Administration Guide

iPlanet™ Portal Server 3.0

806-5246-01
May 2000

Contents

Preface

iPlanet™ Portal Server 3.0 enables remote users to securely access their organization's network and its services over the Internet. Additionally, it gives your organization a secure Internet portal, providing access to content, applications, and data to any targeted audience—employees, business partners, or the general public.

iPlanet Portal Server runs on the Solaris™ 2.6, 2.7 and 8.0 Operating environment. This *Administration Guide* contains instructions for configuring and administering iPlanet Portal Server.

Who Should Use This Book

This guide assumes that you are network or system administrator experienced in managing UNIX systems and TCP/IP networks. You are responsible for administering iPlanet Portal Server at the global platform or individual domain level. If you are responsible for the iPlanet Portal Server global platform, you must have root access and full file permissions to configure machines, users, and applications that will comprise the platform. If you are responsible for a single iPlanet Portal Server domain, you do not need root permission for the machines comprising the platform.

How This Manual Is Organized

The *Administration Guide* is divided into the following chapters and appendixes:

Chapter 1 introduces the iPlanet Portal Server and describes the role tree.

Chapter 2 describes how to create portals.

Chapter 3 explains how to configure the user desktop.

Chapter 4 introduces the Membership Module.

Chapter 5 presents information about Policies of user access.

Chapter 6 presents all the other authentication methods.

Chapter 7 describes how to configure the Netlet.

Chapter 8 describes how to configure the Gateway.

Chapter 9 describes how to add Gateways and Servers.

Chapter 10 presents Data Logging.

Chapter 11 discusses maintenance, backup and restore, as well as troubleshooting.

Related Books

Other documents in iPlanet Portal Server documentation set are:

- *iPlanet Portal Server 3.0 Installation Guide*
- *iPlanet Portal Server 3.0 Programer's Reference Guide*

Accessing Sun Documentation Online

The `docs.sun.com` Web site enables you to access Sun technical documentation online. You can browse the `docs.sun.com` archive or search for a specific book title or subject. The URL is `http://docs.sun.com/`.

Typographic Conventions

The following table describes the typographic changes used in this book.

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	Command-line placeholder: replace with a real name or value	To delete a file, type `rm` *filename*.
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User's Guide*. These are called *class* options. You *must* be root to do this.

Shell Prompts in Command Examples

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

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

Chapter 1

Introducing iPlanet Portal Server 3.0

iPlanet™ Portal Server 3.0 provides secure access to an intranet for remote users on UNIX-based or Windows-based personal computers.The iPlanet Portal Server software offers a customized palette of applications and information including:

- HTTP
- X-Windows
- Microsoft NT
- 3270/5250 terminal emulation
- heterogeneous file systems, plus
- External content from providers of your choice.

NOTE The tasks and concepts in this Administration Guide assume that the default installation of iPlanet Portal Server has been completed. If installation is needed, refer to the *iPlanet Portal Server Installation Guide.*

This chapter introduces iPlanet Portal Server and covers the following topics:

- What is a Portal
- Features of iPlanet Portal Server
- Administering iPlanet Portal Server
- Using the iPlanet Portal Server from a Remote Client
- iPlanet Portal Server Architecture
- Structure of your iPlanet Portal Server installation

- Where to go for information about iPlanet Portal Server
- Tasks of the iPlanet Portal Server administrator

What is a Portal?

A portal is a community-based web site that securely holds a collection of data related to different topics, including such things as news and stock quotes, applications, and services.The iPlanet Portal services reflect the same concept as a portal.

The available data content may be customized by the user that has write permission to change providers, display of data, and links to other allowable web sites from those available. Services can include the use of provider applications and utilities; for example email and file management and storage facilities.

A corporate portal is a personalized web page that brings together data and productivity tools relevant to corporate users. Corporate users can include employees, vendors, marketing partners, customers, and allied business users. From a corporate portal, customers can purchase a product in a secure e-business transacting environment. Likewise, vendors can provide product to the corporation.

Features of the iPlanet Portal Server

The iPlanet Portal Server system includes the following features:

- Cost-effective, efficient and secure access to internal corporate information, personal email, productivity applications, and internal web sites.
- Leverage to the Internet and Internet service providers (ISPs) to reduce costs.
- Simplification of remote access for end users.
- Selective authentication scheme from one of six included modules
- Customization of authentication via pluggable modules.
- Independent software interfaces for users and administrators.
- Local or remote administration through a web-based console from either Internet Explorer or Netscape browsers.
- Controlled user access to corporate resources at any level of granularity.

- Customizable desktop widgets
- APIs to facilitate new iPlanet Portal Server applications

Administering iPlanet Portal Server

iPlanet Portal Server includes two administration interfaces; the *administrator console* and the *command line interface*. Most administration tasks are performed through the web-based Administration Console. The Administration Console can be accessed locally or remotely from a web browser. However, tasks such as file modification must be administered through the UNIX command line.

iPlanet Portal Server supports two types of system administrators, the *Super Administrator* and the *Domain Administrator*. The Super Administrator has permission to administer all aspects of the iPlanet Portal Server installation, including creating a delegated administrator known as a Domain Administrator. The Domain Administrator can only administer aspects of iPlanet Portal Server that apply to their assigned domain.

Getting Information for Administering iPlanet Portal Server

This guide contains conceptual information and describes tasks to help both the Super Administrator and the Domain Administrator configure and manage the iPlanet Portal Server. In addition, online help is available for the Administration Console by clicking the Help links on the web pages.

NOTE For instructions for administering the iPlanet Portal Server from the command line or, for creating custom applications and scripts, please refer to the *iPlanet Portal Server Programmer's Reference Guide*.

The installation CD-ROM for the iPlanet Portal Server software contains a documentation directory with complete documentation in HTML and PDF formats: `/docs/en_US`.

After installation, look for the documentation at:

`http://[servername]:8080/docs/en_US/.`

This documentation URL contains other links to hard copy format (PDF) and HTML format copies of the complete documentation set, as well as links to both the administrator and end user online help.

Using the iPlanet Portal Server Desktop From a Remote Client

Users access iPlanet Portal Server by logging in to the web-based iPlanet Portal Server Desktop through their assigned authentication scheme. The log in request is authenticated by the configured authentication module. Upon successful authentication, the user session is established with the iPlanet Portal Server and the assigned desktop portal page is displayed. The desktop includes a Help button that can be accessed for online help.

Where to Go Next

The remainder of this chapter provides the information needed to administer the iPlanet Portal Server.

- **If you are new to iPlanet Portal Server**, read the rest of this chapter and continue with Chapter 2, “Creating A Multi-Domain Portal”.
- **If you want to begin setting up your iPlanet Portal Server platform and are familiar with the earlier iPlanet products**, go on to Chapter 3, “Configuring The Desktop”.

iPlanet Portal Server Components

The iPlanet Portal Server architecture is Internet and web-based. The native communication protocols include HTTP and HTTPS. Additional applications running through iPlanet Portal Server, in particular remote windowing software and specific communication components (such as site certificate helpers), use their native TCP-based, encrypted communication protocols and pass them through the configured SSL port.

By relying on these protocols, iPlanet Portal Server supports standard web browsers for both secure end-user access to applications and secure iPlanet Portal Server administration. All remote-user traffic uses the SSL port, while administrative access uses HTTP or HTTPS, depending on the choices made during iPlanet Portal Server installation.

The iPlanet Portal Server configuration includes four major components:

- iPlanet Portal Server
- iPlanet Profile Server
- iPlanet Portal Server Gateway
- Firewall

These components can be installed on individual computers, or, if necessary, on one computer. The portal server structure utilized with the installed iPlanet Portal Server components includes the use of a *role tree*. Collectively, the installed iPlanet Portal Server components and structure are referred to as the *iPlanet Portal Server platform*.

Introducing the Server

The iPlanet Portal Server has two main functions: as a portal server and as an application server. As a portal server, iPlanet Portal Server handles all authorization, policy, and user profile access and management throughout the platform. As an application server, iPlanet Portal Server enables the included mail and file management utilities.

Introducing the Profile Server

Within the portal server function, iPlanet Portal Server includes a profile-management system called the *profile server*. The profile server stores the profiles associated with iPlanet Portal Server objects such as domains, roles, and users. In a basic iPlanet Portal Server configuration, the profile server is installed on the same machine as the iPlanet Portal Server server. In a multi-server platform, only one iPlanet Portal Server server is designated as profile server.

Introducing the Gateway

The iPlanet Portal Server gateway provides the interface and security barrier between the remote user sessions originating from the Internet and your corporate intranet. The iPlanet Portal Server gateway has two main functions:

1. **Providing basic authentication services** to incoming user sessions, including establishing identity and allowing or denying access to the portal server.
2. **Providing mapping and rewriting services** to allow users access to web-based links containing intranet content.

Choosing a Firewall

Although not required for operation of the iPlanet Portal Server, a firewall provides greater security. When utilized, the iPlanet Portal Server firewall application can be run as part of the iPlanet Portal Server software. Alternatively, the iPlanet Sunscreen 3.1 firewall product can be used, or, a third-party firewall application.

For sample configurations showing the use of a firewall with iPlanet Portal Server, refer to “To Configure the iPlanet Portal Server Firewall Application” on page 221. For more information about the iPlanet Portal Server firewall, refer to Appendix A, “Administering the Firewall Application”.

Basic iPlanet Portal Server Installation

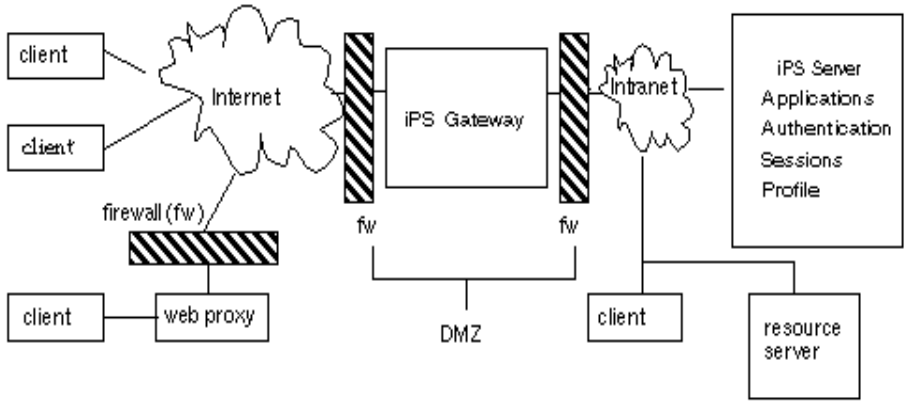

Figure 1-1 Basic iPlanet Portal Server Installation

Figure 1-1 shows the basic iPlanet Portal Server platform, as introduced in the *iPlanet Portal Server 3.0 Installation Guide.* Here, iPlanet Portal Server is installed on two computers, one functioning as the iPlanet Portal Server gateway and firewall, and one functioning as the Portal Server including the profile server.

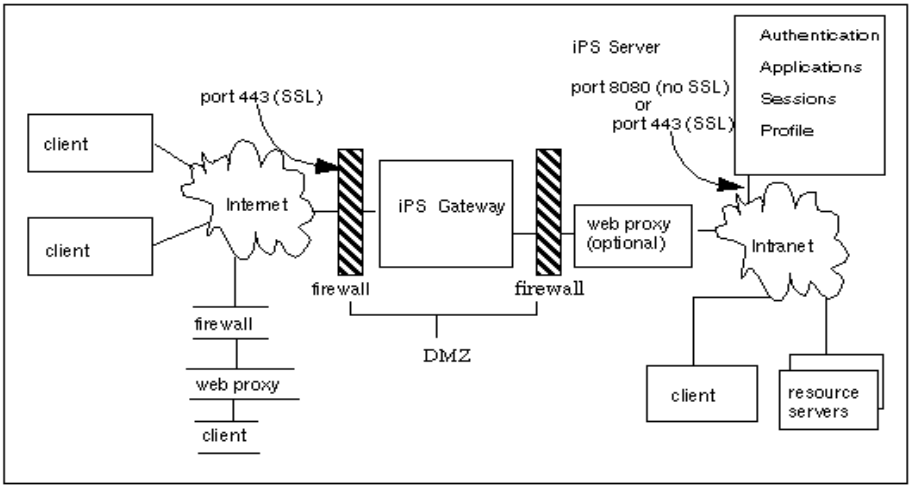

Figure 1-2 Typical Two-Machine Configuration with SSL Ports Noted

Figure 1-2 shows the basic configuration with the default port numbers. SSL is used to encrypt the connection between the client and the iPlanet Portal Server gateway over the Internet. SSL can also be used to encrypt the connection between the iPlanet gateway and server

Additional servers and gateways can be added for site expansion. Or, the gateway and server can be configured on the same computer. For more information on configuring SSL encryption, see Chapter 11, “Maintaining iPlanet Portal Server”.

Structure of the iPlanet Portal Server Role Tree

A major part of implementing the iPlanet Portal Server platform involves organizing users and applications into a hierarchy called the *role tree*. Through the role tree structure, an administrator can be designated to manage gateways and servers, control access to the site’s intranet, design the portal page, and determine the look and feel of users’ desktops.

The iPlanet Portal Server role tree has four levels:

- Root
- Domain
- Role
- User

Root Level

The root level is the top of the role tree for the iPlanet Portal Server platform. It is where all global attributes of the platform are defined. The root level is the parent of all configured domain levels for the platform. The root level is administered only by the Super Administrator, who has read and write privileges for all attributes throughout the platform. Platform level attributes are unique and apply globally; they are not passed down to the domains.

iPlanet Portal Server supports two types of attributes: global and user-configurable. *Global attributes* apply to the entire platform and are configured only by the Super Administrator. Examples of global attributes include values assigned to gateways and servers.

Domain Role-User Attributes

User-configurable attributes apply to underlying levels of the role tree, as described in the following sections. A delegated Domain Administrator can configure these attributes for the domain, parent role, child role, and user levels. At the user level of the role tree, some attributes can be customized for each user, as needed.

Inheritance in the Role Tree

The role tree has the notion of *parent* and *child* levels, much in the same way as the UNIX file system. For example, a User is the child of a Role. The Role, though parent of the User, is a child of the Domain. A role can also be a child of a parent. A domain can not have a child domain, nor can a user have a child user. Depending on how the role tree is set up, child levels can *inherit* attributes defined at their parent level.

The goal of role tree design results in a structure that is easy to administer, using inheritance. Subordinate levels of the role tree can have policies and attributes that are more restrictive, more permissive, or both, depending on the circumstances. However, because policies and attributes must be tracked, a simple structure is easier to maintain.

Domain Level

In iPlanet Portal Server, a *Domain* is used to administer large amounts of resources and users for the corporate intranet. In a small organization, one domain may be sufficient to represent the entire company. However, a large company with many divisions may best be served to have multiple domains; perhaps one domain for each represented division.

To further illustrate the domain concept, consider an enterprise site where all users are part of the same company. Within one domain, multiple roles are created representing the various departments or categories of users. However, when considering an application service provider (ASP) or Internet service provider (ISP) that serves a number of client corporations, each client member would have its own domain and role tree structure completely independent and secured from each other.

NOTE Do not confuse the iPlanet Portal Server concept of a "domain" with a DNS, NIS, or NIS+ domain. If an iPlanet Portal Server platform has only one domain, the users in the iPlanet Portal Server domain might correspond exactly to the members of the company's DNS domain. But this direct correspondence of members has nothing to do with how iPlanet Portal Server (or DNS) functions or is administered.

Inheritance at the Domain Level

Domains are the children of the Root Level and parents of roles in the platform role tree. Additionally, either the Super Administrator or the designated Domain Administrator can define user-level attributes that apply to a particular domain. These domain-specific attributes are inherited by roles but cannot be passed upward to the root level. Therefore, for a platform with multiple domains, a unique set of attributes can be defined for each domain.

When attributes are initially defined at the domain level, they are inherited by the subordinate child role and user levels. Changes to attributes at the domain level can be propagated down to subordinate child levels using the 'Apply Changes to all Subroles' attribute. Keep in mind that under such propagating circumstances, any customized role or user-defined attribute will be overwritten by the same attribute changed at the domain level, necessitating a reconfiguration of the customized role or user level attribute.

Figure 1-3 shows the top of a role tree with two domains, `Example 1` and `Example 2`.

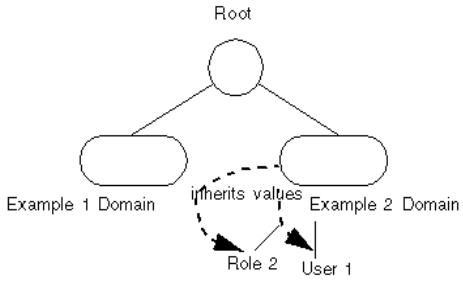

Figure 1-3 Role Tree With Two Domains

In this scenario, Example 2 roles inherit attribute values from the Example 2 domain. In addition, Example 1 and Example 2 have domain level attributes defined, which are specific to each domain and not known or used by each other.

Role Level

A *role* defines a group of users who are members of that role. The role contains a set of attributes and policies that define a user's desktop policy. This set of attributes and policies are inherited by child roles and users. Customization of a particular attribute or policy can still occur at the child role or user level.

When iPlanet Portal Server is installed, the roles *AdminRole* and *defaultRole* are created in the selected default domain name. The default role name for the domain can be changed. The AdminRole is a special case and can not be deleted as this role is used for Super Administrator privileges. Also, any role can have child roles that can inherit attributes from the parent role when changes are applied to child roles from that parent role profile. Additionally, each child role can contain customized attributes unique to that child role and unknown to other parent and child roles in the domain.

When users attempt to log in to the iPlanet Portal Server desktop for the first time, they must be authenticated by the iPlanet Portal Server gateway. If authentication is successful, the user's desktop session assumes the characteristics of the assigned user profile. New authenticated users not assigned to a particular role are added to the defaultRole for the domain.

Inheritance at the Role Level

Figure 1-4 shows a role tree that might be set up for multiple domains, roles, and child roles.The Default Domain is the name of the domain specified during installation.

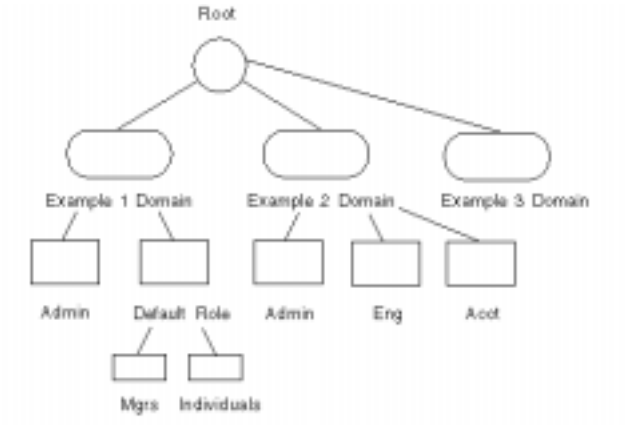

Figure 1-4 Role Tree With Parent Roles and Child Roles

The domain `Example 1` has the parent roles AdminRole and DefaultRole, which in turn have the child roles Mgrs and Individuals, respectively. In this scenario;

- **AdminRole** inherits all domain-level attributes and policies.
- **DefaultRole** inherits all domain-level attributes and policies, but has no knowledge of, and cannot use, attributes and policies assigned to the Admin role.
- **Mgrs role** inherits the attributes from DefaultRole but might also have special policies or applications available only to members of this child role.
- **Individual child role** inherits the attributes from DefaultAll role and may have permission to run applications not available to the Mgrs role. Moreover, the Individuals child role has no knowledge of, and cannot use, special privileges or special applications delegated to those in the Mgrs child role.

The domain Example 2 has the roles Admin, Eng, and Acct, with no child roles assigned. Attributes can be customized at any role level if inheritance is not needed.

User Level

The *User* level consists of individuals permitted to use iPlanet Portal Server. Each user has a unique set of attributes inherited from higher levels of the role tree, plus unique attributes that determine how the user will run theiPlanet Portal Server desktop.

In a default installation, a user can log in, and, if the user has not been pre-assigned to a role, the user automatically becomes a member of the default Role for the domain. Each iPlanet Portal Server user can belong to only one role. Administrators are a special case, and belong to one role with special administrative privileges.

Inheritance at the User Level

Figure 1-5 shows a full role tree that might be set up for an ISP.

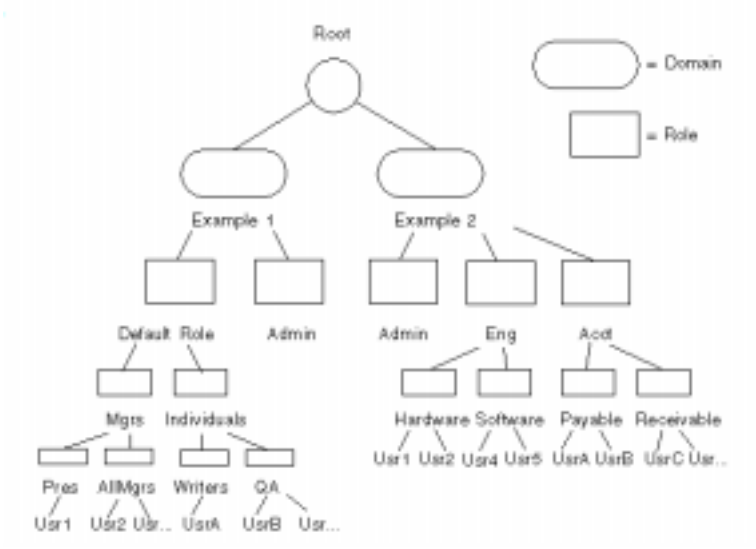

Figure 1-5 Role Tree for an ISP Hosting Domains Example1 and Example2

In the Example 1 domain, both Individuals and Mgrs inherit the policies and attributes of the DefaultAll role, but do not inherit the policies and attributes of the Admin role. Likewise, the Writers role, a child of the Individuals role, inherits the policies and attributes of the Individuals role, but does not inherit the policies and attributes of the Mgrs child role. Moreover, while users in the Writers and QA child roles inherit policies and attributes from Individuals, unique attributes can be defined for each child role that do not apply to the other child role.

In the Example 2 domain, due to role inheritance, all users in the Eng tree can only see certain information and access certain tools that only they need to see. Conversely, all users in the Acct tree might be able to access other tools but not necessarily development tools.

NOTE Users can be created as a child of any role (i.e., a parent role, a child role of a parent role)

When a role tree is established, privileges, attributes, and applications can be set to allow or deny access to such resources further down the role tree. For instance, the root user at the top of a role tree can be assumed to have blanket policies and attributes. Conversely, role members and users can have subsets of the root user policies and attributes, or, can override policy restrictions and have different characteristics entirely.

Figure 1-6 illustrates the way the value of an attribute can be inherited or changed at each level. For instance, at the Role 5 level, when ‘white’ is overridden to ‘red’ this attribute is denoted as customized. Similarly, when user 2 inherits ‘white’ from Role 2, this attribute is inherited.

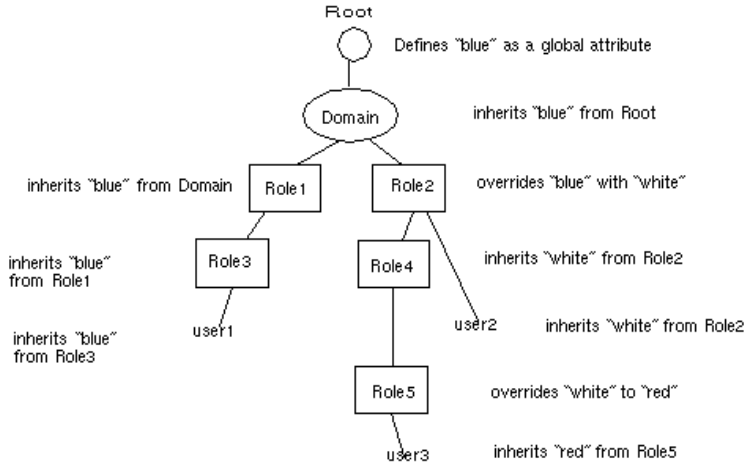

Figure 1-6 How Attributes Are Inherited in the Role Tree

Introducing the Administration Console

This section describes the overall structure of the iPlanet Portal Server Administration Console and explains how to use it.

Logging in to the Administration Console

1. Do the following based on the type of administrator that you are:

For the Super Administrator:

- Go to your preferred browser and type the URL:

```
http://iPS_server:8080/console
```

where *iPS_server* is the server name given to the iPlanet Portal Server at installation.

For a Domain Administrator:

- Go to your preferred browser and type the URL:

```
http://iPS_server:8080/console/domain_name
```

where *iPS_server* is the server name of the iPlanet Portal Server and *domain_name* is the name of your assigned domain.

If your server is configured to use SSL:

- Use the following URL to access the Administration Console (the port number is that defined for SSL at the time of installation (e.g., such as port 443):

```
https://iPS_server:port/console/domain_name
```

The login screen appears as shown in Figure 1-7.

NOTE UNIX authentication is the only authentication method for iPlanet Portal Server Administration Console. Therefore, there are only two ways to access and configure the iPlanet Portal Server platform: as a superuser or as the non-root user entered as the Super Administrator at the time of installation.

