciphers
+rsa_rc4_128_md5,+rsa_3des_sha,+rsa_des_sha,+rsa_rc4_40_md5,+rsa
_rc2
_40_md5,-rsa_null_md5,+rsa_des_56_sha,+rsa_rc4_56_sha
ACLFile
/opt/netscape/server4/httpacl/generated.https-dianne.red.iplanet
.com.acl
ClientLanguage en
AdminLanguage en
DefaultLanguage en
AcceptLanguage off
RqThrottle 1024
StackSize 131072
CGIWaitPid on
CGIWaitPid on
```

3. As root, in a terminal window, do the following:

The `userid` is the name of the user, and `MyGroupid` is the name of the group the user belongs to. If the user, *Jim*, belongs to the *staff* group, then it would be written as:

```
chown -R Jim:staff /opt/netscape
```

```
# chown -R Userid:MyGroupid /opt/netscape
# chown -R Userid:MyGroupid /opt/SUNWips
```

4. Edit the following file, to change the `localuser` to user login name (`Userid`), as shown in bold text:

`/opt/netscape/directory4/slapd-`*`Servername`*`/config/slapd.conf`

```
################################################################################
# /opt/netscape/directory4/slapd-smyrna/config/slapd.conf
# Netscape Directory Server global configuration file
# Do not modify this file while ns-slapd is running
################################################################################
instancedir     "/opt/netscape/directory4/slapd-smyrna"
errorlog        "/opt/netscape/directory4/slapd-smyrna/logs/errors"
errorlog-logging-enabled        on
plugin syntax on "Telephone Syntax"
"/opt/netscape/directory4/lib/syntax-plugin.
so" tel_init
plugin matchingRule on "Internationalization Plugin"
"/opt/netscape/directory4/l
ib/liblcoll.so" orderingRule_init
"/opt/netscape/directory4/slapd-smyrna/config
/slapd-collations.conf"
plugin syntax on "Integer Syntax"
"/opt/netscape/directory4/lib/syntax-plugin.so
" int_init
plugin syntax on "Distinguished Name Syntax"
"/opt/netscape/directory4/lib/synta
x-plugin.so" dn_init
plugin syntax on "Case Ignore String Syntax"
"/opt/netscape/directory4/lib/synta
x-plugin.so" cis_init
plugin syntax on "Case Exact String Syntax"
"/opt/netscape/directory4/lib/syntax
-plugin.so" ces_init
plugin syntax on "Binary Syntax"
"/opt/netscape/directory4/lib/syntax-plugin.so"
 bin_init
return_exact_case       on
include "/opt/netscape/directory4/slapd-smyrna/config/slapd.at.conf"
include "/opt/netscape/directory4/slapd-smyrna/config/slapd.oc.conf"
include "/opt/netscape/directory4/slapd-smyrna/config/ns-schema.conf"
readonly        off
timelimit       3600
sizelimit       2000
lastmod on
idletimeout     0
ntsynch off
ntsynch-port    5009
ntsynchusessl   on
port    8389
secure-port     636
maxdescriptors  1024
schemacheck     off
enquote_sup_oc  on
security        off
```

```
localuser       Userid
userat  "/opt/netscape/directory4/slapd-smyrna/config/slapd.user_at.conf"
useroc  "/opt/netscape/directory4/slapd-smyrna/config/slapd.user_oc.conf"
accesslog       "/opt/netscape/directory4/slapd-smyrna/logs/access"
```

5. Edit the following file, to change the `User` to user login name (`Userid`), as shown in bold text:

`/opt/netscape/server4/https-servername/config/magnus.conf`

```
#ServerRoot /opt/netscape/server4/https-smyrna.red.iplanet.com
ServerID https-smyrna.red.iplanet.com
ServerName smyrna.red.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-smyrna.red.iplanet.com/logs/pid
User Userid
MtaHost localhost
DNS off
Security on
Ciphers +rc4,+rc4export,+rc2,+rc2export,+des,+desede3
SSL3Ciphers
+rsa_rc4_128_md5,+rsa_3des_sha,+rsa_des_sha,+rsa_rc4_40_md5,+rsa_rc2
_40_md5,-rsa_null_md5,+rsa_des_56_sha,+rsa_rc4_56_sha
ACLFile
/opt/netscape/server4/httpacl/generated.https-smyrna.red.iplanet.com.a
cl
ClientLanguage en
AdminLanguage en
DefaultLanguage en
AcceptLanguage off
RqThrottle 1024
StackSize 131072
CGIWaitPid on
CGIWaitPid on
```

6. If the LDAP Directory Server process is also to run as a user other than *root*, edit the following file, to change the `configuration.nsSuiteSpotUser` to user login name (`Userid`), as shown in bold text:

`/opt/netscape/directory4/admin-serv/config/local.conf (partial example)`

```
nsServerID: admin-serv
userPassword: {SHA}/mZi7HWjvvYwFqgGkIRTOg79/Cc=
serverRoot: /opt/netscape/directory4
serverProductName: Administration Server
serverHostName: smyrna.red.iplanet.com
uniqueMember: cn=admin-serv-smyrna, cn=Netscape Administration
Server, cn=Server
 Group, cn=smyrna.red.iplanet.com, ou=iplanet.com, o=NetscapeRoot
installationTimeStamp: 20000914220659Z
configuration.nsServerPort: 8900
configuration.nsSuiteSpotUser: Userid
configuration.nsServerAddress: 192.18.178.52
configuration.nsAdminEnableEnduser: on
configuration.nsAdminEnableDSGW: on
configuration.nsDirectoryInfoRef: cn=Server Group,
cn=smyrna.red.iplanet.com, ou
=iplanet.com, o=NetscapeRoot
configuration.nsAdminUsers: admin-serv/config/admpw
configuration.nsErrorLog: admin-serv/logs/error
configuration.nsPidLog: admin-serv/logs/pid
configuration.nsAccessLog: admin-serv/logs/access
configuration.nsAdminCacheLifetime: 600
configuration.nsAdminAccessHosts: *.red.iplanet.com
configuration.nsAdminAccessAddresses: 192.18.178.52
configuration.nsAdminOneACLDir: adminacl
configuration.nsDefaultAcceptLanguage: en
configuration.nsClassname:
com.netscape.management.admserv.AdminServer@admserv42
.jar@cn=admin-serv-smyrna, cn=Netscape Administration Server,
cn=Server Group, c
n=smyrna.red.iplanet.com, ou=iplanet.com, o=NetscapeRoot
```

7. As root, in a terminal window, do the following:

```
# chown -R Userid:MyGroupid /etc/opt/SUNWips
# chown -R Userid:MyGroupid /var/opt/SUNWips
```

8. Edit the following file, to comment out line 559, `check_root_user`, as shown in bold text:

`/opt/SUNWips/bin/ipsserver (lines 557 through 573)`

```
#####################################################################

# check_root_user
check_usage $# $2
```

```
# cd out of cdrom dir, so as to make sure no process gets started
with
# cwd = the cdrom, otherwise cdrom can't eject
cd /var/opt/SUNWips/debug

umask 077
get_data

case "$1" in
  'create')
    do_debug $2
    $MULTISERVERINSTALL $1
    ;;
```

9. Rename the following files to prevent the iPlanet Portal Server server from automatically being started by root upon reboot:

```
# mv /etc/rc3.d/S42ipsserver /etc/rc3.d/XS42ipsserver
# mv /etc/rc3.d/K42ipsserver /etc/rc3.d/XK42ipsserver
```

10. Start the iPlanet Portal Server server. From a terminal window, as the non-root user, do the following:

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

Configuring User Non-Root on the Gateway

1. Edit the following file, to comment out lines 174 through 178, as shown in bold text:

/opt/SUNWips/bin/ipsgateway (lines 173 through 184)

```
#####################################################################
# Main starts here
#####################################################################

# if test 'id | /usr/bin/awk '{print $1}'' != "uid=0(root)"
```

```
# then
# echo "'$gettext 'You must be root user to run'' $0."
# exit 0
# fi

umask 077
ulimit -n 10240

case "$1" in
'start')
```

2. Edit the following file, to add `ips.gateway.user=`*`Userid`*, as shown in bold text:

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

NOTE Must be a valid *userid* on the iPlanet Portal Server gateway. If `ips.gateway.user` does not match the *userid* for which the procedure has been applied, permission problems will result.

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.29 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=http
ips.server.host=smyrna.red.iplanet.com
ips.server.port=8080
ips.profile.host=smyrna.red.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=smyrna.red.iplanet.com
ips.gateway.user=Userid
ips.gateway.port=8443
ips.virtualhost=smyrna.red.iplanet.com 192.101.107.10
ips.naming.url=http://smyrna.red.iplanet.com:8080/namingservice
ips.notification.url=http://smyrna.red.iplanet.com:8080/notificationserv
ice
ips.daemons=securid radius safeword unix skey
securidHelper.port=8943
radiusHelper.port=8944
safewordHelper.port=8945
unixHelper.port=8946
skeyHelper.port=8947


ips.cookie.name=iPlanetPortalServer
ips.locale=en_US
ips.debug=error
```

```
#
ips.version=3.0
ips.basedir=/opt
ips.logdelimiter=&&
```

3. Rename the following files to prevent the iPlanet Portal Server gateway from automatically being started by root upon reboot:

```
# mv /etc/rc3.d/S90ipsgateway /etc/rc3.d/XS90ipsgateway
# mv /etc/rc3.d/K90ipsgateway /etc/rc3.d/XK90ipsgateway
```

4. Start the iPlanet Portal Server server and gateway. From a terminal window, as the non-root user, do the following:

```
% /opt/SUNWips/bin/ipsserver start
% /opt/SUNWips/bin/ipsgateway start
```

Non-Root Error Messages

Running as a non-root user, there will be error messages on the server and gateway. These messages are expected, and workarounds are offered when appropriate.

Server Error Messages

a. Because a non-root user may not set the maximum file descriptors to a value larger than 1024. The ipsserver script attempts to set it to 10240.

```
/opt/SUNWips/bin/ipsserver: ulimit: exceeds allowable limit
```

b. Failure to start the `doSKey`. This error is not common.

```
starting auth helpers ... ld.so.1: /opt/SUNWips/bin/doSKey:
fatal: libskey.so: open failed: No such file or directory
```

A workaround is to start the doSKey manually as non-root *userid* in /bin/sh:

```
LD_LIBRARY_PATH=/opt/SUNWips/bin
export LD_LIBRARY_PATH
/opt/SUNWips/bin/doSKey -c 8947
```

c. When running as a non-root user, if locally-administered UNIX userid is to be authenticated, then:

```
# chown root:sys /opt/SUNWips/bin/doUnix
# chmod 4555 /opt/SUNWips/bin/doUnix
```

The chmod command setuid's `doUnix`, so that it runs as though `root`, even when started by non-root users.

Gateway Error Messages

a. Non-root users appear to be able to only set ulimit -n 1024 as a maximum number. Running as a non-root user will restrict how much load the gateway can simultaneously handle.

```
/dev/fd/some_number: ulimit: bad ulimit
```

b. The `/opt/SUNWips/bin/ipshttpd` and `/opt/SUNWips/bin/ipsnetletd` scripts should have ulimit commands in them to increase the number of file descriptors the Netlet Proxy and HTTP Proxy, respectively, so that they may support more users. Running as non-root users, they are restricted to the 1024 limit, as well as the >1024 port number restriction.

