Release Notes for iPlanet Portal Server 3.0

Service Pack 3a

Updated October 2, 2001

These release notes contain important information available at the time of the release of iPlanet™ Portal Server Service Pack 3a. Installing this product will update the iPlanet Portal Server 3.0 software to include Service Pack 1, Service Pack 2, and Service Pack 3a. 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 3a.

These release notes are available on the CD as well as on 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:

- What's New in iPlanet Portal Server 3.0, Service Pack 1, Service Pack 2, and Service Pack 3a
- Software and Hardware Requirements
- Service Pack 3a Installation Notes
- Known Problems and Limitations
- Bugs Fixed in Service Pack 1, Service Pack 2, and Service Pack 3a
- Documentation Updates
- Where to Go for More Information
- How to Report Problems
- For More Information

Understanding the Typographic Conventions

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

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% You have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name% su` `Password:`
AaBbCc123	Book titles, new words or terms, words to be emphasized, or glossary terms.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be root to do this.
AaBbCc123	Command-line placeholder; replace with a real name or value	To delete a file, type `rm` *`filename`*. `http://server: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 2 Unix Shell Prompts

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

Table 2 Unix Shell Prompts

Shell	Prompt
Bourne shell and Korn shell superuser prompt	#

Sample Machine Names

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

Table 3 Sample Machine Names

Machine Name	Type of iPlanet Portal Server Component
siroe	iPlanet Portal Server server component acting as the profile server
varrius	iPlanet Portal Server server component not being used as the profile server in multiple server installations
sesta	iPlanet Portal Server gateway component

What's New in iPlanet Portal Server 3.0, *Service Pack 1*, *Service Pack 2, and Service Pack 3a*

The following product enhancements to iPlanet Portal Server 3.0 are included in the Service Pack 3a software release:

- Gateway Performance Enhancements
- Certificate Management
- Web Server Performance Tuning Parameters
- Open Portal Mode
- Configuring Multiple Instances of iPlanet Portal Server
- Configuring iPlanet Portal Server to Run as User Non-Root
- Configuring iPlanet Portal Server to Run as User Nobody

- Installing and Enabling Multiple Locales 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 an E-mail Address as the User's Profile ID
- Login Channel
- JavaServer Pages Provider
- Tabbed Desktop
- Changing Membership Login Password
- Reloading Templates without a Server Restart
- Enabling Anonymous Desktop
- Using Form Control
- Locking a Channel's Position
- Setting Up Full-width Channels
- 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
- Using Novell File Systems with NetFile and NetFile Lite

- Defining Systems and Shares at the Domain and User Levels from the Administration Console
- Defining Hidden Shares
- Alphabetized Shares on Windows NT System
- Addition of `smb.conf` Parameter to `smbclient` Command
- NetFile Usability Enhancements
- Using a Load Balancer in Open Portal Mode
- Loading Multiple Attributes in One Profile Request
- Short-Circuiting for Session and Logging Requests
- Running Desktop Applications on a Macintosh Client
- Unlimited Netlet Connections
- Netlet Windows
- Enabling Secure FTP Using a Netlet Connection
- Using the Netlet Proxy
- Rewriting Javascript Functions Parameters in Javascript
- Rewriting JavaScript Variables in JavaScript
- Rewriting JavaScript Function Parameters Function
- Rewriting Applet / Object Parameter Values List
- Choice Property Keys
- File Lookup
- isPresentable() Method Added to the Provider API
- Setting Session Time-out to the Maximum Value

Gateway Performance Enhancements

The following changes have been made to the iPlanet Portal Server product as a result of enhancing the performance of the gateway.

- Support of Netscape Security Service (NSS) on the Gateway Component
- Attribute Additions
- Open Portal Mode

- Upgrade to iPlanet Web Server 4.1 SP7

Support of Netscape Security Service (NSS) on the Gateway Component

Service Pack 3a introduces support for NSS (JSS) on the gateway component. This new implementation of SSL increases the number of HTTPS operations that can be sustained by the gateway component.

Certificates installed for the previous SSL library are automatically converted to the format required by NSS when Service Pack 3a is installed, however, certificate management for the gateway component is different from previous releases of the iPlanet Portal Server product. For more information on gateway certificate management see, "Web Server Performance Tuning Parameters."

Attribute Additions

A new attribute `ips.gateway.trust_all_server_cert` has been added.

As a new line entry in the `/etc/opt/SUNWips/platform.conf` file `ips.gateway.trust_all_server_certs` offers a true/false statement for the gateway to allow or deny unknown certificate authorities (CAs).

- The default value of this attribute is `false`.
- The value may be changed to `true`. Set the value to `true` you want the gateway component to trust all CAs which present signed certificates to the gateway component during an SSL handshake.

This will also include CAs that the gateway component does not already know about.

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

See "Certificate Management" for instructions on installing a Root CA certificate.

Two cases in which the `ips.gateway.trust_all_server_cert` attribute would be set to true include:

- The iPlanet Portal Server gateway component uses SSL to communicate with a gateway proxy, on which a self-signed certificate is installed.
- The iPlanet Portal Server gateway component uses SSL to communicate with an iPlanet Portal Server server, on which a self-signed certificate is installed.

```
#
# Copyright 03/22/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf    1.38 00/03/22 Sun Microsystems"
#

ips.defaultDomain=iplanet.com
ips.server.protocol=http
ips.server.host=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.profile.port=8080
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=443
ips.gateway.trust_all_server_certs=true
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.iplanet.com:8080/notificationservic
e
ips.daemons=securid radius safeword unix skey
ips.nosession.url=/login
ips.desktop.channelinittimeout=30
```

The following error is generated if the gateway does not recognize the certificate that is being presented, and the `ips.gateway.trust_all_server_cert` attribute is set to false.

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

Attributes Removed in Service Pack 3a

As part of the gateway performance enhancements incorporated in Service Pack 3a, the following settings in the iPlanet Portal Server administration console are no longer used.

- IP Address Validation Enabled
- Trust Server SSL Certificate List

- ReverseProxy Maximum Socket Connections

Although, these settings appear in Administration Console on the *Manage Gateway Profile* page, they do not function. The information in the section "IP address validation" in Chapter 8 "Configuring the Gateway" in the Administration Guide no longer applies.

Gateway Component Performance Tuning Parameters

For better performance under load, increase the value of "Maximum Thread Pool Size". The default value is 200, and should be increased to 500.

Increase this value through the Portal Admin Console:

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

Certificate Management

In Service Pack 3a, the SSL certificate management for the gateway component is different from previous releases due to the replacement of the previous SSL library with the new SSL library.

As a result, the information on SSL certificates for the gateway component presented in Chapter 11 of the iPlanet Portal Server *Administration Guide*, and in Appendix A of the iPlanet Portal Server *Installation Guide* has changed. The following information replaces the existing documentation on SSL certificates for the gateway.

NOTE Previous documentation on certificates for the iPlanet Portal Server server component still applies.

General Information on SSL Certificates for the Gateway Component

In Service Pack 3a, the `certadmin` script in <*installation_directory*>`/SUNWips/bin/` is a script that wraps around the `ipscertutil` command for convenience and consistency with previous certificate administration. The `certadmin` script should satisfy the conventional needs of certificate administration. For any additional functionality, use the `ipscertutil` command directly. For example, use `ipscertutil` to delete a certificate from certificate database. The command `ipscertutil -H` lists usage.

Certificate related files are located in `/etc/opt/SUNWips/cert`. Three of the five certificate files, `cert7.db`, `key3.db` and `secmod.db`, are binary files and contain the data for certificates, keys, and cryptographic modules. These files can be manipulated implicitly by using the `certadmin` script.

The three certificate related binary files have the same formats as the database files used by iPlanet Web Server and are located in <*installation_directory*>`/netscape/server4/alias`. If necessary, they can be shared between the iPlanet Portal Server server and gateway components or the gateway proxy.

The other two files are hidden text files: `.jsspass` and `.nickname`. The `.nickname` file stores the names of the token and certificate that gateway currently uses, in the form of *token_name*:*certificate_name*. If using the default token (the token on default internal software encryption module), omit the token name. In most cases, the `.nickname` file only has the certificate name stored in it.

The `.jsspass` file contains the password for the encryption module that iPlanet Portal Server gateway currently uses. The default module is the internal software module.

During the installation of the iPlanet Portal Server gateway component, a self-signed SSL certificate is created and installed. If necessary, use the `certadmin` script to do additional certificate administration.

Generating a Self-signed SSL Certificate for the Gateway Component

1. As root, run the `certadmin` script. The following example assumes that `/opt` is the installation directory.

```
# /opt/SUNWips/bin/certadmin
```

The Certificate Administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Modify Trust Attributes of Certificate (e.g., for PDC)
6) List Root CA Certificates
7) List All Certificates
8) Quit

choice: [8] 1
```

2. Enter **1** on the menu to generate a self-signed certificate.

The Certificate Administration script asks you if you want to keep the existing database files.

```
Do you want to keep the existing certificate database files?
[y]/n
```

3. Choose whether to keep the existing certificate database files.

- If you answer **y**, the script prompts you to enter certain organization-specific information, token name and certificate name.

```
What is the fully-qualified DNS name of this host?
[host_name.domain_name]
What is the name of your organization (ex: Company)? []
What is the name of your organizational unit (ex: division)? []
What is the name of your City or Locality? []
What is the name (no abbreviation please) of your State or
Province? []
What is the two-letter country code for this unit? []

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

Please enter the token name []
```

```
Enter the name you like for this certificate:
```

The token name (default being empty) and certificate name will be stored in the `.nickname` file under `/etc/opt/SUNWips/cert`.

- If you answer **n** to the question "Do you want to keep the existing certificate database files?" the original certificate directory will be backed up, and the scripts will ask you for organization-specific information, token name, certificate name as shown above, and asks for a passphrase. A passphrase needs to be set because a new set of certificate, key and encryption module database files will be created. The passphrase will be stored in the `.jsspass` file under `/etc/opt/SUNWips/cert`.

```
Enter passphrase []:
```

4. Enter the organization-specific information, certificate name and, if needed, token name and passphrase.

   A self-signed certificate is generated and the prompt returns.

5. Restart the gateway component for the certificate to take effect.

To restart the gateway component, assuming `/opt` is the installation directory, enter the following commands.

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

NOTE Multiple certificates can be stored in the database files, but the one that gets used by the gateway component is identified by the `.nickname` file. This file can manually be edited to switch to a different existing certificate.

Obtaining and Installing an SSL certificate for the Gateway from a Certificate Authority (CA)

During the installation of the gateway component of the Portal Server product, a self-signed certificate is created and installed. At any point after installation, you can install SSL certificates signed by vendors who provide official certificate authority (CA) services, or by your corporate CA.

There are three main steps involved in this task.

- Generating a Certificate Signing Request (CSR)
- Ordering a Certificate from the Chosen CA Using the CSR
- Installing the Certificate from the CA

Generating a Certificate Signing Request (CSR)

1. As root, run the certadmin script. The following example assumes that `/opt` is the installation directory.

```
# /opt/SUNWips/bin/certadmin
```

The Certificate Administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Modify Trust Attributes of Certificate (e.g., for PDC)
6) List Root CA Certificates
7) List All Certificates
8) Quit

choice: [8] 2
```

2. Type **2** on the menu to generate a certificate signing request (CSR).

The script prompts you to type certain organization specific information, web master's email and phone number, and token name.

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

What is the email address of the admin/webmaster for this server
[] ?
What is the phone number of the admin/webmaster for this server
[] ?

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

Please enter the token name []
```

3. Fill in the information.

NOTE Do not leave the web master's email and phone number blank. The information is necessary for getting a valid CSR.

A CSR is generated and stored in the file `/tmp/csr.<`*hostname*`>` and is printed out to the screen which you can copy and paste.

Ordering a Certificate from the Chosen CA Using the CSR

1. Go to the Certificate Authority's web site and order your certificate.

2. Provide the CSR from the last step, as requested by the CA. Provide other information, if requested by the CA.

3. After you receive your certificate from the CA, save it in a file.

The following example omits the actual certificate data.

```
-----BEGIN CERTIFICATE-----
The certificate itself
----END CERTIFICATE-----
```

Include both the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines with the certificate in the file.

Installing the Certificate from the CA

Using the certadmin script, install the certificate from the CA in your local database files in `/etc/opt/SUNWips/cert`.

1. As root, run the certadmin script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

The Certificate Administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Modify Trust Attributes of Certificate (e.g., for PDC)
6) List Root CA Certificates
7) List All Certificates
8) Quit

choice: [8] 4
```

2. Type **4** on the menu to install your certificate from the CA.

The script asks you to enter certificate file name, certificate name and token name.

```
What is the name (including path) of file that contains the
certificate?
Please enter the token name you used when creating CSR for this
certificate []
```

3. Answer the questions respectively.

   The certificate will be installed in `/etc/opt/SUNWips/cert`, and the screen prompt returns.

4. Restart the gateway component, for the certificate to take effect. The following commands assume that `/opt` is the default installation directory.

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

Adding a Root CA Certificate

Importing a root CA certificate into the gateway's certificate database when the gateway is an SSL client allows the gateway component to communicate with an internet or an intranet HTTPS site if the site presents a server certificate signed by a CA that is unknown to the gateway certificate database. The SSL handshake will fail if the gateway component does not recognize the server's CA certificate.

To allow a successful handshake, import the certificate authority's root certificate into gateway's certificate database so that the CA becomes known to the gateway which in this case is an SSL client.

To import a root CA certificate into the gateway component's certificate database:

1. As root, run the certadmin script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

   The Certificate Administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Modify Trust Attributes of Certificate (e.g., for PDC)
6) List Root CA Certificates
7) List All Certificates
8) Quit

choice: [8] 3
```

2. Choose option **3** on the certificate administration menu.
3. Enter the name of the file that contains the root certificate, and enter the name for the certificate.

If the gateway component is set up to communicate with an https site that presents a self-signed certificate, allowing the gateway component to trust any unknown CAs can be a useful approach. However, for a serious deployment, this approach should be used with caution. See "Gateway Performance Enhancements: Attribute Additions" for more information on configuring the gateway component to trust all server certificates.

Most well-known public CAs are already included in the certificate database. The following is the list of all the public CAs included by default and their trust attributes. For information on modifying the trust attributes of a public CA see "Modifying Trust Attributes of a Certificate".

Table 4 Public Certificate Authorities

Certificate Authority Name	Trust Attributes
ABAecom (sub., Am. Bankers Assn.) Root CA	CG,C,C
American Express CA	C,C,
American Express Global CA	C,C,
Baltimore CyberTrust Code Signing Root	„C
Baltimore CyberTrust Mobile Commerce Root	CG,C,
Baltimore CyberTrust Root	CG,C,
BelSign Object Publishing CA	„C
BelSign Secure Server CA	C,,
Deutsche Telekom AG Root CA	C,C,C
Digital Signature Trust Co. Global CA 1	CG,C,C
Digital Signature Trust Co. Global CA 2	CG,C,C

Table 4 Public Certificate Authorities *(Continued)*

Certificate Authority Name	Trust Attributes
Digital Signature Trust Co. Global CA 3	CG,C,C
Digital Signature Trust Co. Global CA 4	CG,C,C
E-Certify Commerce ID	C,,
E-Certify Internet ID	,C,
Entrust.net Premium 2048 Secure Server CA	C,C,C
Entrust.net Secure Personal CA	C,C,C
Entrust.net Secure Server CA	C,C,C
Equifax Premium CA	C,C,C
Equifax Secure CA	C,C,C
Equifax Secure Global eBusiness CA	C,C,C
Equifax Secure eBusiness CA 1	C,C,C
Equifax Secure eBusiness CA 2	C,C,C
GTE CyberTrust Global Root	CG,C,C
GTE CyberTrust Japan Root CA	CG,C,C
GTE CyberTrust Japan Secure Server CA	CG,C,C
GTE CyberTrust Root 2	CG,C,C
GTE CyberTrust Root 3	CG,C,C
GTE CyberTrust Root 4	CG,C,C
GTE CyberTrust Root 5	CG,C,C
GTE CyberTrust Root CA	CG,C,C
GlobalSign Partners CA	C,C,C
GlobalSign Primary Class 1 CA	C,C,C
GlobalSign Primary Class 2 CA	,C,
GlobalSign Primary Class 3 CA	,C,
GlobalSign Root CA	C,C,C
TC TrustCenter, Germany, Class 0 CA	Cw,C,C
TC TrustCenter, Germany, Class 1 CA	,C,
TC TrustCenter, Germany, Class 2 CA	C,C,C
TC TrustCenter, Germany, Class 3 CA	C,C,C

Table 4 Public Certificate Authorities *(Continued)*

Certificate Authority Name	Trust Attributes
TC TrustCenter, Germany, Class 4 CA	C,C,C
Thawte Personal Basic CA	,C,C
Thawte Personal Freemail CA	,C,
Thawte Personal Premium CA	,C,C
Thawte Premium Server CA	CG,,C
Thawte Server CA	CG,,C
Thawte Universal CA Root	CG,C,C
ValiCert Class 1 VA	C,C,C
ValiCert Class 2 VA	C,C,C
ValiCert Class 3 VA	C,C,C
ValiCert OCSP Responder	C,C,C
VeriSign Class 4 Primary CA	CG,C,C
Verisign Class 1 Public Primary Certification Authority	,C,
Verisign Class 1 Public Primary Certification Authority - G2	,C,
Verisign Class 1 Public Primary Certification Authority - G3	,C,
Verisign Class 2 Public Primary Certification Authority	,C,C
Verisign Class 2 Public Primary Certification Authority - G2	,C,C
Verisign Class 2 Public Primary Certification Authority - G3	,C,C
Verisign Class 3 Public Primary Certification Authority	CG,C,C
Verisign Class 3 Public Primary Certification Authority - G2	CG,C,C
Verisign Class 3 Public Primary Certification Authority - G3	CG,C,C
Verisign Class 4 Public Primary Certification Authority - G2	CG,C,C
Verisign Class 4 Public Primary Certification Authority - G3	CG,C,C
Verisign/RSA Commercial CA	C,C,
Verisign/RSA Secure Server CA	C,C,

Viewing the Public CA list

To view the list of Public CAs as shown above:

1. As root, run the certadmin script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

The Certificate Administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Modify Trust Attributes of Certificate (e.g., for PDC)
6) List Root CA Certificates
7) List All Certificates
8) Quit

choice: [8] 6
```

2. Choose option **6** on the certificate administration menu.

Modifying Trust Attributes of a Certificate

In general, the trust attributes of a certificate gives information about whether the certificate is a regular server certificate (also called user certificate) as opposed to a root certificate, whether the certificate (in the case of a root certificate) can be trusted as the issuer of a server or client certificate.

There are three available trust categories for each certificate, expressed in this order: "SSL, email, object signing". In the context of the gateway component, only the first category is useful. In each category position, zero or more of the following attribute codes are used.

The possible attribute values and the meaning of each value are listed below, which help to further explain the usage of trust attributes.