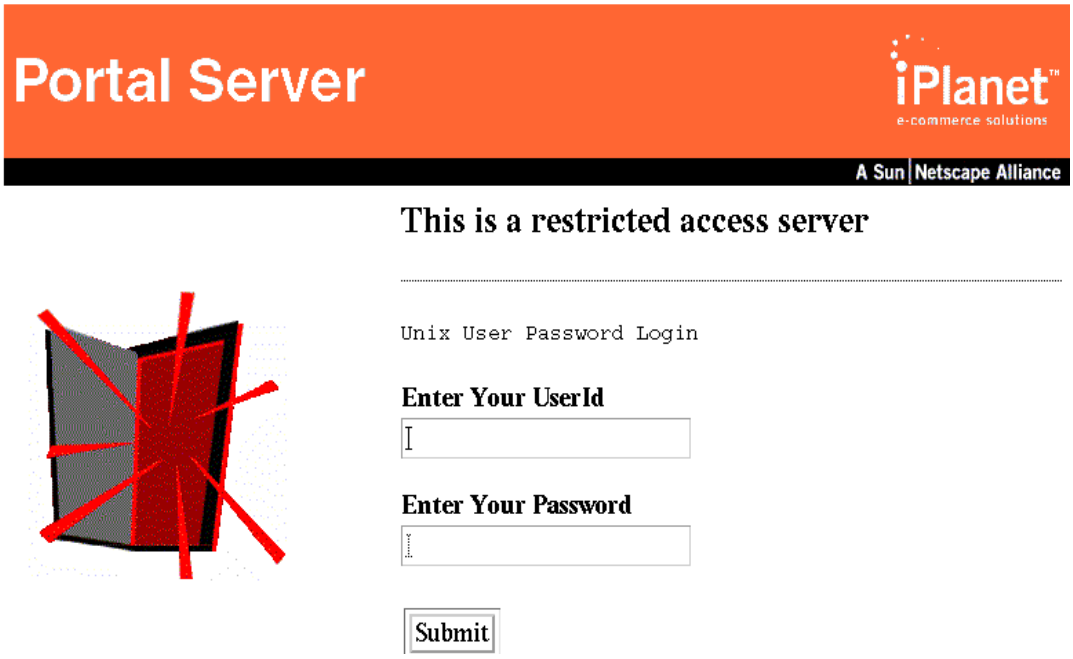

Figure 1-7 Administration Console Login Screen (UNIX Authentication)

How the Administration Console is Organized

The home page of the web-based Administration Console consists of two components, as shown in Figure 1-8. The Task frame is on the left, and the Content Frame is on the right.

Figure 1-8 iPlanet Portal Server Administration Console Main Screen

Main Screen Task Frame

The task frame groups individual tasks that can be performed from the Administration Console. The tasks displayed vary depending upon how you are logged in to the system. For the Super Administrator, all tasks are displayed. For the Domain Administrator, platform-level and portal server specific tasks are not displayed.

The task frame contains five task groups, each of which has one or more activity links. Each task group is described below.

Session Management

This task group contains links to content pages that show the status of the user sessions the site's iPlanet Portal Server platform. If you are a Super Administrator, this section can show all valid sessions for your site. If you are a Domain Administrator, the valid sessions can be viewed for users in your domain.

The session management settings are controlled through attributes and privileges using the Role>Policy>Sessions links to display the Sessions page.

You can terminate an individual user session using the links available in this section.

Portal Server Services

This task group contains links to content pages that enable you to configure and manage gateways and servers in your platform. It also shows the status of the server and gateway. Portal Server Services also contains a link to the logging management screens wherein log profiles for the gateway, authentication, and other system services can be viewed and managed.

You must be Super Administrator to configure the attributes on the content pages accessed through the links in this section. The Super Administrator can allow the Domain Administrator to view the server related logs but not the gateway logs.

Portal Server Platform (Super Administrator Only)

This task group contains links to content pages that can be set up across the platform as global attributes for your installation. The link to set attributes here is Manage Platform Settings.

You will not see this section in the Administration menu if you are a Domain Administrator.

Roles and Users

This section contain links to content pages where you manage the attributes and policies for the domains, roles, and users in your iPlanet Portal Server platform. If you are Super Administrator, the profiles and policies of all domains can be accessed through the iPlanet Portal Server platform. Moreover, following the links in this section, Domain Administrators can be created to configure and manage their own domain.

The Domain Administrator can only access the domain, roles, and users profiles assigned to their domain.

Miscellaneous Section

This task group contains a link to the online help for administrators and a link to log out of the Administration Console.

Content Frame

The Content frame displays the information related to the activity selected in the task frame. The content pages might include:

- Lists of servers and gateways in a platform
- Session statistics for the server and gateways
- Domains in an iPlanet Portal Server platform
- Profiles of domains, roles, and users in an iPlanet Portal Server platform
- Policy pages for the domains, roles, and users of the iPlanet Portal Server

The path designation at the top of the Content frame indicates where you are in the iPlanet Portal Server role tree. This becomes important when configuring attributes at a parent level (i.e, the domain) that will be inherited by its children (roles, child roles, and users if any).

Moving Through the Administration Console Content Pages

Navigating Through the Administration Console

The iPlanet Portal Server role tree is multi-layered. However, to create a user profile within a domain, select the domain of interest from the Manage Domains link to call up that domain. The domain page indicates the role link. Selecting the role link calls up the role page. The Add User link is displayed at the top of this page. This link is selected to create a user profile. The created user profile can then by accessed from the User link that is displayed at the bottom of the role page. An existing user profile can be accessed quickly using the Search link on the domain page.

Screen Shortcuts

- All content pages showing profiles or policies have the Back To Top link that quickly moves you to the top of the page.

- Policy pages are lengthy. Therefore, the policy page begins with an index of links, any of which can be used to jump to a particular section.
- To go back to a previous content page, use the Back to Overview button. Alternatively, the Back button of the browser will display the previously viewed page.

Using the Search Link

The Search link can be used to search for roles and / or users. When this link is clicked, the Search for Roles and / or Users window is displayed, as shown in Figure 1-9.

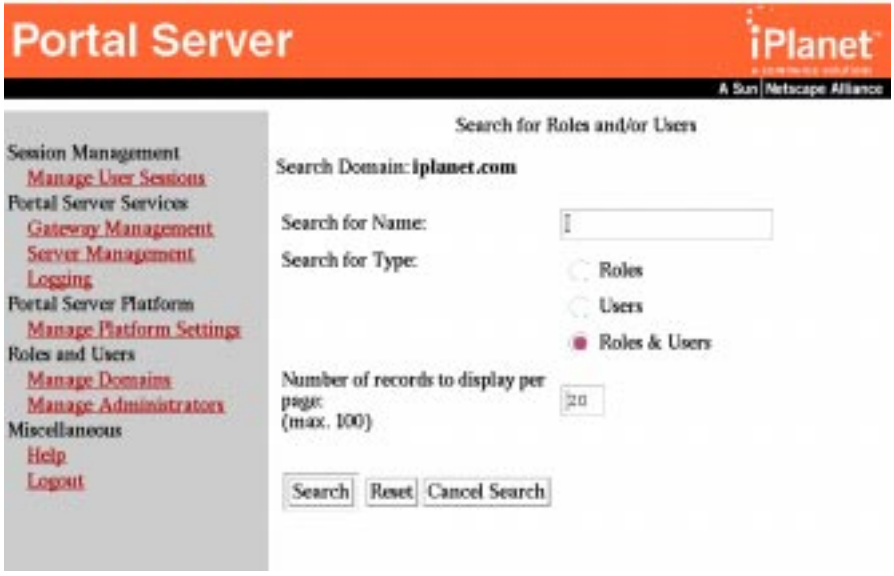

Figure 1-9 Role and / or User Search Window

NOTE The search function works from the current level of the role tree and down; in other words, when doing a search from a child level, the parent level will not be searched.

Interacting With The Administration Console

Modifying Information in the Contents Frame

An attribute setting or policy can be changed only when write permission is enabled. A Domain Administrator can view and change information related to the assigned domain. A Super Administrator can view and change information throughout the iPlanet Portal Server platform.

Read/Write Permissions

When logged in as a Domain Administrator, pages with profile or policy attributes have a show and a hide permissions button at the top of the screen, as shown in Figure 1-10. When permissions are shown, the read / write permissions attributes are displayed to the right of each attribute on the page.

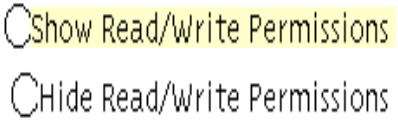

Figure 1-10 Permissions Buttons

NOTE	The Super Administrator will see permissions differently as: Admin: Read / Write on one line and User: Read / Write on a second line.

The Super Administrator has read and write permission for any attribute in the platform. As a Domain Administrator, the permissions viewed are those granted by the Super Administrator.

Hiding the read / write permissions reduces the amount of information displayed in the Contents frame. However, a Domain Administrator might want to show role and user permissions to review attribute settings for those profiles.

Processing Changes to the Profile Server

There are three buttons located at the bottom of profile and policy pages:

- Submit
- Reset
- Cancel

There is also a check box with a text label indicated as ‘Apply changes to all subRoles.’

Submit

The Submit button processes the changes made on the page to the profile server.

Reset

The Reset button restores the values of the attributes to those found when the page was initially displayed.

Cancel

The Cancel button aborts any changes made on the page and returns the previously displayed page.

Apply Changes to All SubRoles

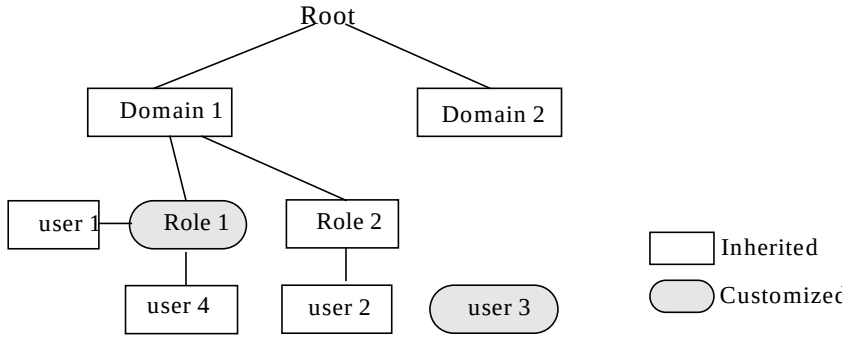

Figure 1-11 Graphical View of Initial Role Tree

To apply changed attributes at one particular level to lower levels of the role tree, click the “Apply changes to all subRoles” check box, and then click the Submit button. Clicking this check box causes all changed attributes to propagate down through child role levels. If the new attributes apply only to this level of the role tree, do not check “Apply changes to all subRoles.”

Figure 1-11 graphically represents a role tree with customized attributes for Role 1 and user 3. If an attribute is changed in Domain 1 that has the same attribute with customized settings in Role 1, clicking the “Apply changes to all subRoles” box will overwrite the customized attribute in Role 1. To reinstate the customized attribute, Role 1 would be accessed to make the change directly and submit it to the Profile Server.

Further, if an attribute is changed in Domain 1 and the “Apply changes to all subRoles” box is not clicked, the corresponding customized attribute in Role 1 and user 3 is not changed but the Domain 1 attribute change is propagated through the roles Role 2, user 2, user 1, and user 4, by inheritance.

CAUTION Use care when specifying Apply changes to all subRoles since any customized attributes at lower levels of the role tree will be removed.

Managing Customized Attributes

When an attribute for a given domain, parent or child role is changed, its state in the Profile Server is marked as customized. This customized notation appears to the right of the attribute in a pull down window that also includes the Make Inherited option. If the make inherited option is desired for a customized attribute, in effect, you are saying that this attribute at this level of the role tree should be returned to its default or inherited value from its parent role (e.g. a role would inherit the domain value setting for the attribute).

When using the Make Inherited state to change an attribute back to its inherited value and also checking the Apply changes to all Subroles, any customized attribute setting in child role levels will be removed.

NOTE Any attribute defined with a numeric datatype cannot be left blank. Also, customized attributes must be set at each level of the role tree for which they are intended. There is no way to propagate a customized value from a parent role to a child role.

Chapter 2

Creating A Multi-Domain Portal

Overview

This chapter is provided to quickly become productive in setting up and managing a corporate intranet portal using iPlanet Portal Server. In this case, the portal will consist of two domains; one for a business to consumer (b-c) solution and one for a business to employee (b-e) solution. The tasks described are to be performed by the Super Administrator unless otherwise noted.

Portions of setting up a multi-domain portal can be done by a delegated Domain Administrator. For each domain, there can be one or more domain admin roles or users. However, domain admin roles and users are assigned to one domain only. No domain admin role or user can be assigned to more than domain.

To create a Domain Administrator, refer to "Setting Up a Delegated Administrator" on page 69. Also, for convenience, the tasks of maintaining roles and users (moving and deleting) are included following setting up a domain administrator.

NOTE The Super Administrator can create a Domain Administrator to delegate administration tasks and activities for his or her assigned domain. See “Setting Up a Delegated Administrator,” on page 69.

The business to consumer facing portal includes the following tasks:

- Creating a domain specific to the consumers
- Creating a role for the consumer profiles
- Configuring self-registration for new consumers
- Configuring policy for access to the portal and resources

- Disabling access to intranet applications and resources

The business to employee facing portal inclues the following tasks:

- Creating a domain specific to your employees
- Enabling an authentication method for the domain
- Configuring the Virtual VPN (Netlet) for TCP application access
- Configuring policy for the domain.
- Customize the Desktop for the domain

Creating a Business to Consumer Portal

The creation of a business to consumer portal includes, (but is not limited to), the following tasks:

- Creating a domain
- Enabling self-registration through the membership module
- Specifying URL access policies
- Specifying application access policies

Creating the Business To Consumer Domain

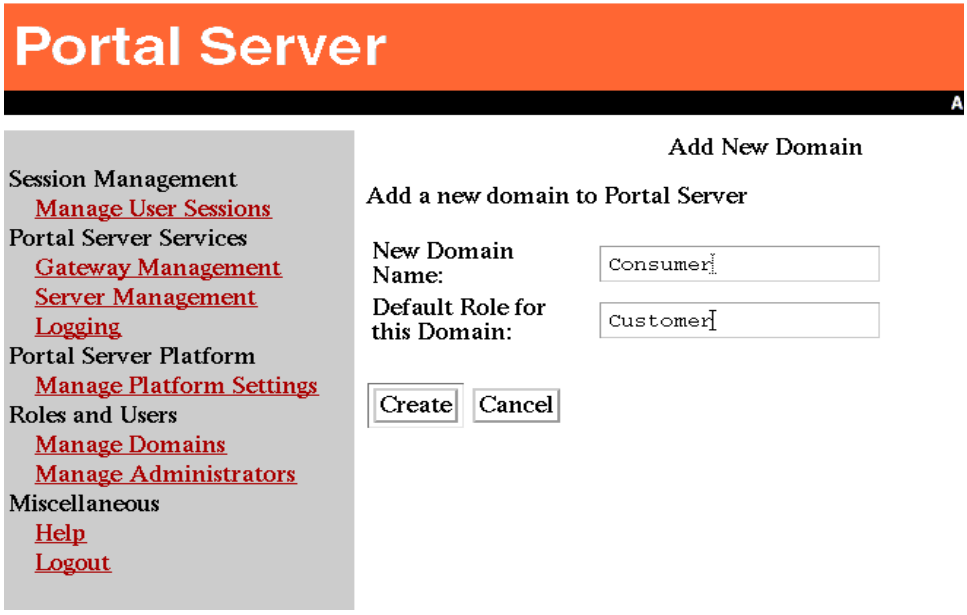

Figure 2-1 Add New Domain Link

To enable a fundamental business-to-consumer portal that allows users to self-register, perform the following steps.

1. Log in to the console as the Super Administrator.
2. Click Manage Domains from the left panel of the display.
3. Click the Add New Domain link. The Add New Domain window is displayed as shown in "Add New Domain Link" on page 43.
4. Type Consumer in the New Domain Name field.
5. In the Default Role for this Domain field, type Customer.
6. Click the Create Button.

7. Following the prompt indicating that the new domain and role have been created, click the Continue button.

   The Domain screen is redisplayed with the added domain link shown with the domain specified at installation. The Customer role is shown under the Consumer domain link when clicked.

Enabling Self-Registration Using the Membership Module

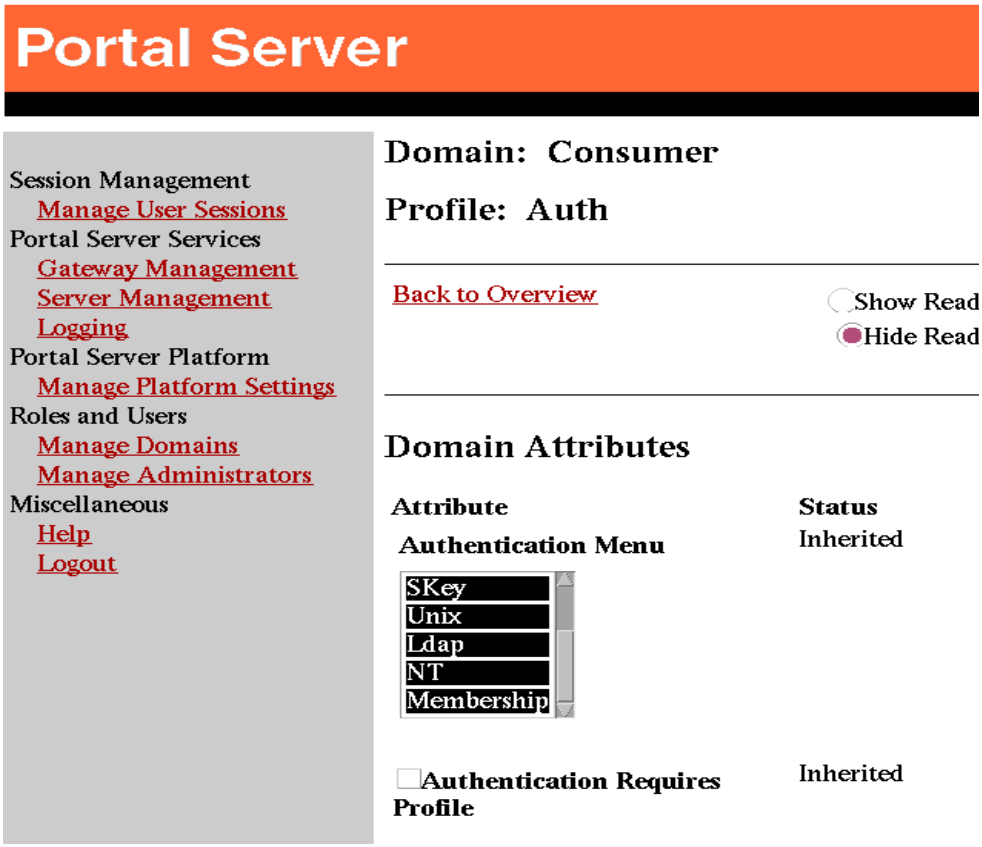

Figure 2-2 Authentication Module List Window

1. From the Domains screen, click the Consumer domain link. The Consumer domain page is displayed.

2. Click the Profiles>Authentication link to call up the Authentication module list window under the Authentication Menu label. The default shows all authentication modules selected, as shown in Figure 2-2.

NOTE Authentication applies to a domain and is set only at the Domain level of the role tree.

3. Select only the Membership authentication module to allow users to self-register. Deselect all other authentication modules.
4. Click the Submit button at the bottom of this page to update the Consumer domain profile on the Portal Server. A message displays indicating successful update of this profile.
5. Click the Continue button to return to the previous page.

Verifying User Self Registration Authentication and Self-registered User Role Placement

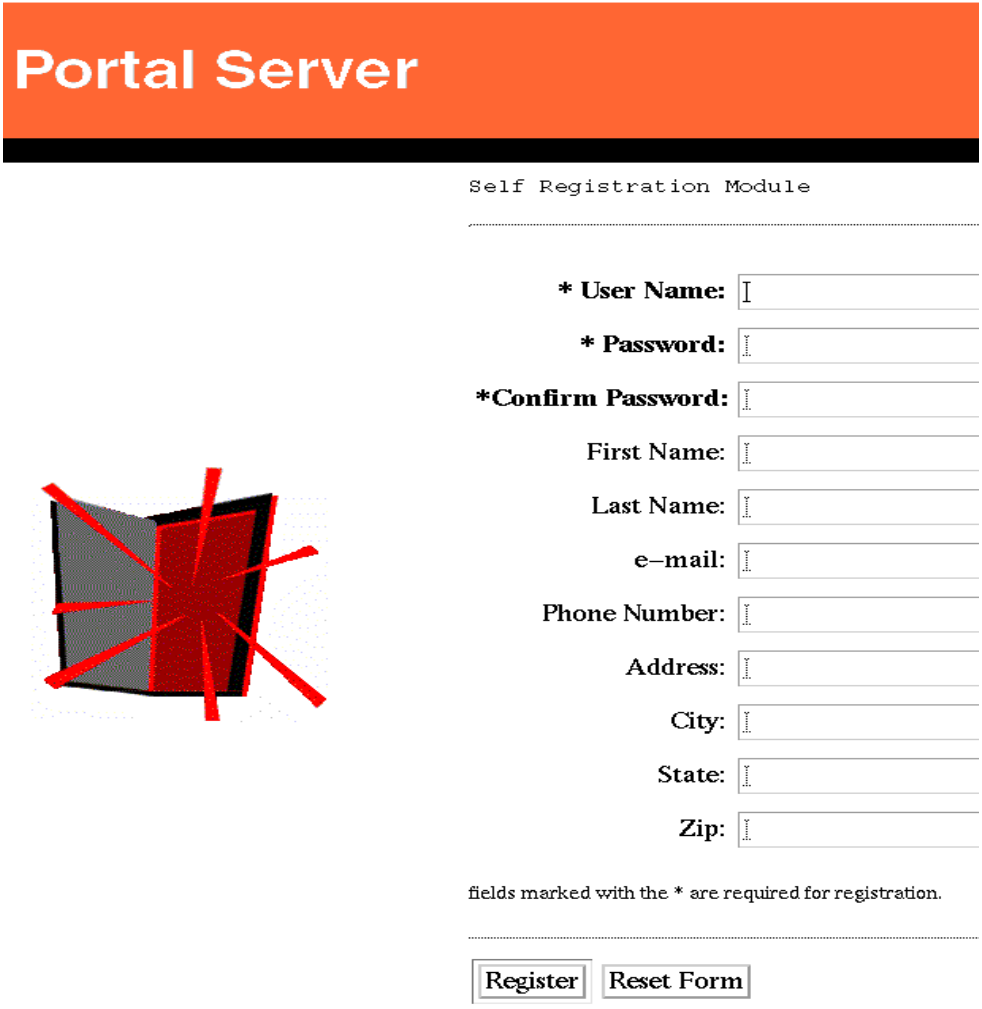

Figure 2-3 Self Registration Form

1. Open a second browser instance from the command line.

NOTE A second browser *instance*, versus a second browser *window*, is necessary to avoid sharing of the same cookie for an iPlanet Portal Server session.

2. Open the following iPlanet Portal Server gateway URL:

   https://gateway/consumer

NOTE There are multiple options available to the user to contact the portal. It may be desirable to use virtual IP or multiple DNS names as opposed to distinguishing between the two different domains. Refer to Chapter 9, Add Gateway Server, for information on setting up a gateway using virtual IP and DNS domains.

3. From the displayed log in page, click the New User button to call up the Self Registration Module form, as shown in Figure 2-3.
4. Select a user name and password (with at least four characters) and add the other pertinent user information indicated. The form can be refreshed to reenter data using the Reset Form button.
5. Click the Register button to continue the registration process with the display of the disclaimer window.
6. Read the disclaimer text and click the Agree button to complete the registration process. The iPlanet Portal Server desktop page for the Consumer domain will be displayed as shown in “iPlanet Portal Server Desktop Home Page,” on page 48.

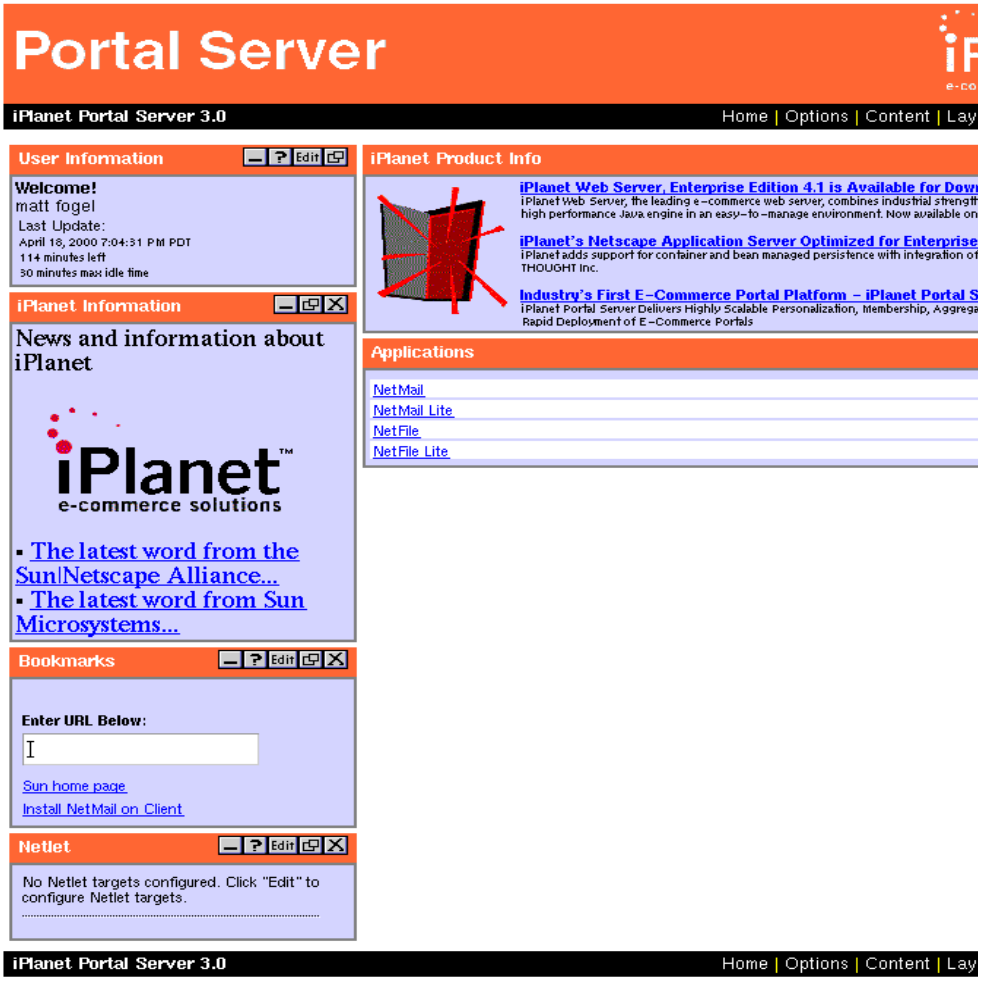

Figure 2-4 iPlanet Portal Server Desktop Home Page

NOTE User registration information may be customized as described in Chapter 4, Membership.