Configuring User Nobody

To configure user `Nobody` on an iPlanet Portal Server 3.0 server, in the following examples, the server and gateway are installed on the same system. If installing the gateway on a separate system, perform the same steps on that system.

Specifying `nobody` as the owner of the iPlanet Portal Server files is a special case, as `nobody` has an impossible resultant (encrypted) password. The user must be `root` to manipulate and execute files `nobody` owns.

When the iPlanet Portal Server server is to run as *nobody*, the server can be configured to listen on port 80, the default web server port. The LDAP server can also run on the default port 389, and the gateway on the default SSL port 443.

Installation Examples

When installing the iPlanet Portal Server 3.0 server, select a non-default install. The following procedures are install examples for both the server and the gateway.

Installing iPlanet Portal Server Server

See the *iPlanet Portal Server 3.0 Installation Guide* for more information on installing the iPlanet Portal Server server.

TIP Non-default entries are shown in bold text.

```
1) Server
2) Gateway
3) Exit

Choice? [3] 1
Installing the iPlanet Portal Server server...
Do you want to use the default settings? [y]/n n

What should the root of the role tree be named? [iplanet.com]
What directory do you want to install the server in? [/opt]

You must install one Profile Server for each
iPlanet Portal Server install group. Please select whether you'd like
```

```
to install the Profile server on this machine, or whether this
iPlanet Portal Server server should reference a Profile server
installed on another host.

Should the local machine be the profile server? [y]/n


What is the host name of the machine
where the Profile Server will run? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]
What port should the LDAP server use? [389]
What is the Portal Server super admin user name? [root]

Will/Do you have multiple servers in this install group? y/[n] n

Will/Do you have multiple gateways in this install group? y/[n] n

What is the host name of the machine
where the Gateway Server will run? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]
Should this/these gateway(s) use a web proxy? y/[n]
What port will the gateway encrypting proxy (eproxy) run on? [443]

Do you want to run SSL between the iPlanet Portal Server
Gateway(s) and Server(s)? y/[n]

What is the Profile Server port? [8080]80

What is the Admin Server port? [8888]

The iPlanet Portal Server admininistration password will be used to
manage and install certificates on the gateway and the server, to
configure the web and LDAP servers, and to allow secure
communication between the gateway(s) and server(s).

Please enter the same password for each server/gateway in this
iPlanet Portal Server install group.

iPlanet Portal Server admin password ( 8 chars minimum ) :
Re-enter iPlanet Portal Server admin password :

Do you want to start the iPlanet Portal Server Server
when installation is complete? y/[n] n

You have selected not to start the iPlanet Portal Server Server.
You will need to start it manually prior to accessing iPlanet Portal Server.


Currently selected settings:
        Portal Server Server       : http://smyrna.red.iplanet.com:80
        Portal Server Gateway      : smyrna.red.iplanet.com:443
        Profile Server             : http://smyrna.red.iplanet.com:80
        LDAP Server                : smyrna.red.iplanet.com:389
        Web Proxy                  : false
        Role Tree Root             : iplanet.com
```

```
        Installation Directory     : /opt
        Start Portal Server Server : n

Are all settings correct? [y]/n
```

Installing iPlanet Portal Server Gateway

See the *iPlanet Portal Server 3.0 Installation Guide* for more information on installing the iPlanet Portal Server gateway.

TIP Non-default entries are shown in bold text.

```
1) Server
2) Gateway
3) Exit

Choice? [3] 2
Installing the iPlanet Portal Server gateway ...
Install the firewall on this system? [y]/n n

Do you want to use the default settings? [y]/n n
What directory do you want to install the gateway in? [/opt]

What is the host name of the machine
where the Gateway Server will run? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]
What port will the gateway encrypting proxy (eproxy) run on? [443]

What is the host name of the machine
where the Profile Server is running? [smyrna]
What is the sub-domain name ("." for none)? [red]
What is the domain name? [iplanet.com]

Do you want to run SSL between the iPlanet Portal Server
Gateway(s) and Server(s)? y/[n]

What is the Profile Server port? [80]
The iPlanet Portal Server admininistration password will be used to
manage and install certificates on the gateway and the server, to
configure the web and LDAP servers, and to allow secure
communication between the gateway(s) and server(s).

Please enter the same password for each server/gateway in this
iPlanet Portal Server install group.

iPlanet Portal Server admin password ( 8 chars minimum ) :
Re-enter iPlanet Portal Server admin password :
```

```
IMPORTANT: You must have a self-signed certificate for the SSL server.

This certificate will be used for the SSL connections. You can
generate a request for a certificate from a Certificate Authority (CA)
and install CA certificates after this installation using the
'/opt/SUNWips/bin/certadmin' script.

No certificate was found on this server.
Creating new self-signed certificate...
NOTE: Certificate field entries cannot contain an = character.

What is the name of your organization (ex: Company)? [] iPlanet
What is the name of your organizational unit (ex: division)? [] Eng
What is the name of your City or Locality? [] Santa Clara
What is the name of your State or Province? [] CA
What is the two-letter country code for this unit? [] US


Do you want to start the iPlanet Portal Server Gateway
when installation is complete? y/[n] n

You have selected not to start the iPlanet Portal Server Gateway.
You will need to start it manually prior to accessing iPlanet Portal Server.

Currently selected settings:
        Profile Server              : http://smyrna.red.iplanet.com:80
        Installation Directory      : /opt
        Portal Server Gateway       : smyrna.red.iplanet.com:443
        Start Portal Server Gateway : n
        Install Firewall            : n

Are all settings correct? [y]/n

Installing packages
    SUNWwtgwd...

Firewall was not installed. Please make sure the port you
configure this gateway to use (during Server install) is open.

iPlanet Portal Server Gateway has been successfully installed.
done.

Select which component to install:

1) Server
2) Gateway
3) Exit

Choice? [3]
```

Configuring User Nobody on the Server

Perform all steps as root, except as noted.

NOTE Install the iPlanet Portal Server 3.0 server, the gateway, the third-party products, and Service Pack 2 before starting execution of the procedure described below. Failure to do this will result in having to redo some of the install steps.

See the *Installation Instructions* for more information on installing Service Pack 2.

After installing the iPlanet Portal Server software do the following:

1. As root, in a terminal window, do the following:

```
# chmod 666 /dev/random
```

2. Edit the following file:

`/opt/netscape/server4/http-`*`servername`*`/config/magnus.conf`

Change the user `root` to the name of the user `nobody`, as shown in bold text.

```
ServerID https-smyrna.red.iplanet.com
ServerName smyrna.red.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/errors
PidLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/pid
User nobody
MtaHost localhost
DNS off
Security off
Ciphers +rc4,+rc4export,+rc2,+rc2export,+des,+desede3
SSL3Ciphers
+rsa_rc4_128_md5,+rsa_3des_sha,+rsa_des_sha,+rsa_rc4_40_md5,+rsa
_rc2
_40_md5,-rsa_null_md5,+rsa_des_56_sha,+rsa_rc4_56_sha
ACLFile
/opt/netscape/server4/httpacl/generated.https-dianne.red.iplanet
.com.acl
ClientLanguage en
AdminLanguage en
DefaultLanguage en
```

```
AcceptLanguage off
RqThrottle 1024
StackSize 131072
CGIWaitPid on
CGIWaitPid on
```

3. As root, in a terminal window, do the following:

```
# chown -R nobody:nobody /opt/netscape
# chown -R nobody:nobody /opt/SUNWips
```

4. Edit the following file, to change the `localuser` to nobody, as shown in bold text:

`/opt/netscape/directory4/slapd-`*`servername`*`/config/slapd.conf`

```
################################################################################
# /opt/netscape/directory4/slapd-smyrna/config/slapd.conf
# Netscape Directory Server global configuration file
# Do not modify this file while ns-slapd is running
################################################################################
instancedir     "/opt/netscape/directory4/slapd-smyrna"
errorlog        "/opt/netscape/directory4/slapd-smyrna/logs/errors"
errorlog-logging-enabled        on
plugin syntax on "Telephone Syntax"
"/opt/netscape/directory4/lib/syntax-plugin.
so" tel_init
plugin matchingRule on "Internationalization Plugin"
"/opt/netscape/directory4/l
ib/liblcoll.so" orderingRule_init
"/opt/netscape/directory4/slapd-smyrna/config
/slapd-collations.conf"
plugin syntax on "Integer Syntax"
"/opt/netscape/directory4/lib/syntax-plugin.so
" int_init
plugin syntax on "Distinguished Name Syntax"
"/opt/netscape/directory4/lib/synta
x-plugin.so" dn_init
plugin syntax on "Case Ignore String Syntax"
"/opt/netscape/directory4/lib/synta
x-plugin.so" cis_init
plugin syntax on "Case Exact String Syntax"
"/opt/netscape/directory4/lib/syntax
-plugin.so" ces_init
```

```
plugin syntax on "Binary Syntax"
"/opt/netscape/directory4/lib/syntax-plugin.so"
 bin_init
return_exact_case       on
include "/opt/netscape/directory4/slapd-smyrna/config/slapd.at.conf"
include "/opt/netscape/directory4/slapd-smyrna/config/slapd.oc.conf"
include "/opt/netscape/directory4/slapd-smyrna/config/ns-schema.conf"
readonly        off
timelimit       3600
sizelimit       2000
lastmod on
idletimeout     0
ntsynch off
ntsynch-port    5009
ntsynchusessl   on
port    389
secure-port     636
maxdescriptors  1024
schemacheck     off
enquote_sup_oc  on
security        off
localuser       nobody
userat  "/opt/netscape/directory4/slapd-smyrna/config/slapd.user_at.conf"
useroc  "/opt/netscape/directory4/slapd-smyrna/config/slapd.user_oc.conf"
accesslog       "/opt/netscape/directory4/slapd-smyrna/logs/access"
```

5. Edit the following file, to change the `User` to nobody, as shown in bold text:

`/opt/netscape/server4/https-`*`servername`*`/config/magnus.conf`

```
#ServerRoot /opt/netscape/server4/https-smyrna.red.iplanet.com
ServerID https-smyrna.red.iplanet.com
ServerName smyrna.red.iplanet.com
Port 80
LoadObjects obj.conf
RootObject default
ErrorLog
/opt/netscape/server4/https-smyrna.red.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-smyrna.red.iplanet.com/logs/pid
User nobody
MtaHost localhost
DNS off
Security on
Ciphers +rc4,+rc4export,+rc2,+rc2export,+des,+desede3
SSL3Ciphers
+rsa_rc4_128_md5,+rsa_3des_sha,+rsa_des_sha,+rsa_rc4_40_md5,+rsa_rc2
_40_md5,-rsa_null_md5,+rsa_des_56_sha,+rsa_rc4_56_sha
ACLFile
/opt/netscape/server4/httpacl/generated.https-smyrna.red.iplanet.com.a
cl
ClientLanguage en
```

```
AdminLanguage en
DefaultLanguage en
AcceptLanguage off
RqThrottle 1024
StackSize 131072
CGIWaitPid on
CGIWaitPid on
```