Table 5 Certificate Trust Attributes

Attribute	Description
p	Valid peer
P	Trusted peer (implies p)
c	Valid CA

Table 5 Certificate Trust Attributes *(Continued)*

Attribute	Description
T	Trusted CA to issue client certificates (implies c)
C	Trusted CA to issue server certificates (SSL only) (implies c)
u	Certificate can be used for authentication or signing
w	Send warning (use with other attributes to include a warning when the certificate is used in that context)

The attribute codes for the categories are separated by commas, and the entire set of attributes is enclosed by quotation marks. For example, the self-signed certificate generated and installed during the gateway installation is marked "u,u,u" which means it is a server certificate (user certificate) as opposed to a root CA certificate.

Viewing Trust Attributes

All certificates and their corresponding trust attributes can be viewed by using the certificate administration script.

To view the trust attributes of a certificate:

1. As root, run the certadmin script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

The Certificate Administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Modify Trust Attributes of Certificate (e.g., for PDC)
6) List Root CA Certificates
7) List All Certificates
8) Quit

choice: [8] 7
```

2. Choose option **7** on the certificate administration menu.

Setting the Trust Attribute for a Certificate

One case in which the trust attributes of a certificate need to be modified is if client authentication is used with the gateway. An example of client authentication is PDC (Personal Digital Certificate) as described in Chapter 6 of Administration Guide. The CA that issues the PDCs must be trusted by the gateway, for example, the CA certificate should be marked "T" for SSL.

To set the trust attribute for a certificate:

1. As root, run the certadmin script. The example assumes that `/opt` is the default location.

```
# /opt/SUNWips/bin/certadmin
```

The Certificate Administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Modify Trust Attributes of Certificate (e.g., for PDC)
6) List Root CA Certificates
7) List All Certificates
8) Quit

choice: [8] 5
```

2. Choose option **5** on the certificate administration menu.

3. Enter the name of the certificate. For example, Thawte Personal Freemail C.

```
Please enter the name of the certificate:
Thawte Personal Freemail CA
```

4. Enter the trust attribute for the certificate. For example, CT,CT,CT (in this case, it is the fault new value, you just need to hit return)

```
Please enter the trust attribute you want the certificate to have
[CT,CT,CT]
```

The certificate trust attribute will be changed, and in the previous example about PDC, the client certificates signed by that CA will be recognized by the gateway.

Web Server Performance Tuning Parameters

Table 6 describes web server parameter settings that will improve the performance of the gateway component. These configuration files are located in:

install_directory/netscape/server4/https-*server_name*/config

Table 6 Web Server Performance Tuning Parameters

Name	Scope	Default	Recommended	Description
RqThrottle	magnus.conf	512	128	With iWS4.1 SP7, the maximum number of active iWS threads is calculated using the formula RqThrottle + MaxKeepAliveConnections. The Portal Administrator may modify slightly the ratio between RqThrottle and MaxKeepAliveConnections but will have to keep the sum of the two parameters around 200 in order to scale properly.
MaxKeepAliveConnections	magnus.conf	200	72	
jvm.minHeapSize	jvm12.conf	1048576	32768000	
jvm.maxHeapSize	jvm12.conf	16777216	805306368	For heavily accessed sites, it is recommended to increase the max JVM heap size to 768 MB in order to avoid a JVM abort problem due to a lack of memory.
jvm.option	jvm12.conf	-Xrunoii		JDK 1.2.2_07 provides better performance and scalability with the following option: "-Xgenconfig:32m,32m,semispaces:32m,768m,markcompact -Xoptimize"

Table 6 Web Server Performance Tuning Parameters *(Continued)*

Name	Scope	Default	Recommended	Description
cache-init	obj.conf	false	true	Enter the following line into `obj.conf` in order to disable the iWS static page cache. `Init fn="cache-init" disable="true"`

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 iPlanet Portal Server 3.0 Service Pack 3a product enables the features necessary for iPlanet Portal Server to be deployed without the services of the gateway.

The Service Pack 3a installation provides the option of installing the iPlanet Portal Server product in open-portal mode. For instructions on installing the iPlanet Portal Server software in open-portal mode, see the section, "Clean installation" under "Installation Instructions."

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

Updating an Existing Gateway/Server Installation to Open Portal Mode

Install iPlanet Portal Server 3.0 Service Pack 3a on the portal server, then do the following:

- To shut down the gateway only, use the `ipsgateway stop` command:

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

- To completely remove the gateway on a different computer from the portal server, remove the `SUNWwtgwd` and `SUNWwtsd` packages using the `pkgrm` command.
- To completely remove the gateway, and the gateway and portal server are on the same machine, remove only the `SUNWwtgwd` package using the `pkgrm` command.

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` if the default http port 80 is configured.

or

  `http://my.sun.com:`*port* where *port* is the non-default port number. For example,

  `http://my.sun.com:8080`

- 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 3a includes functionality which allows the server to access multiple instances of iPlanet Portal Server 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 the 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-siroe.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 3a on the Portal server, then do the following steps.

   See the Service Pack 3a Installation Notes in this document.

NOTE In the following instructions and examples, `/opt` is the 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, enter:

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

To determine if the port desired is available and unused.

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:siroe.iplanet.com-8081
```

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

```
# /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.siroe.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.siroe.iplanet.com:8081

http://ipsserver.siroe.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 Server instances:

```
# /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://siroe.iplanet.com:8080
http://siroe.iplanet.com:8081
http://siroe.iplanet.com:8082
```

If the machine name is `siroe.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.siroe.iplanet.com@8080
/opt/SUNWips/bin/ipsserver.siroe.iplanet.com@8081
/opt/SUNWips/bin/ipsserver.siroe.iplanet.com@8082
```

Updated Command Options

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

`./ipsserver start`	Starts the original server only.
`./ipsserver startall`	Starts the original server and all 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 discusses 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 the 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.siroe.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.siroe.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.siroe.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, go to the `/etc/opt/SUNWips` directory.

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

```
/etc/opt/SUNWips/platform.conf.siroe.iplanet.com
```

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

```
/etc/opt/SUNWips/platform.conf.siroe.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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=https://siroe.iplanet.com:8080/namingservice
ips.notification.url=https://siroe.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=&&
```

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

```
/opt/netscape/server4/https-siroe/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-siroe.iplanet.com
ServerID https-siroe.iplanet.com
ServerName siroe.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog /opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.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-siroe.iplanet.com.acl
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 the 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.siroe.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.siroe.iplanet.com`

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

   `/etc/opt/SUNWips/platform.conf.siroe.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.siroe.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=siroe.iplanet.com
ips.server.port=8081
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8081/namingservice
ips.notification.url=https://siroe.iplanet.com:8081/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=&&
```

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-siroe@port/config/magnus.conf
```

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

```
#ServerRoot /opt/netscape/server4/https-siroe.iplanet.com
ServerID https-siroe.iplanet.com
ServerName siroe.iplanet.com:8081
Port 8081
LoadObjects obj.conf
```

```
RootObject default
ErrorLog /opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.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-siroe.iplanet.com.acl
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://siroe.iplanet.com:8081
```

Configuring iPlanet Portal Server to Run as 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. If User Non-Root was installed in Service Pack 2, and is being upgraded to Service Pack 3a, see the Upgrading a User Non-Root Installation to Service Pack 3a section.

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

NOTE Authentication helpers must be run as root.

The following information is included in this procedure:

- Installation Examples
  - Installing iPlanet Portal Server Server Component
  - Installing iPlanet Portal Server Gateway Component
- Configuring User Non-Root on the Server Component
- Configuring User Non-Root on the Gateway Component
- Upgrading a User Non-Root Installation to Service Pack 3a
- Special Case Configurations
- Non-Root Error Messages
  - Server Error Messages
  - Gateway Error Messages

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 the default installation directory.

Installing iPlanet Portal Server Server Component

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.

```
# ./ipsinstall
***************************************************************
iPlanet Portal Server (3.0sp3 release)
***************************************************************

Installation log at
/var/sadm/install/logs/ipsinstall.18655/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes

Inspecting system.
Patch 106040-15 is recommended/required.
Patch 106409-01 is recommended/required.
Abort installation? [y]/n n

Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.

Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be
removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 2

Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 1

What directory to install in? [/opt]

Are the servers using SSL protocol? y/[n]

Is this a multiple server install? y/[n]

The profile server will run on siroe.iplanet.com
On what port will the profile server run? [8080]
What is the root of the profile role tree? [iplanet.com]
What is the user for the root of the role tree? [root]
The directory server will run on siroe.iplanet.com
On what port will the directory server run? [389] 8389
```

```
On what port will the gateways run? [443] 8443

Is this a multiple gateway install? y/[n]
On what hostname will the gateway run? [MyGateway] siroe
What is the sub-domain name for siroe ("." for none)? []
What is the domain name for siroe? [iplanet.com]

Should the gateway(s) use a web proxy? y/[n]

What is the administrator port for the web server? [8088]

A passphrase is needed to manage and install certificates on the
gateway
and the server, in the configuration of the web and LDAP servers
and to
allow secure communication between the gateways and servers. The
passphrase
must match between gateway and server installations.
What is the passphrase (8 chars minimum) :
Re-enter passphrase :

Start after installation completes? [y]/n

Server settings
Installation Directory : /opt
Server List            : http://siroe.iplanet.com:8080
Gateway List           : siroe.iplanet.com:8443
Profile Server         : http://siroe.iplanet.com:8080
Profile Role Tree Root : iplanet.com
Profile Role Tree User : root
LDAP Port              : 8389
LDAP Admin Port        : 8900
Web Server Admin Port  : 8088
Start Server           : y
Are these settings correct? [y]/n

Installing server.
Installing SUNWwtsdd...
Installing SUNWwtws...
Installing SUNWwtsvd...
Installing SUNWwtdt...
Installing SUNWwtnm...
Installing SUNWwtnf...
Installing SUNWwtrw...
Installing SUNWwtdoc...
Installing SUNWwtsam...
Installing SUNWwtds...

Starting server.
```

Installing iPlanet Portal Server Gateway Component

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.

```
Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 2

Is the profile server using SSL protocol? y/[n]

Should the local machine be the profile server? [y]/n
The profile server will run on siroe.iplanet.com
What is the port for the profile server? [8080]

What is the root of the role tree? [iplanet.com]
What is the user for the root of the role tree? [root]

On what hostname will the gateway run? [siroe]
What is the sub-domain name for siroe ("." for none)? []
What is the domain name for siroe? [iplanet.com]
On what port will the gateway run? [443] 8443

Does this gateway have multiple network interfaces? y/[n]

Install firewall? y/[n]

What is the passphrase (8 chars minimum) :
Re-enter passphrase :

Start after installation completes? [y]/n

Gateway settings
Installation Directory              : /opt
Gateway                             : siroe.iplanet.com:8443
Gateway IP Address                  : 192.168.01.03
Profile Server                      : http://siroe.iplanet.com:8080
Profile Role Tree Root              : iplanet.com
Profile Role Tree User              : root
Install Firewall                    : n
Start Gateway                       : y
Are these settings correct? [y]/n

Self-signed certificate for a SSL connection.
What is the name of your organization? [MyCompany] sun
What is the name of your organizational unit? [MyDivision] iplanet
What is the name of your city or locality? [MyCity] santa clara
What is the name of your state or province? [MyState] california
```

```
What is the two-letter country code? [us]

Installing gateway.
Installing SUNWwtgwd...

Starting gateway.
```

Configuring User Non-Root on the Server Component

Perform all steps as `root`, except as noted.

NOTE Install the Service Pack 3a server, gateway, and the third-party products 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 3a.

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. 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
```

3. 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-siroe/config/slapd.conf
# Netscape Directory Server global configuration file
# Do not modify this file while ns-slapd is running
##########################################################################
instancedir     "/opt/netscape/directory4/slapd-siroe"
errorlog        "/opt/netscape/directory4/slapd-siroe/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-siroe/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-siroe/config/slapd.at.conf"
include "/opt/netscape/directory4/slapd-siroe/config/slapd.oc.conf"
include "/opt/netscape/directory4/slapd-siroe/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-siroe/config/slapd.user_at.conf"
useroc  "/opt/netscape/directory4/slapd-siroe/config/slapd.user_oc.conf"
accesslog       "/opt/netscape/directory4/slapd-siroe/logs/access"
```

4. 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-siroe.iplanet.com
ServerID https-siroe.iplanet.com
ServerName siroe.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog /opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.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-siroe.iplanet.com.acl
ClientLanguage en
AdminLanguage en
DefaultLanguage en
AcceptLanguage off
RqThrottle 1024
StackSize 131072
CGIWaitPid on
CGIWaitPid on
```

5. 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: siroe.iplanet.com
uniqueMember: cn=admin-serv-siroe, cn=Netscape Administration
Server, cn=Server
 Group, cn=siroe.iplanet.com, ou=iplanet.com, o=NetscapeRoot
installationTimeStamp: 200009142206592
configuration.nsServerPort: 8900
configuration.nsSuiteSpotUser: Userid
configuration.nsServerAddress: 192.168.178.52
configuration.nsAdminEnableEnduser: on
configuration.nsAdminEnableDSGW: on
configuration.nsDirectoryInfoRef: cn=Server Group,
cn=siroe.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: *.iplanet.com
configuration.nsAdminAccessAddresses: 192.168.178.52
configuration.nsAdminOneACLDir: adminacl
configuration.nsDefaultAcceptLanguage: en
configuration.nsClassname:
com.netscape.management.admserv.AdminServer@admserv42
.jar@cn=admin-serv-siroe, cn=Netscape Administration Server,
cn=Server Group, c
n=siroe.iplanet.com, ou=iplanet.com, o=NetscapeRoot
```

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

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

7. Edit the following file, to comment out line 410, `check_root_user`, as shown in bold text:

`/opt/SUNWips/bin/ipsserver (lines 408 through 429)`

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

# 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
    ;;
```

8. 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
```

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

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

Configuring User Non-Root on the Gateway Component

1. Edit the following file, to comment out lines 172 through 176, as shown in bold text:

`/opt/SUNWips/bin/ipsgateway (lines 170 through 182)`

```
#####################################################################
# 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 component. 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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.user=Userid
ips.gateway.port=8443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.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=&&
```

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 components. From a terminal window, as the non-root user, do the following:

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

Special Case Configurations

When the iPlanet Portal Server server and gateway components are installed on the same system, both the server and gateway must be configured to run as user *non-root*.

Upgrading a User Non-Root Installation to Service Pack 3a

To upgrade Non-Root userid installation from Service Pack 2 to Service Pack 3a requires that all the user names be reset to root for the upgrade to work. Once Service Pack 3a has been installed the user will have to re-configure the server and gateway to run as Non-Root. Failure to do all these steps will result in loss of data.

The following list is a brief summary of the steps required to upgrade to Service Pack 3a:

1. Stop all services for the iPlanet Portal Server 3.0 server and gateway.

   See "Stopping the Server Component Processes."

2. If the gateway is running on a separate computer from the server, do the following:

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

      Remove `ips.gateway.user=userid`

```
# 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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.user=userid
ips.gateway.port=8443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.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=&&
```

3. Edit the following file, to uncomment line 410 (remove the #), `check_root_user`, as shown in bold text:

   `/opt/SUNWips/bin/ipsserver (lines 408 through 429)`

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

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
    ;;
```

4. Edit the following file, to change the `configuration.nsSuiteSpotUser` to `root`, 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: siroe.iplanet.com
uniqueMember: cn=admin-serv-siroe, cn=Netscape Administration
Server, cn=Server
 Group, cn=siroe.iplanet.com, ou=iplanet.com, o=NetscapeRoot
installationTimeStamp: 20000914220659Z
configuration.nsServerPort: 8900
configuration.nsSuiteSpotUser: root
configuration.nsServerAddress: 192.168.178.52
configuration.nsAdminEnableEnduser: on
configuration.nsAdminEnableDSGW: on
configuration.nsDirectoryInfoRef: cn=Server Group,
cn=siroe.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: *.iplanet.com
configuration.nsAdminAccessAddresses: 192.168.178.52
configuration.nsAdminOneACLDir: adminacl
```

```
nsServerID: admin-serv
configuration.nsDefaultAcceptLanguage: en
configuration.nsClassname:
com.netscape.management.admserv.AdminServer@admserv42
.jar@cn=admin-serv-siroe, cn=Netscape Administration Server,
cn=Server Group, c
n=siroe.iplanet.com, ou=iplanet.com, o=NetscapeRoot
```

5. In a terminal window, do the following:

```
# chown -R root:root /etc/opt/SUNWips
# chown -R root:root /var/opt/SUNWips
# chown -R root:root /opt/netscape
# chown -R root:root /opt/SUNWips
```

6. Edit the following file:

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

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

```
ServerID https-siroe.iplanet.com
ServerName siroe.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog
/opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.iplanet.com/logs/pid
User root
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-florizel.iplanet.c
om.acl
ClientLanguage en
AdminLanguage en
```

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

7. Edit the following file, to change the `localuser` to `root`, as shown in bold text:

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

```
##########################################################################
# /opt/netscape/directory4/slapd-siroe/config/slapd.conf
# Netscape Directory Server global configuration file
# Do not modify this file while ns-slapd is running
##########################################################################
instancedir     "/opt/netscape/directory4/slapd-siroe"
errorlog        "/opt/netscape/directory4/slapd-siroe/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/lib/liblcoll.so" orderingRule_init
"/opt/netscape/directory4/slapd-siroe/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/syntax-plugin.so" dn_init

plugin syntax on "Case Ignore String Syntax"
"/opt/netscape/directory4/lib/syntax-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-siroe/config/slapd.at.conf"
include "/opt/netscape/directory4/slapd-siroe/config/slapd.oc.conf"
include "/opt/netscape/directory4/slapd-siroe/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       root
userat  "/opt/netscape/directory4/slapd-siroe/config/slapd.user_at.conf"
useroc  "/opt/netscape/directory4/slapd-siroe/config/slapd.user_oc.conf"
accesslog       "/opt/netscape/directory4/slapd-siroe/logs/access"
```

8. Install the Service Pack 3a upgrade. See "Upgrading to Service Pack 3a" for the iPlanet Portal Server 3.0.
9. Reconfigure both the server and gateway to run as non-root. See "Configuring User Non-Root on the Server Component" and "Configuring User Non-Root on the Gateway Component".
10. Restore all backed up data, create all server instances, and all special configurations.

Special Case Configurations

When the iPlanet Portal Server server and gateway are installed on the same system, both the server and gateway must be configured to run as *non-root*.

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 a 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

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
```

Configuring iPlanet Portal Server to Run as 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 8080, 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.

NOTE The Netfile and Netfile Lite applications cannot use NFS protocol when running as *nobody*.

NOTE Authentication helpers must be run as `root`.

When the server component is started or restarted, it must be done as `root`.

If user nobody was installed in Service Pack 2, and is being upgraded to Service Pack 3a, see the Upgrading User Nobody to Service Pack 3a section.

The following information is included in this procedure:

- Installation Examples
  - Installing iPlanet Portal Server Server Component
  - Installing iPlanet Portal Server Gateway Component
- Configuring the Server Component to Run as User Nobody
- Configuring the Gateway Component to Run as User Nobody
- Special Case Configurations
- Upgrading User Nobody to Service Pack 3a

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 components.

Installing iPlanet Portal Server Server Component

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

TIP Non-default entries are shown in bold text.

```
# ./ipsinstall
***************************************************************
iPlanet Portal Server (3.0sp3 release)
***************************************************************

Installation log at
/var/sadm/install/logs/ipsinstall.18655/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes

Inspecting system.
Patch 106040-15 is recommended/required.
Patch 106409-01 is recommended/required.
One or more required/recommended patches are missing from your
system.
These patches may or may not apply to your system. Test this by
attempting to install the patches listed above. Please see the
Release
Notes for more information regarding patches.
Abort installation? [y]/n n

Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.