7. Click the Log out link at the top right to close the desktop session. The logout message window is displayed.

8. Go back to the Admin Console.
9. Click the Manage Domains link.
10. Click the Consumer domain link.
11. Click the Customer role link to verify the user profile created in “Creating a UNIX User Profile That Can Be Authenticated,” on page 60
12. Click the User link to display the user name specified in step 4 of "Enabling Self-Registration Using the Membership Module" on page 44. Alternatively, the Search link can be used to find the user name.

Specifying URL Access Policy For the Customer Role

For a business to consumer portal, users will typically only access the portal server URLs only and not corporate Intranet URLs.

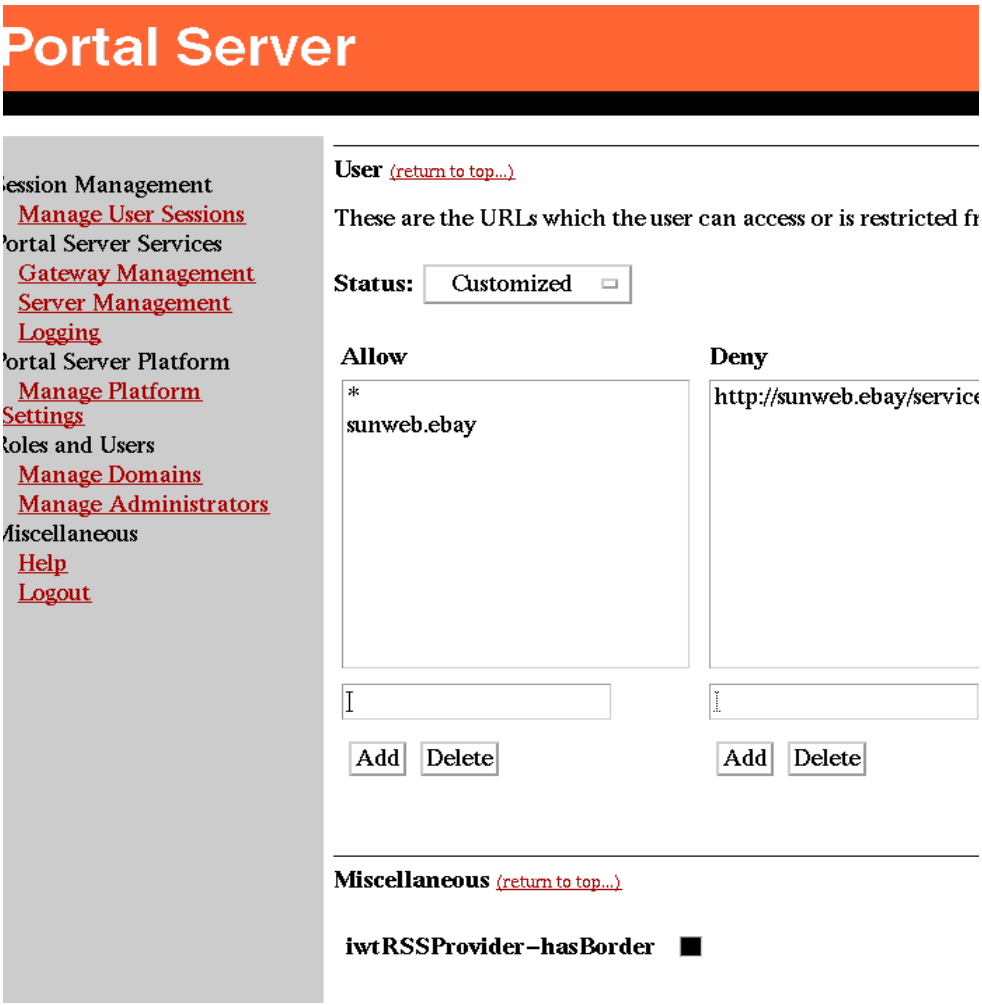

Figure 2-5 URL Access in Consumer>Customer Role Policy Page

1. From the Admin Console, click the Customer Role link under the Consumer Domain.
2. Click the Policy link under Profiles.
3. Locate the User URL Access attribute with the allow and deny windows, as shown in Figure 2-5.

NOTE Shortcut tip: Click the User link in the index section at the top of the Policy page.

4. Type a valid intranet URL in the Allow URL list entry box. Use the form: http://servername.
5. Click the Add button to add the URL specified in step 4 to the Allow list window.
6. Type a valid corporate intranet URL in the Deny URL list entry box.
7. Click the Add button to add access to the URL specified in step 6 to the Deny list window.
8. Click the Submit button at the bottom of this page. The profile update message is displayed.
9. Click the Continue button to return to previous page.

Verifying URL Access Policy From the Desktop

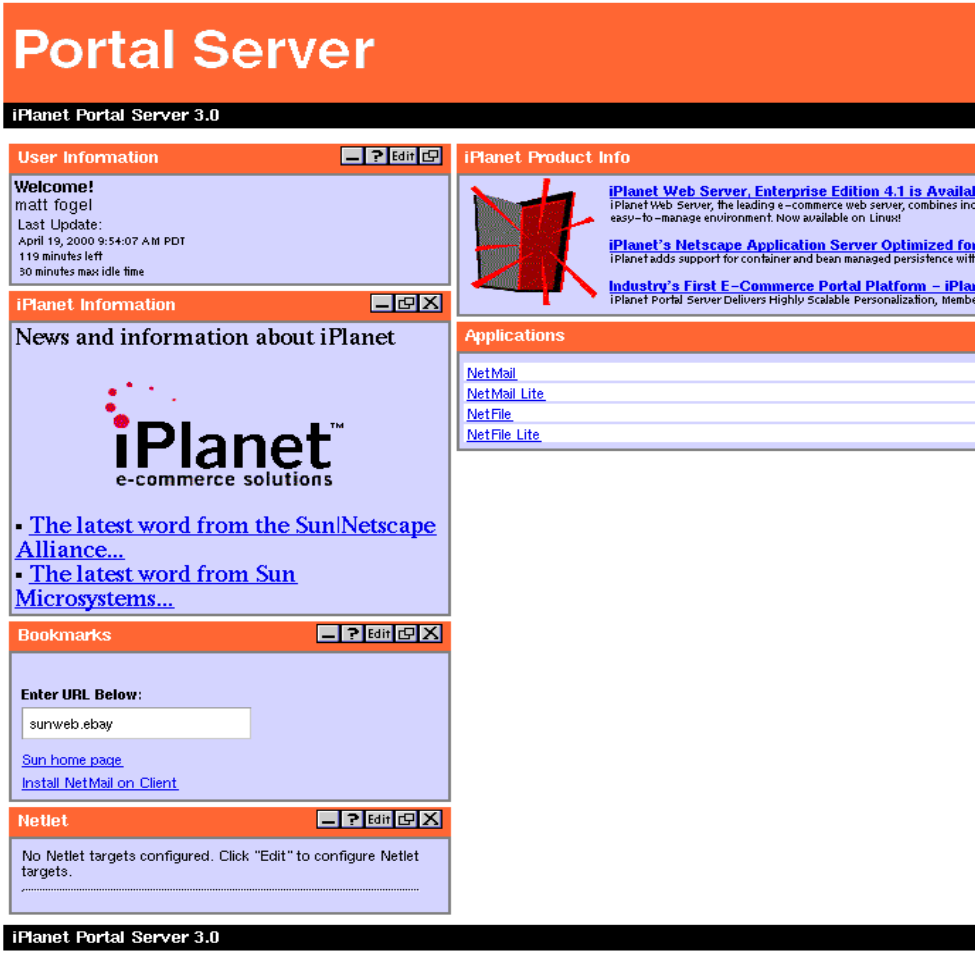

Figure 2-6 Entering URL for Allowed Access

1. In a second browser instance, type the iPlanet Portal Server gateway login URL (https://gw/Consumer). If needed, refer to step 2 of “ on page 46..” Use the same user name and password as that created through self registration earlier.

2. Type the following URL: http: / / server:8080 (from step 4 of “"Specifying URL Access Policy For the Customer Role" on page 49.”), in the Bookmarks URL entry box and press Enter, as shown in “Entering URL for Allowed Access,” on page 52. The webserver index page will be displayed in a new browser window.

NOTE Business to consumer users can also access any internet URL.

3. From the desktop window, type the corporate intranet URL specified in step 6 of “"Specifying URL Access Policy For the Customer Role" on page 49.” in the Bookmarks URL entry box and press Enter. A new browser windows opens with a message indicating that access is denied.
4. Log out of the iPlanet Portal Server Desktop.

Disabling Access To an Application and Other Secure Providers

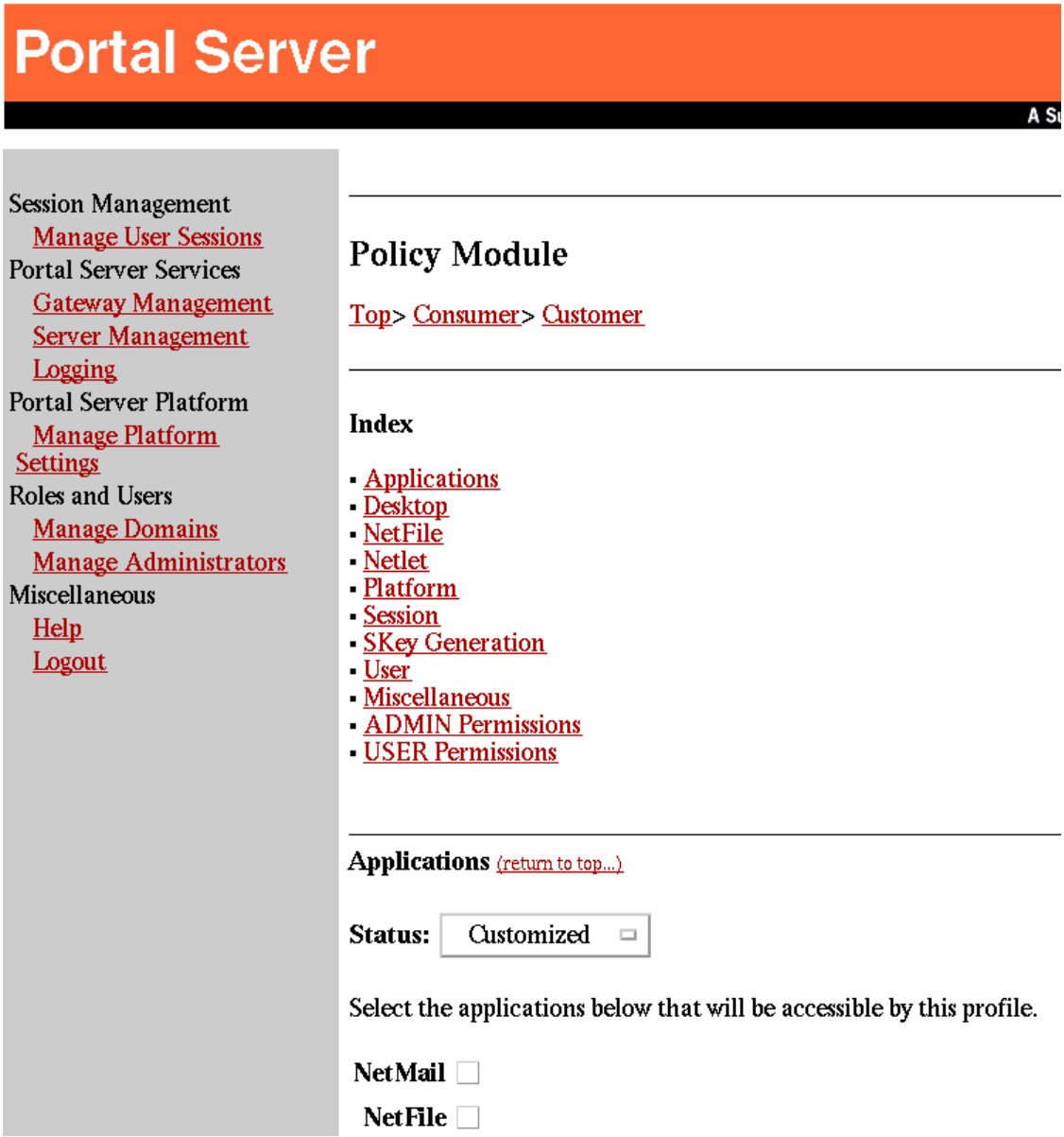

Figure 2-7 Policy for Customer Role Mail Application

1. From the Admin console browser instance, click the Policy link within the Consumer domain.
2. Disable access to NetMail, NetFile, and Netlet by clicking the check box to the right of each application as shown in Figure 2-7. Access to these applications is disabled even if the start up URL is known.
3. Click the Submit button at the bottom of this page.
4. Following confirmation of the Profile update, click the Continue button.

Removing the Disabled Applications from the Available List

1. Click the Consumer domain link to return to the Domain, Roles & Users profile page.
2. Click the key to the left of the Applications link to expand the list.
3. Click the Desktop link to display the Desktop Profile page as shown in “Desktop Profile Page,” on page 56.

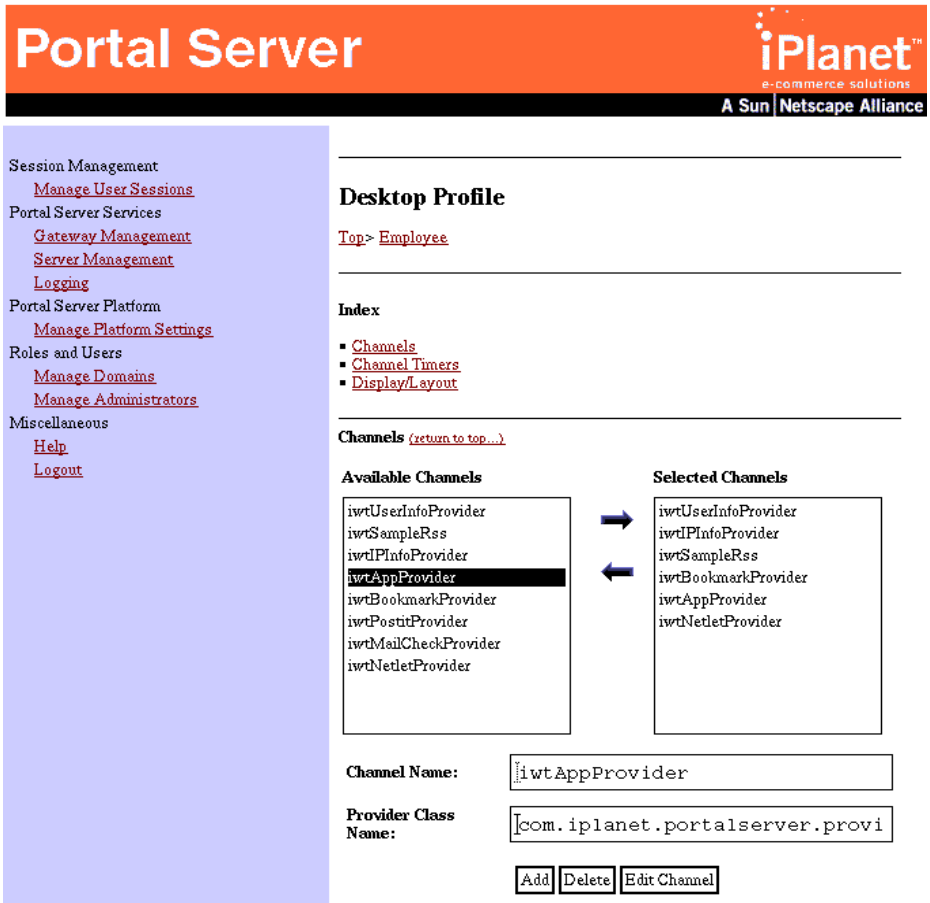

Figure 2-8 Desktop Profile Page

4. Select iwtAppProvider from the Available Channels list window.
5. Click the Edit Channel button to display the AppProvider attribute as shown in Figure 2-9.

Figure 2-9 AppProvider Attribute Window

6. Highlight the NetMail/(java + applet) URL, and the NetFile/(java + applet) URL.
7. Click the Delete button to remove these channels.

NOTE To restore these channels, the Customized pull down will be displayed to the right of the applications attribute window after changes are stored in the Profile Server. Click the pull down arrow and select Make Inherited to restore the NetMail and NetFile URL channel statements.

8. Click the Submit button at the bottom of this page to update all changes made to the Profile Server.
9. Click the Continue button to return to the AppProvider page. Then use the Back to Overview link or the Cancel button to return to the Desktop page.

Verifying Disabled Application Access

1. In a second browser instance, type the iPlanet Portal Server Desktop login URL.
2. Log in to the desktop with a registered membership account for the user in the Consumer domain. The desktop home page will be displayed.
3. Verify that the Applications list on the right side of the content window does not include Netfile or Netmail. Also, attempt to start the NetFile application directly by typing the URL http://server:8080/NetFileApplet in the Bookmarks text box. The policy check returns a denial of service message.
4. Log out of the desktop.

Creating a Business to Employee Portal

The creation of a business to employee portal includes, (but is not limited to), the following tasks:

- Creating the Employee domain
- Enabling an authentication method for the domain
- Setting up VPN for TCP application access
- Setting up policy for the domain
- Customizing the desktop for the domain

Creating the Business To Employee Domain

1. Log in to the console as the Super Administrator.
2. Click the Manage Domains link from the left frame.
3. Click the Add New Domain link. The Add New Domain window is displayed.
4. Type Employee in the New Domain Name field.

5. In the Default Role for the Domain field, type Engineer.
6. Click the Create Button.
7. Following the prompt indicating that the new domain and role have been created, click the Continue button . The Domain screen is redisplayed with the added domain link shown with the domain specified at installation. The role is shown under the domain link when clicked.
8. Click the Add Role link at the top of the domain screen.
9. Type Manager in the new role field.
10. Click the Create button, then click the Continue button. The Engineer and Manager roles are now shown.

Enabling UNIX Authentication

NOTE In practice, a business to employee portal may be configured with any of the iPlanet Portal Server authentication modules. UNIX is used for this example only.

1. From the Domains screen, click the Employee domain link. The Employee domain page is displayed.
2. Click the Profiles>Authentication link to call up the Authentication module list under the Auth Menu attribute. The default shows all authentication modules selected, as previously shown in Figure 2-2.

NOTE Authentication applies to a domain and is set only at the Domain level of the role tree.

3. Select only the UNIX authentication module to employee access to iPlanet Portal Server. Deselect all other authentication modules.
4. Click the check box indicated as “Authentication requires profile” to restrict iPlanet Portal Server access to employees with an existing profile.

NOTE By default, the Authentication requires profile attribute is false so that any user that passes authentication will have a profile dynamically created for them under the default role of Engineer. By setting the attribute true, a pre-population task must be performed to an external LDAP database, as described in the *Release Notes.*

5. Click the Submit button at the bottom of this page to update the Employee domain profile on the Portal Server. A message displays indicating successful update of this profile.
6. Click the Continue button to return to the previous page.

Creating a UNIX User Profile That Can Be Authenticated

1. Using the Admin Console, click the Engineer role under the Employee domain.
2. Click the Add User link.
3. Create a user with a valid UNIX account.
4. Repeat steps 1 through 3 for the Manager role to allow customization of user access by having a valid user for each role authenticate and access iPlanet Portal Server.

Verifying UNIX Authentication at Desktop Log In Screen

1. Open a second browser instance.
2. Open the following iPlanet Portal Server gateway URL:

   https://gateway/Employee

NOTE There are multiple options available to the user to contact the portal. It may be desirable to use virtual IP or multiple DNS names as opposed to distinguishing between the two different domains. Refer to Chapter 9, Add Gateway Server, for information on setting up a gateway using virtual IP and DNS domains.

3. From the displayed log in page indicating UNIX authentication, log in to the desktop using a valid employee account. Upon successful login, the iPlanet Portal Server Desktop home page will be displayed.

4. Click the Logout link to close the desktop session. The logout message window is displayed.

Setting Up a Virtual VPN for the Employee Domain

When access to a non-Web-based application or a TCP application is needed by your employees, it will become necessary to set up a netlet for communication. A netlet creates a virtual private network on the fly without the need for client software.

The following netlet example allows employees remote access to the Netscape Mail client on their browser as if they were at their corporate workstation on the intranet. A similar netlet may be configured for other secure TCP access such as telnet or remote desktop display.

NOTE The netlet is fully described in Chapter 4.

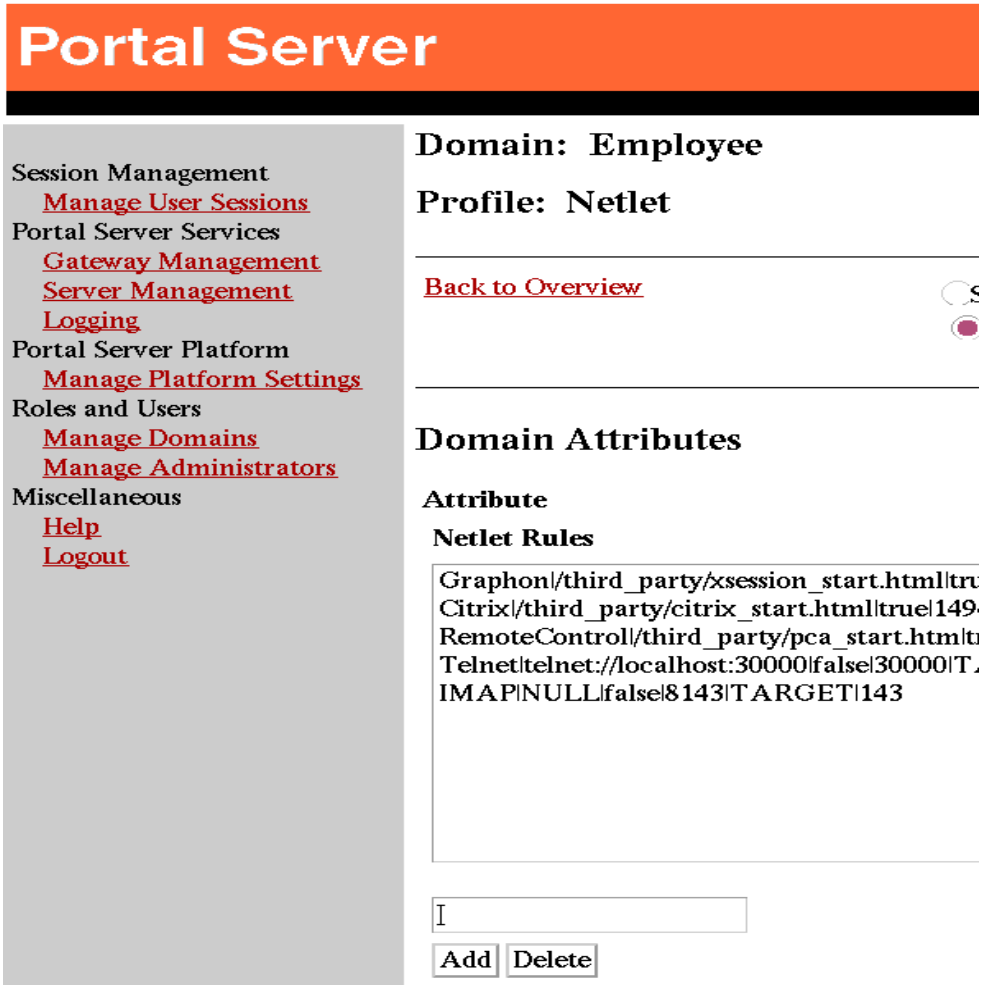

Figure 2-10 Netlet Rules Window

1. From the admin console, select the Employee domain under Manage Domains.
2. Expand the Applications link.
3. Click the Netlet link. The Netlet Rules window is displayed as shown in Figure 2-10.
4. Type the Netlet rule: IMAP | NULL | false | 8143 | TARGET | 143. This rule will enable the use of IMAP mail service for an IMAP client.

NOTE Netlet rules exist at the network layer. The warning pop-up for the connections check box applies to multi-user, multi-platform environments, such as UNIX and Linux; this check box does not apply to a Windows-based client environment.

5. Click the Add button to add this rule to the Netlet application.
6. Click the Submit button at the bottom of the page to process this change to the Profile Server.
7. Click the Continue button to return to the previous page.
8. Open another Netscape browser instance and log in to the desktop using the link: https://gateway/employee.
9. Click the Netlet Edit button on the left of the desktop. The Edit Netlet window is displayed as showin in “Netlet Application Window,” on page 63.

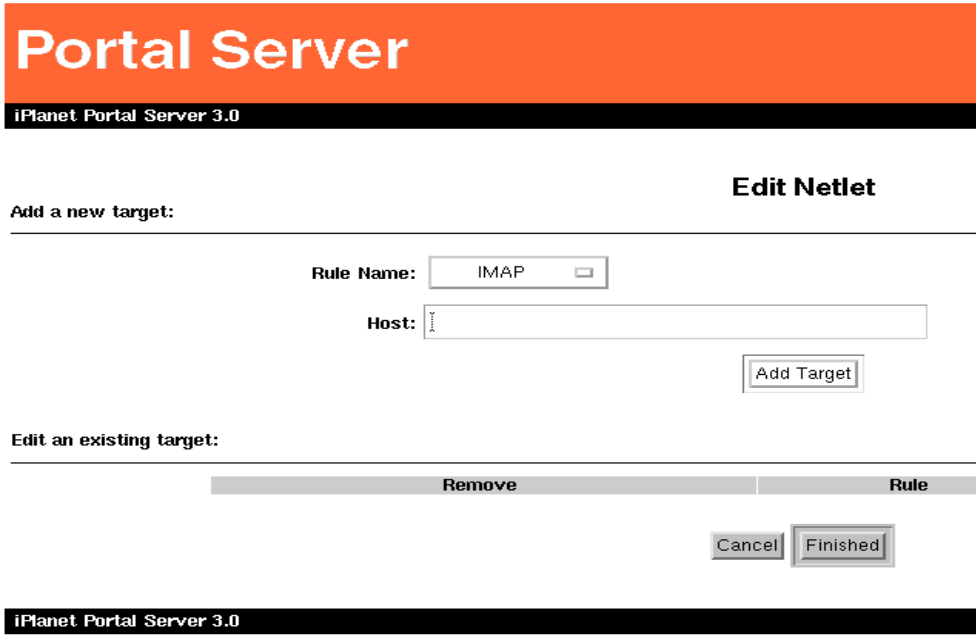

Figure 2-11 Netlet Application Window

10. Select the IMAP rule name and type the servername to be used for mail hosting in the Host text box.
11. Click the Add Target button to complete the mail server configuration.
12. Click the Finished button to process this change to the Profile Server. Remain logged in to the desktop. The indication of 'IMAP on servername' is displayed at the lower left of the desktop page.
13. Open another Netscape browser window and select Edit>Preferences from the Navigator menu.