6. If the LDAP Directory Server process is also to run as a user other than *root*, edit the following file, to change the `configuration.nsSuiteSpotUser` to `nobody`, as shown in bold text:

`/opt/netscape/directory4/admin-serv/config/local.conf`

```
nsServerID: admin-serv
userPassword: {SHA}/mZi7HWjvvYwFqgGkIRTOg79/Cc=
serverRoot: /opt/netscape/directory4
serverProductName: Administration Server
serverHostName: smyrna.red.iplanet.com
uniqueMember: cn=admin-serv-smyrna, cn=Netscape Administration
Server, cn=Server
 Group, cn=smyrna.red.iplanet.com, ou=iplanet.com, o=NetscapeRoot
installationTimeStamp: 20000914220659Z
configuration.nsServerPort: 8900
configuration.nsSuiteSpotUser: nobody
configuration.nsServerAddress: 192.18.178.52
configuration.nsAdminEnableEnduser: on
configuration.nsAdminEnableDSGW: on
configuration.nsDirectoryInfoRef: cn=Server Group,
cn=smyrna.red.iplanet.com, ou
=iplanet.com, o=NetscapeRoot
configuration.nsAdminUsers: admin-serv/config/admpw
configuration.nsErrorLog: admin-serv/logs/error
configuration.nsPidLog: admin-serv/logs/pid
configuration.nsAccessLog: admin-serv/logs/access
configuration.nsAdminCacheLifetime: 600
configuration.nsAdminAccessHosts: *.red.iplanet.com
configuration.nsAdminAccessAddresses: 192.18.178.52
configuration.nsAdminOneACLDir: adminacl
configuration.nsDefaultAcceptLanguage: en
configuration.nsClassname:
com.netscape.management.admserv.AdminServer@admserv42
.jar@cn=admin-serv-smyrna, cn=Netscape Administration Server,
cn=Server Group, c
n=smyrna.red.iplanet.com, ou=iplanet.com, o=NetscapeRoot
```

7. As root, in a terminal window:

```
# chown -R nobody:nobody /etc/opt/SUNWips
# chown -R nobody:nobody /var/opt/SUNWips
```

8. To set the `http` and `netlet proxies` on the server to run as *nobody*, edit the `/etc/opt/SUNWips/platform.conf` file, as shown in bold text:

- `ips.httpproxy.user=nobody`
- `ips.netletproxy.user=nobody`

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.29 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=http
ips.server.host=smyrna.red.iplanet.com
ips.server.port=80
ips.profile.host=smyrna.red.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=smyrna.red.iplanet.com
ips.gateway.port=443
ips.virtualhost=smyrna.red.iplanet.com 192.101.107.10
ips.naming.url=http://smyrna.red.iplanet.com:8080/namingservice
ips.notification.url=http://smyrna.red.iplanet.com:8080/notificationserv
ice
ips.daemons=securid radius safeword unix skey
securidHelper.port=8943
radiusHelper.port=8944
safewordHelper.port=8945
unixHelper.port=8946
skeyHelper.port=8947


ips.httpproxy.user=nobody
ips.netletproxy.user=nobody

ips.cookie.name=iPlanetPortalServer
ips.locale=en_US
ips.debug=error
ips.version=3.0
ips.basedir=/opt
ips.logdelimiter=&&
```

9. Start the iPlanet Portal Proxy server. From a terminal window, as root, do the following:

```
# /opt/SUNWips/bin/ipshttpd stop
# /opt/SUNWips/bin/ipsnetletd stop
# /opt/SUNWips/bin/ipshttpd start
# /opt/SUNWips/bin/ipsnetletd start
```

Configuring User Nobody on the Gateway

The following steps are for configuring user nobody on the gateway, when the gateway is not installed on the same system as the server.

NOTE Install the iPlanet Portal Server 3.0 server, the gateway, the third-party products, and Service Pack 2 before starting execution of the procedure described below. Failure to do this will result in having to redo some of the install steps.

See the *Installation Instructions* for more information on installing Service Pack 2.

After installing the iPlanet Portal Server software do the following on the gateway:

1. As root, in a terminal window, do the following:

```
# chmod 666 /dev/random
# chown -R nobody:nobody /etc/opt/SUNWips
# chown -R nobody:nobody /var/opt/SUNWips
# chown -R nobody:nobody /opt/SUNWips
```

2. Edit the `/etc/opt/SUNWips/platform.conf` file, as shown in bold text:

- `ips.gateway.user=nobody`

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.29 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=http
```

```
#
ips.server.host=smyrna.red.iplanet.com
ips.server.port=80
ips.profile.host=smyrna.red.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=smyrna.red.iplanet.com
ips.gateway.port=443
ips.virtualhost=smyrna.red.iplanet.com 192.101.107.10
ips.naming.url=http://smyrna.red.iplanet.com:8080/namingservice
ips.notification.url=http://smyrna.red.iplanet.com:8080/notificationserv
ice
ips.daemons=securid radius safeword unix skey
securidHelper.port=8943
radiusHelper.port=8944
safewordHelper.port=8945
unixHelper.port=8946
skeyHelper.port=8947


ips.gateway.user=nobody

ips.cookie.name=iPlanetPortalServer
ips.locale=en_US
ips.debug=error
ips.version=3.0
ips.basedir=/opt
ips.logdelimiter=&&
```

When the gateway is configured as user *nobody*, do the following to workaround an invalid session condition when the gateway does a restart:

```
# chmod 4555 /etc/init.d/ipsgateway
```

Special Case Configurations

When the iPlanet Portal Server server and gateway are installed on the same system, and the server has been configured to run as user *nobody or non-root*, BUT the gateway was configured to run on a different *Userid,* do the following:

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

```
# chmod 777 /opt/SUNWips
# chmod 777 /opt/SUNWips/bin
# chmod -R 777 /opt/SUNWips/lib
# chmod -R 777 /opt/SUNWips/locale
# chmod 555 /opt/SUNWips/bin/ipsgateway
# chmod 555 /opt/SUNWips/bin/checkport
# chmod 777 /etc/opt/SUNWips
# chmod 777 /etc/opt/SUNWips
# chmod 444 /etc/opt/SUNWips/.rppass
# chmod 444 /etc/opt/SUNWips/.application
# chmod 666 /etc/opt/SUNWips/rp.keystore
# chmod 444 /etc/opt/SUNWips/platform.conf
# chmod 666 /etc/opt/SUNWips/properties.file
# chmod -R 777 /var/opt/SUNWips/debug
```

Installing and Enabling Multiple Locale for a Domain

This feature provides support for multiple locales per installation. That is, the administrator can specify the locale for domains, roles, and users. For example, one iPS installation with three locale packages installed allows the admin to set up three domains, one for each locale. User's registering in domain1 will use locale 1, users registering in domain2 will use locale2 and so on.

Every time you install a new locale, you must run the `ipsadmin` command to update the `iwtPlatform` attribute. The `iwtPlatform` attribute lists all the locales available for the user. For instance:

```
Attribute for available locale:
    <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 the value for this attribute may look like `en_US` or `ja_JA`, users only see the common name, for instance, English (United States), of the available locale.

To specify the locale for domains:

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

Supporting SSL for Authentication in an Open Portal

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). That is, a portal configured to return all content on the desktop using http can still support user registration or login through https.

The iPlanet Portal Server will support this configuration by running two instances of iPlanet Portal Server; one instance running http and the other instance running https.

See Configuring Multiple Instances of iPlanet Portal Server for detailed information on setting up two instances of iPlanet Portal Server.

After setting up the server instances, convert the second instance of the server to SSL. See Configuring Multiple Instances of iPlanet Portal Server. After configuring the second instance, update the user profiles to redirect to the non-SSL server (instance) after initial authentication. To do this:

To ensure that all unauthenticated sessions on the non-SSL server (instance) are redirected to the SSL server (instance), edit the `platform.conf` file in `/etc/opt/SUNWips/` directory:

1. Become superuser and change directory to `/etc/opt/SUNWips`.
2. In the `platform.conf` file, change the value for the `ips.nosession.url` from `/login` to:

   `http://`*`servername:port`*`/login` (for example port 8080)

   or

   `https://`*`servername:port`*`/login` (for example port 8081)

Here `servername` refers to the host name of the SSL server instance and `port` refers to the port where the server instance is running.

All registrations and login will be directed to the *https server*, and all desktop redirects will be sent to the *http server*.

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.29 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=http
ips.server.host=smyrna.red.iplanet.com
ips.server.port=8080
ips.profile.host=smyrna.red.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=smyrna.red.iplanet.com
ips.gateway.port=8443
ips.virtualhost=smyrna.red.iplanet.com 192.101.107.10
ips.naming.url=http://smyrna.red.iplanet.com:8080/namingservice
ips.notification.url=http://smyrna.red.iplanet.com:8080/notifica
tionservice
ips.daemons=securid radius safeword unix skey
securidHelper.port=8943
radiusHelper.port=8944
safewordHelper.port=8945
unixHelper.port=8946
skeyHelper.port=8947


ips.cookie.name=iPlanetPortalServer
```

```
#
ips.locale=en_US
ips.debug=error
ips.version=3.0
ips.basedir=/opt
ips.logdelimiter=&&
ips.profile.port=8080
ips.nosession.url=https://servername:8081/login
ips.pcookie.name=iPSpCookie
ips.gateway.retries=6
```

3. Edit `/etc/opt/SUNWips/desktop/default/iwtLoginProvider/display.html` as shown in bold text:

   `<FORM ACTION="https:smyrna.red.iplanet.com:444/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://smyrna.red.iplanet.com:444/login/Membership?arg =newsession&page=1&Submit=New%20User">Sign Me Up</A></FONT>`

4. In the administration console set the user profile to point to the non-SSL port on the open portal. Do the following instructions:

   a. Log in to the administration console and select *Manage Domains*.

   b. Select your *domain* and select *User* (under Profiles).

   c. Select *Show Advanced Options*.

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

      `http://servername:port/DesktopServlet`

   e. Select the *Submit* button, at the bottom of the page, and save the changes.

   f. Select the *Continue* button on the *Profile Successfully Updated* page.

Anonymous Authentication

For iPlanet Portal Server 3.0 Service Pack 2, an anonymous authentication module has been added.

This zero-page `auth module` is specifically intended for supporting *open portal* installations, where just the iPlanet Portal Server server is installed without a gateway, although anonymous authentication may be used with a secure portal.

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

There is also a feature where a list of userid's that may login to the anonymous user's desktop can be specified. The list may be entered or modified through the administration console:

Managing Anonymous Username

If *userid* is in the *List of Anonymous Usernames*, then access to the anonymous user's desktop is granted, with the session assigned to the specified userid. If the *userid* is not in the *List of Anonymous Usernames*, then the anonymous desktop is still displayed, but the session is assigned to the *userid* specified in the *Default Anonymous Username.*

Modifying Default Anonymous Usernames

1. Logon as Super Administrator.
2. Select the *Manage Domains* link from the left frame.
3. In the *Portal Server Domains* page, do the following:

   Select the domain.
4. In the *Domain, Role and Users* page:
   a. Expand *Profiles* link.
   b. Expand *Authentication* link.
5. In the *Authentication* Menu:
   a. Select *Anonymous*
6. Select *Show Advanced Options* at the bottom of the page.
   a. In the *List Anonymous User Names*, add a userid in following form:

`http://server:port/login/mydomain?username=userid`

   b. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.
7. Select the *Continue* button on the *Profile Successfully Updated* page.