Preparing to install.

Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
```

```
3) Exit
Choice? [3] 1

What directory to install in? [/opt]

Will this be an open portal install? y/[n]

Are the servers using SSL protocol? y/[n]

Is this a multiple server install? y/[n]

The profile server will run on siroe.iplanet.com
On what port will the profile server run? [8080]

The directory server will run on siroe.iplanet.com
What is the port for the directory server? [389]

What is the root of the profile role tree? [iplanet.com]
What is the user for the profile role tree? [root]

On what port will the gateways run? [443]

Is this a multiple gateway install? y/[n]
On what hostname will the gateway run? [MyGateway] siroe
What is the sub-domain name for siroe ("." for none)? []
What is the domain name for siroe? [iplanet.com]

Should the gateway(s) use a web proxy? y/[n]

What is the administrator port for the web server? [8088]

A passphrase is needed to manage and install certificates on the
gateway
and the server, in the configuration of the web and LDAP servers
and to
allow secure communication between the gateways and servers. The
passphrase
must match between gateway and server installations.
What is the passphrase (8 chars minimum) :
Re-enter passphrase :

Start after installation completes? [y]/n

Server settings
Installation Directory : /opt
Server List            : http://siroe.iplanet.com:8080
Gateway List           : siroe.iplanet.com:443
Profile Server         : http://siroe.iplanet.com:8080
Profile Role Tree Root : iplanet.com
Profile Role Tree User : root
LDAP Port              : 389
LDAP Admin Port        : 8900
Web Server Admin Port  : 8088
Start Server           : y
Are these settings correct? [y]/n
```

```
Installing server.
Installing SUNWwtsdd...
Installing SUNWwtws...
Installing SUNWwtsvd...
Installing SUNWwtdt...
Installing SUNWwtnm...
Installing SUNWwtnf...
Installing SUNWwtrw...
Installing SUNWwtdoc...
Installing SUNWwtsam...
Installing SUNWwtds...

Starting server.
```

Installing iPlanet Portal Server Gateway Component

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.

```
Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 2

Is the profile server using SSL protocol? y/[n]

Should the local machine be the profile server? [y]/n
The profile server will run on siroe.iplanet.com
What is the port for the profile server? [8080]

What is the root of the role tree? [iplanet.com]
What is the user for the root of the role tree? [root]

On what hostname will the gateway run? [siroe]
What is the sub-domain name for siroe ("." for none)? []
What is the domain name for siroe? [iplanet.com]
On what port will the gateway run? [443]

Does this gateway have multiple network interfaces? y/[n]

Install firewall? y/[n]

A passphrase is needed to manage and install certificates on the gateway
and the server, in the configuration of the web and LDAP servers and to
allow secure communication between the gateways and servers. The passphrase
must match between gateway and server installations.
```

```
What is the passphrase (8 chars minimum) :
Re-enter passphrase :

Start after installation completes? [y]/n

Gateway settings
Installation Directory              : /opt
Role Tree Root                      : iplanet.com
Gateway                             : siroe.iplanet.com:443
Gateway IP Address                  : 192.168.01.03
Profile Server                      : http://siroe.iplanet.com:8080
Profile Role Tree Root              : iplanet.com
Profile Role Tree User              : root
Install Firewall                    : n
Start Gateway                       : y
Are these settings correct? [y]/n

Self-signed certificate for a SSL connection.
What is the name of your organization? [MyCompany] sun
What is the name of your organizational unit? [MyDivision] iplanet
What is the name of your city or locality? [MyCity] santa clara
What is the name of your state or province? [MyState] california
What is the two-letter country code? [us]

Installing gateway.
Installing SUNWwtgwd...

Starting gateway.
```

Configuring the Server Component to Run as User Nobody

Perform all steps as root, except as noted.

NOTE Install the Service Pack 3a server, gateway, and the third-party products 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 3a.

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. In this example *servername* would be siroe; use the servername that applies to your setup:

   `/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-siroe.iplanet.com
ServerName siroe.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog /opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.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-florizel.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-siroe/config/slapd.conf
# Netscape Directory Server global configuration file
# Do not modify this file while ns-slapd is running
#########################################################################
instancedir     "/opt/netscape/directory4/slapd-siroe"
errorlog        "/opt/netscape/directory4/slapd-siroe/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/lib/liblcoll.so" orderingRule_init
"/opt/netscape/directory4/slapd-siroe/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/syntax-plugin.so" dn_init

plugin syntax on "Case Ignore String Syntax"
"/opt/netscape/directory4/lib/syntax-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-siroe/config/slapd.at.conf"
include "/opt/netscape/directory4/slapd-siroe/config/slapd.oc.conf"
include "/opt/netscape/directory4/slapd-siroe/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-siroe/config/slapd.user_at.conf"
useroc  "/opt/netscape/directory4/slapd-siroe/config/slapd.user_oc.conf"
accesslog       "/opt/netscape/directory4/slapd-siroe/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-siroe.iplanet.com
ServerID https-siroe.iplanet.com
ServerName siroe.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog /opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.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-siroe.iplanet.com.acl
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: siroe.iplanet.com
uniqueMember: cn=admin-serv-siroe, cn=Netscape Administration Server,
cn=Server
 Group, cn=siroe.iplanet.com, ou=iplanet.com, o=NetscapeRoot
installationTimeStamp: 20000914220659Z
configuration.nsServerPort: 8900
configuration.nsSuiteSpotUser: nobody
configuration.nsServerAddress: 192.168.178.52
configuration.nsAdminEnableEnduser: on
configuration.nsAdminEnableDSGW: on
```

```
nsServerID: admin-serv
configuration.nsDirectoryInfoRef: cn=Server Group, cn=siroe.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: *.iplanet.com
configuration.nsAdminAccessAddresses: 192.168.178.52
configuration.nsAdminOneACLDir: adminacl
configuration.nsDefaultAcceptLanguage: en
configuration.nsClassname:
com.netscape.management.admserv.AdminServer@admserv42
.jar@cn=admin-serv-siroe, cn=Netscape Administration Server, cn=Server Group,
cn=siroe.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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.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.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 the Gateway Component to Run as User Nobody

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 Service Pack 3a server, gateway, and the third-party products before starting execution of the procedure described below. Failure to do this will result in having to redo some of the install steps.

NOTE When the gateway component is started or restarted, it must be done as root.

See the *Installation Instructions* for more information on installing Service Pack 3a.

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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.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.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, both the server and gateway must be configured to run as user nobody.

Upgrading User Nobody to Service Pack 3a

To upgrade user nobody from Service Pack 2 to Service Pack 3a requires that all the user names be reset to root for the upgrade to work. Once Service Pack 3a has been installed the user will have to re-configure the server and gateway to run as nobody. Failure to do all these steps will result in loss of data.

The following list is a brief summary of the steps required to upgrade to Service Pack 3a:

1. Stop all services for the iPlanet Portal Server 3.0 server and gateway.

   See "Stopping the Server Component Processes."

2. If the gateway is running on a separate computer from the server, do the following:

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

      Remove `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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.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.gateway.user=nobody

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

b. In a terminal window, do the following:

```
# chown -R root:root /etc/opt/SUNWips
# chown -R root:root /var/opt/SUNWips
# chown -R root:root /opt/SUNWips
```

3. Edit the following file, to change the `configuration.nsSuiteSpotUser` to `root`, 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: siroe.iplanet.com
uniqueMember: cn=admin-serv-siroe, cn=Netscape Administration Server,
cn=Server
 Group, cn=siroe.iplanet.com, ou=iplanet.com, o=NetscapeRoot
installationTimeStamp: 20000914220659Z
configuration.nsServerPort: 8900
configuration.nsSuiteSpotUser: root
configuration.nsServerAddress: 192.168.178.52
configuration.nsAdminEnableEnduser: on
configuration.nsAdminEnableDSGW: on
```

4. In a terminal window:

```
# chown -R root:root /etc/opt/SUNWips
# chown -R root:root /var/opt/SUNWips
# chown -R root:root /opt/netscape
# chown -R root:root /opt/SUNWips
```

5. Edit the following file:

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

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

```
ServerID https-siroe.iplanet.com
ServerName siroe.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog /opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.iplanet.com/logs/pid
User root
MtaHost localhost
DNS off
Security off
```

6. Edit the following file, to change the `localuser` to `root`, as shown in bold text:

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

```
return_exact_case       on
include "/opt/netscape/directory4/slapd-siroe/config/slapd.at.conf"
include "/opt/netscape/directory4/slapd-siroe/config/slapd.oc.conf"
include "/opt/netscape/directory4/slapd-siroe/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       root
userat  "/opt/netscape/directory4/slapd-siroe/config/slapd.user_at.conf"
useroc  "/opt/netscape/directory4/slapd-siroe/config/slapd.user_oc.conf"
accesslog       "/opt/netscape/directory4/slapd-siroe/logs/access"
```

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

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

```
#ServerRoot /opt/netscape/server4/https-siroe.iplanet.com
ServerID https-siroe.iplanet.com
ServerName siroe.iplanet.com
Port 8080
LoadObjects obj.conf
RootObject default
ErrorLog /opt/netscape/server4/https-siroe.iplanet.com/logs/errors
PidLog /opt/netscape/server4/https-siroe.iplanet.com/logs/pid
User root
MtaHost localhost
DNS off
Security on
```

8. Install the Service Pack 3a upgrade. See "Upgrading to Service Pack 3a" for the iPlanet Portal Server 3.0.

9. Reconfigure both the server and gateway to run as `nobody`. See "Configuring User Non-Root on the Server Component" and "Configuring User Non-Root on the Gateway Component."

10. Restore all backed up data, create all server instances, and all special configurations.

Installing and Enabling Multiple Locales 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. Users 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-availableLocales` attribute lists all the locales available for the user. For instance:

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

Although 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 `root` and change directory to `/etc/opt/SUNWips`.

2. In the appropriate platform.conf files, change the value for the `ips.nosession.url` from `/login` to:

`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.

If using multiple iPlanet Portal Server server instances, edit the platform.conf file associated with each instance.

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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=https
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=8443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.iplanet.com:8080/notifications
ervice
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://siroe:8081/login
ips.pcookie.name=iPSpCookie
ips.gateway.retries=6
```

3. Edit, the following file, as shown in bold text:

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

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

   and

   ```
   <FONT FACE="[tag:iwtDesktop-fontFace1]" SIZE="-1"><A
   HREF="https://siroe.iplanet.com:8081/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

The 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*, change default value "anonymous" to the desired 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.

Setting the Default Anonymous Username

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 Name*, change the default userid "anonymous," to the desired 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 can 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.sun.com` after successful authentication, the login link will be the following:

`http://sun.`*domain:port*`/login?goto=http://my.sun.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://sun.`*domain:port*`/logout?goto=http://sun.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 3a 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?domain=/<`*`mydomain`*`>&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.sun.com")
```

where `http://www.sun.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 an E-mail Address as the 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 Pages Provider

The JavaServer Pages™ 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_de_DE/chan.jsp
/etc/opt/SUNWips/desktop/SunBlue/myChan/chan.jsp
/etc/opt/SUNWips/desktop/SunBlue/chan.jsp
/etc/opt/SUNWips/desktop/default_de_DE/myChan/chan.jsp
```

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

For more information on implementing JSP-based channels, see the javadocs that are shipped with Service Pack 3a.

Tabbed Desktop

Service Pack 3a 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.
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 pointing to the right, 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 Provider 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 without a Server Restart

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

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

The length of time between checking to see if the disk files have been updated is the *template scan interval*. This interval 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 Anonymous Authentication Module and Login Channel delivered with Service Pack 3a.

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 provided 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 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>
```

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 *auth module* entry selected in the field after 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 3a. 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 reinstated 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
```

3. Logon as Super Administrator.

4. Select the *Manage Domains* link from the left frame.

5. In the *Portal Server Domains* page, do the following:
   a. Select the *domain* to add the Unix authentication.
6. In the *Domain, Role and Users* page:
   a. Expand *Profiles* link.
   b. Select *Authentication* link.
   c. Scroll down to, and select *Show Advanced Options.*
7. 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.
8. 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.

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

```
public static final int provider.EDIT_SUBSET ;

public static final int provider.EDIT_COMPLETE ;
```

New methods 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, so some restrictions apply 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`. 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 `Provider.EDIT_SUBSET`. Modifying the `-editType` attribute will cause a malfunction. A new channel must return `Provider.EDIT_SUBSET`, or `Provider.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 channel's 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. (Optional) Select the *Removable* check box so the channel can be removed from the desktop.
5. Select the *Submit* button.

Setting Up Full-width Channels

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 must re-login to 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

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

To view this and observe the impact, 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.

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.

As root, 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 headers. 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 7 `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
`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

Table 7 `HttpServletRequest and Responses` *(Continued)*

Methods	Returns
`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 3a, gateway default logging is disabled. To enable gateway logging do the following:

NOTE In the following instructions and examples, `/opt` is the 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 1.2.2_07
- iPlanet Web Server (iWS) 4.1 SP7
- Solaris 2.6, Solaris 7 and Solaris 8

Setting Up a Non-iPlanet Portal Server 3.0 Server

NOTE In the following instructions and examples, `/opt` is the 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=siroe.iplanet.com
ips.server.port=8080
ips.profile.host=siroe.iplanet.com
ips.gateway.protocol=http
ips.gateway.host=siroe.iplanet.com
ips.gateway.port=443
ips.virtualhost=siroe.iplanet.com 192.168.01.01
ips.naming.url=http://siroe.iplanet.com:8080/namingservice
ips.notification.url=http://siroe.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
```

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.properties

   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.PLLNotificationServlet

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 the 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 the 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.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.

Using Novell File Systems with NetFile and NetFile Lite

Service Pack 3a offers File Transfer Protocol (FTP) support for Novell file systems through the NetFile and NetFile Lite applications. The following procedures describe how Novell systems are added to the NetFile and NetFile Lite Network Neighborhood.

Adding a Novel File System to NetFile

1. Start Netfile by selecting the *Netfile* link in the *Applications* channel of the iPlanet Portal Server desktop.

2. Select *File -> Add System*.

3. Enter the fully qualified system name.

4. Choose *AUTO DETECT* or *NETWARE* as the system type, and select *OK*.

5. Add a *share* by double clicking on the system in the Network Neighborhood.

6. Enter your Netware username and password and select a directory to mount.

7. Double click on the *share* under the system name in the Network Neighborhood to browse the directory

NetFile users can now perform Netfile functions as for any other host type.

NOTE Netware adheres to an 8.3 file naming convention, so you may have to modify your filenames in order to upload them to a Netware host using Netfile. This limitation may also be evident if you are trying to compress a file on the Novell file system which already has a file extension.

Adding a Novell File System to NetFile Lite

1. Start Netfile Lite by clicking on the *Netfile Lite* link in the *Applications* channel of the Portal desktop.
2. Fill in the form field for *System Name* and select the *Machine Type* as *AutoDetect* or *NETWARE*.
3. Fill in the next form fields for *User Name*, *Password*, *Directory to mount*, and select *Enter*.
4. Select the *View Systems* link.
5. Select the *host name* from the list and select *Enter*.

Netfile functions can now be performed by using the checkboxes next to the file names and selecting an action using a button at the bottom of the page.

Defining Systems and Shares at the Domain and User Levels from the Administration Console

Service Pack 3a offers the ability to define Systems and Shares for NetFile and Netfile Lite at the domain, role and user levels. By setting the common host data attribute in the administration console, administrators can define systems and shares to be displayed in the end user's Network Neighborhood.

The following NetFile profile attributes have changed to allow administrators to define systems and shares.

- The `iwtNetFile-hostlist` attribute can no longer be edited from the administration console.
- The `iwtNetFile-commonhostdata` attribute is a new attribute that has been created for NetFile. It allows administrators to predefine systems and shares for the user.

See the following sections for instructions on defining systems and shares.

- Defining Systems and Shares at the Domain Level
- Defining Systems and Shares at the Role Level
- Defining Systems and Shares at the User Level

Defining Systems and Shares at the Domain Level

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

   To modify the common host `data` attribute, use the following format to enter (in one string with no spaces) the name, domain, type, and share information:

   `name=`*fully_qualified_host_name*`|domain=`*domain_ name*`|type=`*host_type*`|share=`*share_directory*

   - *NAME* is the remote host name
   - *DOMAIN* is the NT/WIN domain. The domain field can be "NULL" if inapplicable.
   - *TYPE* can be NT or WIN or NFS or FTP or NETWARE.
   - *SHARE* the host data can have one or more shares or directories listed.

   Some examples are:

```
name=xyz.iplanet.com|domain=workgroup|type=NT|share=tempshare|share=C$
name=abc.iplanet.com|domain=NULL|type=NETWARE|share=/sys/share1|share=/sys/sha
re2
name=pqrs.iplanet.com|type=FTP|share=/myshare
name=abcedf|domain=NULL|type=WIN|share=WINDOWS|share=DESKTOP|share=TEMP
```

7. For each entry, select *Add* to add the host and share to the list.
8. When finished, select *Submit* from the bottom of the page.

   To apply changes to subroles, select the *Apply changes to all subRoles* checkbox prior to selecting *Submit*.

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

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

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

Defining Systems and Shares at the Role Level

1. Log in to the iPlanet Portal Server administration console as the Super Administrator.
2. Select *Manage Domains*.
3. Select the desired domain.
4. Select the desired role.
5. Expand the key next to *Applications* and select *NetFile*.
6. Modify the common host data attribute in the *prepopulated Host list/type and share information* field.

   To modify the common host data attribute, use the following format to enter the name, domain, type, and share information:

   name=*fully_qualified_host_name* | domain=*domain_ name* | type=*host_type* | share=*share_directory*

   - *NAME* is the remote host name
   - *DOMAIN* is the NT/WIN domain. The domain field can be "NULL" if inapplicable.
   - *TYPE* can be NT or WIN or NFS or FTP or NETWARE.
   - *SHARE* the hostdata can have one or more shares or directories listed.

   Some examples are:

```
name=xyz.iplanet.com|domain=workgroup|type=NT|share=tempshare|share=C$
name=abc.iplanet.com|domain=NULL|type=NETWARE|share=/sys/share1|share=/sys/sha
re2
name=pqrs.iplanet.com|type=FTP|share=/myshare
name=abcedf|domain=NULL|type=WIN|share=WINDOWS|share=DESKTOP|share=TEMP
```

7. For each entry, select *add* to add the system and share to the list.
8. When finished, select *Submit* from the bottom of the page.

NOTE End users are not able to delete defined hosts and shares—even if they remove them and choose to save their session upon exit.

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

1. Login to the iPlanet Portal Server desktop.
2. Start NetFile or NetFile Lite application.
3. Select desired host and select *Edit Host Info .*
4. Enter username and password for the required host or share.

Defining Systems and Shares at the User Level

1. Log in to the iPlanet Portal Server administration console.
2. Select *Manage Domains*.
3. Select the desired domain.
4. Select the desired role.
5. Select *Users*.
6. Select the desired user name.
7. Expand the key next to *Applications* and select *NetFile.*
8. Modify the common host data attribute in the *prepopulated Host list/type and share information* field by entering the common host data in the following format:

   To modify the common host data attribute, use the following format to enter the name, domain, type, and share information:

   name=*fully_qualified_host_name* | domain=*domain_ name* | type=*host_type* | share=*share_directory*

   - *NAME* is the remote host name
   - *DOMAIN* is the NT/WIN domain. The domain field can be "NULL" if inapplicable.
   - *TYPE* can be NT or WIN or NFS or FTP or NETWARE.
   - *SHARE* the hostdata can have one or more shares or directories listed.

   Some examples are:

```
name=xyz.iplanet.com|domain=workgroup|type=NT|share=tempshare|share=C$
name=abc.iplanet.com|domain=NULL|type=NETWARE|share=/sys/share1|share=/sys/sha
re2
name=pqrs.iplanet.com|type=FTP|share=/myshare
name=abcedf|domain=NULL|type=WIN|share=WINDOWS|share=DESKTOP|share=TEMP
```

9. For each entry, select *add* to add the system and share to the list.
10. When finished, select *Submit* from the bottom of the page.

NOTE End users are not able to delete defined hosts and shares—even if they remove them and choose to save their session upon exit.

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

1. Login to the iPlanet Portal Server desktop.
2. Start NetFile or NetFile Lite application.
3. Select desired host and select *Edit Host Info .*
4. Enter username and password for the required host or share.

Defining Hidden Shares

Administrators and desktop users can define NT hidden shares for use in NetFile. The Common Host Data attribute allows administrators to define NT hidden shares through the administration console. The procedure for defining hidden shares through the administration console is the same as that for defining regular shares. See "Defining Systems and Shares at the Domain and User Levels from the Administration Console."

Desktop users can add hidden NT shares the same way they would add a regular share as long as they use the correct user name and password for the hidden share.

Alphabetized Shares on Windows NT System

Windows NT shares in NetFile are alphabetized. Because all shares on a Windows NT system are automatically displayed when a user double-clicks a system name, alphabetizing the list of shares makes it easier to locate the desired share.

Addition of `smb.conf` Parameter to `smbclient` Command

The `smb.conf` parameter has been added to the `smbclient` command. The `smb.conf` parameter allows NetFile to display ISO8859-1 character sets in file names and provides a way for administrators to configure the NetFile application to take advantage of other `smbclient` features.

An example `smb.conf` file which could be used for the Portal Server follows:

```
# Samba config file created using SWAT
# from foo.iplanet.com (1.2.3.4)
# Date: 2001/01/16 18:16:51

# Global parameters
[global]
        path=/
        workgroup = MYWORKGROUP
        security = user
        hosts allow = localhost 1.2.
        username map = /opt/samba/lib/users.map
        encrypt passwords = yes

[tmp]
        comment = temporary files
        path = /tmp
        read only = yes
        user = root

[homes]
        comment = Users' home directories
        path = /u/%S
        writeable = Yes

[printers]
        path = /tmp
        guest ok = Yes
        printable = Yes

[CTEServer]
        comment = site of web server
        path = /opt/netscape/server4

[iPortal]
        comment = top directory for iPortal files
        path = /opt/SUNWips
```

An accompanying map file, which would need to be in `/opt/samba/lib/users.map`, might look like:

```
root = admin administrator
```

For more information about Samba-specific configurations, refer to the samba website at:

```
http://samba.org/samba
```

NetFile Usability Enhancements

The Service Pack 3a product offers the following NetFile enhancements that make NetFile easier to use.

- NetFile files can be opened by double-clicking the file name.
- Multiple files can be selected for download.
- The maximum file size for uploading files with the NetFile application has been increased to 500MB. NetFile Lite still has a maximum file size of less than 5 MB.

Using a Load Balancer in Open Portal Mode

With Service Pack 3a, iPlanet Portal Server supports using a load balancer in open portal mode.

In order for the iPlanet Portal Server server to work with a load balancer in open mode, the load balancer must support persistent connections, sometimes referred to as sticky sessions based on cookies. If the load balancer supports persistence based on a cookie name and value this feature must be enabled.

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

For this feature to work correctly, the load balancer must be able to recognize the cookie on the first reply from portal. It should then continue to send all requests with that cookie name and value to that same server. Some cookie persistence algorithms will not recognize the cookie on the reply, but on the *post* or *get to* the server. This type of cookie persistence will not work since the first and second request can end up on different servers.

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

Each server defines a special cookie that the load balancer will be configured to recognize and always forward requests with that cookie to that specific server. Each portal server instance will set this cookie along with the usual portal session cookie.

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

To Use a Load Balancer in Open-Portal Mode:

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

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

```
ips.lbcookie.name=<iPSlbCookie>
ips.lbcookie.value=<some_unique_server_string>
```

NOTE Resonate™ is an example of a load balancer for which you would edit the `platform.conf` file.
When Resonate's administration console is used to create the cookie persistence rule for each server instance, the same cookie name <*iPSlbCookie*> should be used there.

3. In the administration console, add the load balancer cookie domain name to the *Cookie Domain List*.

   This step is optional. If the load balancer domain name is the same as the domain name of the servers, this step is not necessary.

   To add the load balancer domain name to the server's *Cookie Domain List*:

   a. Login to the administration console as the super administrator.
   b. Select *Server Management*.
   c. Select *Manage Server Profile*.

d. Add the load balancer domain name to the *Cookie Domain List* and select *Add*.

For example, if the cookie domain is `sun.com`, add the domain name in the following way. Note the preceding ".":

```
.sun.com
```

e. Select *Submit*.

4. Add the load balancer name to *Domain URLs* list:

a. In the administration console, select the desired domain.

b. Select *Authentication*.

c. Add the load balancer name three times to *Domain URLs* list. The following example assumes that the load balancer domain name is `sun.com`. Add the load balancer URL in the following ways (shown in bold):

```
siroe.sun.com
siroe.sun.com/sun.com
siroe.sun.com/login
192.168.66.15
192.168.66.15/sun.com
192.168.66.15/login
www.sun.com
www.sun.com/sun.com
www.sun.com/login
```

5. Edit the URL for channels that reference their content from the iPlanet Portal Server 3.0 server.

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

a. In the administration console, select the desired domain.

b. Click the key next to *Applications* to expand the list choices, and select *Desktop*.

c. Edit the URL scraper channels that reference their content from the server. Change the attribute to a relative URL by removing the protocol, server and port number from the URL.

For example, if the URL scraper channel value is:

```
http://siroe.sun.com:8080/ipinfo.html
```

Change the URL attribute so that the value is:

```
/ipinfo.html
```

d. Select *Submit*.

Loading Multiple Attributes in One Profile Request

This feature allows the desktop and other applications to load multiple attributes from multiple components in one operation. A new method called `Profile.loadAttributes` can be used to load multiple attributes in one profile request by passing in a set of attribute names that can contain wildcards for multiple profile components. The returned attribute values are cached in the profile object which allows a subsequent call to retrieve these attributes faster thereby improving overall iPlanet Portal Server performance.

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

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

Short-Circuiting for Session and Logging Requests

Short-circuiting for session and logging requests is a performance enhancement that reduces the number of HTTP requests for logging and session services, thereby improving the overall performance of the iPlanet Portal Server product.

Short-circuiting works in the following way. If the logging client and the logging server are in the same JVM, the http connection is bypassed during client and server communication. Likewise, if the session client and the session server are in the same JVM, there is no http connection in order for them to communicate. Short-circuiting also eliminates XML parsing for session and logging requests, enhancing overall performance.

Running Desktop Applications on a Macintosh Client

Service Pack 3a supports the ability to run the NetFile, NetMail, and Netlet applications on Macintosh client computers.

The NetFile and NetMail applications work on a Macintosh similar to the way they work on other supported platforms. However, the Netlet application, when used on a Macintosh, does not support the dynamic loading feature; if the Netlet is enabled, Macintosh clients automatically load the Netlet when the Netlet Channel is enabled on the desktop.

Table 8 lists the minimum system requirements for running the Netlet, NetMail, and NetFile applications on a Macintosh client.

Table 8 Minimum system requirements for running the Netlet, NetFile, and NetMail applications on a Macintosh client

Component	Description
Operating environment	Macintosh 8.6 – 9.1
Browser	Microsoft Internet Explorer 5.0
Java Virtual Machine	Macintosh OS Runtime for Java (MRJ) 2.2.3

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

Any other certificate can be used.

Unlimited Netlet Connections

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

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

Netlet Windows

The Service Pack 3a product adds an interim status window when a Netlet connection is established. This window lets the user know when the Netlet is finished loading. The contents of this interim window can be changed by modifying the nc3 value in the following file:

```
<install_dir>/SUNWips/locale/iwtNetletServlet.properties
```

```
iwtNetlet-desc=Netlet config profile
a1=Netlet Rules
a2=Warning Popup For Connections
a3=Default Loopback Port
X-x1=Debugging attribute
p1=Access To Netlet Rules
p2=Netlet access to hosts
p3=Execute Permission
p4=Netlet access to domains
ntitle=<HEAD><TITLE>Netlet</TITLE></HEAD>
nc1=<h2>Netlet runs from this browser window.</h2><p><b><font
color=red>Note:</font>  Do not close this window while using
netlet connections.  You may close this window when you no longer
want to use netlet connections.</b>
nc2=<h2>Netlet not loaded.</h2><p>Netlet is either not configured
on your desktop or has not finished loading.
ntitle2=<HEAD><TITLE>Netlet Loading</TITLE></HEAD>
nc3=<h2>Netlet is loading.</h2><p>The Netlet is still loading.
Once the Netlet has completed loading, click this button to
continue with your Netlet session.
nc4=<h2>Netlet is loading.</h2><p>Please wait while the Netlet
finishes loading. This message should change once loading is
complete.
```

```
macLoadErr=<h2>Netlet not loaded.</h2><p>Netlet is either not
configured on your desktop or use the link below to cause the
Netlet to load.<P><A HREF="#"
onClick="opener.location='/DesktopServlet?action=content&provide
r=iwtFrontProvider&macload=dynamic';
setTimeout('window.close()', 4000);">Load Netlet</A>

contButton=Continue

ntxcolor=#000000
nbgcolor=#FFFFFF

iwtNetlet-debug.on=On
iwtNetlet-debug.off=Off
iwtNetlet-debug.log=Log Messages
```

To edit the message displayed in the status window when a static rule has been defined for the current user, see the following file example, and edit as shown in bold text:

iwtNetletProvider.properties

```
#########################################################################
#########
#
# NetletProvider class msgs
#
NetletProvider-noTargets=No Netlet targets configured. Click 'Edit'
to configure Netlet targets.\n
NetletProvider-targets=Click any link to perform a Netlet function.
NetletProvider-wait=Wait until the Netlet popup initializes before
using any Netlet operations.\n
NetletProvider-nonAsciiHostname=Hostname must be ASCII characters!

iwtNetletProvider-width.Thin=thin
iwtNetletProvider-width.Thick=thick
iwtNetletProvider-width.full_top=full top
iwtNetletProvider-width.full_bottom=full bottom
iwtNetletProvider-editType.edit_subset=edit subset
iwtNetletProvider-editType.edit_complete=edit complete
```

The values in the following file are used when a Macintosh client attempts to use an automatic proxy configuration file, or when the Netlet cannot determine the Macintosh browser's proxy settings:

iwtNetletApplet.properties

```
#
lang=en
country=US
variant=
pwd.1=Netlet Connection Attempt
pwd.2=A connection attempt is being made to port
pwd.3=press OK to continue, Cancel to stop the connection
pwd.4=OK
pwd.5=Cancel
pwd.6=Don't warn again
pad.1=Netlet Proxy Authentication
pad.2=Proxy Authentication Required
pad.3=Please enter Proxy Username and Password:
pad.4=Username:
pad.5=Password:
pad.6=OK
pad.7=Cancel
ned.1=Netlet Error
ned.2=Unknown Error
ned.3=OK
ppd.1=Netlet Proxy Port
ppd.2=Netlet was unable to determine your browser proxy port setting.
ppd.3=Please enter your browser Proxy Port setting below:
ppd.4=OK
ppd.5=Cancel
pwarn.1ns=Netlet was unable to determine your browser proxy settings.
If your browser preferences are set to use Automatic Proxy
Configuration:\n\n - set the Security proxy in your browser proxy
configuration\n - close and then reopen the 'Remote File and
Windowing' window\n\nSee your network adminstrator for the correct
settings
pwarn.2ie=Netlet was unable to determine your browser proxy settings.
If your browser preferences are set to use Automatic Proxy
Configuration:\n\n - set the Security proxy in your browser proxy
configuration\n - restart your browser\n\nSee your network
adminstrator for the correct settings
pwarn.3mac=Netlet was unable configure your browser proxy settings. In
your browser's Preferences->Network->Proxies section:\n\n - add these
entries to the 'List of sites that you want to connect to
directly':\nlocalhost\n\127.0.0.1
pwarn.3=Invalid Proxies Set
pwarn.4=OK
psconn.1=Proxy authentication no username/password
psconn.3=Proxy Digest Authentication Not Supported
rwgroup.1=Unable to connect to security proxy server:
rwgroup.2=Unable to connect to Gateway:
```

The following file shows values that are used when the Netlet is started from a link within the Netlet channel itself; as opposed to being launched following a successful login as is the case with a static rule. The **nc4** value, and the **contButton** value are displayed in the *intermediate status window*:

iwtNetletServlet.properties

```
iwtNetlet-desc=Netlet config profile
a1=Netlet Rules
a2=Warning Popup For Connections
a3=Default Loopback Port
X-x1=Debugging attribute
p1=Access To Netlet Rules
p2=Netlet access to hosts
p3=Execute Permission
p4=Netlet access to domains
ntitle=<HEAD><TITLE>Netlet</TITLE></HEAD>
nc1=<h2>Netlet runs from this browser
window.</h2><p><b><fontcolor=red>Note:</font> 
Do not close this window while using netlet connections.
You may close this window when you no longer want to
use netlet connections.</b>
nc2=<h2>Netlet not loaded.</h2><p>Netlet is either
not configured on your desktop or has not finished
loading.
ntitle2=<HEAD><TITLE>Netlet Loading</TITLE></HEAD>
nc3=<h2>Netlet is loading.</h2><p>The Netlet is still loading.
Once the Netlet has completed loading, click this button
to continue with your Netlet session.
nc4=<h2>Netlet is loading.</h2><p>Please wait while
the Netlet finishes loading. This message should change
once loading is complete.
macLoadErr=<h2>Netlet not loaded.</h2>
<p>Netlet is either not configured on your desktop or
use the link below to cause the Netlet to load.<P>
<A HREF="#"
onClick="opener.location='/DesktopServlet?action=content&provider=iwt
FrontProvider&macload=dynamic'; setTimeout('window.close()',
4000);">Load Netlet</A>

contButton=Continue

ntxcolor=#000000
nbgcolor=#FFFFFF

iwtNetlet-debug.on=On
iwtNetlet-debug.off=Off
iwtNetlet-debug.log=Log Messages
```

Enabling Secure FTP Using a Netlet Connection

Service Pack 3a is designed to provide FTP service to a single FTP Server, with controlled end user accounts, which will make for secure remote FTP transfers from an end user system to a single location.

Without having a username, an FTP URL is interpreted as an anonymous FTP connection.

NOTE You *must* define port 30021 as the client port for your Netlet FTP rule.

- For example a secure FTP URL would be shown as:

  `ftp://username@localhost:30021`

- And an anonymous FTP URL shown as:

  `ftp://localhost:30021`

Setting up the FTP service to a single FTP server can be done using a static Netlet rule added to a users' desktop. This enhancement does *not* support dynamic FTP using a Netlet connection.

Setting up the Static Netlet Rule

The Netlet enhancement requires creating a Netlet rule which will listen for FTP requests.

Create a static FTP Netlet rule for the Default Role as follows:

1. As root, login to the Portal console at:

   `http://server.domain.subdomain:port/console`

2. Select *Manage Domains* and the domain to set the Netlet rule.
3. Select *DefaultRole*.
4. Expand the key next to *Applications*.
5. Select *Netlet*.
6. Select form field below the *Netlet Rules* text area and add a Netlet rule similar to this:

   `ftp|null|false|30021|your_ftp_server.your_domain|21`

7. Select *add* below the form field and then *Submit* at the bottom of the page
8. Logout from the Administration Console.

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 from the gateway to the platform server. The Netlet proxy offers improved security benefits through data encryption but may increase the use of system resources.

NOTE If configuring the iPlanet Portal Server 3.0 to run as nobody with the netlet utility, see "Configuring the Gateway Component to Run as User Nobody," before reading these instructions.

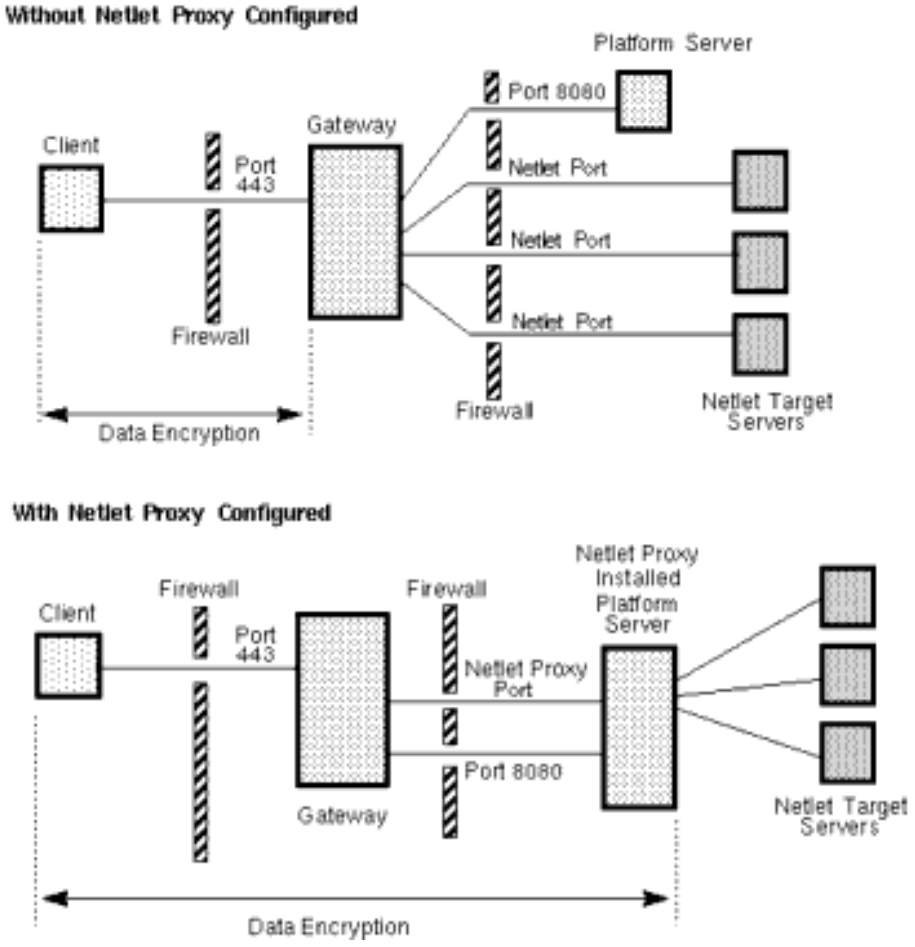

Figure 1 Netlet Proxy Implementation

Configuring the Netlet Proxy

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

1. Logon as root.
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*, enter the desired (unused) port number to be used (for example: 8048).

TIP From the command line, enter:

`netstat -a | grep` <*port_number*> **`| wc -l`**

To determine if the port desired is available and unused.

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 configure a automatic 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 iPlanet Portal Server server, repeat these steps for each server.

Configure the Netlet Proxy in the iPlanet Portal Server Administration Console before starting the portal server and gateway. See "Using the Netlet Proxy" for instructions.

In a terminal window, as root, 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* automatically start the netlet proxy when the machine is rebooted.

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

Using Automatic Proxy Configuration with the Netlet

In Service Pack 3a, the Netlet applet can be used with web browsers that are configured to use automatic proxy configuration (PAC) files. The automatic proxy configuration feature is supported in the Netscape Navigator and Internet Explorer browsers. For detailed information about atuomatic proxy configuration and PAC files, see the Netscape Developer's website.

Rewriting Javascript Functions Parameters in Javascript

The gateway will rewrite JavaScript variables or JavaScript functions according to any other existing rules specific to that variable, or that function, in the gateway profile.

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

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

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

If the list has an entry:

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

and the rewriter's input is:

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

The gateway will try to rewrite `func2` and `var3`.

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

Rewriting JavaScript Variables in JavaScript

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

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

If the list has the following entries:

- `jsvarjs1`
- `jsvarjs2`

and the rewriter's input is:

```
<html>

        <script language="JavaScript">

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

        </script>

</html>
```

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

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

Rewriting JavaScript Function Parameters Function

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

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

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

If the list has an entry:

```
func1:y
```

and the rewriter's input is:

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

Then the output will become:

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

The `iplanet` function is the same as described in Chapter 8 of the iPlanet Portal Server 3.0 Administration Guide *Rewriting JavaScript Variables Function*.

Rewriting Applet/Object Parameter Values List

The Rewrite Applet / Object Parameter Values list can be edited by using the iPlanet Portal Server administration console's Gateway Profile page. Each entry in this list has this syntax:

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

- If `url_pattern` is omitted, the value of the applet / object parameter is examined as a single URL, and the gateway will rewrite accordingly.
- If `url_pattern` is included, then the gateway will rewrite according to the pattern matching.
  - The `url_pattern` consists of *, or **, plus the separation character used in the original parameter value to separate multiple fields, one wild card (*) matches any field which is *not* to be rewritten, and two wild card (**) matches any field which *is* to be rewritten. The separation character, for example, could be "," or "|".
  - The last field to be rewritten does not have to be indicated by **, that is the `url_pattern` matches the start of the string in the parameter value, then the remainder of the value will be considered a URL to be rewritten.

If the gateway receives a request for the URL:

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

And the response is:

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

Then if the `Rewrite Applet/Object Parameter Values List` contains the following example entries, the corresponding URLs will be rewritten as noted in Table 9 below:

Table 9 Rewrite Applet/Object Parameter Values List

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

Choice Property Keys

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

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

File Lookup

In Service Pack 3a, a generic file path search utility for all data file types has been added to support the iPlanet™ Portal Server: Mobile Access Pack architecture.

All components will use the use the same utility for file lookup, including:

- Desktop template lookup

- JSP file lookup

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

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

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

The following example asks for filename `foo.template` with the values:

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

The File Lookup utility will search the following paths in order and return the first file, with the given filename, that is encountered:

```
/etc/opt/SUNWips/desktop/myType_en_US/iwtMyChannel/wml/Nokia/generic/foo.templ
ate
/etc/opt/SUNWips/desktop/myType_en_US/iwtMyChannel/wml/Nokia/foo.template
/etc/opt/SUNWips/desktop/myType_en_US/iwtMyChannel/wml/foo.template
/etc/opt/SUNWips/desktop/myType_en_US/iwtMyChannel/foo.template
/etc/opt/SUNWips/desktop/myType_en_US/foo.template
/etc/opt/SUNWips/desktop/myType/iwtMyChannel/wml/Nokia/generic/foo.template
/etc/opt/SUNWips/desktop/myType/iwtMyChannel/wml/Nokia/foo.template
/etc/opt/SUNWips/desktop/myType/iwtMyChannel/wml/foo.template
/etc/opt/SUNWips/desktop/myType/iwtMyChannel/foo.template
/etc/opt/SUNWips/desktop/myType/foo.template
/etc/opt/SUNWips/desktop/default_en_US/iwtMyChannel/wml/Nokia/generic/foo.temp
late
/etc/opt/SUNWips/desktop/default_en_US/iwtMyChannel/wml/Nokia/foo.template
/etc/opt/SUNWips/desktop/default_en_US/iwtMyChannel/wml/foo.template
/etc/opt/SUNWips/desktop/default_en_US/iwtMyChannel/foo.template
/etc/opt/SUNWips/desktop/default_en_US/foo.template
/etc/opt/SUNWips/desktop/default/iwtMyChannel/wml/Nokia/generic/foo.template
/etc/opt/SUNWips/desktop/default/iwtMyChannel/wml/Nokia/foo.template
/etc/opt/SUNWips/desktop/default/iwtMyChannel/wml/foo.template
/etc/opt/SUNWips/desktop/default/iwtMyChannel/foo.template
/etc/opt/SUNWips/desktop/default/foo.template
```

isPresentable() Method Added to the Provider API

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

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

```
contentType=text/html
```

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

An iPlanet Portal Server 3.0 channel can generate content from two methods:

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

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

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

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

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

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

Setting Session Time-out to the Maximum Value

The session time out unit of measurement is in minutes. In the Administration console, do the following to set the session time-out to the maximum possible value:

1. As Super Administrator, login to the iPlanet Portal Server administration console.
2. Select *Manage Domains*.
3. Select the name of the desired domain.

4. Select *Session* under *Profiles*.
5. Make value of *Maximum Idle Time* to the maximum value of: **153722867280912930**.
6. Make value of *Maximum Session Time* to the maximum value of: **153722867280912930**.
7. Select *Submit*.

Deprecated Features in Future Releases

The following features and products will no longer be supported in future releases of the iPlanet Portal Server product.

- Firewall software that is currently included with the iPlanet Portal Server product
- NetFile Lite
- GraphOn server and client (client still available for download)
- Citrix (available for download)
- PCAnywhere Java client (available for download)
- Mail check channel (replaced by mail channel)

Although the GraphOn client, Citrix software, and PCAnywhere Java client will no longer be included as third party software with the iPlanet Portal Server product, they will continue to work with the iPlanet Portal Server product and will be available from their respective websites.

Software and Hardware Requirements

This section describes the system requirements for Service Pack 3a software. The system requirements depend on how the iPlanet Portal Server 3.0 product is used.

- Table 10 describes the system requirements for developing a portal.
- Table 11 describes the system requirements for deploying a portal.

Table 10 System Requirements for Developing a Portal

Component	Description
Computer type	Two-CPU Ultra Sparc machine.

Table 10 System Requirements for Developing a Portal

Component	Description
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 MB of memory.
Partition space	/tmp (swap space) 500 MB
	/var 500 MB
	/usr 1 GB
	/opt 1 GB
	/etc 500 MB
	Installation directory 500 MB
	If the installation directory is `/opt`, increase this partition to 1.5 GB
Software	Coexistence with other software is not supported.
Patches	Required or recommended Solaris patches are located in./patches/<*solaris_version*>/<*solaris_version_patch_cluster*>. For more information on installing the required or recommended patches, see "Installing the Required Solaris Patches."
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 enabled.
PATH environment	The PATH environment must include `/usr/sbin:/usr/bin`.

Table 11 System Requirements for Deploying a Portal

Component	Description
Computer type	Two-CPU Ultra Sparc 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.

Table 11 System Requirements for Deploying a Portal *(Continued)*

Component	Description
Partition space	/tmp (swap space) 2 GB
	/var 1 GB
	/usr 1 GB
	/opt 1 GB
	/etc 500 MB
	Installation directory 500 MB
	If the installation directory is `/opt`, increase this partition to 1.5 GB
Software	Coexistence with other software is not supported.
Patches	Required or recommended Solaris patches are located in ./patches/<*solaris_version*>/<*solaris_version_patch_cluster*>. For more information on installing the required or recommended patches, see "Installing the Required Solaris Patches."
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 enabled.
PATH environment	The PATH environment for the administrative user must include `/usr/sbin:/usr/bin`.

Service Pack 3a Installation Notes

The iPlanet Portal Server 3.0 Service Pack 3a is a cumulative service pack. It includes all Service Pack 1, Service Pack 2, Service Pack 3a bug fixes and related hotpatch fixes. It can be used to install the iPlanet Portal Server product as a new install on a machine with no previous installations of the iPlanet Portal Server software, and to upgrade the following installations:

- iPlanet Portal Server 3.0
- iPlanet Portal Server 3.0 + Service Pack 1
- iPlanet Portal Server 3.0 + Service Pack 2

Software Dependencies for the Service Pack 3a Upgrade

The iPlanet Portal Server Service Pack 3a installation process provides the following dependency upgrades to the iPlanet Portal Server 3.0 product.

- iPlanet Directory Server (iDS) 4.14
- iPlanet Web Server (iWS) 4.1 SP7
- JDK 1.2.2_07
- JSS 2.1 which includes NSS 2.8.4

NOTE Certificates installed on the gateway component for the previous SSL library are automatically converted to the format required by NSS when Service Pack 3a is installed.

Contents of `iPS3.0SP3-01.tar`

The iPlanet Portal Server 3.0 Service Pack 3a (iPS3.0SP3-01) software can be downloaded from the iPlanet web page as a series of tar files. Once assembled into one tar file, the following directories and files are included in `iPS3.0SP3-01.tar`. For instructions on downloading and assembling the tarfiles see “Downloading the Service Pack 3a Software Package.”

- iPlanet Portal Server Service Pack 3a packages and scripts
  - SUNWicgSA
  - SUNWicgSS
  - SUNWj2dem
  - SUNWj2dev
  - SUNWj2man
  - SUNWj2rt
  - SUNWwtdoc
  - SUNWwtds
  - SUNWwtdt
  - SUNWwtfw
  - SUNWwtgwd
  - SUNWwtnf

- SUNWwtnm
- SUNWwtrw
- SUNWwtsam
- SUNWwtsvd
- SUNWwtsdd
- SUNWwtws
- attribute
- ipsinstall
- patches
- locale
- property
- template
- update

Preparing for Installation

Before you begin installing Service Pack 3a, see the following sections for pre-installation tasks.

- Installed Software Modules, Customizations, and Third Party Products
- Downloading the Service Pack 3a Software Package
- Installing the Required Solaris Patches
- Stopping the Server Component Processes
- Stopping the Proxies and the Gateway Component's Processes
- Saving the Certificates Used by the Server Component
- Stopping the Third-party Software Processes and the Channels

When using the `tar` and `ps` commands called for in the following procedures, use the commands found in `/usr/bin`.

Installed Software Modules, Customizations, and Third Party Products

If iPlanet Portal Server 3.0 software has been previously installed and other modules have been configured to run on top of this software, it is important to read all release notes and updates that pertain to the added modules. It may be required to install patches and additional configuration steps. Also, any customizations must be backed up or documented before Service Pack 3a is installed, so the customizations can be implemented again after the upgrade.

Third party software that was originally included as a separate CD with the iPlanet Portal Server product, is available for download from the iPlanet website, `www.iplanet.com`. The iPlanet website contains a third party download directory in which the third party software file, `ThirdParty.tar.gz`, is located.

Instructions for installing third party products shipped with iPlanet Portal Server 3.0 remain the same for the Service Pack 3a release as for the iPlanet Portal Server 3.0 release. See "Appendix B" in the iPlanet Portal Server *Installation Guide* for instructions on installing third party software shipped with the iPlanet Portal Server product.

NOTE The Samba software is removed by performing an upgrade, by removing the current iPlanet Portal Server installation, and by performing an installation in which the previous installation is automatically removed.

Downloading the Service Pack 3a Software Package

The iPlanet Portal Server 3.0 Service Pack 3a software package is available from the iPlanet.com web page:

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

The software package has been split into twelve 20-Megabyte files to make the Service Pack 3a product easier to download. In addition to downloading the Service Pack 3a tar files, download the checksums file and the `assembleiPS3SP3` script for assembling the individual files into a single Service Pack 3a. The following instructions describe how to check the integrity of the files once they have been downloaded and how to assemble the files for installation.

NOTE If the iPlanet Portal Server 3.0 installation contains individual gateway and platform servers, the Service Pack 3a package must be installed on both servers.

---

1. In a terminal window, become root.

2. Change directories to /opt and create a directory in which to download the Service Pack 3a tar files. For example

```
# cd /opt
# mkdir ips_sp3
```

3. Download the following files into the directory created in step 2.
   - iPS3.0SP3-01.tar.gz.aa
   - iPS3.0SP3-01.tar.gz.ab
   - iPS3.0SP3-01.tar.gz.ac
   - iPS3.0SP3-01.tar.gz.ad
   - iPS3.0SP3-01.tar.gz.ae
   - iPS3.0SP3-01.tar.gz.af
   - iPS3.0SP3-01.tar.gz.ag
   - iPS3.0SP3-01.tar.gz.ah
   - iPS3.0SP3-01.tar.gz.ai (On the ftp site, this file is named iPS3.0SP3-01.tar.gz.es)
   - iPS3.0SP3-01.tar.gz.aj
   - iPS3.0SP3-01.tar.gz.ak
   - PS3.0SP3-01.tar.gz.al
   - checksums
   - assembleiPS3SP3
4. In `/opt/ips_sp3`, run the `assembleiPS3SP3` script to verify that the files are all present and that the file data has not been corrupted.

```
# /usr/bin/ksh ./assembleiPS3SP3
```

If the script determines that the correct number of files are present and that their data has not been corrupted, a single tar file `iPS3.0SP3-01.tar.gz` is created, which contains all the Service Pack 3a packages.

5. Run the `gunzip` command to extract the `iPS3.0SP3-01.tar.gz` file.

```
# gunzip iPS3.0SP3-01.tar.gz
```

6. Run the `tar` command to extract the contents of the `iPS3.0SP3-01.tar` file.

```
# /usr/bin/tar -xvf iPS3.0SP3-01.tar
```

NOTE Use the Solaris version of the tar command.

Installing the Required Solaris Patches

The iPlanet Portal Server product is shipped with Solaris patches that are required or recommended for the iPlanet Portal Server software. The directory `/opt/ips_sp3/patches` contains patch directories for each supported version of Solaris. Use the patches in the directory that corresponds to the version of Solaris on which you are installing the iPlanet Portal Server product. Solaris patches are periodically updated, and can be downloaded from `www.sunsolve.sun.com`.

To install the required or recommended Solaris patches:

1. As root, change directories to the patch directory that corresponds to the version of the Solaris operating system on which the iPlanet Portal Server product is installed. For example, if the iPlanet Portal Server product is installed on Solaris 8:

```
# cd /opt/ips_sp3/patches/solaris8/solaris_2.8_patch_cluster
```

2. Run the install_cluster installation script:

```
# ./install_cluster
```

3. Reboot your computer.

```
# reboot
```

Stopping the Server Component Processes

Before upgrading or installing the Service Pack 3a software, stop the following services:

- Directory server
- Web server

NOTE The following instructions assume that the installation directory is `/opt`.

1. Issue the following command to see which directory server and web server processes are running. By viewing the processes that are currently running, you can reissue the command after stopping the processes to verify that have been stopped.

```
# /usr/bin/ps -eo pid,args | grep /opt/netscape
446 ./ns-slapd -f
/opt/netscape/directory4/slapd-siroe/config/slapd.conf -i /opt/
467 ns-httpd -d
/opt/netscape/server4/https-siroe.iplanet.com/con
458 ./uxwdog -d /opt/netscape/server4/https-admserv/config
466 ./uxwdog -d
/opt/netscape/server4/https-siroe.iplanet.com/con
459 ns-httpd -d /opt/netscape/server4/https-admserv/config
29857 ./ns-admin -d /opt/netscape/directory4/admin-serv/config
```

In this example, the process id numbers correspond with the following processes.

process id	process
446	directory server process
467	web server process
458	watchdog process for web server admin service
466	watchdog service for the web server
459	admin service for the web server
29857	admin service for the directory server

2. Stop the iPlanet Portal Server server component. This step stops the directory server and web server processes.

- If running iPlanet Portal Server 3.0 or iPlanet Portal Server Service Pack 1, start and stop the server component.

```
# /etc/init.d/ipsserver start
stopping auth helpers ... done.
stopping web server ... done.
stopping directory server ... done.
starting auth helpers ... done.
starting directory server ... done.
starting web server ... done.
# /etc/init.d/ipsserver stop
stopping auth helpers ... done.
stopping web server ... done.
stopping directory server ... done.
```

- If running iPlanet Portal Server Service Pack 2, stop the server component.

```
# /etc/init.d/ipsserver stopall
stopping auth helpers ... done.
stopping web server ... done.
stopping directory server ... done.
```

3. Verify that all directory server and web server processes are stopped. The processes that were running in step 1 should no longer be displayed.

```
# /usr/bin/ps -eo pid,args | grep /opt/netscape
```

   - If any of the processes are still running, issue a `kill -TERM` *`process_id`* for each directory server process or web server process that is running under iPlanet Portal Server. For example:

```
# kill -TERM 446
```

Stopping the Proxies and the Gateway Component's Processes

Before upgrading to or installing Service Pack 3a, the following processes need to be stopped.

- ipshttpd proxy process
- ipsnetletd proxy process
- gateway component process

1. Issue the following command to see which gateway processes are running. By viewing the processes that are currently running, you can reissue the command after stopping the processes to verify that have been stopped.

```
# /usr/bin/ps -eo pid,args|grep java
481 /usr/java/bin/../jre/bin/../bin/sparc/native_threads/java
-ms32m -mx128m -class
503 /usr/java/bin/../jre/bin/../bin/sparc/native_threads/java
-ms32m -mx128m -class
741 /usr/jave/bin/../jre/bin/../bin/sparc/native_threads/java
-ms32m -mx128m -class
```

In this example the process id numbers correspond with the following processes.

process id	proxy process
481	ipshttpd process
503	ipsnetletd process
741	gateway process

2. Stop the ipshttpd or ipsnetletd proxies that are running on the server component.

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

3. Stop the iPlanet Portal Server gateway component.

```
# /etc/init.d/ipsgateway stop
```

4. Verify that the processes have been stopped. The processes that were running in step 1 should no longer be displayed.

```
# /usr/bin/ps -eo pid,args|grep java
```

- If any of the processes are still running, issue a `kill -TERM` *`process_id`* for each proxy process that is running under iPlanet Portal Server. For example:

```
# kill -TERM 481
```

Stopping the Third-party Software Processes and the Channels

Before performing a clean installation of or upgrading to Service Pack 3a, stop all iPlanet Portal Server third-party software and channels that push data to the iPlanet Portal Server product.

It is especially important to stop channels that push data to the iPlanet Portal Server product because some channels write into iPlanet Portal Server directories. For example, iSyndicate writes to `/var/opt/SUNWips/debug` which interferes with Service Pack 3a.

Consult the manuals for each channel and for third-party software for instructions on shutting down.

Saving the Certificates Used by the Server Component

If using certificates on the iPlanet Portal Server server component, save the certificates in a safe location before the upgrade process, and restore them after the upgrade is complete.

The following procedure assumes that `/opt` is the installation directory.

To save the certificates:

1. As root, change directories to the certificate directory. In the following example, `/opt` is the base directory.