NOTE The layout of the Netscape mail settings may vary depending upon your installed version.

14. Expand the Mail and Newsgroups option and click on Mail Servers.
15. Click on Edit to the right of Incoming Mail Servers.
16. Change the Sever Type to IMAP.
17. Change Server Name to: localhost:8143.
18. Click the OK button. At this point, the use of the Netlet with IMAP email service using Netscape Messenger is configured.

Verifying Netlet Service on Port 8143

1. Open a terminal window.
2. Run the command: netstat -an | grep 8143. A listening message on port 8143 will be returned.
3. Alternatively, launch the Netlet IMAP on servername link to start the netlet. Then, open the Netscape Messenger window.

Denying Access to a URL and an Application for a Role

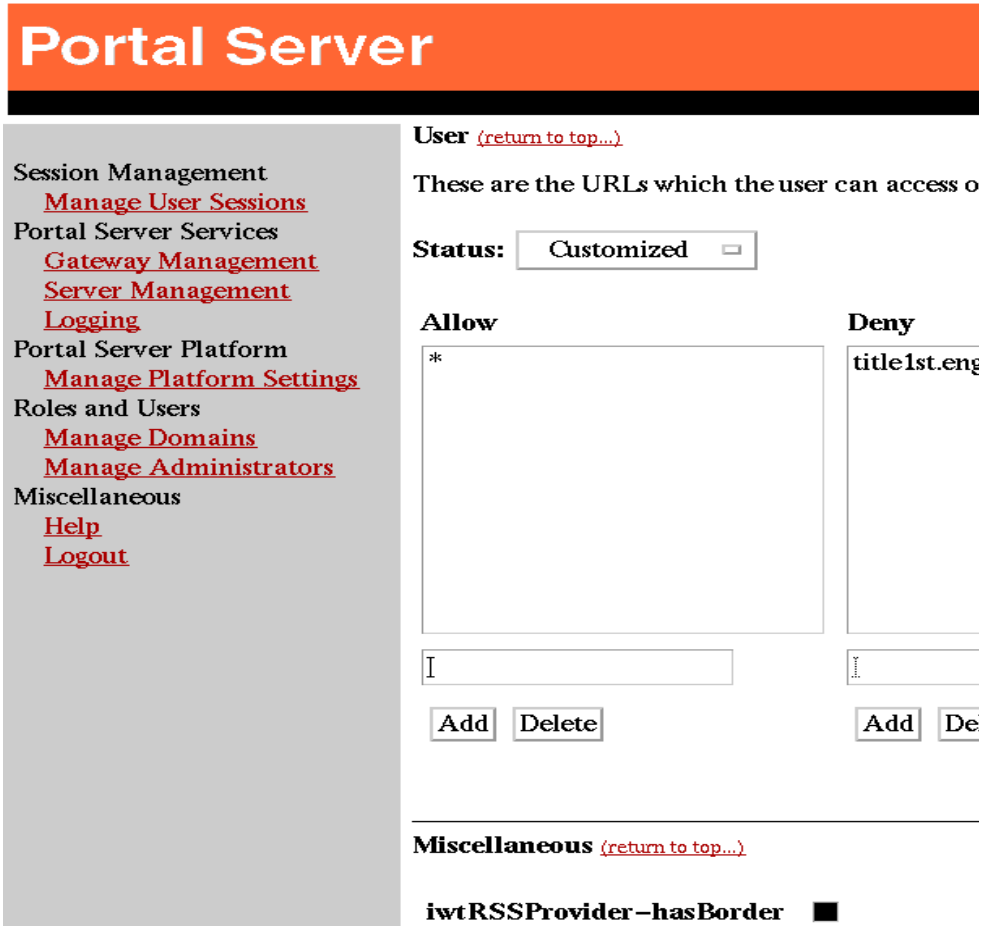

Figure 2-12 Engineer Role User URL Policy Attribute Window

1. From the Admin Console, click the Engineer role under the Employee domain.
2. Click the Policy link to display policies.
3. Click the User link in the index section at the top of the page to display the User policy attributes for the Engineer role profile.

4. Locate the URL Policy attribute, as shown in Figure 2-12. In the Deny list text box, type a well-known URL on the Intranet that should not be used by the Engineer role. Use the form:

   http://hostname

5. Click the Add button.
6. Uncheck the NetFile application in the Application section of the Policy page to deny access for the Engineer role.
7. Click the Submit button to update the profile and then click Continue.
8. Click the Employee domain link to return to the Domain, Roles & Users profile page.
9. Click the key to the left of the Applications link to expand the list.
10. Click the Desktop link to display the Desktop Profile page as shown in Figure 2-8.
11. Select iwtAppProvider from the Available Channels list window.
12. Click the Edit Channel button to display the available applications attribute window as shown in Figure 2-9.
13. Highlight the NetFile/... URL.
14. Click the Delete button to remove this URL channel.

NOTE To restore this channel, the Customized pull down will be displayed to the right of the applications attribute window after the change is stored in the Profile Server. Click the pull down arrow and select Make Inherited to restore the NetFile URL channel statement.

15. Click the Submit button at the bottom of this page to update the change to the Profile Server.
16. Click the Continue button to return to the Profiles page.

Verifying Denied Access to Engineer User to URL and Application

1. In another browser instance, log in to the Portal Server desktop as the created user from “Creating a UNIX User Profile That Can Be Authenticated”.

2. In the Bookmark URL entry box, type the URL specified in step 4 of on page 65. An error message indicating access denied will be displayed.
3. Verify that the Netfile application is not in the Application provider list.

Customizing the Desktop With a Welcome Message

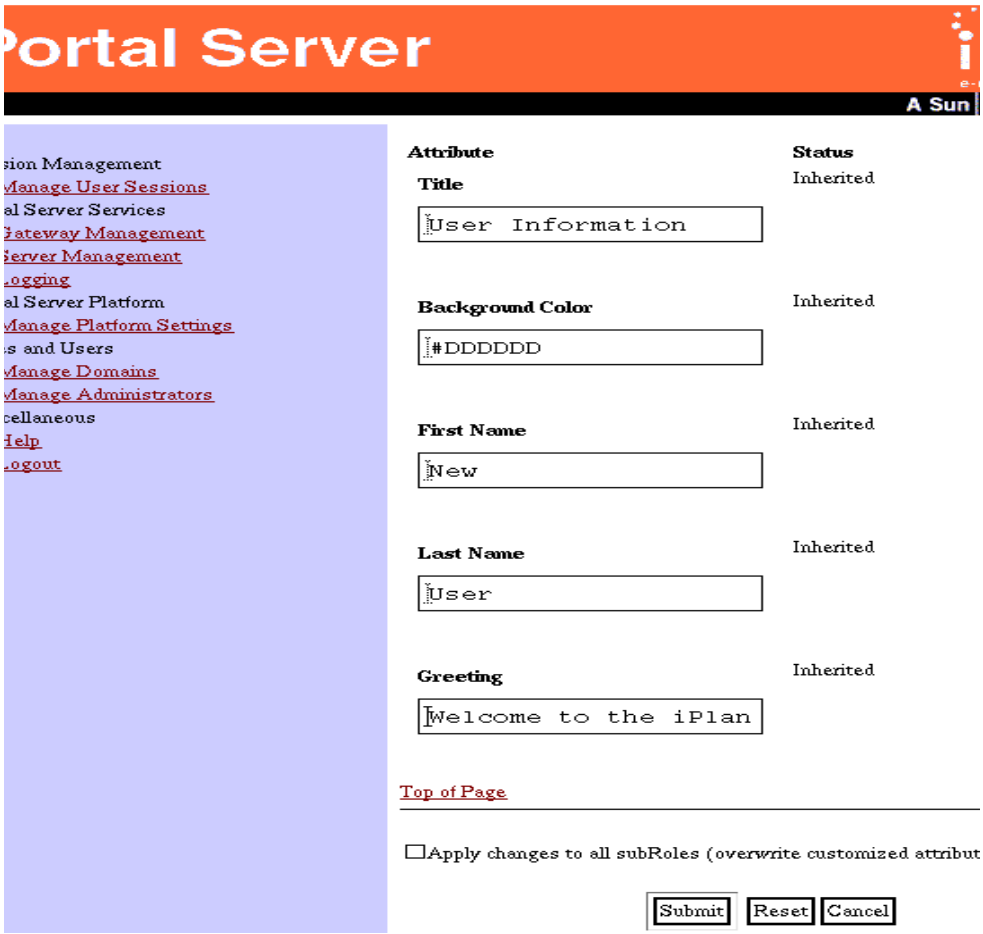

Figure 2-13 Welcome Message under Application>Desktop iwtuserinfo Provider

1. From the Admin console under Manage Domains, click on the Employee domain.
2. Click the Engineer role.

3. Expand the Applications link.
4. Click the Desktop link.
5. From the Channels section, Available Channels list, click the iwtUserInfoProvider.
6. Click the Edit Channel button to display the userInfoProvider page.
7. Scroll to the greeting text entry box and change the greeting to: Welcome Engineer!, as shown in Figure 2-13.
8. Click the Submit button at the bottom of the page to process this change to the Profile Server.
9. Repeat steps 1 through 7 for the Manager role and have the greeting say: Welcome Manager!

Verifying the Customized Desktop Welcome Message

1. From another browser instance, log in to the Desktop as an employee user in the Engineer role.
2. Verify that the message greeting under User Information is as specified in step 7 of on page 67.

NOTE When the iwtAppProvider attributes allow the user to have editable rights, under the Admin Console Policy>Desktop Profile at the role or user level of the role tree, the user can elect to change the greeting using the User Information Edit button to get to the greeting text box.

3. Repeat steps 1 and 2 for the Manager role to verify the greeting in step 9 of on page 67.
4. Log out of the desktop.

Setting Up a Delegated Administrator

NOTE The first delegated Domain Administrator is configured by the Super Administrator only. Thereafter, a domain admin can create other admin roles and users.

Adding a New Role

1. Click the Employee domain.
2. Click the Add New Role link.

   The Add New Role window is displayed.
3. Type the name of the new role (e.g., EmployeeAdmin) in the New Role Name field and click the Create button. A message appears indicating that the new role has been created.
4. Click the Continue button. The new role is shown at the bottom of the page.

Assigning Admin Privileges to the New Role

1. Click on the added admin role.
2. Click on the Administrator link under Profiles. The admin profile for this role is displayed.

NOTE The Administrator link under profile is only available at the role level of the role tree.

3. Click the Role Policy attribute check box to enable admin privileges for this role. The clicked box should appear filled in.
4. Click the Submit button to submit this change to the Profile Server. Click Continue when the profile update message is displayed.

Adding a New User for the Admin Role

1. Click the created admin role link under the Employee domain.
2. Click the Add New User link at the top of the page.The Add New User window is displayed.

3. Type the name of the new user (with a valid UNIX account) in the New User Name field and click the Create button. A message appears indicating that the new user has been created.
4. Click the Continue button. The new user is indicated at the bottom of the page.

Managing Roles and Users

This section describes the tasks to:

- Move a User
- Delete a User
- Move and delete a role

Move Users

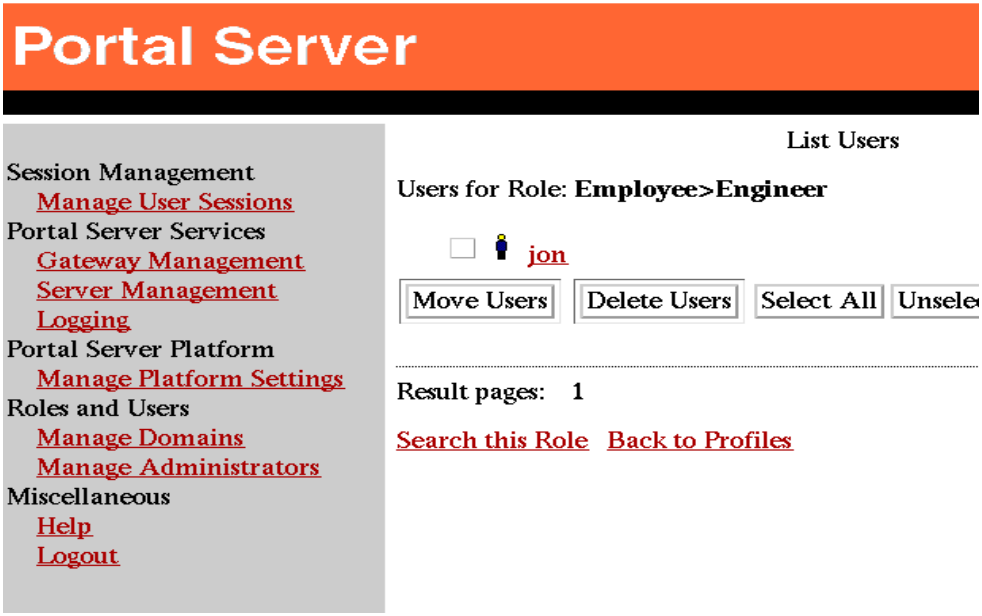

Figure 2-14 Move Users List Users Window

1. From the Domain>Role page, click the User link. The List Users screen is displayed as shown in Figure 2-15 on page 71.

2. Click the box to the left of each user to be moved.
3. Click the Move Users button to display the Move Users window as shown in Figure 2-15 on page 71..

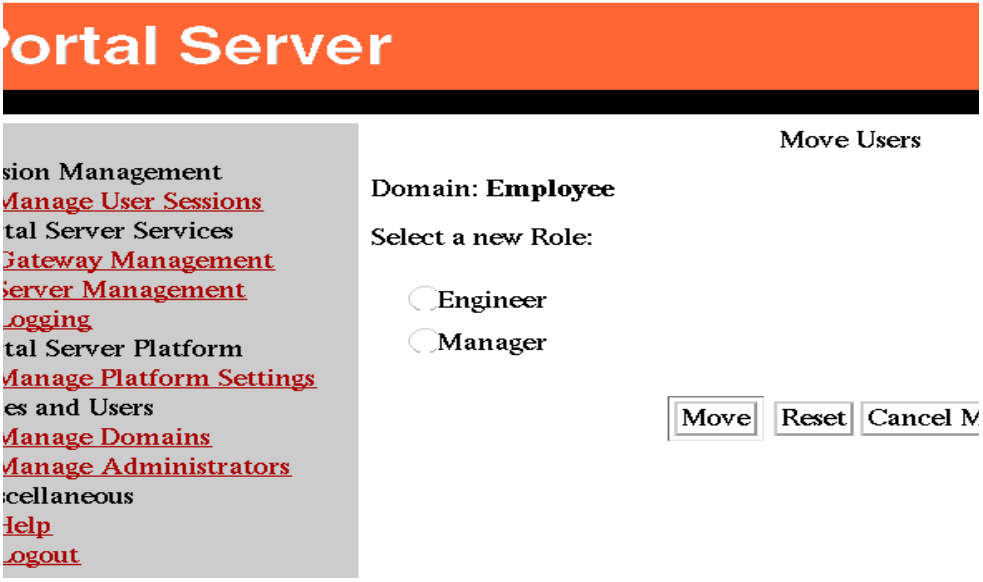

Figure 2-15 Move Users to Another Role Window

4. Click the radio button to the left of the desired role assignment to reassign the user(s) to that role.

NOTE You may receive a security prompt on this submission action. If so, click OK to proceed. Note that at this point you can use the Cancel Move button to cancel this action and return to the Domain>role page. The Reset button is used to clear selected role radio buttons.

5. Click the Move button to complete this role reassignment request. You will be prompted that the move has occurred and click the Continue button to proceed back to the Domain>Role page.

Delete Users

1. From the Domain>Role page, click the Users link to the display the List Users screen as shown in Figure 2-14
2. Click the radio button next to each user to be deleted.
3. Click the Delete Users button to commit this change.

CAUTION When deleting users, there is no confirm prompt following the Delete Users button. Also, when a user has an active session and is deleted, the session will still continue to be active unless the user's session is invalidated from the Manage User Sessions>servername link to display the user sessions page. From this page, click on the user session to be deleted and click the Invalidate Sessions button to end the user's session immediately.

---

4. Click the Continue button to return to the List Users page.

Delete a Role

If a role contains users, the users must first be deleted as described in the section "Delete Users" on page 72. Following that, the role of interest can be deleted by clicking its check box from the subject domain's Domain, Role and Users page. Roles cannot be moved.

Chapter 3

Configuring The Desktop

This chapter describes the following topics related to configuring the client desktop:

- Adding a Custom Provider
- Configuring an available channel
  - Specifying channel column and row layouts
- Setting desktop colors for a channel
- Specifying a customized logo for the portal home page
- Introducing the Channel Wizard

Adding a Custom Application Provider

An application provider is the source of information, in the form of a java class, that can be displayed to a user. When the provider is added to the iPlanet Portal Server selected list of applications, the user can then choose to display this source data to an indicated area on their desktop. The displayed information is referred to as a channel. The prerequisites to loading a provider include having the java class file. Also, for a channel that will use the iPlanet Portal Server Profile Service, a corresponding .xml file would be needed.

For example, a quotation provider is added as follows. In practice, also remember to use fully qualified class names.

Copying the Class File

1. Copy the quotation provider class file into the class path of the web server. The path begins with the root install directory (for this example, the install root directory was /opt).

   In this case, the sample quotation provider is part of the Java package com.iplanet.portalserver.providers.quotations. Any sample provider included with the product must be user compiled. Upon compiling the provider, the class file would automatically be put into the class path of the web server. Therefore, for this example, treat this class file as if it came from an external source. The file is copied to:

   ```
   /opt/SUNWips/lib/com/iplanet/portalserver/providers/quotations
   ```

   To do this, the following commands are used:

```
# mkdir -p
/opt/SUNWips/lib/com/iplanet/portalserver/providers/quotations

# cd /opt/SUNWips/lib/com/iplanet/portalserver/providers/quotations

# cp /opt/SUNWips/sample/desktop/classes/com/iplanet/portalserver/\
providers/quotations

# cp QuotationProvider.class
```

2. Import the provider's xml file using ipsadmin as follows:

```
# cd /opt/SUNWips/sample/desktop/xml

# /opt/SUNWips/bin/ipsadmin -import iwtQuotationProvider.xml
```

Adding the Channel to the Available Channels List

1. Log in to the admin console.
2. Click the Manage Domains link and select the default domain (for this example, sun.com).
3. Expand the Applications link and select Desktop. The Available and Selected Providers list windows will appear as shown in Figure 2-8 on page 56.
4. Type iwtQuotationProvider in the Channel Name text box. For the Class Name text box, type:

```
com.iplanet.portalserver.providers.quotations.QuotationProvider
```

5. Click the Submit button at the bottom of this page to update the Profile Server.

Adding the Channel to a Desktop

1. Log in to the desktop as a user. Follow authentication instructions if a new user.
2. Select the Content link and add the listed Quotations channel to the desktop. The quotations channel information will be displayed.

Configuring an Available Channel

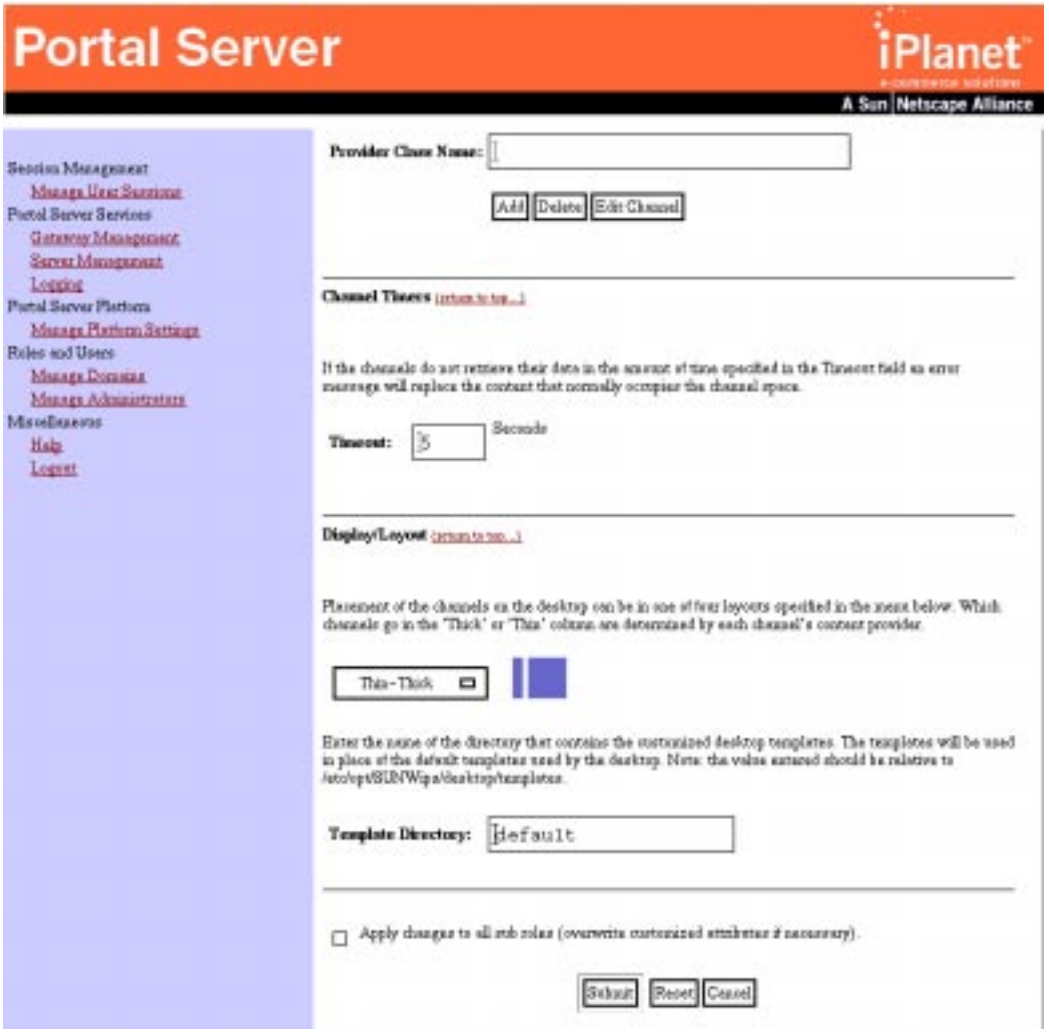

Figure 3-1 Specifying Column and Row Layout for the Desktop

For any selected channel, attributes can be configured to restrict or allow users control over how the channel is displayed. For example, attributes can include, but are not limited to:

- Column layout
- Additional channel display attributes
  - position and size within defined column layout
  - inclusion or omission of help
  - use of a border

Specifying Column Layout

1. Locate the display layout attribute on the Desktop profile page under Applications, as shown in Figure 3-1 on page 76.
2. Select either thin-thick, thick-thin, thin-thick-thin, or thin-thin-thin layouts. The available channels will be displayed as follows.
   - for thin-thick, or thick-thin layouts, channels are displayed in the order of the selected provider list. Channel data is filled from the leftmost column with the first channel representing the first provider and so forth.
   - for the thin-thick-thin layout, thin channels are populated in the leftmost window and thick layouts are located in the center window.
   - for the thin-thin-thin layout, channels are displayed in the leftmost window only.

Additional Channel Display Attributes

From the Domain>Applications>Desktop link, the desired channel can be selected from the Available Channels List window to display its attributes. For example, a channel border can be included or omitted. In addition, other channel display attributes can be set as shown in Figure 3-2 on page 78. For example, if the channel is not to be removed, the removable box will be unchecked. If the channel is to include a Help button, the Help attribute will be checked, and so forth.

Figure 3-2 Channel Display Attributes

Setting Desktop Colors and Content

The colors for the desktop can be modified by editing the desktop templates found in the directory /etc/opt/SUNWips/desktop. The default directory contains the templates that all users get by default. To create a “new” desktop for users copy the default directory to a new location. Modify the new templates as desired (using HTML commands to change colors). In the console, under the desktop profile, select the Display/Layout option and enter the new directory name in the Template Directory field.

NOTE Admin Console colors are located under the /public_html folder off of the installation path. There are a series of style sheets (denoted with a .css file extension) that represent various components of the admin console display. For example, navigation controls can have a different color specified in the nav.....css file. The prerequisite for changing colors on the admin console is familiarity with HTML commands and syntax.

Specifying a Custom Name and Logo for the Portal Home Page

The portal home page includes a default name for the portal page and a GIF file that displays the default logo. To customize these elements of the desktop, use the directory path:

<install path>/SUNWips/public_html/images

Within that directory are the file names representing the Product Logo and Product Name. The image file specified for the Product Logo (e.g., productLogot.gif) can be changed to the name for a loaded custom logo image file. The image file representing the Product Name (e.g., productName.gif) can also be modified to the product name for the site owner.

NOTE The logo and name images are used by more than just the desktop. These images are also referenced by the admin console, the applications, and the login templates. To create a new image for just the desktop, create a new image entry and change the templates to point to this new file.

Introducing The Channel Wizard

The Channel Wizard is an administrative module that assists an administrator with creating and configuring channels for the iPlanet Portal Server desktop. To start the Channel Wizard, use the administrative console to navigate to the profile of the domain, role, or user for which the channel is to be added. This is accomplished using the Manage Domains link on the iPlanet Portal Server console menu bar. In the profile menu, the Channel Wizard is identified by a link called Desktop Channel Wizard.

Creating a channel consists of the following steps:

1. Select a name and description for the new channel.
2. Choose the type of channel to create (i.e., URL scraper or Rich Site Summary).
3. Type the title to be displayed by the desktop.
4. Type the URL of the site to fetch the content.

The first page of the Wizard prompts for the channel name, which Content Provider to use, and a description of the channel. The name of the channel may only contain letters and numbers. This name is used for naming purposes within the system and is only visible to the administrator.