Adding Userid to Default Anonymous Usernames

1. Logon as Super Administrator.
2. Select the *Manage Domains* link from the left frame.

3. In the *Domain, Role and Users* page:
   a. Expand *Profiles* link.
   b. Expand *Authentication* link.
4. In the *Authentication* Menu:
   a. Select *Anonymous*
5. Select *Show Advanced Options* at the bottom of the page.
   a. In the *Default Anonymous User Names*, add a userid.
   b. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.
6. Select the *Continue* button on the *Profile Successfully Updated* page.

Redirecting the User Using the goto Parameter

The goto parameter enables applications to instruct auth to redirect the user to a URL other than the default URL stored in the user's profile upon login or logout.

When a user authenticates, the application will prompt the user to specify the URL to which the user will be redirected to instead of sending the user to the default desktop URL stored in the user's profile.

The `goto` parameter allows the calling application to specify where the user will be redirected upon successful login. For example, if an application wanted the user to be redirected to `my.yahoo.com` after successful authentication, the login link will be the following:

```
http://server.domain:port/login?goto=http://my.netscape.com
```

An api developer can include the `goto` parameter used in conjunction with the logout URL to specify where the user should be redirected upon logout. If the application wanted to redirect the user to `nasdaq.com` after logging out, the logout link will be the following:

```
http://server.domain:port/logout?goto=http://nasdaq.com
```

To demonstrate the `goto` parameter, open a browser and in the Location field, enter:

`http://<server.domain>:<port>/login?goto=<URL>`

The `goto` parameter is valid for this auth session only and it will not change the default URL stored in the user's profile.

Setting Persistent Cookies

This enhancement enables setting persistent cookies. That is, when a user closes the browser or when the user's session expires, the user will not be required to re-authenticate.

Persistent Cookie Mode is set by the user by selecting the *Remember My Username and Password* checkbox using the Login Channel. If the Persistent Cookie Mode is enabled:

- The user will not be required to login when re-opening the browser
- When the user subsequently revisits the *my_site*.com URL, the user's personal desktop will be immediately displayed without any login process.

However, if the user explicitly logs out, login is required on the next visit.

To set persistent cookie for a domain:

1. Log in to the administration console and select *Manage Domains*.
2. Select your domain and select *Profiles* and *Authentication*.
3. Select *Show Advanced Options* in the *Profile:Auth* page.
4. Specify the maximum age of the cookie in the *Persistent Cookie MaxAge Value* text box.

   Specify the cookie expiry time in seconds.
5. Select the *Enable Persistent Cookie Mode* check box.

   This will enable the persistent cookie mode for users in this domain.

To demonstrate the persistent cookie mode, open a browser and in the Location field, enter:

`http://server.domain:port/login/domain?iPSPCookie=yes`

If the value for the parameter `iPSPCookie` is yes, then the persistent cookie mode is enabled.

Extending Authentication

No authentication is required if a valid session is present. That is, if a user wanted to switch from anonymous user to a 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. In Service Pack 2 this has been corrected.

When a registered user authenticates from the anonymous desktop, the application will get the information about the user and present the user's desktop from the user's profile. When a new user registers from the anonymous desktop, the user's current session (from the anonymous desktop) is destroyed before calling the `auth module` in the URL for the user's default desktop. 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 will send the following URL to allow an anonymous user to register with the membership module:

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

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

Setting the Default URL

This feature allows setting up the user's default URL in the pluggable interface in addition to the user's profile. This method doesn't change the default URL in the user's profile. When the user authenticates successfully, the user will be 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. This method does not change the user's attribute in the user profile. This method will override the goto parameter. See Redirecting the User Using the goto Parameter, in the initial auth URL.

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

Here the URL parameter is replaced with the user's default URL. For example:

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

where *`http://www.yahoo.com`* is set as the user's default URL.

Getting and Setting User Properties

This feature allows the authentication module to set and get user properties from the user session. Two new methods called `setUserSessionProperty` and `getUserSessionProperty` in the `pluggable auth` API enables authentication modules to get and set properties in the user session. This allows authentication modules to communicate with channels, applications, or other authentication modules by setting session properties. For example, a custom authentication module may add the user password to the session, so that an application may retrieve this property, for single sign on at a later time.

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

Here the parameter name is the property name and the parameter value is the property value.

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

Here the parameter name is the property name and this returns the property value.

Using E-mail Address As User's Profile ID

This feature provides the ability to use an E-mail address on the certificate as the user's profile ID.

To use the E-mail address as profile ID:

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 *what field in cert to use to access user info in profile*.

   This allows the administrator to specify what to use to access the user's profile id. If *email address* is selected, the `cert auth module` will search for the field `emailAddr` in the certificate's user subject `dn` field for the attribute tag `emailaddr` and use its value to access the user's profile id.

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

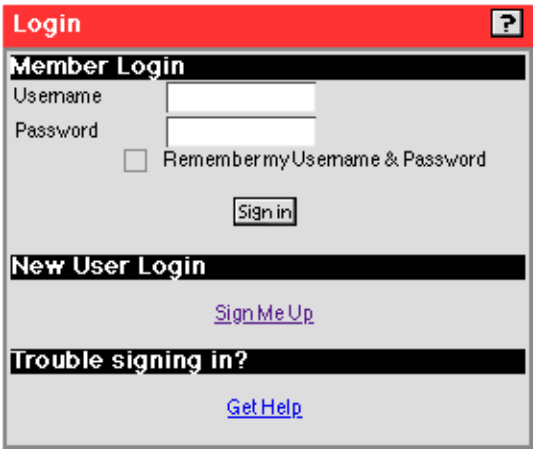
5. Select the *Submit* button.

Login Channel

The Portal Server 3.0 currently contains a membership authentication module which is useful for open portal installations. Combined with an *anonymous* user, unregistered users can view static content in a portal, and registered users can log in and view personalized content. The addition of a login channel on the desktop provides a simple way for registered users to access the portal while allowing non-registered users to still view static content and provides a simple mechanism to register with the portal and receive personalized pages.

The login channel also provides an option to the user to enable persistent cookies. Persistent cookie support is a feature of the authentication system which puts the user's login information into a cookie so that the user can be automatically logged in for subsequent sessions. The channel provides a check box that allows the user to enable persistent cookie support for their login, based on whether or not this domain allows for this option.

The user interface for the login channel does not have an edit page, as there are no user editable preferences.



JavaServer Page Provider

The JavaServer™ Page Provider (JSPProvider) feature allows providers for desktop channels to be written using JavaServer Pages (JSP).

Support for JSP-based channels is provided through a class called JSPProvider. A JSP Provider-based channel has, in addition to the regular attributes that other channels have, the following configured attributes:

- `contentPage` - the JSP that is used to generate the channel content using the `getContent` method
- `editPage` - the JSP that is used to generate the edit page content using the `getEdit` method
- `processPage` - the JSP that is used to process the results of an edit page using the `processEdit` method
- The `contentPage` JSP generates the HTML content for the channel. The generated HTML must contain only those tags that are appropriate for display within a channel.
- The `editPage` JSP generates the internal content for the edit form that is displayed when the user clicks the Edit button for the channel. This page is optional, and if not specified, the `isEditable` method for the provider returns false. As with the `contentPage` JSP, the JSP has access to iPlanet Portal Server platform services.
- The `contentPage` and `editPage` JSPs can be used in various combinations. For example, a JSP can be used to generate the content while the edit page can be generated using Java code in the provider class.

There are several options for handling the processing of an edit form for a JSP-based provider. Typically, 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 either a display of the desktop (in the case of success) or a display of the edit page, possibly with some error information for the user (in the case of a failure). To handle the processing of an edit form, the JSP-based provider has the following options:

- Define a `processPage` JSP. If defined, this JSP is invoked via a POST request and the JSP can process 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.
- Extend the JSPProvider class and implement the `processEdit` method. The `processPage` attribute is left blank.

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 for the user using the same algorithm as for other desktop templates including the locale setting.

In the following example:

- The user's locale is `de_DE`
- Desktop type is `SunBlue`
- A JSP attribute is set to `myChan/chan.jsp`

The system searches for the following JSP files:

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

For more information on implementing JSP-based channels, see the javadocs that are shipped with Service Pack 2.

Tabbed Desktop

Service Pack 2 offers tab functionality to the user desktop. The desktop can use the tabs feature to organize content. Tabs are not active by default, and must be turned on for any given domain. The Tab Provider is enabled by the super administrator through the Administrator's console, and tabs are then configured, or removed in a chosen domain. Tabbed desktop pages can be individually modified to configure the desktop in a personalized way, as shown in the following procedures.

Configuring the Tab Desktop in the Administration Console

This procedure presumes that *Tab Desktop* is not configured in a particular domain. To enable the *Tab Desktop*, do the following in the iPlanet Portal Server Administration Console:

1. Log on as Super Administrator.
2. Select the *Manage Domains* link from the left frame.
3. Select a *domain* in the right frame, to configure the *Tab Desktop*.
4. Expand the *Applications* link in the right frame.
5. Select the *Desktop* link.
6. Select *Show Advanced Options* at the bottom of the *Profile: Desktop* page.
7. In the *Profile: Desktop* page, scroll down to the *Channels* Field.
8. If the *iwtTabProvider* **is shown** in the *Available Channels* window then do the following:
   a. Highlight *iwtTabProvider* in the *Available Channels* window.
   b. Select the arrow, and the *iwtTabProvider* should then appear in the *Selected Channels* field.
9. If the *iwtTabProvider* **is not shown** in the *Available Channels* window then do the following:
   a. In the *New Channel Name* window, enter a new channel name, *iwtTabProvider*.
   b. In the *Provider Class Name* window, enter a new provider class:

      ```
      com.iplanet.portalserver.providers.tab.TabProvider
      ```

   c. Select *Add*.
   d. *iwtTabProvider* will now be shown in the *Available Channels* window.
   e. Highlight *iwtTabProvider* in the *Available Channels* window.
   f. Select the arrow, and the *iwtTabProvider* should then appear in 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. See the following 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 will always be 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 will contain. The following string is an example. Change the name, providers, and description to create a custom tab:

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

13. In the *Tab Pattern* field, enter in a string, the name of a tab content template, and the providers to be included. See Step 12.

14. In the *Make From Scratch Tab* field, enter a suitable heading title, and all the content providers that will appear on the *Edit Tab Provider* page. See the following string as an 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, enter a number.

    This will be the total number of tabs that may be on the desktop. **4** is a default value.

16. Select the *Submit* button, at the bottom of the page, and save the changes.

17. Select the *Continue* button on the *Profile Successfully Updated* page.

Configuring the Tab Desktop on the Desktop

Any user can configure the tabs on the desktop. The tab's channel edit page allows a user to create, rename, or remove tabs from their desktop. Additionally a user can select which tab should be present on the initial desktop page.