```
# cd /opt/netscape/server4
```

2. Create a tar file of the alias directory and copy it to a safe location. In the following example the compressed alias directory is copied to `/usr/tmp`.

```
# tar cf /usr/tmp/alias.tar alias
```

See “Upgrading to Service Pack 3a” for instructions on upgrading the iPlanet Portal Server product to Service Pack 3a.

Installation Instructions

The Service Pack 3a installation script offers the choice of upgrading the existing version of the product or performing a clean installation of the product. Choosing the upgrade option upgrades the iPlanet Portal Server product to Service Pack 3a.

Performing a clean installation removes all aspects of a previous iPlanet Portal Server software installation. A clean installation can be useful if an existing installation has problems that might be resolved by a fresh installation.

NOTE The Service Pack 3a software can also be installed as a new iPlanet Portal Server installation requiring no previous iPlanet Portal Server installations.

Sample Machine Names

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

Table 12 Sample machine names

Machine Name	Type of iPlanet Portal Server Component
siroe	iPlanet Portal Server server component acting as the profile server
varrius	iPlanet Portal Server server component not being used as the profile server in multiple server installations
sesta	iPlanet Portal Server gateway component

The installation procedures documented in this section are categorized based on the following types of installations. Select the installation procedures which best suit the type of installation you want to perform.

- Upgrading to Service Pack 3a

- Standard Upgrade
- Upgrading a User Non-Root Installation to Service Pack 3a (requires performing the standard upgrade procedure first)
- Upgrading User Nobody to Service Pack 3a (requires performing the standard upgrade procedure first)

- Clean installation
  - Open-portal Installation Using a Single Machine
  - Open-portal Installation Using Multiple Machines
  - Secure Portal Installation on a Single Server (Followed by gateway installation)
  - Secure Portal Installation on Multiple Servers (Followed by gateway installation)
  - Gateway Component Installation

NOTE If iPlanet Portal Server 3.0 software has been previously installed and other modules have been configured to run on top of this software, it is important to read all release notes and updates that pertain to the added modules. This is especially applicable to the Compass 3.01C Release Notes found on: `http://docs.iplanet.com`

Upgrading to Service Pack 3a

NOTE If this is an upgrade of user `non-root`, or user `nobody`, go to the appropriate sections in these release notes.

- "Upgrading a User Non-Root Installation to Service Pack 3a
- "Upgrading User Nobody to Service Pack 3a

Standard Upgrade

If the Samba software has been installed, this procedure removes it. The Samba software, along with other third party software originally shipped with the iPlanet Portal Server product, is contained in a file called ThirdParty.tar.gz and can be downloaded from the `www.iplanet.com` website. See "Appendix B" in the iPlanet Portal Server *Installation Guide* for instructions on installing the Samba software.

To upgrade the iPlanet Portal Server software:

1. Backup the iPlanet Portal Server 3.0 installation.
2. If the iPlanet Portal Server processes are running, stop all iPlanet Portal Server processes. See "Stopping the Server Component Processes."
   - If installing from the CD-ROM, perform step 3, step 4, and continue with step 6.
   - If installing from a download, go to step 5.
3. As root, mount the Service Pack 3a CD-ROM.

```
# volcheck
```

4. Change directories to /cdrom/cdrom0 and run the ipsinstall script.

```
# cd /cdrom/cdrom0
# ./ipsinstall
```

5. As root, change directories to `/opt/ips_sp3` and run the `ipsinstall` script. The `ipsinstall` script must be run from the directory in which it exists.

```
# cd /opt/ips_sp3
# ./ipsinstall
```

   The installation script then displays the Service Pack 3a license agreement.

6. Enter **yes** to accept the license agreement and continue with the installation.

```
************************************************************
iPlanet Portal Server (3.0-SP3a release)
************************************************************
Installation log at
/var/sadm/install/logs/ipsinstall.2406/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes
```

NOTE If the installation script detects missing Solaris patches, a warning message is displayed. See "Installing the Required Solaris Patches" for information on installing the necessary Solaris patches.

The installation script attempts to determine name and IP address information about the machine on which you are installing. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the portal.

7. Accept the default values or enter the correct name and IP address information.

```
Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.
```

The script displays the task menu.

8. Enter **1** to upgrade an existing iPlanet Portal Server installation.

```
Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be
removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 1
```

NOTE If any of the iPlanet Portal Server processes are still running, the installation script displays a warning message and process information. If the processes detected by the script are related to the iPlanet Portal Server, abort the upgrade, and stop the processes before proceeding. See “Stopping the Server Component Processes” and “Stopping the Proxies and the Gateway Component’s Processes” for instructions.

NOTE If any ports used by the iPlanet Portal Server product are in use, the installation script displays a warning message and port information. If other applications are running on the ports required by the iPlanet Portal Server product, exit the applications and wait for the ports to close before proceeding.

The script displays the following status:

```
Reading current configuration.

Checking running status.

Pre-upgrade processing.

Installing server.
Installing SUNWwtsdd...
Installing SUNWwtws...
Installing SUNWwtsvd...
Installing SUNWwtdt...
Installing SUNWwtnm...
Installing SUNWwtnf...
Installing SUNWwtrw...
Installing SUNWwtdoc...
```

```
Installing SUNWwtsam...
Installing SUNWwtds...

Starting server.

Installing gateway.
Installing SUNWwtgwd...

Starting gateway.

Post-upgrade processing.

Starting server.

Starting gateway.

Upgrade complete.
Please look in /var/sadm/install/logs/ipsinstall.611
for saved certificates, attributes, properties and templates.
If you have made any customizations to iPS before this upgrade,
you may need to merge your changes back.
```

When the upgrade process is finished, your screen prompt is returned. Look in `/var/sadm/install/logs/ipsinstall.<`*process.id*`>/install.log` to verify that no errors in the upgrade have occurred.

If your previous iPlanet Portal Server installation was customized, see “Restoring Customizations” for more information.

Restoring Customizations

If you performed customizations on your previous iPlanet Portal Server installation, the installation script saves these customizations in `/var/sadm/install/logs/ipsinstall.<`*process_id*`>`. Generally, the same steps used for the initial customization development can be used when reinstating your customizations into Service Pack 3a installation. If you reinstate previous customizations, run the iPlanet Portal Server product to verify that your customizations still work. Certain customizations could be affected by changes in Service Pack 3a.

TIP	By using the `diff` command to compare pre-Service Pack 3a files and the new Service Pack 3a files, changes can be viewed so that previous customizations can be reinstated.

See “After Installation” for information on Restoring Certificates.

Clean installation

The instructions for performing a clean installation of the iPlanet Portal Server Service Pack 3a server and gateway components assume the following:

- A previous version of an iPlanet Portal Server software is installed
- The Service Pack 3a software package has been downloaded to `/opt/ips_sp3`

If the Samba software has been installed, performing a clean installation in which the previous installation is removed also removes the Samba software. The Samba software, along with other third party software originally shipped with the iPlanet Portal Server product, is contained in a file called `ThirdParty.tar.gz`, which can be downloaded from the `www.iplanet.com` website. See "Appendix B" in the iPlanet Portal Server *Installation Guide* for instructions on installing the Samba software.

Open-portal Installation Using a Single Machine

In open-portal mode, the gateway, which provides encryption services and URL rewriting, is not required. For more information, see "Open Portal Mode."

To install the server component on a single machine:

1. Backup the iPlanet Portal Server 3.0 installation.
2. If the iPlanet Portal Server processes are running, stop all iPlanet Portal Server processes. See "Stopping the Server Component Processes."
    - If installing from the CD-ROM, perform step 3, step 4, and continue with step 6.
    - If installing from a download, go to step 5.
3. As root, mount the Service Pack 3a CD-ROM.

```
# volcheck
```

4. Change directories to /cdrom/cdrom0 and run the ipsinstall script.

```
# cd /cdrom/cdrom0
# ./ipsinstall
```

5. As root, change directories to `/opt/ips_sp3` and run the `ipsinstall` script. The `ipsinstall` script must be run from the directory in which it exists.

```
# cd /opt/ips_sp3
# ./ipsinstall
```

The installation script then displays the Service Pack 3a license agreement.

6. Enter **yes** to accept the license agreement and continue with the installation.

```
************************************************************
iPlanet Portal Server (3.0-SP3a release)
************************************************************
Installation log at
/var/sadm/install/logs/ipsinstall.28532/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes
```

NOTE If the installation script detects missing Solaris patches, a warning message is displayed. See "Installing the Required Solaris Patches" for information on installing the necessary Solaris patches.

The installation script attempts to determine name and IP address information about the machine on which you are installing. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

7. Accept the default values or enter the correct name and IP address information.

```
Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.
```

The script displays the task menu.

8. Choose **2** to perform a fresh installation of the iPlanet Portal Server components.

```
Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 2

Removing current installation.
```

The script displays the component menu.

9. Choose **1** to install the server component.

```
Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 1
```

10. Accept the default installation directory, or enter another directory in which to install.

```
What directory to install in? [/opt]
```

11. Choose **y** for an open-portal installation.

```
Will this be an open portal install? y/[n]
```

12. Choose whether you want to use Secure Sockets Layer (SSL) to communicate with the server component. SSL provides encrypted communication to the server. For information about using SSL with the iPlanet Portal Server product, see the iPlanet Portal Server *Administration Guide*.

```
Are the servers using SSL protocol? y/[n]
```

13. Choose **n** for a single server installation.

```
Is this a multiple server install? y/[n]
```

14. Accept the default profile server port number or enter an available port number.

```
The profile server will run on siroe.iplanet.com
On what port will the profile server run? [8080]
```

15. Press Return to accept the default for the role tree root, or enter another name.

```
What is the root of the profile role tree? [iplanet.com]
```

NOTE The name of the role tree root does not have to be a DNS domain name; it can be any name you choose. See Chapter 1 of the *iPlanet Portal Server 3.0 Administration Guide* for more information about the role tree.

16. Accept the default or enter the correct name for the root user.

```
What is the user for the profile role tree? [root]
```

17. Accept the default port number for the directory server, or enter an available port number.

```
On what port will the directory server run? [389]
```

18. Accept the default administrator port number or enter an available port number.

```
What is the administrator port for the web server? [8088]
```

The installation script prompts you to enter and verify a passphrase. This passphrase is not the root user's password. It is used internally for SSL communication to the server and for access to the iPlanet Webserver administration console.

19. Enter and verify the passphrase.

```
What is the passphrase (8 chars minimum) :
Re-enter passphrase :
```

The installation script displays the settings and asks if they are correct.

20. Answer **y** to install the server. The installation script installs the server packages.

```
Server settings
Installation Directory : /opt
Server List            : http://siroe.iplanet.com:8080
Profile Server         : http://siroe.iplanet.com:8080
Profile Role Tree Root : iplanet.com
Profile Role Tree User : root
LDAP Port              : 389
LDAP Admin Port        : 8900
Web Server Admin Port  : 8088
Start Server           : y
Are these settings correct? [y]/n
```

NOTE If you choose **n**, the script repeats the questions and gives you the opportunity to change the settings.

The installation script installs the following packages.

```
Installing server.
Installing SUNWwtsdd...
Installing SUNWwtws...
Installing SUNWwtsvd...
Installing SUNWwtdt...
Installing SUNWwtnm...
Installing SUNWwtnf...
Installing SUNWwtrw...
Installing SUNWwtdoc...
Installing SUNWwtsam...
Installing SUNWwtds...
```

After the installation process has been completed, the script automatically starts the server component.

For information on configuring multiple-instances of the iPlanet Portal Server product on a single server machine, see “Configuring Multiple Instances of iPlanet Portal Server.”

Open-portal Installation Using Multiple Machines

In open-portal mode, the gateway, which provides encryption services and URL rewriting, is not required. For more information, see “Open Portal Mode.”

NOTE If installing the server component on multiple machines, designate only one machine as the profile server, and configure the other servers to reference that machine as the profile server.

To install the server component:

1. Backup the iPlanet Portal Server 3.0 installation.
2. If the iPlanet Portal Server processes are running, stop all iPlanet Portal Server processes. See “Stopping the Server Component Processes.”
   - If installing from the CD-ROM, perform step 3, step 4, and continue with step 6.
   - If installing from a download, go to step 5.
3. As root, mount the Service Pack 3a CD-ROM.

```
# volcheck
```

4. Change directories to /cdrom/cdrom0 and run the ipsinstall script.

```
# cd /cdrom/cdrom0
# ./ipsinstall
```

5. As root, change directories to `/opt/ips_sp3` and run the `ipsinstall` script. The `ipsinstall` script must be run from the directory in which it exists.

```
# cd /opt/ips_sp3
# ./ipsinstall
```

The installation script then displays the Service Pack 3a license agreement:

6. Enter **yes** to accept the license agreement and continue with the installation.

```
************************************************************
iPlanet Portal Server (3.0-SP3a release)
************************************************************
Installation log at
/var/sadm/install/logs/ipsinstall.28532/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes
```

NOTE If the installation script detects missing Solaris patches, a warning message is displayed. See "Installing the Required Solaris Patches" for information on installing the necessary Solaris patches.

The installation script attempts to determine name and IP address information about the machine on which you are installing. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

7. Accept the default values or enter the correct name and IP address information.

```
Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.
```

The script displays the task menu.

8. Choose **2** to perform a fresh installation of the iPlanet Portal Server components.

```
Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 2
```

The script displays the following component menu.

9. Choose **1** to install the server component.

```
Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 1
```

10. Accept the default installation directory, or enter another directory in which to install.

```
What directory to install in? [/opt]
```

11. Choose **y** for an open-portal installation.

```
Will this be an open portal install? y/[n] y
```

12. Choose whether you want to use Secure Sockets Layer (SSL) to communicate with the server component. SSL provides encrypted communication to the server. For information about using SSL with the iPlanet Portal Server product, see the iPlanet Portal Server *Administration Guide.*

```
Are the servers using SSL protocol? y/[n]
```

13. Choose **y** for a multiple server installation.

```
Is this a multiple server install? y/[n] y
```

14. Choose whether you want the local computer to be the profile server.

- Enter **y** to make the local computer the profile server. If you have not already installed the profile server on another computer, you can choose **y** to make the local computer the profile server. Go to step 16.
- Enter **n** if you have already installed the profile server on another computer or if you will install the profile server on another computer. Continue with step 15.

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

NOTE If your Service Pack 3a environment includes servers installed on multiple machines, install the profile server on only one of the machines; configure all other server components to reference that machine as the profile server.

If the local machine is not the profile server, the installation script asks for information about the profile server.

15. Enter the profile server information. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component. Go to step 17.

```
On what hostname will the profile server run? [MyProfileServer] siroe
What is the sub-domain name for siroe("." for none)? []
What is the domain name for siroe? [iplanet.com]
On what port will siroe run? [8080]
What is the ip address of siroe.iplanet.com? [192.168.01.01]
```

If the local machine is the profile server, the installation script asks for the profile server port number.

16. Accept the default profile server port number or enter the correct number for the port.

```
The profile server will run on siroe.iplanet.com
On what port will the profile server run? [8080]
```

17. Press Return to accept the default for the role tree root, or enter another name.

```
What is the root of the profile role tree? [iplanet.com]
```

NOTE The name of the role tree root does not have to be a DNS domain name; it can be any name you choose. See Chapter 1 of the *iPlanet Portal Server 3.0 Administration Guide* for more information about the role tree.

18. Accept the default root user name or enter the correct name for the root user.

```
What is the user for the profile role tree? [root]
```

19. Accept the default port number for the directory server or enter an available port number.

```
On what port will the directory server run? [389]
```

- If the local machine is not the profile server, go to step 21.
- If the local machine is the profile server, the installation script asks you the following set of questions about the server components of the Service Pack 3a product. Continue with step 20.

20. Enter the server component information. Go to step 22.

If the local computer is the profile server and you specified multiple server components, the script repeats the set of questions until you have specified information for all the desired server components. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

The script repeats the set of questions, allowing you to enter name and IP address information for each server component in a multiple server environment. Enter a "." after you have finished adding the information for all the server components.

```
On what hostname will the server run ("." when done)? [MyServer] varrius
What is the sub-domain name for varrius ("." for none)? []
What is the domain name for varrius? [iplanet.com]
On what port will varrius run? [8080]
What is the ip address of varrius.iplanet.com? [192.168.01.02]
On what hostname will the next server run ("." when done)? [MyServer] .
```

21. Accept the default server port number for the machine on which you are installing or enter an available port number.

```
On what port will the server run on this machine? [8080]
```

22. Accept the default web server administrator port number or enter the correct port number.

```
What is the administrator port for the web server? [8088]
```

The installation script prompts you to enter and verify a passphrase. This passphrase is not the root user's password. It is used internally for SSL communication to the server and for access to the iPlanet Webserver administration console.

23. Enter and verify the passphrase.

```
What is the passphrase (8 chars minimum) :
Re-enter passphrase :
```

The installation script displays the settings and asks if they are correct.

24. Answer **y** to install the server. The installation script installs the server packages.

```
Server settings
Installation Directory : /opt
Server List            : http://siroe.iplanet.com:8080
                       : http://varrius.iplanet.com:8080
Profile Server         : http://siroe.iplanet.com:8080
Profile Role Tree Root : iplanet.com
Profile Role Tree User : root
LDAP Port              : 389
LDAP Admin Port        : 8900
Web Server Admin Port  : 8088
Start Server           : y
Are these settings correct? [y]/n
```

NOTE If you choose **n**, the script repeats the questions and gives you the opportunity to change the settings by repeating the installation questions.

The installation script installs the following packages.

```
Installing server.
Installing SUNWwtsdd...
Installing SUNWwtws...
Installing SUNWwtsvd...
Installing SUNWwtdt...
Installing SUNWwtnm...
Installing SUNWwtnf...
Installing SUNWwtrw...
Installing SUNWwtdoc...
Installing SUNWwtsam...
Installing SUNWwtds...
```

After the installation process has been completed, the script automatically starts the server component. Repeat this procedure for each server component in a multiple-server environment.

For information on configuring multiple-instances of the iPlanet Portal Server product on a single server machine, see “Configuring Multiple Instances of iPlanet Portal Server.”

CAUTION If you are upgrading your iPlanet Portal Server 3.0 to Service Pack 3a, and Compass 3.01C was already installed, it is also necessary to install Compass 3.01C Patch 1. This patch can be found at the iPlanet.com web page: `http://iplanet.com/downloads/patches`

Secure Portal Installation on a Single Server

In secure mode, the gateway, which provides encryption services and URL rewriting, is required. For instructions on installing the gateway component, see "Gateway Component Installation."

NOTE If installing a single server component, the machine on which you install must be the profile server.

To install the server component:

1. Backup the iPlanet Portal Server 3.0 installation.
2. If the iPlanet Portal Server processes are running, stop all iPlanet Portal Server processes. See "Stopping the Server Component Processes."
   - If installing from the CD-ROM, perform step 3, step 4, and continue with step 6.
   - If installing from a download, go to step 5.
3. As root, mount the Service Pack 3a CD-ROM.