The next page of the Wizard prompts for the channel attributes used to build the channel data. The two most important attributes are the Title and the URL. The title is the name that is displayed in the channel on desktop. The URL is the name of the site that contains the data to be rendered by the provider in the channel. Clicking Finish on this page causes the Channel Wizard to create the channel and display a completion message.

Once a channel is created using the Channel Wizard, it is managed using the Desktop administrative module, just as with other channels. For example, if the administrator wants to have the new channel be one of the channels that are selected by default for all new users, the channel would first be created using the Channel Wizard and then it would be added to the selected channel list using the Desktop module.

Chapter 4

Configuring Membership

Overview

Previous versions of the iPlanet Portal Server supplied only a proxy model for authentication. The proxy model integrates well with existing corporate security schemes where authentication databases are independent of the Portal Server. In the iPlanet Portal Server, there are client interfaces to many standard authentication types: UNIX, RADIUS, SafeWord, LDAP, SecurID, NT, etc.

This version offers an additional method which does not rely on a customer authentication database–Membership Authentication. When the iPlanet Portal Server is configured for a consumer audience, the administrator may want them to self-register onto the portal on their first visit. This allows the Portal Server to act as both client and server, instead of accessing an independent authentication database (e.g.: UNIX, RADIUS, SafeWord, LDAP, SecurID, NT, etc.)

The iPlanet Membership Authentication procedure is similar to the my.yahoo.com, my.netscape.com or mysun.sun.com registration procedures. The *new user* creates an account and personalizes it without the aid of an administrator. Once the new user has created their account, they access it as a *registered user* with their chosen user name and password, as well as viewer interface, saved on the iPlanet user profile database as authorization data and user preferences.

The administrator may configure and/or customize this module in three ways:

- Look and feel: what is displayed on the new user's screen
- Content: what data is requested from the new user
- Function: how the new user interacts with the data requests.

Functionality

The goal of the Membership Module is to self-register new users into the Portal Service framework in a simple manner.

The Membership Module performs the following tasks:

- Requests specific information from the new user
- Requests password twice and performs simple confirmation check
- Places the new user in the administrator-configured default domain
- Creates new user profile
- Stores the user profile in the profile server

The Membership Module does not perform these tasks:

- Modify user profiles
- Allow the new user to re-register in order to change their profile
- Delete user profiles

User Types

Three groups interact with the Membership Module: new and registered users, and system administrators.

- New Users: A new user is someone creating a new user ID within the server. New users will need to enter a user name and a password. They can also enter any optional data set by the administrator.
- Registered Users: During subsequent sessions, when the user (now registered) logs in, they only need to enter their user name and password and then select the Login button. A successful login will send them to the desktop.
- System Administrators: The system administrator is responsible for the interface presented to the user, customizing the type and amount of data, as well as changing any functionality of the Membership Module.

Screens

Two screens are displayed by the Membership Module:

- Login Screen: This screen requests the user name and password from a registered user. If the user name and password are authenticated by the profile server, the registered user is allowed onto the portal. Users accessing the membership module for the first time should select the 'New User' button which will direct them to the Registration screen.
- Registration Screen: This screen requests data from the new user. The new user registers by completing this form which includes a password confirmation sequence and confirmation of a unique user name. If this is a user's first time, they need to select the new user button. No other input is needed. When their registration is accepted by the profile server, they are directed to the disclaimer page.

User Data

There are eleven data fields which are displayed in the Registration Screen. The new user is requested to fill out values for these fields as part of the registration process. The first three data fields are required in the default Membership Module configuration. The default configuration may be customized as described earlier in this chapter.

- Required
  - *User Name
  - *User Password
  - *Confirm User Password
- Optional
  - First Name
  - Last Name
  - Phone Number
  - E-mail Address
  - Street Address
  - City

- State
- Zip Code

Components

There are three components to Membership Authentication:

- XML Data definition which defines the membership profile: **iwtAuthMembership.xml**
- HTML Form to present the data file to new user for input: **register.html**
- Pluggable Authentication API Properties file: **Membership.properties**

There is a one-to-one relationship between the XML file, the HTML form and the Auth properties file. Each attribute listed in the Auth properties file corresponds to one input element in the HTML form, which corresponds to one attribute in the XML file. There is a one-to-one mapping between the properties file and the HTML file. The attributes listed in the properties file is a subset of the attributes in the XML file.

Customization

The default data and interface shipped with the Membership Authentication Module is generic so as to fit into any domain.You may want to configure it to reflect your corporate branding, special data and information specific to your product. There are three ways of customizing the Membership Module:

- Look and feel
- Content
- Function

The administrator may customize the Membership Module as long as:

- The one-to-one relationship of the three files (XML, HTML, Auth Properties) is maintained.
- The elements required by the Membership Module are retained (see requirements section below).

CAUTION Be careful when you make changes to one of these files, you must also change the other two files, so as to reflect the changes across all three files.

Look and Feel

To customize the look and feel of the user registration page, the administrator may modify the default HTML files shipped with the iPlanet Portal Server. The default files are membership.html (the login screen), register.html (the new user registration screen), and 12 HTML files used for error screens. The error screens are listed in Memebershp.properties.

Change these files to create a look and feel which follows your corporate branding. Everything is configurable, the gifs, colors, text and fonts, and the layout of the data fields. The default logos are installed in: `<installdir>/SUNWips/public_html/images`.

NOTE The images used by the Membership Module are also used in other parts of the product

Content

To change which data is requested, which is required, and which is optional, requires, at a minimum, editing the Membership.properties. It may also be necessary to modify the HTML files and the xml definition.

All attributes used by the Membership module are defined in Membership.properties. To add a new field to the registration page, the attribute name must be added to the Membership.properties file, and to the register.html file. The name used in both files is the name defined in the iwtAuthMemberhip.xml file. For example, if the attribute to display was iwtAuthMembership-userAge, the entry in Membership properties would be:

```
ATTRIBUTE iwtAuthMemberhip-userAge
```

When a new attribute is added, it not only needs to be put in Membership.properties, but it also must go in register.html. Without this the user would never see the new field. The name used in the HTML file must match the name used in properties file.

To make this attribute a required entry field, the letters "REQ_" need to be prepended to the attribute name.

```
ATTRIBUTE REQ_iwtAuthMemberhip-userAge
```

To let the user know which attributes are required and which are not, register.html defines the entries in bold text and with an '*'. While this is not a requirement, it is recommended. It would be impossible for a user to know which fields are required and which are not. Any method for indicating the required fields is allowed, it is not restricted to those used by the default module.

If the data definition supplied with iwtAuthMembership does not meet your needs, it can be altered by adding and removing attributes as needed. Alternatively, a new XML definition can be created and substituted for the default. If this is done Membership.properties, and register.html will need to be updated to reflect the new attribute names. Also in register.html is a hidden field which contains the name of the profile to store the user data. This must be the name of the xml definition you substituted. If a new XML definition issued with the default module, a few required attributes must be present:

```
password
```

```
passwordLength
```

```
userName
```

Function

To allow you to customize the behavior of the Membership Module itself and create your own self-registration module, the code for the Membership Module is shipped with iPlanet Portal Server. This allows you to write a module that, for example, performs tighter password checking, cross-references data-fields or allows multiple screen authentication.

Membership Module Requirements

Certain elements required by the Membership Module must be retained. These elements are specified below. They are necessary for the default Membership Module to work properly.

- Required Input
  - Required registration fields are indicated by prepending **REQ_** to the attribute name in the HTML file.
- Registration Page Hidden Fields
  - Name of the profile used to store the user data.
  - Attribute name that stores the password minimum length.
  - User name and password.
- Processing
  - A button on the Login page to login to the server.
  - A button on the Login page to redirect to the Registration page.
  - A button on the Registration page to submit the data.
- Error Messages
  - To indicate that the user profile is not found.
  - To indicate that the user name is not found.
  - To indicate that the user password is not found.
  - To indicate that the user has entered the wrong password.
  - To indicate that the selected user name is not unique.
  - To indicate that the user password is not confirmed.
  - To indicate that a required field is empty when form is submitted.
  - To indicate that the user name and password are identical.
  - To indicate that the password and confirm password values are not identical.
  - To indicate a configuration error.
  - To indicate a profile exception within the server.
  - To indicate that the password is invalid.

Chapter 5

Configuring Policy

Overview

Identification (Who are you?) and *Authentication* (How do I know you are who you say you are?) are two of the three components in the iPlanet Portal Server computing environment.

The third component, *Policy*, (What rights do you have? Do you belong here?) is described in this chapter. Access to approved system resources on the iPlanet Portal Server is controlled by looking up the value of privileges that delineate specific rights and permissions, based on the profile attached to the user's domain, role, or user name.

A subset of privilege values defines the policy attached to the profile for domains, roles, and users. The policy is implemented by interpreting the privilege values.

Privileges are of two types: boolean and list. Boolean privileges have a value of either true or false. List privileges have an Allow list and a Deny list. A Deny list has precedence over an Allow list. The wildcard character "`*`" in an Allow or Deny list has the meaning of all.

For example, a User URL Access privilege of "`*`" in the Allow list and "`http://company1.com`" in the Deny list enables access to all URLs that do not contain `company1.com` in the host portion of the URL.

You configure these values in the Policy page of the Administration Console, which lists Policies of iPlanet Portal Server.

Configuring Policy

This section describes how to configure policy at the domain, role, and user level.

When configuring policy at the domain level, all roles and users that are children of the domain inherit the policy unless explicitly overridden. When configuring policy at the role level, all subroles, and users of the role and subroles, inherit the policy unless explicitly overridden. Configuring policy at the user level applies only to that specific user.

To Configure Policy at the Domain, Role, and User Levels

1. From the Admin Console, click the Manage Domains link.
2. Click the Domain, or Domain > Roles, or Domain > Roles > Users link, depending on the level of the role tree for which the policy is to be configured.
3. Click the Policy link under Profiles.
4. Modify the appropriate policy.

   In general, privileges are allowed or denied by clicking a checkbox, or by typing entries in the Allow and Deny lists.

   See “Policy Details” for a description of the attributes for each policy.
5. Click the Submit button at the bottom of this page.

   The profile update message is displayed.
6. Click the Continue button to return to the previous page.

Policy Details

The policies that can be configured include:

- Applications
- Desktop
- Logging
- NetFile
- Netlet
- Platform
- Session

- S/Key Generation
- User
- Miscellaneous

Using Lists and Checkboxes

The Policy screen uses two methods to set privileges:

- Checkboxes – A privilege is enabled when the checkbox is selected, and disabled when unselected.
- Lists – Allow and Deny lists provide a means to grant or deny access to resources. A Deny list has precedence over an Allow list. The wildcard character "*" in an Allow or Deny list has the meaning of all.

Applications Policy

Every iPlanet Portal Server application has a "can this user execute" privilege defined in its profile. When a user starts an application, the application makes a call to the Policy API to verify if this user can execute the application. The following applications have this execute privilege; use the appropriate checkboxes to allow or deny access to these applications:

- NetMail
- NetFile
- Desktop
- Netlet

Each application has application-specific attributes. See "Desktop Policy" on page 91, "NetFile Policy" on page 92, and "Netlet Policy" on page 93 for more information.

Privileges on these applications are enforced by the applications themselves (not the iPlanet Portal Server gateway).

Desktop Policy

For each channel that the user has available, use the appropriate checkboxes to allow or deny these capabilities:

- Minimizable: The user can minimize the window in which the channel is running.
- Detachable: The user can detach the window in which the application is running.
- Help: Help is available or not to the user for the application.
- Editable: If the channel is editable, the value of this attribute will allow or deny the user's ability to edit this channel.
- Removable: The user can or cannot remove the application from the desktop.
- Border: The user can or cannot change the border around the application window.

Logging Policy

Use the checkbox to allow or deny Domain Administrators the capability to view log files in their domains. If set to false (unchecked), the Domain Administrator cannot view any logs in the system. If set to true (checked), the Domain Administrator can view log records that are only in that domain.

Only Super Administrators can delete logs and log records.

In general, configure this policy only at the Admin role level to ensure proper security of the iPlanet Portal Server environment.

NetFile Policy

Use the appropriate checkboxes to allow or deny privilege to perform the following operations from the NetFile application:

- Delete Files on Remote Systems
- Change User ID
- Change Machine Domain

Use the Allow and Deny lists to enter host names to which the NetFile application allows and denies access.

Netlet Policy

The Netlet policy defines three levels of policy checking for users:

- DNS domain level – Configurable only by the Super Administrator. This privilege ensures that the Netlet target host is within the DNS domain of the user. For example, if the Allow list contains "`*.sun.com`" then only Netlet targets in the `sun.com` DNS domain can be executed by the user.
- Netlet target host – Enables Super Administrators and Domain Administrators to restrict access to certain hosts. For example, an administrator can set up the Allow list with five hosts that the user is allowed to telnet to, or use only the Deny list and restrict access to a few confidential servers.
- Netlet rule name – Each netlet rule is defined by a name. Administrators can allow or deny users based on the Netlet rule names.

Use the appropriate checkboxes to allow or deny privilege to domains, hosts, and rules.

See Chapter 7, "Configuring The Netlet" for more information.

Platform Policy

Use the Allow and Deny lists to enter servers which can or cannot be restarted.

By default, the Allow list is empty, which means this privilege is not enabled. Enter servers that you want to be able to restart, or "`*`" to enable restart of all servers.

There is no platform privilege to allow or deny restarting of iPlanet Portal Server gateway servers. Only Super Administrators can restart a gateway server.

In general, configure this policy only at the Admin role level to ensure proper security of the iPlanet Portal Server environment. Do not change the restart servers permission at the domain level, as this would enable all roles and users in that domain to restart the iPlanet Portal servers.

Session Policy

Use the checkbox to allow or deny applications using the Session API to create session listeners to all session platform notifications. In general, configure this policy only at the Admin role level to ensure proper security of the iPlanet Portal Server environment.

Super Administrators and Domain Administrators can view iPlanet Portal Server sessions through the Manage Sessions page in the Administration Console. Administrators can also delete a user session from this page.

Get Valid Sessions Privilege

This privilege allows or denies Super Administrators or Domain Administrators the capability to view user sessions. The administrator is able to view all users' sessions whose domains are listed in the Allow list, and is denied viewing users' sessions whose domains are listed in the Deny list.

Delete Sessions Privilege

The ability to delete sessions is defined by these lists. Only sessions from the domains in the Allow list and not in the Deny list can be deleted by the administrator in this role.

S/Key Generation Policy

Use this checkbox to allow or deny privilege for those in the role to generate S/Key pass phrases on behalf of others, including themselves. Great care should be exercised in granting this privilege since a user with this privilege could invalidate another user's pass phrase by creating a new list. Therefore, the granting of this privilege should be limited to Domain Administrators and above.

User Policy

The Access list shows the URLS that can be accessed by a user. The Deny list shows the URLs to which the user is denied access. The Deny list has precedence over Allow list. The wildcard character '*' in the Allow or Deny list has the meaning of all. The URL entered must be a prefix match starting with either "`http://`" or "`https://`."

For example, entering "`http://*.company1.com`" in the Deny list and "`*`" in the Allow list enables a user to access all URLs except those in the `company1.com` domain. Entering "`http://myhost.company1.com/privatedoc.html`" in the Deny list and "`http://*.mycompany.com`" in the Allow list enables the user to access all URLs in the `mycompany.com` domain except the HTML page in the Deny list.

The default for this privilege is to enable access to all URLs.

User policy for URL access is enforced at the iPlanet Portal Server gateway.

Miscellaneous

Policy-related privileges for applications developed using the iPlanet Portal Server API are listed here. See the *iPlanet Portal Server 3.0 Programmer's Reference Guide* for more information.

ADMIN and USER Permissions

Use the check boxes in the ADMIN and USER Permissions section of the Policy page to modify read and write permissions of the policy, that is, to grant or take away the ability to view or change a policy. The default for Admin read and write permissions is both enabled. The default for User read and write permissions is read enabled and write disabled.

The Super Administrator has read and write permissions to all attributes in the platform.

Chapter 6

Managing Authentication

This chapter explains how to setup and administer authentication for your iPS portal, and how to customize authentication modules, if needed. Topics covered include:

- An overview of iPlanet Portal Server authentication methods
- Managing authentication attributes
- How to set up authentication for users
- How to customize authentication modules on your portal

Overview of iPlanet Portal Server Authentication

This section briefly describes how authentication works on your portal.

iPlanet Portal Server uses authentication to verify the identity of users trying to access your portal. You primarily use the Administration Console and iPlanet Portal Server desktop to set up authentication.

NOTE The iPlanet Portal Server product includes several authentication modules and a public API that enables you to add more modules, if needed. See the *iPlanet Portal Server Programmer's Reference Guide* for more information.

Default Authentication Methods

When you install iPlanet Portal Server using a standard (not customized) iPlanet Portal Server installation, the following authentication modules are enabled on your portal:

- S/Key
- SecurID
- SafeWord
- UNIX/NIS
- Windows NT
- LDAP
- Personal Digital Certificates (PDCs)
- RADIUS
- Membership

The iPlanet Portal Server product includes only the client modules for RADIUS, SafeWord, SecurID (ACE/client, NT primary domain controller), and LDAP. You must obtain the server modules for these authentication types from a third-party supplier to have the full implementation.

Common Authentication Tasks

Some common tasks involving customizing authentication include:

- Setting up modules that require site-specific information (for example, an LDAP server name and DN to start search, RADIUS server and shared secret)
- Limiting authentication modules, by disabling modules not needed in your environment
- Customizing prompts and screens for authentication (and failure messages).
- Customizing the behavior subsequent to authentication to automatically launch specific applications or Web sites

Files Used for Authentication

You might need to view the iPS configuration files directly, for example, to verify a specific setting. Moreover, you need to directly edit configuration files on the iPS server for some authentication settings and customization. Table 6-1 describes the files that iPS authentication uses.

NOTE All paths and file names specified in this chapter assume a default installation in /opt. (Configuration files are always in /etc/opt). If you have changed the installation location, your paths will differ from those listed in this chapter.

Table 6-1 Files and directories related to authentication settings.

Files	Purpose
`/etc/opt/SUNWips/platform.conf`	Lists the authentication process to start with iPlanet Portal Server, on the lines starting with ips.daemons and the subsequent lines containing port settings for each of the listed specified process.
`/etc/opt/SUNWips/auth/default/*.html` and `/etc/opt/SUNWips/auth/default/*.properties`	Contain the base pages displayed during the authentication process. Review this chapter before changing these files.

How the Users Experience the Authentication Process

When end users first access the login URL, they may be presented with an HTML authentication page, depending on the domain of the end user and whether the administrator has configured the system to prompt for authentication. If the iPlanet Portal Server server is configured with multiple authentication modules, end users are presented with a menu of authentication types and the kind of

information requested depends on the option they choose. If only one authentication module is configured and some form of authentication entry is required, the end user bypasses the authentication menu and sees only the specific authentication page.

If user-based authentication has been configured for the domain, the user is prompted for a userID first. Then the authentication types enabled for that user are presented in a menu.

If end users fail authentication, they are directed to an authentication-failed page. This page does not indicate to the end user the specific reason that authentication failed. After a successful authentication, end users are redirected to the iPlanet Portal Server Desktop.

NOTE Upon a failed Administration authentication attempt, a message describing the reason for the failure is sent to the authentication log.

Setting Up User Authentication for a Multiple Domain Portal

When configuring a multiple-domain portal, you must tell users how to authenticate to the correct domain. You can do this by either:

- Requiring users to type their domain names at the time of authentication
- Using a virtual host name for the gateway

Requiring the User to Type a Domain Name

Suppose you have two domains named `eng` and `corp`, and a gateway named `gateway.eng.sun.com`. Click Manage Domains, and then choose one of the domains. If you have added more gateways after initial installation, in the Authentication profile for that domain, you can add `gateway.eng.sun.com/corp` to the Domain URLs attribute for the `corp`. The default domain URL, `/corp`, should already be there. Do the same for the `eng` domain.

To connect to iPlanet Portal Server, users in the `eng` domain authenticate by typing the URL `https://gateway.eng.sun.com/eng`, and users in the `corp` domain type `https://gateway.eng.sun.com/corp`.

You can use multiple strings for each domain, but at least one must match what the user enters as the URL.

Using a Virtual Host Name for the Gateway

You can use a virtual host name for the gateway, or have multiple DNS names for one gateway interface. For example, assume that your gateway has both the DNS names `gateway.eng.sun.com` and `gateway.corp.sun.com`. Users from the `eng` domain would authenticate by typing `https://gateway.eng.sun.com`, and users from the `corp` domain would authenticate by typing `https://gateway.corp.sun.com`.

To configure your iPlanet Portal Server installation to allow this, click Manage Domains link at the left from, select the desired domain, expand the Authentication link and modify the Domain URL attribute in each domain. The attribute for the named domain will then have the string `hostname.domainname` and the attribute for the named domain would have the string `gatewayname.domainname`.

Managing Authentication Attributes

You can define authentication attributes on a platform-wide and on a domain-specific basis using the Administration Console.

To Define Platform-Wide Authentication Attributes

Use the Administration Console to define platform-wide authentication attributes. You must be the Super Administrator to define platform-wide attributes.

1. Click Manage Platform Settings at the left of the Administration Console screen.
2. Click the Authentication link on the right of the Portal Server Platform.
3. Click the Show Advanced Options on the Component Profile: Auth screen.

   From this page, you can set values for the various attributes that apply to the authentication scheme for the entire portal.

To Define Domain-Specific Authentication Attributes

Use the Administration Console to define domain-specific authentication attributes. You can be a delegated administrator for the particular domain or Super Administrator to perform the next steps.

1. Click Manage Domains at the left of the Administration Console.
2. Click the link for the domain to be administered, as displayed on the Portal Server Domains page.
3. Click the Authentication link on the Domain, Role & User Profiles page and configure attributes that pertain to the domain.
4. Press Submit to activate your changes, and then press Continue to return to the Authentication profile page.
5. Click the Back to Overview link to return to the Domain, Role & User profile page.
6. Expand the Authentication tree to display links for each supported authentication type.
7. Click the link for the authentication type that you want to configure.

   You display the profile page for the particular authentication type.
8. Define the attributes for the authentication method as needed for your portal.

Setting Up Authentication for Users

This section explains how to set up the available authentication types for users. Topics covered include:

- Configuring authentication for administrators
- Generating S/Key passwords for users
- Configuring LDAP authentication for users
- Configuring PDCs and devices
- Configuring Windows NT authentication for users
- Configuring SafeWord authentication for users

- Configuring SecurID authentication for users
- Configuring RADIUS authentication for users
- Configuring UNIX/NIS or Membership authentication for users

Configuring Authentication for Administrators

To configure the authentication type for an administrator, follow these steps:

1. Select Manage Administrators from the Administration Console main menu, under Roles and Users.
2. Click the adminRole for the domain you want to configure.

   For a delegated administrator, click Manage Domains from the left pane -> View Domain Administrator Roles, and then the appropriate Admin Role.
3. Click Authentication to view the Authentication profile.
4. Change the Admin Authenticator attribute to reflect the authentication type for that administrator
5. Press Submit to activate the changes.

Configuring S/Key Authentication

S/Key is the one-time password system developed by Bellcore. S/Key users must be valid UNIX/NIS users known to the iPlanet Portal Server server system.

Although each iPlanet Portal Server Server can support multiple domains, S/Key's reliance on the UNIX/NIS authentication restricts all domains to the single set of UNIX/NIS userIds the iPlanet Portal Server Server system can authenticate as valid.

When the user logs in using S/Key as an authentication type, the initial S/Key authentication screen prompts for the user's Unique UserID (UUID) and Personal Identification Number (PIN). If these are validated, then the user is prompted for the next expected one-time password. (This password is actually a six-word passphrase).

Only one of the attributes for S/Key is worth mentioning: S/Key Maximum Passphrases To Generate. Since each time a user logs in, S/Key requests a different passphrase from a list of passphrases specifically generated for that user, S/Key is set up to create such a list upon demand by a user or a system administrator. While maximum number of passphrases that can be set is 400, most system administrators find it more convenient to use the default of 100 when producing a passphrase list.

A system administrator must remember to generate a list of S/Key passwords for a user before that user attempts remote access for the first time.

S/Key Password Generation

Anyone with a valid UNIX userID on the iPS server can generate S/Key passwords for themselves to use with iPlanet Portal Server. Those with “S/Key Generation” authority (usually administrators) can generate new S/Key passwords for others to use when authenticating themselves to the iPlanet Portal Server desktop.

After you have set the S/Key generation privilege for the AdminRole, you can go on to generate actual keys for the users. Or you can show users how to generate their own S/Key. However, point out to your users that they must be careful to generate new password lists before logging out of a session, as stated in the Note under step 7 of "To Have Users Generate Their Own S/Key" on page 106.

To Enable S/Key Generation

NOTE You must be Super Administrator to perform this procedure.

1. Access the Administration Console and click Manage Domains.
2. Click the name of the Domain you want to administer, and then click View Domain Administrator Roles.
3. Click the name of the administrator Role, for example, AdminRole for the Super Administrator of the default domain.
4. Click Policy to display the Policy Module.
5. Click S/Key Generation to move to the S/Key Generation privilege.
6. Ensure that the Generate S/Keys box is checked to enable this privilege.
7. Press the Submit button to submit the change to the Profile Server. Click the Continue button when prompted that the change has been made.

To Generate S/Keys for Users

1. Log in as the Super Administrator or the delegated Administrator to the iPlanet Portal Server desktop.
2. Edit the URL by changing the ending `/DesktopServlet` to `/SKeyGeneration`.

   The Generate S/KEY Passwords Login screen is displayed, as shown in Figure 6-1.