1. As a user, log in to the iPlanet Portal Server desktop.

2. In the desktop, select the *Edit* button, on the right of the tab banner.

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

Creating Customized Tabs

1. In the *Edit Tab Provider* page, do the following:

   a. In the *Tab Name* field, enter the name of the tab being created.

b. In the *Tab Topics* field, select the radio button for *Make From Scratch.*

c. Select *Finished* at the bottom of the page.

2. In the *Channels* page, do the following:

a. Select the desired *channels*, to customize the desktop page.

Thin and thick channels are determined by the administrator, when configuring *Desktop Pages* and layout in the administration console.

b. Select *Finished* at the bottom of the page.

3. The desktop screen will return back to the *User Desktop Page.*

Creating Default Content Tabs

1. In the *Edit Tab Provider* page, do the following:

a. In the *Tab Name* field, enter the name of the tab being created.

b. In the *Tab Topics* field, select the radio button of a pre-made *Tab Content Provider.*

c. Select *Finished* at the bottom of the page.

2. The desktop screen will return back to the *User Desktop Page.*

Changing Membership Login Password

To change the membership login password, the user must choose the *Edit* icon from the *User Information channel* menubar.

In the *Membership Password* area are fields for:

- Original password
- New password
- Confirm new password

The user enters the original password, and the new and confirm passwords must match for the change to be successful. Password checking is subject to the same rules as the membership authentication module.

The user must have authenticated via *Membership* for changes to the Membership password.

Reloading Templates with No 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 may be changed in the iPlanet Portal Server 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, do the following in the iPlanet Portal Server Administration Console:

1. Log on as Super Administrator.
2. Select the *Management Platform Settings* link from the left frame.
3. Expand the *Applications* link in the right frame.
4. Select the *Desktop* link.
5. In the *Component Profile: Desktop* page, scroll down to the *Template Scan Interval* Field.

   This field can be edited. 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.

Enabling Anonymous Desktop

The following is the recommended procedure for enabling an anonymous desktop using the new Anonymous Authentication Module and Login Channel delivered with Service Pack 2.

Configuring Anonymous Authentication

To enable the Anonymous Desktop, in the iPlanet Portal Server Administration Console, do the following:

1. Logon as Super Administrator.
2. Select the *Manage Domains* link from the left frame.

3. In the *Portal Server Domains* page, do the following:

   Select the domain.

4. In the *Domain, Role and Users* page:

   a. Expand *Profiles* link.

   b. Select *Authentication* link.

5. In the *Authentication* Menu:

   a. Select *Anonymous* and de-select all other authentication modules

      The portal server is now defaulted to the *Anonymous authentication module* in all cases and will display the *anonymous desktop* by default.

   b. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.

6. Select the *Continue* button on the *Profile Successfully Updated* page.

7. Select *Show Advanced Options* at the bottom of the page.

   a. In the *Non Interactive Modules*, add *Membership*.

      This will enable users to use the login channel to use Membership authentication instead of having to use the built-in membership login page.

   b. Select *Enable Persistent Cookie Mode.*

      Select this option only if *Persistent Cookies* are desired.

   c. 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.

Customizing Templates for Anonymous Desktop

To customize a user logout from the desktop redirect to the anonymous user desktop, do the following:

1. Edit the `/etc/opt/SUNWips/desktop/default/iwtDesktop/menubar.html` as shown in the code example, in bold text.

   Change the HREF for the Log Out link to:

   ```
   /logout?goto=/login/Anonymous?domain=mydomain.
   ```

   This will set the logout from the desktop to be redirected to the anonymous desktop in all cases.

```
<!--
Copyright 2000 Sun Microsystems, Inc. All Rights Reserved.
"@(#)menubar.html"
-->

<TABLE BORDER="0" CELLPADDING="3" CELLSPACING="0" WIDTH="100%">
<TR BGCOLOR="#000000">
<TD VALIGN="MIDDLE" NOWRAP>
<FONT
COLOR="#FFFFFF"
FACE="[tag:iwtDesktop-fontFace1]">
 <B>[tag:productName]</B>
</FONT>
</TD>
<TD ALIGN="RIGHT" VALIGN="MIDDLE"  NOWRAP>
<P ALIGN="RIGHT">
<FONT COLOR="#FFCC00" FACE="[tag:iwtDesktop-fontFace1]"
SIZE="+0">
<A
HREF="/DesktopServlet?action=content&provider=iwtFrontProvider">
<FONT COLOR="#FFFFFF" CLASS="nonuw">Home</FONT></A> |
<A
HREF="/DesktopServlet?action=edit&provider=iwtOptionsProvider">
<FONT COLOR="#FFFFFF"
CLASS="nonuw">Options</FONT></A> |
<A
HREF="/DesktopServlet?action=edit&provider=iwtContentProvider">
<FONT COLOR="#FFFFFF"
CLASS="nonuw">Content</FONT></A> |
<A
HREF="/DesktopServlet?action=edit&provider=iwtLayoutProvider">
<FONT COLOR="#FFFFFF" CLASS="nonuw">Layout</FONT></A> |
[tag:help_link] |
<A HREF="/logout?goto=/login/Anonymous?domain=mydomain">
<FONT COLOR="#FFFFFF" CLASS="nonuw">
<B>Log Out</B>
</FONT></A> 
</FONT>
</P>
</TD>
</TR>
</table>
```

To customize the Help page for the anonymous desktop, do the following:

1. Logon as Super Administrator.
2. Select the *Anonymous User Desktop.*
3. Select the *Manage Domains* link from the left frame.

a. Select the domain.

b. Select *Default Role*.

c. Select *Users*.

d. Select *Anonymous*.

e. Expand *Applications*.

f. Select *Desktop*.

g. Scroll down to, and select *Show Advanced Options*.

h. Modify the value for *Front Page Help*.

The value in Front Page Help is assumed to be relative from the directory:

`/opt/SUNWips/public_html/docs/en_US/online_help`

i. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.

4. Select the *Continue* button on the *Profile Successfully Updated* page.

Enabling Anonymous Desktop for Other Domains

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

1. Copy `/var/opt/SUNWips/iwtAnonymousUser.xml-orig` file to a temporary location (`/tmp`)

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

2. Edit the `/tmp/iwtAnonymousUser.xml-orig` file as shown in the example, in bold text.

Change the string INST_DEFAULT_DOMAIN to the name of the other domain.

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

3. Use the `./ipsadmin` command to load the new anonymous user profile to the profile service. Type the following commands in a terminal window:

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

4. To access the authentication menu for the new domain in the browser location, type:

```
http://your_server/login?domain=/other_domain
```

Disabling the Anonymous Desktop

To disable the Anonymous Desktop, in the iPlanet Portal Server Administration Console, do the following:

1. Logon as Super Administrator.
2. Select the *Manage Domains* link from the left frame.
3. In the *Portal Server Domains* page, do the following:
   a. Select the domain.
4. In the *Domain, Role and Users* page:
   a. Expand *Profiles* link.
   b. Select *Authentication* link.
5. In the *Authentication* Menu:
   a. De-select the *Anonymous auth module.*

      There must be at least one other *auth module* entry remaining in the field when de-selecting any module.

   b. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.
6. Select the *Continue* button on the *Profile Successfully Updated* page.

Modifying the Login Channel

The login channel can be modified to work with other authentication modules, other than the default login channel shipped with Service Pack 2. 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, do the following:

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

1. As root, in a terminal window, make a copy of the following file:

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

2. Replace the `display.html` file with the following file:

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

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

1. Logon as Super Administrator.
2. Select the *Manage Domains* link from the left frame.
3. In the *Portal Server Domains* page, do the following:
   a. Select the *domain* to add the unix authentication.
4. In the *Domain, Role and Users* page:
   a. Expand *Profiles* link.
   b. Select *Authentication* link.

c. Scroll down to, and select *Show Advanced Options*.

5. In the *Non Interactive Modules* field:

a. Add *Unix*.

b. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.

6. Select the *Continue* button on the *Profile Successfully Updated* page.

The login channel will now use Unix authentication.

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

Using Form Control

A method has been added to the provider API which 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

Several changes are required in the provider API to support form control.

There are integer constants to define the form types, which are `return type` from the `.getEditType()` method:

```
public static final int provider.EDIT_SUBSET ;

public static final int provider.EDIT_COMPLETE ;
```

New methods are added to query and set the form type.

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

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

The desktop servlet is expecting some particularities as edit forms are posted, there are some restrictions on 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`, if the form should be submitted to the desktop servlet. When returning a complete HTML form, a channel must submit valid actions to the desktop as defined in the Desktop URL javadocs.

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 will be 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.

The iPlanet Portal Server default channels all return `EDIT_SUBSET`. Modifying the `-editType` attribute will cause a malfunction. A new channel must return `EDIT_SUBSET`, OR `edit_COMPLETE` depending on how the `.getEdit()` method is implemented.

Locking a Channel's Position

This feature enables an administrator to lock a channel's position. When a channel's position is locked, the user cannot move the channel from its position on the desktop. The purpose of locking a channel is to force the user to see particular content.

With this enhancement, a channel can be locked, which means the user will not be able to change the position on the desktop.

The Layout page that allows the user to arrange channels on the desktop will not list a locked channel.

To lock a channel's position:

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

   If you select the *Movable* check box, the channels can be moved around in the desktop.
4. Deselect the *Removable* check box, so the channel may not be removed from the desktop.

   Selecting the *Removable* check box will allow the user to remove the channel from the desktop.
5. Select the *Submit* button.

To unlock a channels position, do the following:

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

   If you select the *Movable* check box, the channels can be moved around in the desktop.
4. Select the *Submit* button.

Setting Up Full-width Channel

Full-width channels have content that spans the full-width of the desktop, either at the top or bottom. A full-width channel can be simple static images or forms that need to be submitted.

To configure full width channels:

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

6. Select the *Submit* button.

Setting Up Frameless Channels

This feature enables setting up unframed channels in the desktop. The standard channel is displayed with a title, some set of controls, and inside a frame that appears similar to a window. The controls consist of icons linking to functions such as remove, edit, minimize etc. With this enhancement, you can set up a channel without a frame (that is, without the title and the controls).

To configure frame-less channels:

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

   If the *Framed?* check box is selected, the channel will be displayed with a title and controls.
6. Select the *Submit* button.

NOTE The channel will be displayed with a border. If you wish to modify the border of the channel, edit the `hasBorder` attribute in the Policy page.

Selecting the Locale

This feature allows users to choose their locale from a list of available locales on the platform. The provider displays a list of languages to the user, allows them to select one, and then stores the selection in the user profile. The user can refresh the desktop or re-login and get the new locale.

To choose their locale:

1. Log in to the desktop and select *Edit* to proceed to the *Edit User Information* screen.
2. Select the language from the list of available languages pull-down menu.

URL Scraping with No Gateway Installed

Some rewriting facilities from the *Gateway Component Profile* are used when configuring parameters for URL scraping. 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

In the Administration console, do the following to access the *Gateway Component Profile* page:

1. Logon as Super Administrator.
2. Select the *Gateway Management* link from the left frame.
3. Select the *Manage Gateway Profile* link in the right frame.
4. Select the *Gateway Component Profile* page.

   When the Open Portal mode is installed the selections on this page are not greyed out even though most selections are disabled because there is no Gateway running.