```
# volcheck
```

4. Change directories to /cdrom/cdrom0 and run the ipsinstall script.

```
# cd /cdrom/cdrom0
# ./ipsinstall
```

5. As root, change directories to `/opt/ips_sp3` and run the `ipsinstall` script. The `ipsinstall` script must be run from the directory in which it exists.

```
# cd /opt/ips_sp3
# ./ipsinstall
```

The installation script then displays the Service Pack 3a license agreement.

6. Enter **yes** to accept the license agreement and continue with the installation.

```
*************************************************************
iPlanet Portal Server (3.0-SP3a release)
*************************************************************
Installation log at
/var/sadm/install/logs/ipsinstall.28532/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes
```

NOTE If the installation script detects missing Solaris patches, a warning message is displayed. See "Installing the Required Solaris Patches" for information on installing the necessary Solaris patches.

The installation script attempts to determine name and IP address information about the machine on which you are installing. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

7. Accept the default values or enter the correct name and IP address information.

```
Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.
```

The script displays the task menu.

8. Choose **2** to perform a fresh installation of the iPlanet Portal Server component.

```
Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 2
```

The script displays the component menu.

9. Choose **1** to install the server component.

```
Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 1
```

10. Accept the default installation directory, or enter another directory in which to install.

```
What directory to install in? [/opt]
```

NOTE If installing the server and gateway components on the same machine, install both components in the same directory.

11. Enter **n** to perform a secure portal installation.

```
Will this be an open portal install? y/[n]
```

12. Choose whether you want to use Secure Sockets Layer (SSL) to communicate with the server component. SSL provides encrypted communication to the server. For information about using SSL with the iPlanet Portal Server product, see the iPlanet Portal Server *Administration Guide*.

```
Are the servers using SSL protocol? y/[n]
```

13. Choose **n** for a single server installation.

```
Is this a multiple server install? y/[n]
```

14. Accept the default profile server port or enter the correct number for the profile server port.

```
The profile server will run on siroe.iplanet.com
On what port will the profile server run? [8080]
```

15. Press Return to accept the default for the role tree root, or enter another name.

```
What is the root of the profile role tree? [iplanet.com]
```

NOTE The name of the role tree root does not have to be a DNS domain name; it can be any name you choose. See Chapter 1 of the *iPlanet Portal Server 3.0 Administration Guide* for more information about the role tree.

16. Accept the default root user or enter the correct name for the root user.

```
What is the user for the profile role tree? [root]
```

17. Accept the default port number for the directory server or enter an available number for the port.

```
On what port will the directory server run? [389]
```

18. Accept the default port number for the gateway component or enter the correct port number.

```
On what port will the gateways run? [443]
```

19. Choose whether the iPlanet Portal Server environment will use multiple gateways or a single gateway.

```
Is this a multiple gateway install? y/[n]
```

The installation script asks a set of questions about the gateway.

20. Enter the information for the gateway or gateways. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

```
On what hostname will the gateway run ("." when done)? [MyGateway]
sesta
What is the sub-domain name for sesta ("." for none)? []
What is the domain name for sesta? [iplanet.com]
What is the ip address of sesta.iplanet.com? [192.168.01.03]
```

NOTE If you chose a multiple gateway installation in step 19, the script repeats the set of questions so you can enter host and domain information for each gateway. Enter a "." when you are finished entering the information for all the gateways.

21. Choose whether the gateway should use a web proxy.

```
Should the gateway(s) use a web proxy? y/[n]
```

- If you choose **n**, go to step 23.
- If you choose **y**, the installation script asks the following set of questions about the web proxy. Continue with step 22.

22. Enter the information for the web proxy.

```
On what hostname will the web proxy run? [sesta]
What is the sub-domain name for sesta ("." for none)? []
What is the domain name for sesta? [iplanet.com]
On what port will sesta run? [8080]
```

NOTE If you choose a web proxy name that is different from the name of the current machine, the script also asks for the IP address of the web proxy.

23. Accept the default administrator port for the web server or enter the correct port number.

```
What is the administrator port for the web server? [8088]
```

The installation script asks you to enter and verify a passphrase. This passphrase is not the root user's password. It is used internally for SSL communication to the server and for access to the iPlanet Webserver administration console.

24. Enter and verify the passphrase.

```
What is the passphrase (8 chars minimum) :
Re-enter passphrase :
```

25. Choose whether you want the script to start the server component after the installation is complete.

```
Start after installation completes? [y]/n
```

The installation script displays the settings and asks if they are correct.

26. Answer **y** to install the server. The installation script installs the server packages.

```
Server settings
Installation Directory : /opt
Server List            : http://siroe.iplanet.com:8080
Gateway List           : siroe.iplanet.com:443
```

```
Profile Server         : http://siroe.iplanet.com:8080
Profile Role Tree Root : iplanet.com
Profile Role Tree User : root
LDAP Port              : 389
LDAP Admin Port        : 8900
Web Server Admin Port  : 8088
Start Server           : n
Are these settings correct? [y]/n
```

NOTE If you choose **n**, the script repeats the questions and gives you the opportunity to change the settings by repeating the installation questions.

The installation script installs the following packages.

```
Installing server.
Installing SUNWwtsdd...
Installing SUNWwtws...
Installing SUNWwtsvd...
Installing SUNWwtdt...
Installing SUNWwtnm...
Installing SUNWwtnf...
Installing SUNWwtrw...
Installing SUNWwtdoc...
Installing SUNWwtsam...
Installing SUNWwtds...
```

When the installation is complete, the component menu is displayed.

27. Choose **3** to exit or **2** to install the gateway on the current machine. See “Gateway Component Installation” for complete instructions on installing the gateway component.

```
Select which component to install:
1) Server
2) Gateway
3) Exit
Choice? [3]
```

If you chose not to have the script start the server component, start the server by using the following command:

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

For information on configuring multiple-instances of the iPlanet Portal Server product on a single server machine, see “Configuring Multiple Instances of iPlanet Portal Server.”

Secure Portal Installation on Multiple Servers

In secure mode, the gateway, which provides encryption services and URL rewriting, is required. For instructions on installing the gateway component, see “Gateway Component Installation.”

NOTE If installing the server component on multiple machines, designate only one machine as the profile server, and configure the other servers to reference that machine as the profile server.

To install the server component:

1. Backup the iPlanet Portal Server 3.0 installation.
2. If the iPlanet Portal Server processes are running, stop all iPlanet Portal Server processes. See “Stopping the Server Component Processes.”
   - If installing from the CD-ROM, perform step 3, step 4, and continue with step 6.
   - If installing from a download, go to step 5.
3. As root, mount the Service Pack 3a CD-ROM.

```
# volcheck
```

4. Change directories to /cdrom/cdrom0 and run the ipsinstall script.

```
# cd /cdrom/cdrom0
# ./ipsinstall
```

5. As root, change directories to `/opt/ips_sp3` and run the `ipsinstall` script. The `ipsinstall` script must be run from the directory in which it exists.

```
# cd /opt/ips_sp3
# ./ipsinstall
```

The installation script then displays the Service Pack 3a license agreement.

6. Enter **yes** to accept the license agreement and continue with the installation.

```
************************************************************
iPlanet Portal Server (3.0-SP3a release)
************************************************************
Installation log at
/var/sadm/install/logs/ipsinstall.28532/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes
```

NOTE If the installation script detects missing Solaris patches, a warning message is displayed. See “Installing the Required Solaris Patches” for information on installing the necessary Solaris patches.

The installation script attempts to determine name and IP address information about the machine on which you are installing. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

7. Accept the default values or enter the correct name and IP address information.

```
Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.
```

The script displays the task menu.

8. Choose **2** to perform a fresh installation of the iPlanet Portal Server components.

```
Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 2
```

The script displays the component menu.

9. Choose **1** to install the server component.

```
Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 1
```

10. Accept the default installation directory, or enter another directory in which to install.

```
What directory to install in? [/opt]
```

NOTE If installing the server and gateway components on the same machine, install both components in the same directory.

11. Enter **n** to perform a secure portal installation.

```
Will this be an open portal install? y/[n]
```

12. Choose whether you want to use Secure Sockets Layer (SSL) to communicate with the server component. SSL provides encrypted communication to the server. For information about using SSL with the iPlanet Portal Server product, see the iPlanet Portal Server *Administration Guide*.

```
Are the servers using SSL protocol? y/[n]
```

13. Choose **y** for a multiple server installation.

```
Is this a multiple server install? y/[n] y
```

14. Choose whether you want the local computer to be the profile server.

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

NOTE If your Service Pack 3a environment includes servers installed on multiple machines, install the profile server on only one of the machines; configure all other server components to reference that machine as the profile server.

- Enter **y** to make the local computer the profile server. If you have not already installed the profile server on another computer, you can choose **y** to make the local computer the profile server. Go to step 16.
- Enter **n** if you have already installed the profile server on another computer. Continue with step 15.

If the local machine is not the profile server, the installation script asks for information about the profile server.

15. Enter the profile server information. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component. Go to step 17.

```
On what hostname will the profile server run? [MyProfileServer] siroe
What is the sub-domain name for siroe("." for none)? []
What is the domain name for siroe? [iplanet.com]
On what port will siroe run? [8080]
What is the ip address of siroe.iplanet.com? [192.168.01.01]
```

16. Accept the default profile server port or enter an available number for the profile server port.

If the local machine is the profile server, the installation script asks the question:

```
The profile server will run on siroe.iplanet.com
On what port will the profile server run? [8080]
```

17. Press Return to accept the default for the role tree root, or enter another name.

```
What is the root of the profile role tree? [iplanet.com]
```

NOTE The name of the role tree root does not have to be a DNS domain name; it can be any name you choose. See Chapter 1 of the *iPlanet Portal Server 3.0 Administration Guide* for more information about the role tree.

18. Accept the default root user name or enter the correct name for the root user.

```
What is the user for the profile role tree? [root]
```

19. Accept the default directory server port number or enter an available number for the directory server port.

```
On what port will the directory server run? [389]
```

- If the local machine is *not* the profile server, go to step 26.
- If the local machine is the profile server, the script asks the following questions about the server components in the Service Pack 3a installation environment. Continue with step 20.

20. Enter the server component information for the server components.

```
On what hostname will the server run ("." when done)? [MyServer] varrius
What is the sub-domain name for varrius ("." for none)? []
What is the domain name for varrius? [iplanet.com]
On what port varrius run? [8080]
What is the ip address of varrius.iplanet.com? [192.168.01.02]
On what hostname will the next server run ("." when done)? [MyServer] .
```

If the local computer is the profile server and you specified multiple server components, the script repeats the set of questions until you have specified information for all the desired server components. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

The script repeats the set of questions, allowing you to enter name and IP address information for each server component in a multiple server environment. Enter a "." after you have finished adding the information for all the server components.

21. Accept the default port number or enter the correct port number for the gateway or gateways.

```
On what port will the gateways run? [443]
```

22. Choose whether the iPlanet Portal Server environment will use multiple gateways or a single gateway.

```
Is this a multiple gateway install? y/[n]
```

23. Enter the information for the gateway or gateways.

The installation script asks the following set of questions about the gateway.

```
On what hostname will the gateway run ("." when done)? [MyGateway] sesta
What is the sub-domain name for sesta ("." for none)? []
What is the domain name for sesta? [iplanet.com]
What is the ip address of sesta.iplanet.com? [192.168.01.03]
```

NOTE If you chose a multiple gateway installation in step 22, the script repeats the set of questions so that host and domain information can be entered for each gateway. Enter a "." when you are finished entering the information for all the gateways.

24. Choose whether the gateway should use a web proxy.

```
Should the gateway(s) use a web proxy? y/[n]
```

- If you choose **n**, go to step 27.
- If you choose **y**, the installation script asks the following set of questions about the web proxy. Continue with step 25.

25. Enter the information for the web proxy. Go to step 27.

```
On what hostname will the web proxy run? [sesta]
What is the sub-domain name for sesta ("." for none)? []
What is the domain name for sesta? [iplanet.com]
On what port will sesta run? [8080]
```

NOTE If you choose a web proxy name that is different from the name of the current machine, the script also asks for the IP address of the web proxy.

26. Accept the default server port number for the machine on which you are installing or enter an available port number.

```
On what port will the server run on this machine? [8080]
```

27. Accept the default administrator port for the web server or enter the correct port number.

```
What is the administrator port for the web server? [8088]
```

The installation script asks you to enter and verify a passphrase. This passphrase is not the root user's password. It is used internally for SSL communication to the server and for access to the iPlanet Webserver administration console.

28. Enter and verify the passphrase.

```
What is the passphrase (8 chars minimum) :
Re-enter passphrase :
```

29. Choose whether you want the script to start the server after the installation is complete.

```
Start after installation completes? [y]/n
```

The installation script displays the settings and asks if they are correct.

30. Answer **y** to install the server component. The installation script installs the server packages.

```
Server settings
Installation Directory : /opt
Server List            : http://siroe.iplanet.com:8080
                       : http://varrius.iplanet.com:8080
Gateway List           : sesta.iplanet.com:443
Profile Server         : http://siroe.iplanet.com:8080
Profile Role Tree Root : iplanet.com
Profile Role Tree User : root
LDAP Port              : 389
LDAP Admin Port        : 8900
Web Server Admin Port  : 8088
Start Server           : n
Are these settings correct? [y]/n
```

NOTE If you choose **n**, the script repeats the questions and gives you the opportunity to change the settings by repeating the installation questions.

The installation script installs the following packages.

```
Installing server.
Installing SUNWwtsdd...
Installing SUNWwtws...
Installing SUNWwtsvd...
Installing SUNWwtdt...
Installing SUNWwtnm...
Installing SUNWwtnf...
Installing SUNWwtrw...
Installing SUNWwtdoc...
Installing SUNWwtsam...
Installing SUNWwtds...
```

When the installation is complete, the component menu is displayed.

31. Choose **3** to exit or **2** to install the gateway on the current machine. See “Gateway Component Installation” for complete instructions on installing the gateway component.

```
Select which component to install:
1) Server
2) Gateway
3) Exit
Choice? [3]
```

If you chose not to have the script start the server component, you can start the server component by using the following command:

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

Repeat this installation procedure on each server component in a multiple-server environment.

For information on configuring multiple-instances of the iPlanet Portal Server product on a single server machine, see "Configuring Multiple Instances of iPlanet Portal Server."

Gateway Component Installation

To install the gateway component:

1. Backup the iPlanet Portal Server 3.0 installation.
2. If the iPlanet Portal Server processes are running, stop all iPlanet Portal Server processes. See "Stopping the Server Component Processes."
   - If installing from the CD-ROM, perform step 3, step 4, and continue with step 6.
   - If installing from a download, go to step 5.
3. As root, mount the Service Pack 3a CD-ROM.

```
# volcheck
```

4. Change directories to /cdrom/cdrom0 and run the ipsinstall script.

```
# cd /cdrom/cdrom0
# ./ipsinstall
```

5. As root, change directories to `/opt/ips_sp3` and run the `ipsinstall` script. The `ipsinstall` script must be run from the directory in which it exists.

```
# cd /opt/ips_sp3
# ./ipsinstall
```

The installation script then displays the Service Pack 3a license agreement.

6. Enter **yes** to accept the license agreement and continue with the installation.

```
************************************************************
iPlanet Portal Server (3.0-SP3a release)
************************************************************
Installation log at
/var/sadm/install/logs/ipsinstall.28532/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes
```

NOTE If the installation script detects missing Solaris patches, a warning message is displayed. See “Installing the Required Solaris Patches” for information on installing the necessary Solaris patches.

The installation script attempts to determine name and IP address information about the machine on which you are installing. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

7. Accept the default values or enter the correct name and IP address information.

```
Inspecting network.
What is the iPS hostname of this machine? [sesta]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of sesta.iplanet.com? [192.168.01.03]

Inspecting iPS components.
```

The script displays the task menu.

8. Choose one of the following options to perform a fresh installation of the iPlanet Portal Server components.

```
Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 2
```

- Choose **2** if the Service Pack 3a server component is *not* already installed on the current machine.
- Choose **3** if the Service Pack 3a server component is already installed on the current machine.

The script displays the component menu.

9. Choose **2** to install the gateway component.

```
Select which component to install:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 2
```

10. Specify whether the sever component is using SSL. For information about using SSL with the iPlanet Portal Server product, see the iPlanet Portal Server *Administration Guide*.

```
Is the profile server using SSL protocol? y/[n]
```

11. Specify whether the local machine is the profile server.

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

- If you chose **y**, go to step 13.
- If you chose **n**, the installation script asks the following questions about the profile server. Continue with step 12.

12. Enter profile server information. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component. Go to step 14.

```
On what hostname will the profile server run? [MyProfileServer] siroe
What is the sub-domain name for siroe("." for none)? []
What is the domain name for siroe? [iplanet.com]
On what port will siroe run? [8080]
What is the ip address of siroe.iplanet.com? [192.168.01.01]
```

13. Accept the default profile server port number, or enter the number for the profile server port.

```
The profile server will run on siroe.iplanet.com
What is the port for the profile server? [8080]
```

14. Accept the default for the role tree root, or enter another name.

```
What is the root of the profile role tree? [iplanet.com]
```

NOTE The name of the role tree root does not have to be a DNS domain name; it can be any name you choose. See Chapter 1 of the *iPlanet Portal Server 3.0 Administration Guide* for more information about the role tree.

15. Accept the default root user name or enter another name for the root user.

```
What is the user for the root of the role tree? [root]
```

16. Accept the default information for the gateway component or enter the correct gateway information.

```
On what hostname will the gateway run? [sesta]
What is the sub-domain name for sesta ("." for none)? []
What is the domain name for sesta? [iplanet.com]
On what port will sesta run? [443]
```

17. Choose whether the gateway component has multiple network interfaces. If the machine on which the gateway is being installed has multiple network interfaces, the iPlanet Portal Server gateway component can be restricted to use only one interface.

```
Does this gateway have multiple network interfaces? y/[n]
```

- If you answer **n**, go to step 20.
- If you answer **y**, continue with step 18.

18. Choose whether to limit the use of the gateway component to one network interface.

- If you answer **n**, go to step 20.
- If you answer **y**, continue with step 19.

```
Limit use to one network interface? y/[n]
```

19. Accept the default IP address or enter the correct IP address for the network interface that the gateway component will use.

```
What is the ip address of that network interface? [192.168.01.03]
```

20. Choose whether you want the firewall software to be installed on the gateway component. Install the firewall only if the gateway component has more than one network interface.

If installing on Solaris 2.6 and Solaris 7, the installation script asks the question:

```
Install firewall? y/[n]
```

NOTE This question is omitted if installing on Solaris 8 because the firewall included with the iPlanet Portal Server product is not supported on Solaris 8.

The installation script asks you to enter and verify a passphrase. This passphrase is not the root user's password. It is used internally for SSL communication to the server and for access to the iPlanet Webserver administration console.

21. Enter and verify the passphrase.

```
What is the passphrase (8 chars minimum) :
Re-enter passphrase :
```

22. Choose whether you want the script to start the gateway after installation.

The installation script asks the question:

```
Start after installation completes? [y]/n
```

The installation script displays the settings and asks if they are correct.

23. If the setting are correct, answer **y** to install the gateway component. The installation script installs the gateway packages.