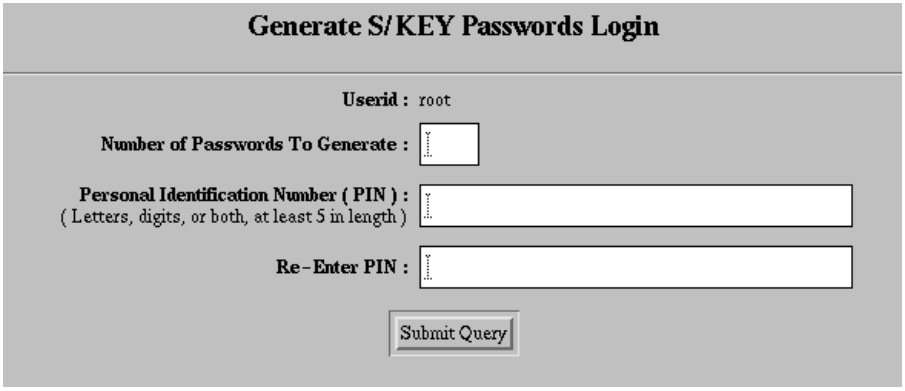

Figure 6-1 Generate S/Key Login Screen

3. Specify the UNIX userID, number of S/Key passwords to generate, and the PIN to use for that particular user.
4. Press Submit Query.

   The new one-time passwords generated for the user are displayed.
5. Print the resulting list so that you can provide it to the user.
6. Return to the iPlanet Portal Server desktop by changing the ending of the URL from `/SKeyGeneration` to `/DesktopServlet`.
7. Repeat the steps above for each user to receive S/Key passwords.

   When you generate the passwords on behalf of end users, give them the unique userID (UUID) and list of passwords and, separately, give them the PIN that you used. For security, the end users should keep this PIN separate from the UUID and the list of passwords.

To Have Users Generate Their Own S/Key

End users can generate their own set of S/Key passwords. Give the users the following steps:

1. Start a Web browser, and enter the URL to display the iPlanet Portal Server system login menu.
2. Select UNIX authentication and type your UNIX userID (UUID) and password.

   The iPlanet Portal Server Desktop is displayed.
3. Edit the URL by changing the ending `/DesktopServlet` to `/SKeyGeneration`.

   The Generate S/KEY Passwords Login screen is displayed with your UNIX userID printed at the top.
4. Specify the number of S/Key passwords to generate.
5. Type a PIN of five alphanumeric characters or more, press Return, and then retype the PIN.
6. Press Submit Query.

   Your new one-time passwords appear in the browser. You can print them out using the browser's print feature.

NOTE If you use the last password and log out before generating a new list of passwords, then either your iPlanet Portal Server administrator has to generate a new list of S/Keys for you, or you have to repeat S/Key generation as described, beginning in Step 1.

Generating more S/Key passwords supersedes the previously generated list. Also, the UUID for that user will change.

---

7. Return to the iPlanet Portal Server Desktop by changing the ending of the URL from `/SKeyGeneration` to `/DesktopServlet`.
8. Log out of the Desktop, and then return to the desktop login.
9. Authenticate yourself by clicking S/Key Authentication.

   The S/Key login screen appears, as shown in Figure 6-2:

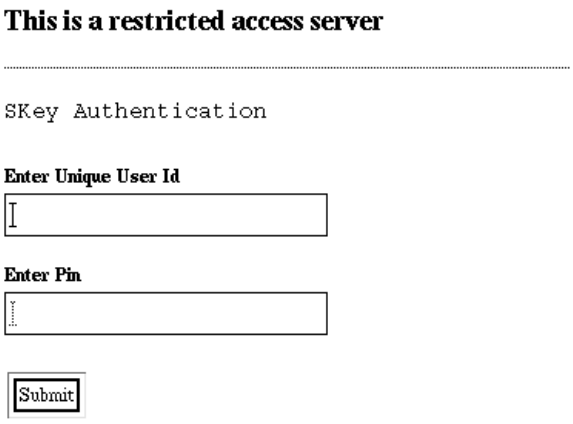

Figure 6-2 S/Key Login Screen

10. Type the Unique User ID (UUID) from the list in the appropriate box, and then press Return.
11. Type the PIN.
12. Click Submit

    The S/Key Authentication screen is displayed.

Figure 6-3 S/Key Authentication Screen

13. Type the list of one time passwords for the sequence requested and press Submit.

If authentication is successful, the iPlanet Portal Server desktop is displayed.

Reinstalling the iPlanet Portal Server software deletes all S/Key password information for all users.

Authentication Using the LDAP Server

iPlanet Portal Server supports both the LDAP v2 and LDAP v3 servers.

It is important to distinguish between the user authenticating with the iPlanet Portal Server LDAP authentication module and the LDAP authentication module itself when authenticating to the LDAP directory. The iPlanet Portal Server user is simply sending a userID and password to the gateway, which then binds to the LDAP directory and verifies the user's userID and password in the directory. If the userID and password are in the directory, the user is allowed access and is set up with a valid iPlanet Portal Server session.

In order to access the Directory Service, a Directory Service client needs to first authenticate itself to the service. That is, the client needs to tell the Directory Service who is going to be accessing the data, so that the server can decide what the client is allowed to see and do. in iPlanet Portal Server's case, the client is the LDAP authentication module. There are two options for authenticating the iPlanet Portal Server authentication module to the Directory Service:

1. **Anonymous authentication.** This method means that the iPlanet Portal Server authentication module does not need to authenticate to the Directory Service before checking whether the Directory Service has a valid userID and user password in the directory. By not setting the following attributes, anonymous authentication will be used:

   ```
   iwtAuthLdap-bindDN
   iwtAuthLdap-bindPasswd
   ```

2. **Password-based (simple) authentication**. This method requires the iPlanet Portal Server authentication module to bind to the directory with its distinguished name (DN) and user password before validating the user. By setting the following attributes, iPlanet Portal Server will bind to the directory before validating the user:

   ```
   iwtAuthLdap-bindDN o=sun.com,ou=engineering,uid=admin
   iwtAuthLdap-bindPasswd mypassword
   ```

Security

By default, the information sent from the iPlanet Portal Server authentication module to the Directory Service is in clear text. This means the data could be read by someone listening on the network. If this is a concern, you may choose to use SSL between the iPlanet Portal Server authentication module and the Directory Service. Your Directory Service must be configured to use SSL in order for this to work. Then you need to set the following attribute to true (the default is false):

```
iwtAuthLdap-sslEnabled = true
```

Which LDAP Server to Use?

The *iwtAuthLdap-server* attribute specifies the LDAP server which iPlanet Portal Server uses to validate your users. The format is *server:port*, where *:port* is necessary only if you are not using the default LDAP port of 389. For example, if your server name is *ldserver.eng.sun.com* and it listens on port 876, then the attribute `iwtAuthLdap-server` should be set to *ldserver.eng.sun.com:876*. If the Directory Service listens on 389, it should be set to *ldserver.eng.sun.com*.

If you have a multiple domain configuration, you may configure a different LDAP server for each domain. Please refer to the section Authentication in Multiple Domains for more information.

Configuring LDAP Authentication

To configure LDAP authentication:

1. Click Manage Domains from the Administration Console menu.
2. Click the link for the domain for which you want to configure LDAP authentication.
3. Expand the Authentication tree, and then click Ldap.
4. Configure the following attributes to specify the necessary properties for LDAP Authentication.

   For example, if you want to use *anonymous bind* and *one level search* from `cn=Eng,ou=Engineering,o=sun.com`, then provide the following information:

LDAP authentication server	`myserver.eng`
DN to start search	`cn=Eng,ou=Engineering,o=sun.com`
scope for the userId search	`ONELEVEL`

Or, if you want to use *admin bind* and *subtree search* from `o=sun.com`, with *SSL enabled*, then provide the following information:

LDAP authentication server	`myserver.eng`
DN to start search	`o=sun.com`
DN for root user bind	`uid=admin,ou=Engineering,o=sun.com`
Password for root user bind	`12345`
scope for the userId search	`SUBTREE`
Enable SSL to LDAP server	Checked

Configuring Personal Digital Certificates (PDCs) and Encoded Devices Authentication

iPlanet Portal Server lets users authenticate using PDCs and encoded devices such as smart cards and Java Cards. The encoded devices carry an electronic equivalent of a PDC stored on the card. If a user logs in using one of these mechanisms, no login screen appears and no authentication screen appears.

The authentication process for PDCs involves several steps:

1. At a browser, the user types a connect request:

`http://my.ips.com`

The response to this request depends on whether the gateway to my.ips.com has been configured to accept certificates.

2. When a gateway is configured to accept certificates, it will accept only logins with certificates, not any other kind of login. If it has not been configured to accept certificates and no other authentication modules are enabled, the user's connection request is denied.

To configure the PDC and encoded devices with the gateway, do the following:

1. Go to the Admin Console.
2. Select Gateway Management from the menu at the left.
3. Select the Manage Gateway Profile link
4. Click in the text box under the PDC Enabled field and enter the fully qualified name that is configured for the PDC and any used encoded devices.
5. Click the Add button to add this name to the list window.

   When configured, the gateway asks the user for their certificate and the connect process continues.
6. The user sees a Select Certificate dialog box and types in a password.
7. The gateway looks at the certificate, checks that the certificate was issued by a known Certificate Authority, has not expired, and has not been tampered with. If the certificate is deemed valid, the gateway lets the user proceed to the next step in the authentication process.
8. The gateway contacts the PDC authentication module in the server and passes it the certificate.

   The server checks how two attributes, "check CRL" and "check certstore," have been set.

   If "check CRL" has been set to yes, the server checks to see if the certificate matches an existing certificate revocation list inside the LDAP server. If a match exists, the user is allowed to proceed; if not, the user is denied access.

   If "check certstore" has been set to yes, the server attempts to match the certificate received from the client with an existing certificate inside the LDAP server. If a match exists, the user is allowed to proceed; if not, the user is denied access.

.

NOTE Certificate management tools that manage the addition and deletion of certificates in LDAP are to be provided by the customer or by vendors of certificates. Sun does not provide these tools.

Managing PDC Attributes

The Certificate authentication module attributes can be managed from within the platform.conf file. This file contains the attributes described in "PDC Attributes" on page 112.

Table 6-2 PDC Attributes

Attribute entry in platform.conf file	What it does
iwtAuthCert-chkCertInLDAP	Check user certificate to see if it is in LDAP. If certificate has been issued previously, it will be in the LDAP server. Initial value is false.
iwtAuthCert-chkCRL	Check user certificate against Certificate Revocation List in LDAP. Initial value is false.
iwtAuthCert-ldapFactory	Location of LDAP class library.
iwtAuthCert-ldapProviderUrl	URL of LDAP certificate server. Default value is ldap:/ /LDAP host:389.
iwtAuthCert-startSearchLoc	Name (DN) of node in LDAP where search for certificate should start.
iwtAuthCert-securityType	LDAP access authentication method: none = access to LDAP does not require a principal name or password simple= access to LDAP does require a principal name and password; these will be sent to LDAP in plain text. CRAM-MD5=access to LDAP does require a principal name and password; these will be sent to LDAP encrypted.
iwtAuthCert-principleUser	Principal user (usually system administrator) for the certificate LDAP server.
iwtAuthCert-principlePasswd	Principal user's password.
iwtAuthCert-useSSL	Use SSL to access the certificate LDAP server.
iwtAuthCert-userProfileMapper	Which field in Certification should be used to verify user profile information? (issuer | serial number | subject DN | Certificate)
iwtAuthCert-debug	Debugging flag. Default value is false.
iwtAuthCert-aliases	Name of field in Certification to match user profile; used by authentication daemon to map a name field to a user profile.

Configuring Windows NT Primary Domain Controller Authentication

Many enterprise customers have environments in which end users are required to be authenticated against a NT Primary Domain Controller. This type of authentication is specified from the admin console as follows.

1. Choose Manage Domains.
2. Click on the domain of interest.
3. Expand the Authentication link.
4. Click the NT profile in the Administration Console to see the application attributes for NT.

The iPlanet Portal Server NT Authentication module lets users authenticate the username and password they would normally use when accessing their NT desktops.

The following attributes are used by the iPlanet Portal Server authentication module to determine where to send the request to validate the user. By default, the user is prompted for username, password, and NT host. The NT domain where the host resides is taken from `iwtAuthNT-domain`.

The default properties file for the NT authentication module is in `/etc/opt/SUNWips/default/auth/NT.properties` and contains the following:

```
SCREEN

TIMEOUT 60

TEXT NT Authentication

TOKEN Host

TOKEN User Name

PASSWORD Password
```

The NT authentication module can be configured to prompt the user to enter userID, password, NT host, and NT domain. In this case, user entries are used instead of stored attributes.

In this case, the properties files should be modified to look like the contents of `/etc/opt/SUNWips/auth/(DOMAIN)/NT.properties`. Properties should be ordered as follows:

```
SCREEN

TIMEOUT 60
```

```
TEXT NT Authentication
TOKEN Host
TOKEN Domain
TOKEN User Name
PASSWORD Password
```

The properties file can be configured to prompt the user only for username and password. In this case, both the server name and domain name are taken from the attributes set in the Administration Console. The properties file should then be the following, in order:

```
SCREEN
TIMEOUT 60
TEXT NT Authentication
TOKEN User Name
PASSWORD Password
```

Configuring SafeWord Authentication

The iPlanet Portal Server Server SafeWord authentication client is implemented using Secure Computing's SafeWord remote client API. The SafeWord server does not have to reside on the iPlanet Portal Server Server.

The SafeWord authentication system uses hardware tokens, which are obtained from Secure Computing. When logging onto the iPlanet Portal Server Server using SafeWord authentication, you initially supply only your userid. Subsequently you must supply a response (generated by your SafeWord token) to the challenge issued by the SafeWord server.

Follow these steps:

1. Enter the URL to display the system login menu and select SafeWord authentication.
2. Enter your login information in the iPlanet Portal Server Authentication screen.

   You receive a "challenge" from the SafeWord authentication server.
3. Turn on your token and enter the Personal Identification Number (PIN).
4. Enter the challenge from Step 1 on your token.

5. Enter the response from your token in response to the challenge from the SafeWord authentication server.

The SafeWord token configuration has no known restrictions. The SafeWord token can be used over RADIUS when authenticating to a SafeWord RADIUS server. See the section "Configuring RADIUS Authentication" on page 117.”

Each iPlanet Portal Server Server can support multiple domains. Since each domain can have its own dedicated SafeWord server, the information needed to configure the SafeWord authentication helper is defined at the domain level. Information about all of the known SafeWord servers is sent to the iPlanet Portal Server Server SafeWord authentication helper during its configuration; to update the helper’s configuration, restart the iPlanet Portal Server Server. The SafeWord helper is described in "Starting Debugging Using the SafeWord Helper" on page 210.

Viewing or Changing SafeWord Attributes

To view or modify the SafeWord attributes, follow these steps:

1. Log in to the iPlanet Portal Server Administration Console.
2. In the left frame, click on the Manage Domains link. In the right frame, click on the domain of interest, then the SafeWord link from the expanded list of iPlanet Portal Server Authentication profiles.
3. You must change at least the SafeWord Server Hostname attribute (initially null) for SafeWord authentication to work in your installation. Enter the hostname of your SafeWord Server.
4. The SafeWord Server Identifier field is set by the SafeWord authentication module during helper configuration time.
5. Use the default SafeWord system values for Server’s Port (7842) and System name (STANDARD). If you have a simple SafeWord system installation, neither of these need changing.
6. Unless a problem cannot be solved using the steps described in the Debugging section, the SafeWord Logging Level can and should remain 0 (no logging).
7. Click the Submit button to update your changes in the Profile Server. The iPlanet Portal Server Server must be restarted for your changes to take effect in the SafeWord authentication module and helper.

Configuring SecurID Authentication

The iPlanet Portal Server Server SecurID authentication client is implemented using Security Dynamics' ACE/Client API. The ACE/Server is usually installed on a system other than the iPlanet Portal Server Server. The SecurID token (available from Security Dynamics) may also be used over RADIUS when authenticating to an ACE/Server RADIUS server.

iPlanet Portal Server may support multiple domains. Since each domain may have its own dedicated ACE/Server, the information needed to configure the SecurID authentication helper is defined at the domain level. Information about all of the known ACE/Servers is sent to the iPlanet Portal Server Server SecurID authentication helper during configuration. To update the helper's configuration, restart the iPlanet Portal Server server.

When logging into the iPlanet Portal Server server using SecurID authentication, you supply your userID and the concatenation of your PIN and your token's current value. You may receive other prompts if you enter the "next Token" or "new PIN" modes during your authentication session.

Viewing or Changing SecurID Attributes

To view or modify SecurID attributes, follow these steps:

1. Log into the Administration Console.
2. Click on the Manage Domains menu option at the left.
3. Click on the Authentication link. In the right frame, click on the domain of interest, then the SecurID link from the expanded list of iPlanet Portal Server Authentication profiles.
4. You may have to change the SecurID Server's Configuration Path (initially /opt/ace/data) for SecurID to work in your installation, especially, if your installation has multiple domains with SecureID authentication. Change this path to reflect where the domain's ACE/Server configuration file, sdconf.rec, is located.

   This path may not actually contain any configuration information, so it may remain the default /opt/ace/data path. However, if there are multiple ACE/Servers, discrete SecurID Server Configuration Paths must be specified. Additionally, the sdconf.rec files from the corresponding ACE/Server systems must be placed in those directories.
5. The SecureID user configuration path can usually remain as the default /opt/ace/prog even if your installation has multiple domains with SecureID authentication.

6. The default SecurID system values for “SecurID Server Identifier Name” may remain the default value (Server000), though this value can be changed to reflect the Server Identifier (Local).
7. Click the Submit button to update your changes.

Configuring RADIUS Authentication

The RADIUS module is a client implementation of Remote Authentication Dial In User Service (*RFC 2138, not including the accounting features of RFC 2139*).

RADIUS authentication uses a password assigned by the RADIUS server system to the workstation making an authentication request.

Each iPlanet Portal Server Server may support multiple domains. Since each domain may have its own dedicated RADIUS servers, the servers and shared secret are configured at the domain level.

The following RADIUS codes are supported:

- Access-Request
- Access-Accept
- Access-Reject
- Access-Challenge

Viewing or Changing RADIUS Attributes

To view or modify RADIUS attributes, follow these steps:

1. Log in to the iPlanet Portal Server Administration Console.
2. In the left frame, click on the Manage Domains link. In the right frame, click on the domain of interest, then the RADIUS link from the expanded list of iPlanet Portal Server Authentication profiles.
3. Change the RADIUS shared secret and the RADIUS Server 1 and Server 2 fields for RADIUS to work in your installation.

   Enter the shared secret (default is “nosecret”) through the Administration Console.

   Enter the hostname or IP address for both Server1 and Server2 (defaults are 127.0.0.1). If a Server2 is not present, clear the RADIUS Server2 field and leave it blank.

4. Change the RADIUS Server's Port value from 1645 to the actual port number, if it doesn't use the default value.
5. Click the Submit button to update your changes in the Profile Server. The iPlanet Portal Server Server must be restarted for your changes to take effect in the SafeWord authentication module and helper.

When logging into the iPlanet Portal Server Server using RADIUS authentication, supply your userID and password. You may subsequently need to supply more information in the form of responses to challenges, especially if you are using SafeWord or SecurID tokens over RADIUS.

Attributes for RADIUS authentication include the following:

- User-Name
- User-Password
- NAS-IP-Address
- NAS-Port
- Reply-Message
- State

"User-Name" and "User-Password" are the userID and password you used to login. NAS-IP-Address and NAS-Port refer to the Network Access Server's IP address and port used to access the network.

"Reply-Message" is the message the server sends in its reply to a RADIUS client's access request. In an Access-Accept, it's the success message; in an Access-Reject, it's the failure message; in an Access-Challenge, it is the dialog message (for example, when using a RADIUS-to-SafeWord RADIUS server, it would be the SafeWord challenge).

For RADIUS debugging issues, refer to "Debugging RADIUS" on page 213.

Configuring UNIX Authentication

Most iPlanet Portal Server system administrators already have UNIX userIDs and passwords associated with the Solaris systems they are running. A quick and easy way to become an authenticated user on a new iPlanet Portal Server installation is to use that UNIX userID and password. Once set up, of course, the system administrator may prefer to use a different form of authentication.

Although each iPlanet Portal Server Server may support multiple domains, UNIX authentication restricts all domains to the single set of UNIX/NIS userIDs the iPlanet Portal Server Server system can authenticate as valid.

The UNIX/NIS authentication module validates `userid-password` pairs. The system administrator can administer `userids` locally (through, for example, `admintool`) or through NIS.

If you are using a UNIX userID and password (local file, NIS, or both) for authentication, then you must make sure that the `passwd:` entry in the `/etc/nsswitch.conf` file on the iPlanet Portal Server server is set up correctly.

Customizing Authentication on Your Portal

This section explains how to tailor authentication to your portal's needs by customizing the authentication modules.

Editing the Properties Files

You can see the authentication screen properties for each authentication module in a properties file that can be edited from the command line. The properties files for the module are located in `/etc/opt/SUNWips/auth/default` on the iPlanet Portal Server server. For example, the UNIX authentication modules properties file is `/etc/opt/SUNWips/auth/default/UNIX.properties`.

Each authentication module has a `TIMEOUT` parameter that can be modified in the corresponding file:
`/etc/opt/SUNWips/auth/default/authentication_module.properties`.

This time-out specifies the number of seconds that the end users have to submit the screen before the time-out page displays. The default for each module is 60 seconds.

For example, if you want to make sure that the end users using a UNIX login have two minutes (120 seconds) to log in, change the TIMEOUT parameter in the `/etc/opt/SUNWips/auth/default/UNIX.properties` from 60 to 120.

The doUNIX helper (and helpers in general) also has a time-out attribute value that is separate from this TIMEOUT value. If they are of different values, the component (authentication module or helper) with the shorter time-out value will terminate the authmodule-helper session, and the authentication request fails. (For complete information on helpers, refer to "Authentication Helpers (daemons)," on page 123.)

Each HTML page that is sent for the authentication module has a keyword `SCREEN` followed by keyword TEXT, followed by any number of the keywords `TOKEN` and `PASSWORD`. Each screen might also contain an optional `TIMEOUT` keyword.

For example, the `UNIX.properties` file contains the following entries as shown in Code Example 6-1, with keyword definitions provided in "Properties File Keywords" on page 120.

Code Example 6-1 Sample `UNIX.properties` File

```
SCREEN
TIMEOUT 60
TEXT UNIX User Password Login
TOKEN Enter Your UserId
PASSWORD Enter Your Password
```

NOTE You cannot change the ordering of any of the tokens

Table 6-3 Properties File Keywords

Keyword	What it means
`TIMEOUT`	This keyword specifies the number of seconds the authentication module will wait before sending the user a login session time-out page.
`TEXT`	Each screen has one `TEXT` keyword. This is the text that is displayed at the top of the authentication page. It is typically used to describe the authentication module or as an informational message to the end user.
`TOKEN`	Each `TOKEN` keyword causes an input box to be displayed. The text after the keyword is displayed above the input box. You cannot change the ordering of the tokens.

Table 6-3 Properties File Keywords

Keyword	What it means
PASSWORD	Each PASSWORD keyword causes an input box to be displayed. The text after the keyword will be displayed above the input box. The only difference between the TOKEN and PASSWORD is the PASSWORD text will not be echoed, but will be asterisks. You cannot change the ordering of the tokens.
IMAGE	This keyword instructs the authentication module to replace the standard iPlanet Portal Server image with the image following the keyword. The image should be placed in /etc/opt/SUNWips/auth/default/optionaldomain. This image should be a GIF file.
HTML	This keyword tells the authentication module to override the dynamic HTML generation and supply your own HTML page. The authentication modules expect to receive URL parameters specific to each type of authentication. If you override the HTML for a module, your HTML page must supply the correct number and names of the parameters and show a small section of the HTML necessary for the UNIX page. One such sample is shown in Code Example 6-2 below.

The following HTML code will be generated given the UNIX properties file shown in Code Example 6-2. The user does not have to create this.

Code Example 6-2 Section of HTML Code for the UNIX Page

```
<P><STRONG>Enter Your UserId</STRONG><BR>
<INPUT TYPE=" NAME=TOKEN0 SIZE="22"></P>
<P><STRONG>Enter Your Password</STRONG><BR>
<INPUT TYPE="PASSWORD" NAME=TOKEN1 SIZE="22"></P>
```

The UNIX module expects the userID and password in the parameters `TOKEN0` and `TOKEN1`. To ensure you have the correct HTML you should go to that authentication page and view the HTML source.

Adding or Removing Modules From the Menu

When multiple modules are enabled, the end users see a menu of all the possible authentication modules. When end users click the link for a specific module, the authentication server loads that module. The end users receive the HTML pages for that module. If only one module is enabled, then no menu is sent, and the user is sent directly to the enabled authentication module.

Adding or Removing an Authentication Module from the Platform

You cannot add or remove authentication modules using the Administration Console. You must use the `ipsadmin` command to do this. See the instructions for using `ipsadmin` in the *iPlanet Portal Server Programmer's Reference* for procedures for adding or removing authentication modules.

You must stop and start the servers for it to recognize the changes. You can do this at the command line with the following command:

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

Changing the Look of Authentication Modules on a Per-Domain Basis

By default, all authentication module pages that are presented to users are identical across all domains. If you want to customize the look and feel of each domain's authentication, you must follow the procedure described below.

By default, all templates for creating authentication pages are in the `/etc/opt/SUNWips/auth/default` directory.

To Customize an Authentication Module on a Per-Domain Basis

1. Create a subdirectory in `/etc/opt/SUNWips/auth` and give it the name of the domain you are customizing.
2. Copy all files from `/etc/opt/SUNWips/auth/default` to that directory.

   All authentication pages for that domain will now be built from the files in the directory corresponding to the domain's name. You can customize the HTML code, colors, etc.

Authentication Helpers (daemons)

Some of the authentication modules provided with iPlanet Portal Server use authentication type-specific "helpers." These helpers are independently running processes with which the corresponding authentication module communicates. Usually, the helper is what is actually communicating with the remote authentication server. Helpers can assist in the debugging process for authentication modules.

When you install iPlanet Portal Server, several authentication helpers are configured and set to start automatically. Each of the helpers is listed in the `ips.daemons` entry in `/etc/opt/SUNWips/platform.conf` on each server. By default, this line looks like this:

```
ips.daemons=securid radius safeword unix skey
```

If you have started your iPlanet Portal Server gateway, you can confirm that each of these helpers is running by typing:

```
# ps -e | grep do
```

To return the list of running daemons, including doRadius, doSafeWord, doSKey, doSecurID, and doUNIX.