Forwarding Cookies

This feature allows the URL scraper to forward cookies which were passed in the HTTP request to the desktop. That is, the URL scraper will send cookies when it makes a connection to the target site to retrieve the content it is scraping. The URL scraper will also send set-cookie requests to the browser. That is, it will get all cookies from set-cookie headers and add them to the HTTP response to the client browser.

By default, no cookies are forwarded. For the affected domain, role, or user, the list of cookies to forward must be set from the administration console. To forward cookies:

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.

Configuring Restart of the HTTP Proxy

To automatically configure a restart of the http proxy whenever rebooting the system server, use the command line interface on the iPlanet Portal Server server to do the following:

NOTE If using more than one server, repeat these steps for each server.

1. As root edit the following file, as shown in bold text:

   ```
   /opt/SUNWips/bin/ipshttpd
   ```

```
#!/bin/sh
# Copyright 10/04/99 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)ipshttpd 1.18 99/10/04 Sun Microsystems

umask 077
ulimit -n 10240

BASE=/opt/SUNWips
```

2. In a terminal window, do the following:

```
# cd /opt/SUNWips/bin
# cp ipshttpd /etc/rc3.d/K55ipshttpd
# cp ipshttpd /etc/rc3.d/S55ipshttpd
# chmod 500 /etc/rc3.d/K55ipshttpd
# chmod 500 /etc/rc3.d/S55ipshttpd
```

This *will* autostart the http proxy when the machine is rebooted.

This *will not* autostart the http proxy when iPlanet Portal Server 3.0 is restarted using `ipsserver start`.

Enabling Access to HTTP Requests and Responses

This feature allows a provider to get access to the HTTP request and response. This is desirable for single sign-on, setting cookies, getting parameters for the HTTP headers, and for inserting data into the headers.

The following are three new methods in the Content Provider interface:

```
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` will call the old versions of the `getContent`, `getEdit`, and `processEdit` methods. The `HttpServletRequest and Responses` objects passed to the new methods have the following indicated behaviors:

Table 1 `HttpServletRequest and Responses`

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

Table 1 HttpServletRequest and Responses *(Continued)*

Methods	Returns
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
setContentLength(int)	UnsupportedOperationException
setContentType(String)	UnsupportedOperationException

Gateway Logging

When gateway logging is enabled, logging traffic between the gateway and the portal server can impact portal performance. In Service Pack 2, gateway default logging is disabled. To enable gateway logging do the following:

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

1. Logon as Super Administrator.
2. Select the *Gateway Management* link from the left frame.
3. Select the *Manage Gateway Profile* link in the right frame.
4. In the *Component Profile: Gateway* page, do the following:
   a. Scroll to the end of the page and select the *Show Advanced Options* button.

b. Scroll to near the bottom of the page to the *Logging Enabled* check box, and select the box to enable the gateway logging.

c. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.

5. Select the *Continue* button on the *Profile Successfully Updated* page.

6. Stop and restart the gateway:

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

Running Applications on a Non-iPlanet Portal Server

This section explains how to run applications written using the iPlanet Portal Server APIs on a non-iPlanet Portal Server server. The application may be either a standalone java application (with some limitations) or a servlet application running on the iPlanet Web Server server.

NOTE iPlanet Portal Server 3.0 public APIs are supported only on Solaris operating systems.

Software versions supported

- JDK / JRE 1.2.1 or greater
- iPlanet Web Server 4.1 or greater
- Solaris 2.6 or greater

Setting Up a Non-iPlanet Portal Server 3.0 Server

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

1. Create the following directories on the non-iPlanet Portal Server server host.

   `/opt/SUNWips`

   `/opt/SUNWips/lib`

   `/opt/SUNWips/locale`

   `/etc/opt/SUNWips`

2. Copy `/etc/opt/SUNWips/platform.conf` to the same location on the non-iPlanet Portal Server server.

3. In order to receive notifications, the application's run time environment must support servlets.

   Modify the `ips.notification.url` parameter in the `platform.conf` to be the fully qualified domain name of the server the application will be running on. See the example (in bold text):

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.29 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=http
ips.server.host=smyrna.red.iplanet.com
ips.server.port=8080
ips.profile.host=smyrna.red.iplanet.com
ips.gateway.protocol=http
ips.gateway.host=smyrna.red.iplanet.com
ips.gateway.port=443
ips.virtualhost=smyrna.red.iplanet.com 192.101.107.10
ips.naming.url=http://smyrna.red.iplanet.com:8080/namingservice
ips.notification.url=http://auth.red.iplanet.com:8080/notificationservice
ips.daemons=securid radius safeword unix skey
securidHelper.port=8943
radiusHelper.port=8944
safewordHelper.port=8945
unixHelper.port=8946
skeyHelper.port=8947


ips.cookie.name=iPlanetPortalServer
ips.locale=en_US
ips.debug=error
ips.version=3.0
ips.basedir=/opt
ips.logdelimiter=&&
```

4. Copy from `/opt/SUNWips/lib` the following files:

   - `ips_sdk.jar`

- `xml.jar`
- `jndi.jar`

to the same location on the non-iPlanet Portal Server server.

5. Copy from `/opt/SUNWips/locale` the following files:
   - `iwtPll.properties`
   - `iwtProfile.properties`
   - `iwtSession.properties`
   - `iwtLogging.properties`
   - `iwtNaming.properties`

   to the same location on the non-iPlanet Portal Server server.
6. If the client application will be running 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. Update the following iPlanet Web Server file:

   `iws_server_root``/https-`*`your_server`*`/config/rules.properites`

   by adding the following line:

   ```
   /notificationservice=notificationservice
   ```
8. Update the following iPlanet Web Server file:

   `iws_server_root``/https-`*`your_server`*`/config/servlets.properties`

   by adding the following line:

   ```
   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

The iPlanet Portal Server session and profile APIs have a notification feature which allows the application to listen for profile and session state changes. If the application is running as a standalone application the following conditions are in effect:

- Cannot receive session or profile notifications
- The client side cache will not be updated when attributes change in the profile. Only after the user logs out and logs back in will the application see the changes.
- After the user session times out on the iPlanet Portal Server session server, the user will still have a valid session until the cache refresh timer is reached.

TIP Reduce the cache seconds attribute in the *session profile* in the iPlanet Portal Server 3.0 Administration Console.

Running Client Applications Using SSL

If the iPlanet Portal Server 3.0 server is configured to use SSL, then the iPlanet Portal Server APIs will also be using 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 a default installation directory.

In order to enable SSL connections by servlets, do the following:

1. Copy from `/opt/SUNWips/lib` the following files:
   - ssl.jar
   - x509v1.jar

   to the same location on the non-iPlanet Portal Server server.
2. Update the classpath on the iPlanet Web Server:

   `iws_server_root``/https-`*`your_server`*`/config/jvm12.conf`

   In the classpath, include:
   - ssl.jar

- x509v1.jar

3. Copy the following file to the *iws_server_root*/bin/https/lib directory:

```
/opt/SUNWips/lib/solaris/sparc/libjssl.so
```

4. Restart the iPlanet Web Server after updating these files.

Running Applications Through the iPlanet Portal Server Gateway (Secure Portal)

When using the iPlanet Portal Server gateway, the gateway must be configured to forward the iPlanet Portal Server cookies to the application host. If the URL of the server the application is running on is not added to this attribute, the iPlanet Portal Server cookie will not be forwarded, and the application will have an invalid user session. By default the gateway will only forward the cookie to the iPlanet Portal Server server.

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

1. In the iPlanet Portal Server Administration Console, do the following:
   a. Logon as Super Administrator.
   b. Select the *Gateway Management* link from the left frame.
   c. Select the *Manage Gateway Profile* link in the right frame.
   d. Scroll down to the *Forward Cookie URL List* attribute.
   e. Enter the URL of the server the application is running on in this field, for example:

```
http://auth.red.iplanet.com:8080
```

   f. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.
   g. Select the *Continue* button on the *Profile Successfully Updated* page.
2. Restart the gateway:

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

Running Applications Without the iPlanet Portal Server Gateway (Open Portal)

When running the application 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 will not be forwarded to the application, and the user session will be invalid.

Software and Hardware Requirements

This section describes the system requirements for Service Pack 2 software. The system requirements depend on how the iPlanet Portal Server 3.0 product is used.

- Table 2 describes the system requirements for developing a portal.
- Table 3 describes the system requirements for deploying a portal.

Table 2 System Requirements for Developing a Portal

Component	Description
Computer type	Two-way CPU class machine.
Operating environment	Solaris™ 2.6, Solaris 7, and Solaris 8
Memory	Each server component of iPlanet Portal Server 3.0 should have a minimum of 256 Mbytes of memory.
Disk space	iPlanet Portal Server 3.0 iPS3.0SP2-01.tar (compressed) file is 25Mbytes.
	iPlanet Portal Server 3.0 iPS3.0SP2-01 (uncompressed) is 50Mbytes.
Software	Coexistence with other software is not supported.
Network interfaces	The gateway needs more than one network interface, if a firewall is installed on its machine.
Web browsers	Netscape Communicator v 4.06 or higher (except v4.6) or Microsoft Internet Explorer v4.0 or higher with SSL v3.0, JavaScript software, JDK software 1.1.

Table 3 System Requirements for Deploying a Portal

Component	Description
Computer type	Two-way CPU class machine.
Operating environment	Solaris 2.6, Solaris 7, and Solaris 8.
Memory	One GB of memory per two-CPU setup. Two GB in swap space for the portal server.
Disk space	iPlanet Portal Server 3.0 iPS3.0SP2-01.tar (compressed) file is 25Mbytes.
	iPlanet Portal Server 3.0 iPS3.0SP2-01 (un-compressed) is 50Mbytes.

Table 3 System Requirements for Deploying a Portal *(Continued)*

Component	Description
Web browsers	Netscape Communicator v 4.06 or higher (except v4.6) or Microsoft Internet Explorer v4.0 or higher with SSL v3.0, JavaScript software, JDK software 1.1.

Service Pack 2 Installation Notes

The iPlanet Portal Server 3.0 Service Pack 2 is a cumulative patch. It includes all Service Pack 1 and Service Pack 2 bug fixes and it can be used to upgrade the following:

- iPlanet Portal Server 3.0
- iPlanet Portal Server 3.0 + Service Pack 1

Contents of `iPS3.0SP2-01.tar`

The iPlanet Portal Server 3.0 Service Pack 2 (iPS3.0SP2-01) software is downloaded from the iPlanet web page and is a tar file. The following directories and files are included in `iPS3.0SP2-01.tar`:

- `directory-4.12-domestic-us.sparc-sun-solaris2.6.tar` (iPlanet Directory Server software upgrade required for Service Pack 2)
- `dsupgrade` (upgrade script for the iPlanet Directory Server)
- `readme.txt`
- rn3sp2 (Release Note 2 document directory)
  - rn3sp2.htm
  - rn3sp2.pdf
- `Patch 110169-01`
  - `Install.info`
  - `installpatch`
  - `backoutpatch`
  - `postbackout`

- postpatch
- prepatch
- build_date
- diPatch
- SUNWTdoc
- SUNWwtnf
- SUNWwtnm
- SUNWwtds
- SUNWwtsdd
- SUNWwtdt
- SUNWwtsvd
- SUNWwtgwd
- SUNWwtws

Installation Instructions

NOTE Service Pack 2 can only be applied to an iPlanet Portal Server 3.0 non-evaluation installation. The following installation instructions are for the en_US release of iPlanet Portal Server 3.0 Service Pack 2 *only*. If an installation of a localized version of Service Pack 2 is being performed, refer to the installation instructions available with that localized package.

iPlanet Portal Server 3.0 Service Pack 2 software package is available from the iPlanet.com web page:

```
http://iplanet.com/downloads/patches
```

NOTE If the iPlanet Portal Server 3.0 installation contains individual gateway and platform servers, the Service Pack 2 package must be installed on both servers.

The iPlanet Portal Server 3.0 Service Pack 2 software package includes iPlanet Directory Server 4.12 software. Upgrading to the iPlanet Directory Server 4.12 is required before installing Service Pack 2. See Upgrading iPlanet Directory Server to extract and upgrade the iPlanet Directory Server software.

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

Upgrading iPlanet Directory Server

1. Backup the iPlanet Portal Server 3.0 machine.
2. Change directories to `/opt` and create a directory for the Service Pack 2 `iPS3.0SP2-01.tar`

```
# cd /opt
# mkdir sp2
```

3. Download the Service Pack 2 package to `/opt/sp2`.
4. In a terminal window, become root.
5. In `/opt/sp2`, run the `tar` command to extract the package contents.