```
Gateway settings
Installation Directory              : /opt
Gateway                             : sesta.iplanet.com:443
Gateway IP Address                  : 192.168.01.03
Profile Server                      : https://sesta.iplanet.com:443
Profile Role Tree Root              : iplanet.com
Profile Role Tree User              : root
Install Firewall                    : n
Start Gateway                       : n
Are these settings correct? [y]/n
```

NOTE If you choose **n**, the script repeats the questions and gives you the opportunity to change the settings by repeating the installation questions.

The installation script asks the following set of organization specific information for the self-signed certificate.

24. Enter the information for your organization.

```
Self-signed certificate for a SSL connection.
What is the name of your organization? [MyCompany] sun
What is the name of your organizational unit? [MyDivision]
iplanet
What is the name of your city or locality? [MyCity] santa clara
What is the name of your state or province? [MyState] california
What is the two-letter country code? [us]
```

If you chose not to have the script start the gateway component, you can start the server component by using the following command:

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

Removing the Service Pack 3a Software

This procedure assumes that the Service Pack 3a packages were downloaded to `/opt/ips_sp3`.

1. Backup the iPlanet Portal Server 3.0 installation.

2. Stop all iPlanet Portal Server processes. See “Stopping the Server Component Processes.”

- If installing from the CD-ROM, perform step 3, step 4, and continue with step 6.
- If installing from a download, go to step 5.

3. As root, mount the Service Pack 3a CD-ROM.

```
# volcheck
```

4. Change directories to /cdrom/cdrom0 and run the ipsinstall script.

```
# cd /cdrom/cdrom0
# ./ipsinstall
```

5. Change directories to the Service Pack 3a directory and run the `ipsinstall` script. The `ipsinstall` script must be run from the directory in which it exists.

```
# cd /opt/ips_sp3
# ./ipsinstall
```

The installation script then displays the Service Pack 3a license agreement.

6. Enter **yes** to accept the license agreement and continue with the backout.

```
************************************************************
iPlanet Portal Server (3.0-SP3a release)
************************************************************
Installation log at
/var/sadm/install/logs/ipsinstall.17169/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a
Binary Software Evaluation license with, Sun Microsystems, to
legally use this product.
Do you accept? yes/[no] yes
```

The installation script attempts to determine name and IP address information about the machine on which you are installing. If the machine on which you are installing uses multiple IP addresses or multiple domains, verify that the IP address displayed by the script is the correct one for the iPlanet Portal Server component.

7. Accept the default values or enter the correct name and IP address information.

```
Inspecting network.
What is the iPS hostname of this machine? [siroe]
What is the subdomain ("." for none)? []
What is the domain? [iplanet.com]
What is the ip address of siroe.iplanet.com? [192.168.01.01]

Inspecting iPS components.
```

The script displays the task menu.

8. Enter **4** to remove the Service Pack 3a product.

```
Options:
1) Continue upgrade
2) Continue as a clean install (current installation will be removed)
3) Continue install (current installation will not be removed)
4) Remove current installation
5) Exit
Choice? [5] 4
```

9. Select which component to remove.

```
Select which component to remove:
1) iPlanet(TM) Portal Server
2) iPlanet(TM) Portal Server: Secure Remote Access Pack (Gateway)
3) Exit
Choice? [3] 1
```

The script asks you to verify your choice.

10. Choose **y** to remove the iPlanet Portal Server component.

The script proceeds with the removal process. When the component is removed, the script returns you to the component menu.

11. Select which component to remove, or choose **3** to exit the script.

```
Select which component to remove:
1) Server
2) Gateway
3) Exit
Choice? [3] 1
```

Removing a Partial Installation

If the installation process gets interrupted and only some of the iPlanet Portal Server packages have been installed, the packages that were installed must be removed before attempting to reinstall or use the product.

To remove a partial installation:

1. As root, change directories to the Solaris package database directory.

```
# cd /var/sadm/pkg
```

2. List the iPlanet Portal Server software directories.

```
# ls -d SUNWwt*
```

3. Look for any of the following directories:

SUNWicgSA/	SUNWj2man/	SUNWwtdt/	SUNWwtnf/	SUNWwtsd/	SUNWwtsvd/
SUNWicgSS/	SUNWj2rt/	SUNWwtfw/	SUNWwtnm/	SUNWwtsdd/	SUNWwtws/
SUNWj2dem/	SUNWwtdoc/	SUNWwtgw/	SUNWwtrw/	SUNWwtsmb/	
SUNWj2dev/	SUNWwtds/	SUNWwtgwd/	SUNWwtsam/	SUNWwtsv/	

4. Remove any directories that match the list above. For example:

```
# rm -rf SUNWicgSS
```

5. Change directories to `/var/sadm/install/logs` and list the iPlanet Portal Server software directories.

```
# cd /var/sadm/install/logs
# ls
```

6. Look for any of the directories listed in step 3.
7. Remove any directories that matched the list of iPlanet Portal Server software directories. For example:

```
# rm -rf SUNWicgSS
```

After Installation

Setting the Environment Variable IPS_ROOT

Set the environment variable IPS_ROOT to the iPlanet Portal Server 3.0 installation directory. The following example assumes that /opt is the installation directory.

```
# IPS_ROOT=/opt
```

Restoring Certificates

To restore server certificates after upgrading the iPlanet Portal Server:

1. As root, stop the iPlanet Portal Server server.

```
# /etc/init.d/ipsserver stop
```

2. Change directories to the directory in which the certificates are to be restored. In the following example, `/opt` is the base directory.

```
# cd /opt/netscape/server4
```

3. Un-compress the alias.tar file created before the upgrade process. See "Saving the Certificates Used by the Server Component."

```
# /usr/bin/tar xvf /usr/tmp/alias.tar
```

4. Restart the iPlanet Portal Server server.

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

5. Open a browser window, and go to the iPlanet Web Server administration console. For example:

   `http://siroe:8088`

6. Login as admin.

NOTE The password for the web server administration console is the same passphrase entered during the iPlanet Portal Server installation.

7. Select *Manage*.
8. Select *Apply*.
9. Select *Load configuration files*.
10. Select *Preferences*.

11. Select Encryption *On/Off*.
12. Select the *On* button.
13. Save the configuration.
14. In a terminal window, restart the iPlanet Portal Server server.

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

Known Problems and Limitations

Here are known problems with the iPlanet Portal Server 3.0 software that have not been fixed in Service Pack 3a, with workarounds where appropriate.

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.

Desktop

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.

4358738

Using bookmark provider with IE4 client on open portal gets a script error.

Workaround:

None. IE4 bug, not reproducible with IE5.X or Netscape Browsers.

4447005

`delAttribute` permits deletion of a profile attribute without write permission.

Workaround:

None.

4454833

Administrator can delete their own account.

Workaround:

I. In a terminal window, become root.

II. At the prompt, enter the following string:

```
# echo '<iwt:Att
name="iwtUser-role"><Val>/$DOMAIN/AdminRole</Val></iwt:Att>' |
/opt/SUNWips/bin/ipsadmin create user /$DOMAIN/root/dev/stdin
```

III. Select *Return.*

Where `$DOMAIN` is the default domain and `AdminRole` is the administrator's role.

4457299

Descriptions for channels created with channel wizard cannot be localized.

Workaround:

To localize the description and title for a channel created with the channel wizard, do the following:

1. On each iPlanet Portal Server 3.0 server, create a file called:

   ```
   /opt/SUNWips/locale/channel_locale.properties
   ```

   where *channel* is the fully qualified name of the channel and *locale* is the name of the locale to be supported.

   - The fully qualified name of the channel is printed on the last page of the channel wizard, and it is also shown in the available channels list in the desktop profile
   - The locale is a language and country combination, for example, en_US

2. Within this file, create entries for the description and title, as follows:

   ```
   description=This is the description

   title=This is the title
   ```

   The `.properties` file must use Java Unicode encoding, where multi-byte characters are represented as ˇXXXX where the Xs are hexidecimal digits.

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

NOTE A separate `.properties` file is necessary for each locale to be supported.

Gateway

4324617

External bookmark URLs are not redirected.

Prevention:

Remove `openURL` 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.

Install

4448387

Installing the iPlanet Portal Server product over a previous installation that did not install correctly causes the installation log file to get very large.

Workaround:

After installation, remove the installation log file:

`/var/sadm/install/logs/ipsinstall.<process_id>/install.log.`

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:

```
# /opt/SUNWips/bin/ipsserver.servername.iplanet.com@port start
```

4472975

Heavy loads for an extended duration cause components in the operating system to fail.

Workaround:

None.

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.

4293370

NetFile Lite does not check the size of a file before attempting to upload. If the file is greater than 5 MB, the upload fails.

Workaround:

None.

4372826

Uploading tar files greater than the 5 MB limit in NetFile Lite, and tar files greater than the 500 MB limit in Netfile generates an incorrect error message.

Workaround:

None.

4463515

The Netfile application allows users to access denied hosts if those hosts were added to the desktop before a deny rule was added in the iPlanet Portal Server administration console.

Workaround:

None.

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, Service Pack 2, and Service Pack 3a

The following bugs have been fixed in iPlanet Portal Server 3.0 Service Pack 1, Service Pack 2, and Service Pack 3a.

Table 13 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
4387384	The key in the xml files and the `.properties` files do not match, so some translated strings are not displayed in the administration console, instead, the administration console displays the strings in the default language which is English.	Fixed in SP3
4365124	Missing choice value (CVal) key value pairs in the `iwtAuthCert.properties` file, and spaces in the keys in the `iwtAuthCert.properties` file prevent some translated strings from being displayed in the administration console, instead, the strings are displayed in the default language which is English.	Fixed in SP3
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
4362849	Certificate without cn causes Java IO exception.	Fixed in SP3
4378157	Authentication fails when platform server is configured to use `https`.	Fixed in SP3
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 SP2

Table 13 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
4401121	`URLScraperProvider` does not preserve backward compatibility.	Fixed in SP3
4412806	Relative URL redirects from JSPProvider `processEdit` fails.	Fixed in SP3
4412336	Changes to TimeZone not effective till user relogs.	Fixed in SP3
4448938	Changing to layout *Option Four* causes wide channels to be removed	Fixed in SP3
4450801	Selecting *Open all pages in the desktop* when editing bookmarks causes the javascript function `openURL` to call the server twice in the URL	Fixed in SP3
4426023	SunBlue templates do not work with SP2	Fixed in SP3
4387813	Occasionally, the desktop is displayed only after the entire timeout—the default timeout is 30 seconds.	Fixed in SP3
4394315	Detaching all channels on the desktop causes an unrecoverable error which makes the desktop unusable.	Fixed in SP3
4396908	Desktop provider does not catch throwable, resulting in a desktop error page with the message “A fatal error has occurred” displayed in the channel window.	Fixed in SP3
4397293	Desktop logs expired or invalid sessions as an error instead of a warning in the debug log files, causing the debug files to grow unnecessarily large.	Fixed in SP3
4401145	Date formatting does not work properly in Japanese locale.	Fixed in SP3
4353071	The weather provider templates should not get installed; the product does not contain a weather provider.	Fixed in SP3
4403468	Channel titles are always displayed in the language stored in the profile service.	Fixed in SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Status
4394038	Some attribute strings for desktop tabs are displayed in English for other locales.	Fixed in SP3
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
4389707	In some cases the gateway or gateway proxy would not respond due to CLOSE_WAIT sockets accumulating, and not getting closed.	Fixed in SP3
4381501	The URL rewriter incorrectly rewrites relative URLs by using the document's URL instead of its instead of its base URL (indicated by the BASE tag).	Fixed in SP3
4352555	The JavaScript rewriter mishandles escaped double quote.	Fixed in SP3
4358856	If the server and the gateway are installed on two different machines, iwtGateway.properties file is not installed in *basedir*`/SUNWips/locale` directory of the server machine. The gateway related strings are displayed in the default language, English, for foreign languages on the server machine.	Fixed in SP3
4350023	The `ipshttpd` script does not set the maximum number of file descriptors to a high enough value for the gateway proxy process, causing the `ipshttpd` process to run out of file descriptors. When that happens, `ipshttpd` stops responding.	Fixed in SP3
4430846	Internet Explorer 5.5 cannot display webmail application when used with the Gateway.	Fixed in SP3
4344066	Referer headers need to be forwarded so servers can track the user's URL.	Fixed in SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Status
4396142	If an applet is between <OBJECT> and </OBJECT> the URL rewriter doesn't rewrite the URL.	Fixed in SP3
4396151	The URL rewriter does not rewrite the applet parameter value if there is space between an HTML tag's parameter name and value.	Fixed in SP3
4380531	Rewriter misplaces iplanet() function.	Fixed in SP3
4392892	CLASSPATH needs to be added to the javah command in the `../gateway/eprox/Makefile`.	Fixed in SP3
4375934	Gateway ceases to resolve DNS hostnames intermittently.	Fixed in SP3
4412431	`certadmin` self-signed certificate validity defaults to 90 days.	Fixed in SP3
4407007	URL Scraper and RSS channel providers fail when load balancing is active.	Fixed in SP3
4342774	HTTP basic auth caching (SSO) fails when using server HTTP proxy.	Fixed in SP3
4354655	Users can't authenticate with Internet Explorer, if hostname contains capital letters.	Fixed in SP3
4416215	URLscraper does not handle the character set from Content-Type.	Fixed in SP3
Install		
4335044	Install needs to check disk space for installing Java packages. If Java packages don't get installed, the install script fails.	Fixed in SP3
4240879	If third-party software is installed before the iPlanet Portal Server software is installed, the error message that is generated incorrectly references an outdated version of the iPlanet Portal Server product.	Fixed in SP3
4350541	The installation script requires a *fully qualified domain name* (FQDN) with three parts (separated by two dots). It will not accept an FQDN with only one dot.	Fixed in SP3
4418223	Miss-matched version string.	Fixed in SP3
4423962	Install script asks for patches not in the image.	Fixed in SP3
4424472	`pkginfo` files should be updated after installation.	Fixed in SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Status
4380586	Gateway will not start when server and gateway use SSL.	Fixed in SP3
4429042	Service pack 3 image should not include `jdk1.2.2_05` patches.	Fixed in SP3
4437706	Installing gateway with profile server, using non-default port for SSL, sets port to 443	Fixed in SP3
4448611	Installing profile server with a web proxy causes `ipsserver` to fail.	Fixed in SP3
4335044	When java packages are not installed user is not notified and install script fails.	Fixed in SP3
4226991	Confirmation message when user is removing components.	Fixed in SP3
4240879	Wrong install script name in error message.	Fixed in SP3
4350541	Installation forces *fully qualified domain names* to be subdomain and domain name.	Fixed in SP3
4341308	Stop script stops all `slapd` processes, and all external LDAP server processes.	Fixed in SP3
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
4363059	Importing privileges after accessing Policy page requires relogging to view.	Fixed in SP3
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
4389604	Stop script does not always stop the directory server.	Fixed in SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Status
4396039	Portal Server hangs if restarted under load.	Fixed in SP3
Japanese Language Version		
4336096	On Japanese localization, Netfile Java did not work on Solaris and Windows NT.	Fixed in SP1
4402583	Incorrect country code for Japan in the `iwtUser.properties` file.	Fixed in SP3
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
4343010	When logging is disabled, the log client still sends the log message.	Fixed in SP3
4401461	Oracle `jdbc` driver does not re-initialize when the database cycles off and on.	Fixed in SP3
NetMail		
4340200	Session timed out when running NetMail without the Gateway.	Fixed in SP1
4378943	Doublebyte nickname entries in NetMail Lite address book are not supported.	Fixed in SP3
4378936	Doublebyte folder names are not supported in NetMail Lite.	Fixed in SP3
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
4365921	NetFile applet occasionally does not pass the sessionid to the servlet during a servlet call, resulting in a session exception that causes the log files to get unnecessarily large.	Fixed in SP3
4361900	NetFile assumes that a system is valid without verifying that the system exists. If the system to which Netfile tries to connect does not exist, the Netfile application eventually times out.	Fixed in SP3

Table 13 Fixed Bug List

Bug ID	Bug Description	Status
4371647	If the server's LANG setting specifies Japanese or Chinese locale, NetFile upload functions for image, HTML, and executable files do not work.	Fixed in SP3
4368446	If the server's LANG setting specifies Japanese or Chinese locale, NetFile download functions for image, HTML, and executable files do not work.	Fixed in SP3
4357835	NetFile Lite can display only one share for Windows systems.	Fixed in SP3
4357841	NetFile Lite does not save changes to host information upon exiting and saving the session.	Fixed in SP3
4357856	Using the host info menu in NetFile to edit host information, such as username and password, removes the shares associated with that host.	Fixed in SP3
4357847	NetFile shares that have been defined through `ipsadmin` can be added again through the NetFile application resulting in duplicate shares.	Fixed in SP3
4357844	NetFile has problems displaying hidden shares that have been defined by the administrator.	Fixed in SP3
4349633	NetFile Lite behavior, under certain circumstances, can compromise password security.	Fixed in SP3
4352059	The profile isAllowed method does not do wildcard matching.	Fixed in SP3
4335215	The NetFile Lite application incorrectly displays compressed filenames when using Windows NT hosts.	Fixed in SP3
4431453	Netfile mail functionality can overwrite iPortal Web Server configuration files.	Fixed in SP3
Netlet		
4332715	Applet download rule section is broken.	Fixed in SP3
4410474	Global encryption version of Netlet Applet incorrectly shipped with domestic version of iPlanet Portal Server 3.0.	Fixed in SP3
4377505	Netlet applet is hardcoded for a maximum of ten connections per rule.	Fixed in SP3
Profile		
4341571	External LDAP attribute mappings did not work with binary type attributes.	Fixed in SP1

Table 13 Fixed Bug List

Bug ID	Bug Description	Status
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
4352059	The profile isAllowed method does not do wildcard matching.	Fixed in SP3
4399031	`ipsadmin` has wrong content type for `UpdateProfileCache` request.	Fixed in SP3
4412089	Profile server enters busy wait loop.	Fixed in SP3
Server		
4394184	A certificate error occurs when using an HTTPS connection when the VIP name does not match the server name.	Fixed in SP3
4388783	The gateway component should use JSS for talking to the platform server in https mode.	Fixed in SP3
Documentation		
4343016	Incorrect URL for documentation.	Fixed in SP1
4373115	Portal server and gateway components on single computer must use same install directory.	Fixed in SP3
4402209	Correct instructions for adding `iwtTabProvider` in selected channels.	Fixed in SP2
4332242	Document required disk space for `/var; /etc; /opt`; and `installation directory`.	Fixed in SP3

Documentation Updates

The following information supplements the iPlanet Portal Server 3.0 *Administration Guide*.

Authentication Chaining

Authentication chaining provides a higher level of security for organizations by requiring users to authenticate against more than one authentication mechanism. For example, if the membership and Unix authentication modules are chained, desktop users would authenticate against both to access the desktop. If all authentication modules are chained, desktop users would authenticate against all to access the desktop.

To set up authentication chaining, do the following.

1. Login to the iPlanet Portal Server administration console as Super Administrator.
2. Select *Manage Domains*.
3. Select the domain for which authentication chaining is to be used.
4. Select *Authentication*.
5. In the Authentication Chaining Modules field, enter the authentication modules to be chained, separated by spaces. For example

```
Membership Unix
```

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

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
```

How to Report Problems

If you have problems with iPlanet Portal Server 3.0 Service Pack 3a, 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 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`