Additionally, each helper requires a configuration port specified in the `/etc/opt/SUNWips/platform.conf` file. The default configuration ports for the five helpers mentioned above are:

```
securidHelper.port=8943

radiusHelper.port=8944

safewordHelper.port=8945

unixHelper.port=8946

skeyHelper.port=8947
```

Note that these helper configuration ports must also be specified in the Profile Server (using the Administration Console). The helpers get their configuration port specified as a command line argument, which the server startup script gets from the `platform.conf` file. The server's authentication modules get that information from the Profile Server. The helper's authentication request listening ports are specified during the configuration process, so they need only be specified in the Profile Server.

See the section"Managing Authentication Attributes," on page 101 to learn to adjust these settings as well as related helper configuration values. For information on starting helpers for different authentication modules, refer to "Troubleshooting Authentication Problems" on page 208.

Platform-wide Authentication Attributes

Some of the attributes that govern the behavior of the authentication modules are platform-wide, since authentication modules handle authentication requests for all domains.

Only Super Administrators can modify platform-wide attributes. Domain Administrators cannot view or modify them.

Appendix B, Table B-1, lists the attributes that are platform-wide. You find them by clicking the Manage Platform Settings link on the iPlanet Portal Server page, then the Profiles->Authentication link on the right side of the window, then the Show Advanced Options button. Authentication attributes that can be changed at the domain level will not appear here. Platform-wide attributes cannot be overridden at lower levels of the role tree.

Appendix B, Table B-2 lists authentication attributes for the Super Administrator profile. These may be found by clicking the links in the order specified:

- Manage Administrators
- Admin Role (under Super Admins)
- Authentication.
- Click the Show Advanced Options button at the bottom.

Authentication Attributes at the Domain Level

Some of the authentication attributes are set only at the domain level. Appendix B, Table B-3 lists the attributes that are domain-wide. Domain-wide attributes, can be customized by either a Domain Administrator or the Super Administrator.

For example, one company may have two domains, each with its own LDAP server, making it necessary to configure a different LDAP server name for each domain. Now suppose Company X has a domain for employees and a domain for partners. The users in the partners domain need to access some special applications. Employees use SafeWord authentication; partners use LDAP.

To implement this scenario, you would do the following after creating the partner domain.

1. Select the Authentication profile under that domain.
2. Edit the Authentication Menu attribute to only select LDAP.
3. Select the LDAP profile and type the name of the server, plus the DN to start search for the partners.
4. Repeat the process for employees, except choose SafeWord as the authentication type.

Once the iPlanet Portal Server server is restarted, partners get the LDAP authentication page and employees get the SafeWord authentication page.

Another example might include two companies sharing the same iPlanet Portal Server installation that must use different authentication methods.

Authentication Attributes at the Role or User Level

Modifying an attribute at the role or user level means that you can customize how iPlanet Portal Server behaves for as many individuals as required. While there are few Authentication attributes that should be customized at the role or user level, some must be, including S/Key settings.

To modify an attribute at the role or user level, navigate to the domain in which this role or user resides, select the specific role or user, select the appropriate authentication module and change the attribute.

Chapter 7

Configuring The Netlet

This chapter describes how to set up applications to run securely between users' remote desktops and the application servers on your site's intranet using the Netlet service. Topics covered include:

- Configuring the Netlet to enable applications to run securely
- Customizing the iPlanet Portal Server profiles to provide links to user-defined applications
- Configuring third-party client/server applications to allow them to work with the Netlet

Providing Secure Applications Through the Netlet

iPlanet Portal Server users will want to run popular or company-specific applications on their remote desktops in a secure fashion. You provide these applications by setting up the iPlanet Portal Server Netlet on your platform. After you implement the Netlet at your site, users can securely run common TCP/IP services, such as Telnet and SMTP, and HTTP-based applications, such as pcANYWHERE or Lotus Notes.

Requirements for the Netlet

You can run any application over the Netlet if:

- It is TCP/IP-based.
- It uses fixed ports.

NOTE You cannot use the Netlet with applications that dynamically allocate ports. For example, you cannot run `FTP` over the Netlet if you run it as part of a `cron` job. The one exception is Microsoft Exchange, for which there is a limited dynamic port capability.

- Fixed ports and servers are available to the iPlanet Portal Server gateway or server without using a web proxy.

Only a limited number of sockets can be opened up on remote PCs.

How the Netlet Works

The *Netlet* is a Java applet that sets up an encrypted TCP/IP connection through fixed ports between the remote client and your intranet. Depending on whether the Netlet proxy is enabled, the connection will be made to the iPlanet Portal Server Gateway or iPlanet Portal Server Server. The Netlet has its own provider on the iPlanet Portal Server desktop, which users can tailor.

In a session involving the Netlet:

1. The remote user logs in and authenticates to the desktop.
2. If any Netlet rules have been defined, the Netlet is automatically loaded onto the remote client.
3. The Netlet listens on `localhost` to the ports defined in the Netlet rules.
4. The user clicks a link in the Netlet provider on the iPS desktop for a TCP/IP application or a UNIX service for which you have defined a Netlet rule.
5. The Netlet sets up an encrypted transaction between client and server over the ports specified in the Netlet rule defined in the Administration Console.
6. The transaction follows the path shown in Figure 7-1, which illustrates the movement of a `telnet` session over the Netlet with the Netlet proxy enabled.

NOTE The Gateway Management>Manage Gateway Profile>Advanced Options include an attribute for enabling the Netlet proxy.

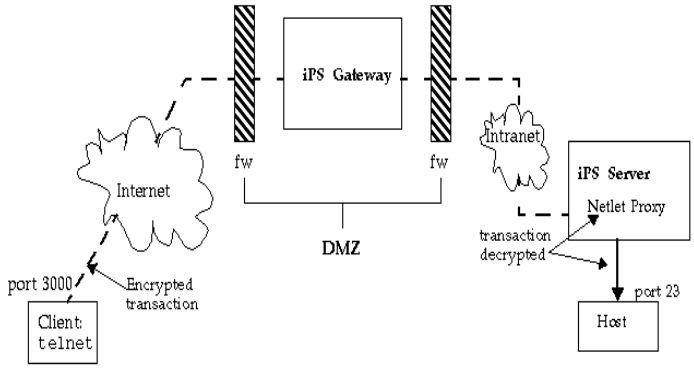

Figure 7-1 Path of a Telnet Session Run Over the Netlet

The entities in the path include:

1. Remote client
2. Internet
3. Company's external firewall
4. DMZ, where the Netlet is forwarded through the iPlanet Portal Server gateway
5. Company's internal firewall
6. Corporate intranet
7. iPlanet Portal Server server
8. Netlet proxy on the iPlanet Portal Server server, which decrypts the transaction
9. Recipient host on the corporate intranet

What Is Involved in Configuring the Netlet?

Setting up the Netlet requires four steps:

1. Create Netlet rules for the applications you want to support at your site.
2. Determine which rules should be domain-, role-, or user-based.
3. Add these rules to each level of the role tree by configuring the Applications profiles in the Administration Console.
4. Define the privileges for each Netlet rule in the policy pages of the Administration Console.

Writing Netlet Rules

Netlet behavior is defined through a series of *Netlet rules* that are configured on the profile pages of the Administration Console. Netlet rules can be configured for domains, roles, or users. The links to get to the Netlet rules are Manage Domains>Domainname>Applications>Netlet. Of course, if the netlet rule is for a role or user, select the desired role or user after selecting the domain name.

Netlet rules exist for:

- Predefined Netlet applications
- User-defined Netlet applications

Netlet rules are either static or dynamic. A static rule specifies a particular destination host. A dynamic rule specifies that the end user allocates destination hosts are allocated dynamically.

Syntax of Netlet Rules

Netlet rules use the following syntax:

name | <*url to invoke*> | <*download applet ?*> | *listen-port* | *destination-info* | *destination-port*

where:

- *name* – Designates a name for this Netlet rule.
- *URL to invoke* – Specifies the URL that the browser opens when the user clicks its associated link in the Netlet provider window. The browser then opens the window for the application, connecting to `localhost` at the port number specified later in the rule.

  URL to invoke can have either of these values:

  - *URL* – URL to the application invoked by the Netlet rule.
  - `null` – Value that you set if the application is not started by a URL or controlled by the desk top.
- *download applet?* – Indicates whether it is necessary to download an applet for this rule. Specify one of these actions in the field:

  - `false` – Do not download an applet.
  - `true` – Download the applet using the default values:

    `localport = iwtNetlet-clientLoopbackPort` - the port on the remote client to be used to retrieve other URLs.

    `downloadServer = ipsServer - the server where the Netlet code resides.`

    `downloadPort = ipsPort - the port on the server where the Netlet code will be retrieved.`
  - *server info* - Gives information about the server. Use the form *cport:server:sport* where:

    sport represents the port on the server used to download the applet.

    server is the server name.

    cport indicates the destination port on the client.

- *listen port* – Port on the client where the Netlet will listen.

NOTE The *listen port* value must be unique. You cannot specify a particular port number in more than one rule only.

- *destination info*– Recipient of the Netlet connection. Specify either of these values for *destination info*:
  - *host* – Name of the host to receive the Netlet connection, used when you are creating a *static rule*. You can use either the simple host name, such as `example1`, or a fully-qualified DNS-style host name, such as `example1.mycompany.com`. The name used here must be what the iPlanet Portal Server uses to get to the destined machine. For example, if the iPlanet Portal Server requires the fully qualified name of the host, specify that.
  - `TARGET` – Represents the host names that the user specifies on the iPlanet Portal Server desktop for the Netlet target list. A rule specifying `TARGET` enables users to select their own destination host when they use this rule. Rules that specify `TARGET` in the syntax are considered *dynamic rules*.
- *destination-port* – the port on the destination host (specified in destination-info)

In addition to the host and target, you must specify a destination port. And in the case where multiple target hosts can be defined, you must have that mentioned here as well.

Ports Used by iPlanet Portal Server

Table 7-1 identifies the ports reserved in iPlanet Portal Server for various applications and services.

Table 7-1 Reserved Listen Ports for Predefined Netlet Rules

Predefined Netlet Rule	Reserved Port
Telnet	30000
GO-Joe	10491
Citrix	1494
pcANYWHERE	4631, 5632
CarbonCopy	1138

Table 7-1 Reserved Listen Ports for Predefined Netlet Rules

Predefined Netlet Rule	Reserved Port
LapLink	51547
RapidRemote	45414
ReachOut	43188
RemotelyPossible	799
loopback*	8000

* loopback is an internal Netlet rule used for internal functions.

Sample Netlet Rules

This section contains some examples of Netlet rules that illustrate how the Netlet syntax works.

Basic Static Rule

This rule supports a Telnet connection from the client to the machine `example1`.

```
myrule|null|false|1111|example1|23
```

where:

- `myrule` is the name of the rule.
- `null` indicates that this application is not invoked by a URL or run through the desktop.
- `false` indicates that the client does not download an applet to run this application.
- `1111` is the port on the client where the Netlet listens for a request for a connection from the target host.
- `example1` is the name of the recipient host in the Telnet connection.

- 23 is the port number on the target host for the connection, in this case the well-known port for Telnet.

How the Netlet Rule Works When Run by the User

The Desktop Netlet provider does not show a link, but Netlet automatically starts and listens on the port specified (1111). Instruct the user to start the client software, in this case a Telnet session that connects to `localhost` on port 1111.

For example, start the Telnet session, the client types the following on the UNIX command line in a terminal:

```
% telnet localhost 1111
```

Static Rule With Multiple Target Hosts

This rule supports a Telnet connection from the client to two machines, `example1` and `example2`.

```
myrule|null|false|1111|example1|23|1234|example2|23
```

where:

- `1234` – port on the client where the Netlet listens for a connection request from the second target host.
- `example2` – name of the second target host, such as example2.
- 23 – Port number on the target host for the connection – well-known port for Telnet.

The first six fields in this rule are the same is in “Basic Static Rule.” The difference is that three more fields identify the second target host. When you add additional targets to a rule, you must add three fields, *listen port*, *target host*, and *target port*, for each new target host.

NOTE You can have multiple sets of three fields describing the connection to each target host. Listen port numbers which are less than 2048 must not be used if the remote client is a solaris machine because low numbered ports are restricted and you must be root to start a listener.

How the Netlet Rule Works When Run by the User

This rule works the same as the previous rule. There are no entries for this rule in the Desktop Netlet Provider. The Netlet automatically starts and listens on the two ports specified (1234). The user needs to start the client software, in this case a Telnet session that connects to `localhost` on port 1111 or local host on port 1234 to connect to host example2.

Dynamic Rule That Invokes a URL

This rule defines a Telnet connection from the client to hosts that are dynamically allocated, enabling the user to Telnet to various hosts over the Netlet.

```
myrule|telnet://localhost:30000|false|30000|TARGET|23
```

where:

- `myrule` is the name of the rule.
- `telnet://localhost:30000` is the URL invoked by the rule.
- `false` indicates that no applets are to be downloaded.
- `30000` is the port on the client where the Netlet will listen for connection requests for this rule.
- `TARGET` indicates that the target host is dynamically allocated from the desktop Netlet target list when the user invokes this Netlet rule.
- `23` is the port on the target host opened by the Netlet, in this case the well-known port for Telnet.

How the Rule Works When Run by the User

After this rule is added, the user must complete some steps to get the Netlet running as expected. Give the user the following instructions:

1. Press the Edit button in the Netlet provider section of the iPlanet Portal Server desktop.

   The new Netlet rule is listed under Rule Name in the Add New Target section.

2. Click the rule name and type the name of the target host.
3. Save the changes.

   You return to the Desktop with the new link visible in the Netlet provider section.

4. Click the new link.

   A new browser is launched that goes to the URL given in the Netlet rule.

NOTE	You can add more than one target host for the same rule by repeating these steps.

Dynamic Rule That Downloads an Applet

This rule defines a GO-Joe connection from the client to hosts that are dynamically allocated. The rule downloads a GO-Joe applet from the application server to the client.

```
gojoe|/gojoe.html|8000:goejoeserve:8080|3399|TARGET|58
```

where:

- `gojoe` is the name of the rule.
- `/gojoe.html` is the path of the HTML page containing the applet, relative to the iPS installation directory `/opt/SUNWips/public_html` (in a default installation.).

- `8000:server:8080` indicates that port 8000 is the destination port on the client to receive the applet, `gojoeserve` is the name of the server providing the applet, and `8080` is the port on the server from which the applet is downloaded.
- `3399` is the port on the client where the Netlet listens for connection requests of this type.
- `TARGET` indicates that the target host is dynamically allocated by the client when the Netlet rule is invoked.
- `58` is the port on the target host opened by the Netlet, in this case the port for GoJoe. Port 58 is the port that the target host listens to for its own traffic. The Netlet passes information to this port from the new applet.

Configuring Netlet Profiles in the Role Tree

You define Netlet rules in the application profile pages for the domain, role, or user levels. Each Netlet profile has an attribute called "Netlet Rules," where you type the rules for the applications to run over the Netlet.

This section contains procedures for setting up and modifying the Netlet profiles. It assumes that you have decided on whether you want Netlets to run on a domain, role, or user basis (or all three), and have composed a few rules. If you need assistance on writing Netlet rules, go to "Writing Netlet Rules," on page 130.

NOTE Consider making most of your Netlets role-based, as opposed to domain or user-level-based.

To Configure a Netlet Profile for a Domain

1. Access the Administration Console.
2. Click Manage Domains under "Roles and Users"

   The Portal Server Domains page is displayed.
3. Click the link for the domain for which you want to configure the Netlet.

   The Domain, Role, and User Profiles page is displayed.

4. Click the icon to the left of Applications to expand the list of Applications profiles.
5. Click the Netlet link to display the Netlet profile for the domain.

   All default Netlet rules already active for the domain are shown in the Netlet Rules attribute box.
6. Scroll down to the field below the listed Netlet rules.
7. Do one of the following to add Netlet rules:

- Add Netlet rules individually by typing each Netlet rule that you want to configure in this field and pressing Add.

  Each new rule is displayed in the Netlet rules box.
- Use this shortcut:

  a. Select and highlight an existing rule in the Netlet rules box that is similar to one that you want to create.

     The text of the highlighted rule is displayed in the input field.

  b. Modify the displayed text to reflect the change for the new Netlet rule.

  c. Click Add to add the new rule.

8. (Optional) You can also change the defaults for other attributes in the Domain Netlet profile, depending on your site's needs. These attributes are:

- Warning Popup for Connections

  This attribute pops up a message on the user's desktop warning that someone is trying to connect to the desktop through the listen port. The message comes up when the user runs the application over the Netlet, but also when an intruder tries to gain access to the desktop through the listen port.

  If you do not want the popup to appear on the user's desktop, deselect this attribute.
- Default Loopback Port

  This attribute specifies the port on the client to be used when applets are downloaded through the Netlet. The default value of 8000 is used unless it is overridden in the Netlet rules.
- Apply changes to subroles

The default is to not apply changes to subroles. To propagate all changes to the Netlet profile down the role tree, select this attribute. If any child of the current entity has customized a field which is currently changed in the HTML form, then those customized fields will be removed from the children.

CAUTION Use care when applying changes to subroles, refer to Section "Inheritance at the Domain Level" on page 24, for a full description of this feature.

9. Click Submit to register these changes.
10. Go on to "To Set Permissions for the Netlet," on page 139.

To Set Permissions for the Netlet

The final step in setting up a Netlet profile is to assign permissions for the Netlet rules. The permissions set apply to each level of the role tree and are inherited relative to the level of the profile being set: Domain, Role, or User.

1. Scroll to the top of the Netlet profile page.
2. Click the Show Read / Write Permissions button to enable viewing of the default permissions
3. Scroll down to the Netlet Rules attribute to view the permissions set for each relevant attribute in the profile.

   "Netlet Permissions" on page 139 shows the default permissions, which you can change depending on the requirements of your site.

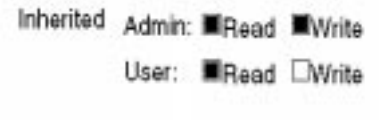

Figure 7-2 Netlet Permissions

- **Admin** indicates the permissions granted to the Domain Administrator for access to the attributes in this profile. The default permissions allow the Domain Administrator to both view and change the attributes. If only Read were selected, the Domain Administrator could view the attribute but not change it.

NOTE The Super Administrator always has read and write permissions for all attributes in the role tree.

- **User** indicates the permissions granted to the application run by the client. By default, the application can read the attribute, for example, the Netlet rule, but cannot change it. If both Read and Write were selected, the application could both read and change the Netlet Rule attribute, for example.

4. Press Submit to activate your changes.

   You get a confirmation message that the profile was updated.

5. Press Continue to return to the Netlet profile.

6. Go on to "Configuring Netlet Privileges for the Role Tree," on page 142 for instructions on setting up policies for the Netlet rules.

To Configure a Netlet Profile for a Role or Users

The procedure is the same as that stated in"To Configure a Netlet Profile for a Domain" except for the role:

- Access the role of interest by navigating to:
  manage domains><role name>.
- Access the user by navigating to:
  manage domains> role> <user name>.

To Delete a Netlet Rule

1. Access the Administration Console.

2. Click Manage Domains under “Roles and Users”

   The Portal Server Domains page is displayed.

3. Click the link for the domain with the Netlet.

   The Domain, Role, and User Profiles page is displayed.

4. Do the following depending on where the Netlet rule you want to delete is located:

- Navigate down to the appropriate profile for the role or user.
- Remain at the domain level.

5. Click the icon to the left of Applications to expand the list of Applications profiles.
6. Press the button to the left of Applications to open the Applications links.
7. Click the Netlet link to display the Netlet profile.
8. Click and highlight the Netlet rule that you want to delete in the Netlet Rules attribute box.
9. Press the Delete button associated with the filed.

   The highlighted rule is removed from the list of rules.

10. Press Submit to activate your changes.

    You get a confirmation message that the profile was updated.

11. Press Continue to return to the Netlet profile.

To Modify an Existing Rule

1. Access the Netlet profile with the rule to be modified, as explained in “To Configure a Netlet Profile for a Domain,” on page 137, “To Configure a Netlet Profile for a Role or Users,” on page 140.
2. Click and highlight the existing rule in the Netlet Rules attribute box.

   The rule text is displayed in the field below the box.

3. Modify the rule text in the field as needed.

4. Click the Add button.

   Both the old rule and the changed rule are displayed in the Netlet Rules attribute box.

5. Click and highlight the old rule in the Netlet.

6. Click the Delete button.

   The highlighted rule is removed from the list of rules.

7. Press Submit to activate your changes.

   You get a confirmation message that the profile was updated.

8. Press Continue to return to the Netlet profile.

Configuring Netlet Privileges for the Role Tree

This section describes how to define policies to be associated with each Netlet profile in the role tree.

To Define Netlet Policies for a Domain

1. Access the Administration Console.

2. Click Manage Domains under “Roles and Users”

   The Portal Server Domains page is displayed.

3. Click the link for the domain for which you want to configure policies for the Netlet.

   The Domain, Role, and User Profiles page is displayed.

4. Click the Policy link under Profiles to display the Policy Module for the domain.

5. Click the Netlet link in the Index to move to the Netlet-related attributes.

   The Setup netlet access to specific hosts attribute boxes are displayed. The Allow box contains the asterisk wild card, allowing all hosts in the domain as Netlet targets.

6. Do either of the following, depending on your site’s policies:

- Leave the asterisk in the Allow box.

- Configure specific host access rights as follows:

  a. Click and highlight the asterisk in the Allow box.

  b. Type the name of a host to be allowed to use the Netlet in the field below the Allow box.

  c. Click Add and then repeat these steps until you have added all hosts to which these privileges must apply.

  d. Type the name of a host to be denied access in the field under the Deny box.

  e. Click Add and then repeat these steps until you have added all hosts that must be denied access to Netlets defined at the domain level.

7. Scroll down to the fields below the Setup netlet access to specific rule's attribute box.

These boxes will use the Netlet *name*, that is, the first part of each Netlet rule.

8. Do either of the following, depending on your site's policies:

- Leave the asterisk in the Allow box.
- Specify names of specific Netlet rules to which you want to allow or deny access on the domain level.

  a. Click and highlight the asterisk in the Allow box.

  b. Type the URL for which you want to allow access in the field below the Allow box.

  c. Click Add and then repeat these steps until you have added all hosts to which these privileges must apply.

  d. Type the URL for which you want to deny access in the field under the Deny box.

9. Click the return to top link and then click Applications from the Index.

The list of applications allowed to be executed from this profile is displayed. By default, the buttons next each application are pushed in (black), indicating that the application can be executed from the profile.

10. Control access to the Netlet as follows:

- To allowing Netlet access to a domain or role or user, ensure that the box next to the Netlet application is pushed in.

- If you want to deny Netlet access to a group of users or members of a role, uncheck the box next to the Netlet application.

11. Scroll down to the bottom of the page when you are done.
12. (Optional) Click the box next to Apply all changes to Sub Roles if you want the lower levels of the role tree to inherit these attributes.
13. Click the Submit button.
14. Click the continue button to return to the previous page.

To Define Netlet Policies for a Role

Repeat the steps in “To Define Netlet Policies for a Domain,” on page 142, but navigate down to the appropriate role level from the Domain, Role, and User Profiles page. From there, define the Netlet policies that are appropriate for the role.

To Define Netlet Policies for a User

Repeat the steps in “To Define Netlet Policies for a Domain,” on page 142, but navigate down to the appropriate user level from the Domain, Role, and User Profiles page. From there, define the Netlet policies that are appropriate for the user.

Rules for Predefined Netlet Applications

Rules for predefined Netlet applications govern using well-known third-party remote-windowing applications. These rules are enabled by default when iPlanet Portal Server is installed. To disable them, either remove them from the Domain, Role, User profile or type the name in the deny list on the Policy page in the “Netlet Access to Specific Rules” field.

In the case of pcANYWHERE and GO-Joe, client applets are shipped and integrated with the iPlanet Portal Server software so that they will be started automatically.

Netlet connections to the predefined applications require that a destination server be specified at the time the connection is established; that is, the predefined rules have no fixed destination server.

Simply giving a rule for either a user-defined application, the name of one of the pre-defined Netlet applications, or using one of the reserved ports, will not cause the rule to be treated as a pre-defined application. Alternatively, disabling a rule for a pre-defined application will not affect any user-defined rules that happen to share the same name or ports. The only way to disable a rule for a user-defined application is to remove it.

For example, if a user-defined rule directs certain traffic to the Telnet port of a specific host (`myTelnet|30001|myServer|23`), this rule will operate independently of the rule for the predefined Netlet application for Telnet. It does not depend on whether or not the predefined Netlet application for Telnet is enabled on the Netlet Administration page of the iPlanet Portal Server Administration Console.

NOTE Netlet rules cannot contain any port number higher than 64000.

Client Specifications and Examples

Configuring Client Software

Clients must be configured to connect through the Netlet, which proxies that connection to the destination server. Since the Netlet resides on the client, the connections must be made to the machine named `localhost`.

Integrating Applet Clients

Java security restrictions require that applets can make connections only to the machine from which they are downloaded. This means that the client applet itself must be downloaded through the Netlet. Creating a Netlet rule to download an applet from the machine `localhost` allows the applet to connect to ports on `localhost`. If Netlet rules accept connections on those ports, the applet will connect to the machines to which those ports are proxied.

Applets following this procedure require no reconfiguration because these applets normally determine the name of the host from which they were served and connect to that machine name. They will attempt to connect to `localhost`, which the Netlet accepts and proxies.

If an applet is configured to connect to a named machine, you have two choices for redirecting the applet to connect to localhost:

- Have each user configure the client to use `localhost` as the server
- Have DNS resolve the destination server's host name to 127.0.0.1 for external queries, and to the actual IP address for internal lookups.

The second choice is recommended solution it requires no changes to the client configuration, and the client will work correctly from the Internet and the intranet.

Use the following procedure to integrate applet clients.

1. To integrate applet clients, you need to create the proper Netlet rule to download the applet and for the applet to make connections back to the server. You also must determine whether this rule must be under a domain, role, or only for a specific user.
2. Once you have determined where in your domain / role / user tree to place the Netlet rule, you then create the rule based on the guidelines that were given earlier in the chapter.