```
# tar xf iPS3.0SP2-01.tar
```

6. Change directories, and create a directory for the iPlanet Directory Server 4.12 tarfile, `directory-4.12-domestic-us.sparc-sun-solaris2.6.tar`.

```
# cd /opt
# mkdir ids_4.12_directory
```

7. Change directories to the sp2 directory and move `directory-4.12-domestic-us.sparc-sun-solaris2.6.tar` to the directory created in Step 6.

```
# cd /opt/sp2
# mv directory-4.12-domestic-us.sparc-sun-solaris2.6.tar
ids_4.12_directory_path
```

8. Change directories and extract the files from `directory-4.12-domestic-us.sparc-sun-solaris2.6.tar`.

```
# cd ids_4.12_directory_path
# tar xf directory-4.12-domestic-us.sparc-sun-solaris2.6.tar
```

9. Change directories to `/opt/sp2` and run the dsupgrade command on the iPlanet Directory Server 4.12 directory.

```
# cd /opt/sp2
# ./dsupgrade ids_4.12_directory
```

TIP `/opt/netscape/directory4/setup/setup.log` contains information on any installation errors that might have occured during the iPlanet Directory Server upgrade.

Installing Service Pack 2

This procedure assumes that `iPS3.0SP2.tar` has already been downloaded and extracted from the tarfile in `/opt/sp2`.

Before restarting the gateway and server check to see that the processes for the directory server and web server are running. See the following example:

1. As root, in a terminal window:

```
# ps -ef | grep ns-slapd
    root 25936     1  0   Nov 28 ?        1:56 ./ns-slapd -f
/opt/netscape/directory4/slapd-smyrna/config/slapd.conf -i /opt/n
    root   298   293  0 14:36:44 pts/11   0:00 grep ns-slapd
```

2. Issue a `kill -TERM` *`process`* for each directory server process that is running under iPlanet Portal Server. For example:

```
# kill -TERM 298
```

3. Verify that all directory server processes for iPlanet Portal Server are stopped:

```
# ps -ef | grep ns-slapd
```

4. Restart the servers.

```
# /etc/init.d/ipsserver start
# /etc/init.d/ipsgateway start
```

5. As root, change directories and run the `installpatch` command (shown in bold text), to install the software on the system.

```
# cd /opt/sp2/110169-10
# ./installpatch .
```

```
WARNING: /usr/sbin/patchadd is being used to install this patch.
Installpatch will be removed from Solaris patches in
the next release of Solaris.

New versions of /usr/sbin/patchadd and /usr/sbin/patchrm exist
that provide essential bug fixes and a speed enhancement.
Please install patch 106125 for significant patch
installation improvements.


Checking installed patches...
Executing prepatch script...
Netscape-Directory/4.12 B00.193.0237
Verifying sufficient filesystem capacity (dry run method)...
Installing patch packages...

Patch number 110169-01 has been successfully installed.
See /var/sadm/patch/110169-01/log for details
Executing postpatch script...

Updating webserver configuration...

Updating classpath...
Creating new attributes in profile...
Updating existing profiles...
Removing obsolete attributes...
It is highly recommended to run the ldapUpdate script to convert
the protected profile attributes, such as membership password
etc, with a more secure encryption algorithm. Please run
    <IPS_ROOT>/SUNWips/bin/ldapUpdate -h
for more instructions.

Postpatch processing complete.
Please restart the iPS Server/Gateway for the changes to take
effect.

Patch packages installed:
    SUNWwtdoc
    SUNWwtds
    SUNWwtdt
    SUNWwtgwd
    SUNWwtnf
    SUNWwtnm
```

```
    SUNWwtsdd
    SUNWwtsvd
    SUNWwtws
```

TIP `/var/sadm/patch/110169-01/log` contains information on any installation errors that might have occurred during the iPlanet Portal Server 3.0 Service Pack 2 installation.

6. Set the environment variable IPS_ROOT to the iPlanet Portal Server 3.0 installation directory.

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

```
# IPS_ROOT=/opt
```

7. Run the `ldapUpdate` script.

TIP See `ldapUdate` Command Options for information about the command line arguments for this script.

```
# ./ldapUpdate -b root_dn -w password
```

```
Searching the ldap database for password attributes ...
Converting the passwords with new algorithm ...
Updating the ldap database with the new passwords ...
modifying entry cn=iplanet,cn=iplanetwebtop,o=iplanet.com
```

```
modifying entry
cn=russp9i,cn=iplanet,cn=iplanetwebtop,o=iplanet.com

modifying entry
cn=newguy,cn=iplanet,cn=iplanetwebtop,o=iplanet.com

Ldap server successfully updated
```

8. Restart the servers.

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

`ldapUdate` Command Options

The following script has been added to the Service Pack 2 package. The following describes the different command arguments for this script:

```
./ldapUpdate -b root_dn -w password [-p port] [-r] [-h]
```

`root_dn`	Search base. The place in the ldap hierarchy from where the administrator chooses to update. Any organization below this level will be affected by the update script. For example, `o=iplanet.com`.
`password`	Password for directory manager.
`port`	Port number of the ldap server.
`-r`	Reverse conversion to old algorithm.
`-h`	Help menu.

Downgrading iPlanet Directory Server

The iPlanet Directory Server 4.11 software package is available from the iPlanet.com website:

`http://www.iplanet.com/downloads/download/index.html.`

To downgrade from iPlanet Directory Server 4.12 to iPlanet Directory Server 4.11:

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

1. As root, restart the servers:

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

2. Backup directory data:

```
# /opt/netscape/directory4/slapd-servername/db2ldif backup_file
```

   This command saves the directory data in a the backup file using `ldif` format. The backup file can be used to restore the directory data later.

3. Change directories and create a new directory for the iPlanet Directory Server 4.11 package:

```
# cd /opt
# mkdir ids_4.11_directory
```

4. Download the iPlanet Directory Server 4.11 software package from the iPlanet web site to the *ids_4.11_directory* created in Step 3.

5. Un-compress and extract the files from the iPlanet Directory Server 4.11 media file:

```
# gunzip directory-4.11-export-us.sparc-sun-solaris2.5.1.tar.gz
# tar xf directory-4.11-export-us.sparc-sun-solaris2.5.1.tar
```

6. Change directories to the directory that contains the dsupgrade script and run the dsupgrade script on the *ids_4.11_directory*.

```
# ./dsupgrade ids-4.11_directory
```

Backing Out the Service Pack 2 Software

This procedure assumes that the Service Pack 2 patch is in /opt/sp2.

1. Backup the iPlanet Portal Server 3.0 machine.
2. Become root.
3. Run the ldapUpdate script to remove the changes to the ldap server.

> **TIP** See ldapUdate Command Options for information about the command line arguments for this script.

```
# ldapUpdate -b root_dn -w password -r
```

4. Change directories to the Service Pack 2 patch directory and run the backoutpatch script.

   See backoutpatch Command Options for information about the command line arguments for this script.

```
# cd /opt/110169-10
# ./backoutpatch 110169-10
```

backoutpatch Command Options

The following describes the different command arguments for this script:

```
.backoutpatch [-f] [-V] [-B backout_dir] [-R root_path | -S service] patch
```

-f	Force the backout regardless of whether the patch was superseded.
-V	Print version number only.
-B *backout_dir*	Save backout data to a location other than the default directory.
-R *root_path*	Define the full path name of a subdirectory to use as the `root_path`. All package system information files are assumed to be located in a directory tree starting in the specified `root_path`. All patch files generated from the `installpatch` will be located in the same directory tree. Cannot be specified with the -S option.
-S *service*	Specify an alternate service, for example Solaris_2.3, for patch package processing references.
patch	The file name of the patch.

Known Problems and Limitations

Here are known problems with the iPlanet Portal Server 3.0 software that have not been fixed in Service Pack 2, with workarounds where appropriate.

4381501

A document can have a *BASE* attribute, which may be a different path than the URL which the document was fetched from. If there is a base URL, then all relative URLs within the document are considered to be relative to the base URL. If there is no base URL, then relative URLs are considered to be relative to the document's URL.

But, when the Gateway encounters relative URLs, the Gateway always uses the document's URL for expanding the relative paths instead of using the base URL. The Gateway expands them to full paths starting with `https://gateway/http://`*`hostname:port/`*.

4381586

The number of valid sessions (as indicated by the *Valid Session* number in the *Manage User Session* page) is inaccurate.

For instance, 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.

4383120

The LDAP authentication module does not allow the admin to specify a search filter when configuring the server for user lookup in the directory. 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 username entered by the user. If the *search filter for userId* contained the value surname or *sn*, then the search filter would become (surname=jim).

Administration

4375670

Desktop comes up blank if no channels are selected in the Administration Console and in the Desktop.

Workaround:

None.

4378030

The `setDomain` method should attempt to retrieve a domain profile before setting the domain.

Workaround:

None

4376634

The Administration console allows duplicate tab names if one attribute is different.

Workaround:

Verify that tab names are not duplicated.

4379326

Contents of `profilestyle.css` can become visible in the Administration Console when adding a new user to a newly created domain.

Workaround:

None.

4352059

The profile `isAllowed` method does not do wildcard matching, therefore, wildcard characters can not be used in domain names or URLs when configuring Netlet access to specific domains or when setting up access to specific URLs respectively.

NOTES

The example "*.sun.com" provided on page 93 of the Administration Guide is inaccurate.

The examples "http://*.company1.com" and "http://*.mycompany.com" on page 94 of the Administration Guide are inaccurate.

The wildcard character "*" can only be used alone.

Workaround:

None.

Authentication

4369280

The link on the Desktop logout page points to the server where the session was created. This implementation breaks load-balancing transparency.

Workaround:

I. In a terminal window, become root.

II. Edit `/etc/opt/SUNWips/auth/default/logout.html`

Remove the line containing the HREF tag (as shown in bold text).

```
<FONT COLOR="#000000">
<H2>You have logged out.</H2>
<BR>
<BR>
```

```
<A HREF=<subst data="XXlogoutXX">/login</subst> target="_top"><FONT SIZE="+2"
COLOR="#000000"><TT><B>Return to Desktop login</B></TT></A>
</FONT>
```

4397140

White space is not allowed in text fields for authentication methods in the administration console.

Workaround:

Verify that there is no white space in the authentication entry string.

Desktop

4329229

Detached providers are not being handled properly by operations in the Content link.

Workaround:

None

4319604

Disabling the Netlet provider in the Administration console for a user causes error message: “Document contained no data”.

Workaround:

Remove the provider from the channel list in the Administration console.

4355280

When using Internet Explorer 5x on Windows 98, closing the Netlet window crashes the web browser.

Workaround:

None.

Gateway

4324617

External bookmark URLs are not redirected.

Prevention:

Remove open URL from the Gateway profile “rewrite JavaScript function parameters”.

Workaround:

Create a second bookmark channel to handle external sites.

The bookmark provider can not be used for URLs which reference Internet URLs that the Gateway cannot or should not fetch.

ipsadmin

4319514

The command `ipsadmin` does not check for the syntax of boolean flags.

Workaround:

When creating an XML file, if the attribute type is boolean, add a true or false statement, as shown in bold in the following 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>
```

ipsserver

4379242

The `ipsserver start` command requires additional arguments if the server is running multiple instances. For more information see Configuring Multiple Instances of iPlanet Portal Server

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:

```
# ipsserver start ipsserver.servername.com@port
```

Logging

4376995

Log records should be written using `iwtPlatform-locale` not `iwtUser-locale`.

Workaround:

None.

NetFile

4342453

The hour glass occasionally keeps running after attempting to add a share in Netfile Java.

Workaround:

Select some other part of NetFile to clear up the hour glass.

NetMail

4321516

A race condition occurs if when replying to a message, selecting send and then immediately deleting the message.

Workaround:

Wait for the reply flag to be set (slow down) or delete the message again.

4307367

IMAP password is displayed in clear text in source of edit.

Workaround:

None

Sample Providers

4389071

The `editType` attribute is missing in the following xml files:

- `iwtHelloWorld3Provider.xml`
- `iwtQuotationProvider.xml`

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>
```

Bugs Fixed in Service Pack 1 and Service Pack 2

The following bugs have been fixed in iPlanet Portal Server 3.0 Service Pack 1 and Service Pack 2:

Table 4 Fixed Bug List

Bug ID	Bug Description	Status
Administration Console		
4343322	Server restart from Administration Console did not work.	Fixed in sp1
4374777	Domain Admin Roles page shows incorrect listing of domain admin roles.	Fixed in sp2
Authentication		
4357503	The option to match the certificate in ldap does not work if the certificate in the LDAP directory is stored as binary.	Fixed in sp2
4346955	The verbose option for doSecureID does not allow logins.	Fixed in sp2
4339793	Unix authentication fails when the server and the doUnix helper are out of sync.	Fixed in sp2
Desktop		
4338083	Removing channel with thin-thick-thin layout caused null pointer	Fixed in sp1
4335174	URL rewriting did not work for relative URLs in URL scraper.	Fixed in sp1
4365483	Content provider should check for null provider in content provider edit page creation.	Fixed in sp2
4349181	The Channel Wizard works incorrectly when an inline channel is created if the iSyndicate connector is installed.	Fixed in sp 2

Table 4 Fixed Bug List

Bug ID	Bug Description	Status
4330685	The URL scraper failed when it tried to fetch a URL which resulted in a redirect.	Fixed in sp1
4343673	URL scraper provider did not handle redirects.	Fixed in sp1
4343674	RSS and URL scraper did not support using a proxy.	Fixed in sp1
Gateway		
4340633	Gateway did not re authenticate when its session died.	Fixed in sp1
4335199	Rewriter for applet tags could only rewrite limited number of URLs in a parameter.	Fixed in sp1
4338888	Membership Module did allow a blank password to authenticate.	Fixed in sp1
4330036	Rewriter didn't work if there was a URL with no leading `http://` and a port number specified.	Fixed in sp1
4343671	`authd` did not support Open Portal login.	Fixed in sp1
4342320	Gateway boot process hangs if the server is not started first.	Fixed in sp2
`ipsadmin`		
4336880	`ipsadmin` did not work if server was running on SSL mode.	Fixed in sp1
4337917	`ipsadmin` did not encrypt "protected" attributes.	Fixed in sp1
4350031	`ipsadmin -import` converts new attributes in previously existing components to lowercase and reports all attributes of new components as already existing. This bug is fixed in iDS 4.12.	Fixed in sp2
`ipsserver`		
4344376	`ipsserver stop` script kills all HTTPD processes running on the server. In doing so, may also kill some external iPlanet Web Servers running on the server. The `ipsserver stop` command should stop only relevant processes.	Fixed in sp2
Japanese Language Version		

Table 4 Fixed Bug List

Bug ID	Bug Description	Status
4336096	On Japanese localization, Netfile Java did not work on Solaris and Windows NT.	Fixed in sp1
Logging		
4343009	When logging was disabled, client API threw exceptions.	Fixed in sp1
4352291	Ability to turn Gateway logging on or off.	Fixed in sp1
NetMail		
4340200	Session timed out when running NetMail without the Gateway.	Fixed in sp1
NetFile		
4342428	NetMail was unable to receive mail with attached text file sent from NetFile.	Fixed in sp1
4340074	Session timed out when running NetFile without the Gateway.	Fixed in sp1
Profile		
4341571	External LDAP attribute mappings did not work with binary type attributes.	Fixed in sp1
4339191	Domain search did not search for users mapped from external LDAP. **Fix limitations**: Search limit for external LDAP users is 400 users only.	Fixed in sp1
4340128	Profile API returns valid profile object for non existing profiles.	Fixed in sp2
Documentation		
4343016	Incorrect URL for documentation.	Fixed in sp1

Documentation Updates

Where to Go for More Information

For document information about the iPlanet Portal Server 3.0, visit:

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

Setting Session Time-out to the Maximum Value

1. As Super Administrator, access *Session Profile*.
2. Make value of *Inactivity* to the maximum value of: **15372286720912930**.
3. Make value of *Maximum* to the maximum value of: **15372286720912930**.

Using the Netlet Proxy

The Netlet proxy is used for the following reasons:

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

NOTE If configuring the iPlanet Portal Server 3.0 to run as *nobody*, including netlet, see Configuring User Nobody on the Gateway, before reading these instructions.

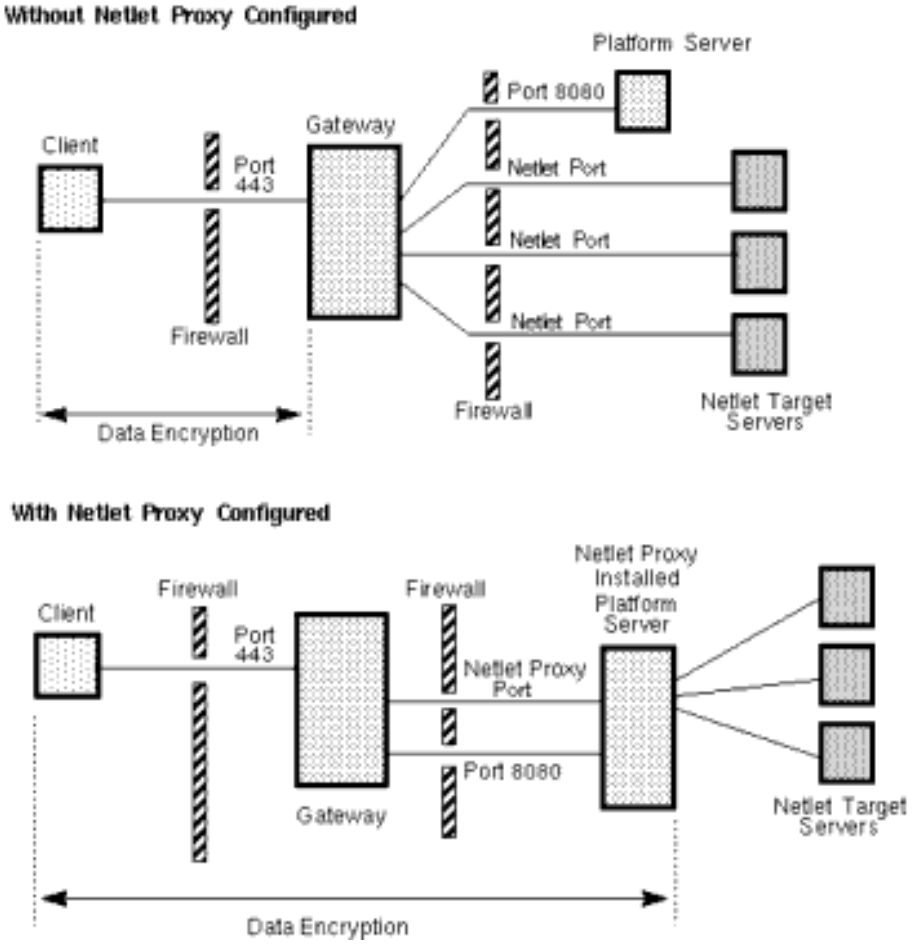


Figure 1 Netlet Proxy Implementation

Configuring the Netlet Proxy

In the iPlanet Portal Server Administration Console, do the following:

1. Logon as Super Administrator.
2. Select the *Gateway Management* link from the left frame.
3. Select the *Manage Gateway Profile* link in the right frame.
4. In the *Component Profile: Gateway* page, do the following:

a. Scroll to the end of the page and select the *Show Advanced Options* button.

b. Scroll to near the bottom of the page to the *Netlet Proxy Enabled* check box, and select the box to enable the netlet proxy.

c. In the *Netlet Proxy Port*, type in the desired (unused) port number to be used (for example: 8048).

TIP From the command line, type:

```
netstat -a
```

This will print out all ports currently assigned and in use.

d. Select the *Submit* button at the bottom of the page to commit these changes to the profile server.

5. Select the *Continue* button on the *Profile Successfully Updated* page.

Configuring Restart of the Netlet Proxy

To automatically configure a restart of the Netlet proxy whenever rebooting the system server, use the command line interface on the iPlanet Portal Server server to do the following:

NOTE If using more than one server, repeat these steps for each server.

NOTE Configure the Netlet Proxy in the iPlanet Portal Server Administration Console before starting the services. See "Configuring the Netlet Proxy" for instructions.

1. As root edit the following file, as shown in bold text:

```
/opt/SUNWips/bin/ipsnetletd
```

```
#!/bin/sh
# Copyright 10/04/99 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)ipsnetletd       1.18 99/10/04 Sun Microsystems

umask 077
ulimit -n 10240

BASE=/opt/SUNWips
```

2. In a terminal window, do the following:

```
# 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
```

This *will* autostart the netlet proxy when the machine is rebooted.

This *will not* autostart the netlet proxy when iPlanet Portal Server 3.0 is restarted using `ipsserver start`.

How to Report Problems

If you have problems with iPlanet Portal Server 3.0 Service Pack 2, 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 iPlanet 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

For 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 Professional Services information --- `http://www.iplanet.com/services/pro_serv/index.html`
- 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`