   Particularly, you will have to pay attention to the <URL to invoke> field and the <download applet?> field. Most likely you will be downloading your applet from a different server than the Portal Server platform server, so you need to use the <cport:server:sport> form of the <download applet?> field to specify the local Netlet listen port and the target server:port that the applet is coming from.

   In the interest of keeping one application's setup consolidated into one rule, you can add multiple listen ports onto the end of one rule. So if you applet needs three ports to talk to its host server on, then it's rule might look like this:

```
arule|/dir/applet.html|2080:appletserv:2080|8030|TARGET|8030|8040|/
TARGET|8040|8050|TARGET|8050
```

3. To make this rule show up in the Netlet provider, you then Click on the Domain (Role and User, if applicable) Applications -> Desktop link, and under the 'Channels' heading,
4. Select the 'iwtNetletProvider' channel, and click on the 'Edit Channel' button.
5. Under the 'Targets' section, add a new target to the Netlet Provider like this:

   ```
   arule|hostname
   ```

   The first part must be the name that you gave to the new Netlet rule that you created step 2 above, and the second part must be the hostname of the server that you want as the default host for this rule to connect to.

NOTE By default, users have read and write privileges on Netlet Provider targets, so they can change the target hosts for the Netlet rules that you add. If you want to fix the rule target hosts, change the read/write permissions so that users only have read permission for this attribute.

6. Click the Add button to add the target to the list of Netlet Provider targets.
7. Click the Submit button at the bottom of the page to submit the changes to the Portal Server.

   To integrate applet clients, navigate from Manage Domains to the domain of interest, then expand the Application link and select the Netlet link.

Integrating Non-Applet Clients

Non-applet clients, such Lotus Notes or Microsoft Exchange, must be directed to connect to the client machine on which they are running. This can be done in either of two ways:

1. Have each user configure the client to use `localhost` as the server.

   or

2. Have DNS resolve the destination server's host name to 127.0.0.1 for external queries and to the actual IP address for internal lookups.

The second choice is the recommended solution because it requires no changes to the client configuration, and client will work correctly from the Internet and the intranet.

Use the following procedure to integrate non-applet clients.

1. To integrate non-applet clients, the proper netlet rule must be created to map the application's TCP port over the Netlet. You also must determine whether this rule must go under a domain, role, or only for a specific user.

2. Click on the Applications>Netlet link (from the Domain, Role, or User page)

   If the application requires multiple ports to be opened, you can either write multiple rules, or add the ports on to the end of a single rule.

   The Netlet rule must be in the form outlined step 2 of "Integrating Applet Clients" on page 145.

   Rule example with 2 port definitions:

   The Netlet listens on ports 9877 and 9878, and connects to ports 17888 and 17889 on the intranet server 'intra-serv', respectively.

```
zrule|null|false|9877|intra-serv|17888|9878|intra-serv|17889
```

NOTE The client-listen-port is arbitrary, but it must be a port that is not used by the client or any other Netlet rule. Ideally, the client-listen-port and the destination-host-port should be the same. A value above 2048 should be used for the client-listen-port because certain operating systems require the end user to be root with a client-listen-port below 2048.

3. Click the Add button to add the rule to the list of Netlet Rules.
4. Click the Submit button at the bottom of the page to submit the changes to the Portal Server.
5. The user can start their client software after they log in and the small Netlet window has appeared and the Netlet has initialized.

Configuring Lotus Notes

You can use the Netlet to allow end users to use Lotus Notes as clients through iPlanet Portal Server.

- By using a Netlet, access is encrypted to Lotus Notes.
- Since Lotus Notes has an HTML client, you can use the bookmark provider on the iPlanet Portal Server Desktop to open it.

Writing a Netlet Rule for the Lotus Notes Web Client

1. Start the iPlanet Portal Server Administration Console.

2. Select the domain of interest and navigate to the Applications > Netlet link.
3. Add a Netlet rule in the Netlet Rules section similar to the following:

```
LotusHTML|null|false|80|lotus-server|80
```

   This rule, called 'LotusHTML', tells the Netlet to listen for the client on port 80 and connect to the server 'lotus-server' on port 80. A requirement of the Lotus Web Client is that the client listen port must match the server port. The following rule would not work:

   ```
   LotusHTML|null|false|80|lotus-server|8080
   ```

   For the above rule, the client port does not match the server port, hence the rule will not work.

4. Click the Add button to Add the rule to the list of netlet rules.
5. Click the Submit button at the bottom of the page to submit the changes to the Portal Server.
6. Click on the Continue button to return to the Applications page.
7. Click on the Back to Overview link to return to the Domain, Roles and Users page. At this point, netlet connections to the Lotus Web Client have been added. What is needed next is a link for the Application Provider to start the Lotus Notes Web Client.
8. From the domain of interest, click on the Applications link to expand it then select Desktop.
9. Below the Available Applications list, add the Lotus Notes application as follows:

   ```
   Lotus Notes Web Client|http://localhost:80/
   ```

   The first part is the name that the user will see in the link, the second part is the link itself.

10. Click the Add button to add this link to the list of available applications.
11. Scroll to the Selected Applications list and add the Lotus Notes application from the Available Applications list. Use the same name.

12. Click the Add button to add the Lotus Notes Web Client application to the Selected Applications list.
13. Click the Submit button at the bottom of the page. This adds a link to the application provider list on the user's desktop.

Writing a Netlet Rule for the Lotus Notes (non-Web) Client

The Netlet rule created in the following procedure lets a Lotus Notes client connect directly to a Lotus Domino server.

1. Start the Administration Console.
2. Click the domain of interest and navigate to the Applications>Netlet link.
3. In the Netlet rules section, add the following rule:

```
LotusClient|null|false|1352|lotus-domino|1352
```

   With this rule, the Lotus Notes client can connect to a Lotus Domino server through the Netlet. Remember that when the client tries to connect to the server it must not point to `localhost` as the server name. It must point to the actual server name of the Lotus Domino server. The server name must be the same as the system name for the server. The client must resolve that name to 127.0.0.1 when using the Netlet. There are two ways to accomplish this:

   a. Set the server name to point to 127.0.0.1 in the client host table.
   b. Export a DNS entry of the name of the server that points to 127.0.0.1.

   The server name must be the same server name that was used to configure the Domino server during setup.

4. Click the Add button to add the rule to the list of Netlet rules.
5. Click the Submit button to submit the changes to the Portal Server.

Writing Netlet Rules for Stand-Alone Email Clients to an IMAP or an SMTP Server

Netlet rules can be written to connect stand-alone email clients to different email servers. Although the procedure shown here uses IMAP and SMTP, this approach will work for all email servers.

1. Start the Administration Console.
2. On the menu on the left, click the Manage Domains.
3. Select the domain of interest (and the role of interest, as applicable), then click the Applications link. Expand the link.
4. Select Netlet and scroll to the "User Defined Netlet Applications," to define a netlet rule for:

   a. IMAP. For example:

```
IMAPRule|null|false|143|imapserver|143
```

   b. SMTP servers. For example:

```
IMAPRule|null|false|25|imapserver|25
```

The Netlet `client-listen-port` on the client side does not have to be the same as the `destination-listen-port` on the server side. If you use anything other than the standard IMAP and SMTP ports, make sure that the client is configured to connect on a port that is different from the standard port.

NOTE End users who use Solaris clients may have trouble connecting to port numbers lower than 1024 unless they are running as root.

5. Click the Add button to add this rule to the list of Netlet rules.

6. Click the Submit button to submit these changes to the Portal Server.

Configuring the Netscape Mail Client

End users may have to configure the Netscape browser they are using for mail servers. The following procedure will help them through this process. The instructions are for Netscape 4.5. See the Netscape documentation for help with configuring other versions of the Netscape browser.

End users must do the following:

1. Start the Netscape browser.
2. In the menu bar of the Netscape browser, click Edit and select Preferences.
3. Click the triangle before Mail & Newsgroups to see the items in this category.
4. Click Mail Servers.
5. In the section “Incoming Mail Servers,” click the Add button to display the window for adding a server and its port.
6. On the General tab for the Server Name, type the following:

```
localhost:any_port_1
```

If port 143 is used as the `client-listen-port`, they only have to type `localhost`.

For the server, type the following:

```
localhost:any_port_2
```

If port 25 is used as the `client-listen-port`, they only have to type `localhost`.

Accessing Netscape Mail

End users must do the following:

1. Log in to the iPlanet Portal Server Desktop. Upon successful login, the netlet application will start and Netscape mail can be accessed.
2. Open the Netscape mail client.

NOTE For information on adding your own link for Netscape Mail to the remote file and windowing window, see Adding LInks to Predefined Applications and to Third-Party Browser-Based Clients the section “Adding Links to Predefined Applications and to Third-Party Browser-Based Clients” elsewhere in this appendix. The URL to add is `HREF= MAILBOX:`.

Configuring Netlet for Use With Microsoft Outlook and Exchange Server

1. Start the Portal Server Administration Console
2. Determine within what domain and at what level within the role tree the Netlet rule will apply.
3. Click on the Applications -> Netlet link.
4. Add a Netlet rule in the ’Netlet Rules’ list window like the following rule:

   ```
   OutlookEx|null|false|135|exchange|135
   ```

   This rule, called ’OutlookEx’, tells the Netlet to listen on the client on port 135 and connect to the server ’exchange’ on port 135. The Outlook client uses this port to make an initial attempt to contact the Exchange Server and determine what subsequent ports it will be using to talk to the server.
5. Click the Add button to add the rule to the list of Netlet Rules.
6. Click the Submit button at the bottom of the page to submit the changes to the Portal Server.
7. Click on the Continue button to continue.
8. On the client machine, the user must change the hostname of the Exchange server that is configured in their Outlook client to be ’localhost’. The location of this option varies with different versions of Outlook.

9. On the client machine, the user must now map the hostname (single and fully qualified) of the exchange server to the IP address 127.0.0.1 using the hosts file.

   On Windows 95/98, the file is in \Windows\Hosts On Windows NT4, the file is in \WinNT\System32†rivers…tc\Hosts.

   The entry looks like this:

   ```
   127.0.0.1     exchange exchange.company.com
   ```

   The exchange server sends back its own name to the Outlook client, and so this mapping is to insure that the Outlook client uses the Netlet client to make the connection back to the server.

End User Access to Microsoft Exchange Server

End users must do the following:

1. Log into the iPlanet Portal Server desktop.
2. Once they have logged into the desktop and the small Netlet window has appeared and the Netlet has started, they are ready to access the Exchange server.
3. Open the Outlook client.

Chapter 8

Configuring the Gateway

This chapter has the following topics:

- Configuring web proxies
- Using virtual IP and multiple DNS names
- Configuring the rewriter
- Running in HTTP mode
- Configuring the gateway proxy
- Enabling PDC
- IP address validation
- HTTP basic authentication
- Forward cookie configuration
- Non-portal server cookie management

Configuring Web Proxies

Web proxies can be configured to contact the Profile Service and to contact the Server and all other machines on the intranet.

Configuring the Web Proxies Used To Contact the Profile Service

Requests from the Gateway to the Server follow the same rules listed below. However these rules do not apply to requests from the Gateway to the Profile Service. Therefore if the Gateway cannot contact the Server directly, and a proxy is necessary, then the following changes must be made on the Gateway, or it will never be able to read its profile information:

1. From the command line, open to edit the gateway file:

```
/opt/SUNWips/bin/ipsgateway
```

2. Add the following entries to the DEFINES variable:

```
-Dhttp.proxyHost=<the name of the proxy host>
```

```
-Dhttp.proxyPort=<the proxy's port>
```

```
-Dhttp.proxySet=true
```

3. Manually restart the Gateway to use the specified proxy for Profile Service requests made to the server.

NOTE The gateway is restarted manually since there is no method to tell the Profile Service of the proxy without restarting the gateway; requests would only be received and not processed.

Configuring the Web Proxies for the Server and All Other Machines

The gateway may be configured to contact HTTP resources using web proxies. Different proxies may be used for different domains and subdomains.

Web Proxies for DNS Domains and Subdomains

These entries tell the gateway what web proxy (if any) to use when contacting specific subdomains in specific domains. The syntax for each entry in this list is:

```
domain_name [web_proxy1:port1]|subdomain1 [web_proxy2:port2]|......
```

* is a wild card that matches everything

The first entry in the list is special. The domain (in the example below, iplanet.com) is considered the 'default domain'. The first subdomain that appears in the first entry (in this case, red) is the 'default subdomain. The default subdomain and domain are relevant for proxying and rewriting URLs that contain hostnames that do not specify a subdomain and domain—the gateway assumes that the hostnames are in the default subdomain and domain, and acts accordingly.

The list entries are processed in order from top to bottom, so the first match that can be made for a requested URL is applied. So, given this example list for DNS Domains and Subdomains:

```
iplanet.com wp1:8080|red wp2:8080|yellow|* wp3:8080

sun.com|eng wp4:9090|corp

* wp5:9090
```

When the destination host in the requested URL is a fully qualified host name, a particular proxy is specified accordingly. Table 8-1 identifies this URL condition.

Table 8-1 Destination Hosts with Fully Qualified Name List

Requested URL's Host	Proxy Indicated	Reason
host1.red.iplanet.com	wp2:8080	find subdomain and use web proxy for the subdomain
host2.yellow.iplanet.com	wp1:8080	find subdomain, but subdomain has no web proxy, so use the web proxy for the domain
host3.blue.iplanet.com	wp3:8080	the subdomain matches the wild card in the last entry for iplanet.com
host4.eng.sun.com	wp4:9090	find subdomain and use web proxy for the subdomain
host5.corp.sun.com	none	find subdomain but subdomain has no web proxy and domain also has no web proxy.
host6.sfbay.sun.com	none	subdomain doesn't match any of the sun.com subdomains, so no proxy used.
host7.eng.netscape.com	wp5:9090	the entry matches the wild card entry at the end of the list.

When the destination host in the URL is not a fully qualified host name, a particular proxy is specified accordingly (see definition of 'default domain' and 'default subdomain' in). Table 8-2 identifies this URL condition.

Table 8-2 Destination Hosts Without Fully Qualified Host Name List

Requested URL's Host	Proxy Indicated	Reason
host8	wp2:8080	Use web proxy for the default subdomain. If there is no web proxy for default subdomain, use the web proxy for default domain (wp1:8080).
host9.red	wp2:8080	Match the subdomain in the default domain and use the web proxy for the subdomain.
host10.yellow	wp1:8080	Match subdomain, but subdomain has no web proxy, so use web proxy for the default domain.

The last two hostnames in Table 8-2 might in fact be fully qualified, and therefore the gateway's assumption that they are in the default domain might be incorrect. However, in most cases this assumption will be correct, since 'red' and 'yellow' are explicitly listed as subdomains in the default domain.

In the final example shown in , however, 'blue' is not in any of the default domain's subdomains. Rather than apply the wildcard subdomain that wp3:8080 applies to, the gateway assumes that this is a fully-qualified name.

To be treated as a host in the default domain, 'blue' would have to be explicitly added to the default domain's list of subdomains, as shown in Table 8-3.

Table 8-3 Destination Host Without A Reference to a Default Domain's Subdomain

Requested URL's Host	Proxy Indicated	Reason
host1.blue	wp5:9090	Subdomain wildcard in default domain does not apply in this case, so apply wildcard in final list entry.

If a web proxy is not indicated for the target URL through the 'DNS Domains and Subdomains' list as described above, the gateway will connect to the destination host directly.

If a web proxy is indicated, the gateway will check the attribute 'Use Intranet Web Proxy'.

If 'Use Intranet Web Proxy' is true, the gateway will make the request via the web proxy unless the requested URL is found in the list 'Don't Use Web Proxy Enabled', which is a list of URLs. If the requested URL is in that list, then the destination host is contacted directly.

If 'Use Intranet Web Proxy' is false, the gateway will send the request to the destination host directly, unless the requested URL is found in the list 'Use Web Proxy Enabled' which is a list of URLs. If the URL appears there, the gateway will fetch the URL using the web proxy that was indicated by the 'DNS Domains and Subdomains' list.

This list also describes to the gateway which URLs it may rewrite -- only references to hosts in the specified sub / domains are candidates for rewriting. (This can be overridden by the Rewrite All URLs Enabled selection, described in “Rewrite All URLs Enabled” on page 160).

When the URL host is a fully qualified host name, the URL is either rewritten or not rewritten, as shown in (from the list of hosts originally defined in Table 8-1). When the URL host is not a fully qualified name, shown by the last three entries in this table, the URL is not rewritten.

Table 8-4 Rewrite URL Status for Destination Host With or Without Fully Qualified Name

Requested URL’s Host	Rewrite URL?	Reason
host1.red.iplanet.com	yes	--
host2.yellow.iplanet.com	yes	--
host3.blue.iplanet.com	yes	match wild card subdomain entry
host4.eng.sun.com	yes	--
host5.corp.sun.com	yes	--
host6.sfbay.sun.com	no	subdomain does not match any sun.com
host7.eng.netscape.com	no	domain wild card does not apply here as it does for proxying

Table 8-4 Rewrite URL Status for Destination Host With or Without Fully Qualified Name *(Continued)*

Requested URL's Host	Rewrite URL?	Reason
host8	yes	
host9.red	yes	
host10.yellow	yes	
host11.blue	no	subdomain wildcard in default domain does not apply in this case

In the final entry of , 'blue' is not in any of the default domains subdomains. Rather than apply the wildcard subdomain, the gateway assumes that this is a fully-qualified name. To be treated as a host in the default domain, 'blue' would have to be explicitly added to the default domain's list of subdomains.

Rewrite All URLs Enabled

If true, the Gateway will rewrite any URL without checking the URLs sub / domains against entries in 'DNS Domains and Subdomains'. If false, the 'DNS Domains and Subdomains' list applies as described above.

Using Virtual IP and DNS Names

Initial user contact with iPlanet Portal Server depends on the gateway configuration and whether a multiple domain configuration exists.

For example, users may contact iPlanet Portal Server through a single gateway and domain configuration named https: / / my.sun.com. Alternatively, each domain within a multi-domain configuration may require users to use different gateway names such as:

`https://employee.sun.com` and `https://partner.sun.com`.

The following sections describe the different configurations which may be deployed.

Using One Gateway Name

This is the default configuration after installation. A user may specify which domain they would like to authenticate to by typing in a keyword after the gateway name in the URL. For example, if the gateway name is my.sun.com and there are two iPlanet Portal Server domains, *sales* and *engineering*, contact with the gateway will occur from the following URLs:

`https://my.sun.com/sales,` for sales domain users

`https://my.sun.com/engineering,` for engineering domain users

Each iPlanet Portal Server domain has an attribute “Domain URLs” which contains a list of all the possible strings which the user's may use when authenticating to a particular domain. When the user enters `http://my.sun.com/eng,` the string `my.sun.com/eng` is used to set the user's domain for that session. If there is no match for `my.sun.com/eng`, then the just the `/eng` is used to check the list. This way if the admin adds a new domain, they do not have to add the name of the gateway.

For example, if the admin wanted to add `/eng` to the list for the engineering domain, the “Domain URLs” attribute for the engineering domain would be stated as follows:

1. From the Manage Domains > <domainname>, click on the Authentication profile and locate the Domain URLs attribute.
2. In the Add text box, type:

   `/engineering`

   `/eng`
3. Click the Add button to add these domain URLs to the list window.
4. Click the Submit button to submit this change to the Profile Server.
5. When the ‘Profile Successfully Updated’ message is displayed, click the Continue button.

Multi-hosting or Multiple Gateway Names

If it is not desirable to require the user to type in their domain, the gateway can be configured to use multiple DNS names or virtual IP addresses. For example, instead of the sales employees using:

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

and your engineering employees using:

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

they would use:

`https://eng.sun.com and https://sales.sun.com.`

In order to configure the gateway for multiple DNS names or virtual IP addresses, perform the following steps.

1. Navigate to the domain of interest (engineering or sales) and click the Authentication profile link to find the Domain URLs attribute.
2. For the engineering domain add the following link:

   `eng.sun.com`

   For the sales domain, add:

   `sales.sun.com`

   To provide both choices for users, add /eng and /sales to the attributes above.
3. Click the Server Management link at the left frame of the admin console.

   If the company domain for the gateway names does not match that of the installed name for the gateway, that domain must be added to the “Cookie Domain List” attribute in the server profile.
4. Click on the Manage Server Profile link.
5. Add the company DNS domain to the “Cookie Domain List” attribute.

NOTE The DNS name added to this attribute must have at least two dots and it must start with a dot. For example, in the case of eng.sun.com, .sun.com would be added to the list of cookie domains. If the company domain is a three-part domain, .eng.sun.com would be added. The subdomain should not be included for this entry.

6. Add the gateway name to the ips.virtualhost parameter in the file `/etc/opt/SUNWips/platform.conf` on the gateway. This parameter is a space separated list of all the gateway names and IP addresses. For this example, the ips.virtualhost parameter appears as follows:

   ```
   ips.virtualhost=eng.sun.com sales.sun.com 129.122.22.33
   ```

7. Restart the gateway. This may be done through the admin console under Gateway Management or via command line as:

   `/opt/SUNWips/bin/ipsgateway start`.

Configuring the Rewriter

The Gateway's Rewriter function allows end users to browse to Intranet web pages, and also makes links and other URL references on those pages (e.g., an image's source) operate correctly.

The basic operation performed by the gateway to achieve this is to pre-pend a reference to itself for each link that it encounters. Thus, within the user's browser, an HTMl fragment such as:

```
<a href="http://mymachine.intranet.com/mypage.html>
```

could be translated by the gateway's rewriter to:

```
<ahref="https://gateway.company.com/http://mymachine.intranet.
   mypage.html>
```

Now, when the user clicks a link associated with this anchor, the browser will contact the gateway, which will then fetch the content of mypage.html from mymachine.intranet.com. Thus machines which are not normally accessible from the intranet may be browsed via the gateway's rewriting function.

The gateway uses several rules to determine what elements of a fetched HTML page will be rewritten. These rules are also referred to as *translation*. Strings starting with "/", “../”, "http" and "https" are considered to be URLs and are candidates for rewriting. If a string is considered a URL, then it must refer to a machine within a subdomain or domain that can be rewritten by the gateway. Subdomains and domains that the gateway rewrites for are determined by the entries in the list 'DNS Domains and Subdomains'. This list is also used to assign web proxies to the various subdomains and domains that are rewritten.

Additionally, the variable syntaxes of JavaScript and Java may require the administrator to specify customized rules to handle web pages on their intranet.

The following lists in the Gateway Profile page allow the administrator to specify URLs for the gateway to rewrite. This customization is necessary in several situations as:

- JavaScript can contain URLs in arbitrary locations, therefore the gateway cannot parse JavaScript and determine which elements are URLs
- Java Applet parameters are interpreted by the applets, so the syntax of the parameters is unpredictable. Hence the gateway cannot locate URLs in applet parameters without guidance.

In the examples below, assume that 'urlX' is a string that appears to the gateway to be a URL. Strings starting with "/", "../", "http" and "https" are considered to be URLs. Strings starting with any other substrings are not considered to be URLs and will not be rewritten.

Rewriting HTML Attributes

This entry contains a list of HTML attributes. The gateway will rewrite URLs in the value of these attributes.

```
<html>
<a href="some URL">some text</a>
</html>
```

By default, "some URL" will be rewritten if 'href' is in the list.

Rewriting Form Input Tags List

Each entry in this list has syntax:

```
object_of_url_with_form form_name input_or_option_name [url_pattern]
```

The url_pattern is used to match the substring before the URL in the value. If url_pattern is missing, the value is a pure URL. The gateway will rewrite the URL in input of option value if there is a match. The wild card will match any string.

Suppose the gateway receives a request with the following URL:

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

The response content is as follows:

```
<html>
<Form name=form1 method=POST action="http://some_server/demo">
<input type=text name=iplanet1 value="url1">
```

```
<input type=text name=iplanet2 value="0|234|test|url2">
<select name="iplanet3">
<option value="url3">text1</option>
<option value="url4">text1</option>
</select>
</Form>
</html>


entry                    url's to be rewritten
* * *                    url1, url3, url4


some.html * *            none
   object_of_url_with_form doesn't match the object of the requested
URL.
/some_dir/some.html * *  url1, url3, url4
*/some.html * *          url1, url3, url4
/some_dir/* * *          url1, url3, url4
* form1 *                url1, url3, url4
* form2 *                none
   form_name doesn't match the form name.
* form* *                url1, url3, url4
* * iplanet*             url1, url3, url4
* * iplanet1             url1
* * *3                   url3, url4
* * iplanet2 *|*|        none
* * iplanet* *|*|*|      url2
   *|*|*| matches 0|234|test|
```

Rewriting HTML Attributes Containing JavaScript

This entry contains a list of HTML attributes. The gateway will rewrite JavaScript in the value string of these attributes.

```
<html>
<body bgcolor="white" onLoad="surl='/index.html';" topmargin="0"
leftmargin="0">
</html>
```

The JavaScript:

```
surl='/index.html'
```

will be rewritten if 'onLoad' is in the list (the default).

Rewriting JavaScript Function Parameters

Each entry in this list has the following syntax:

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

The gateway will rewrite URLs in parameters of JavaScript functions if there is a match.

Suppose the list has 3 entries:

```
func1:y
func2:,,y,,y
func3:y,y,,y
<html>
<script language="JavaScript">
function dummy() {
    func1("url1", "url2", "url3");
    func2("url4", "url5", "url6", "url7", "url8");
    func3("url9", "url10", "url11", "url12", "url13");
}
</script>
</html>
```

The gateway will rewrite url1, url6, url8, url9, url10, url12.

Rewriting JavaScript Variables in URLs

This function contains a list of JavaScript variables. The gateway will rewrite the URL in the value assigned to the variables.

```
<html>
<script language="JavaScript">
function dummy() {
    x1="url1";
    x2="url2";
}
</script>
</html>
```

The gateway will rewrite url1, url2 if x1 and x2 if they are in the list.

Rewriting JavaScript Variables Function

This function contains a list of JavaScript variables. The gateway will wrap the value that is assigned to the variables with a function called iplanet. This function is inserted into HTML pages (if necessary) before they are sent back to the user's browser. The function indicated below programmatically determines whether, and how, to rewrite the URL.

Suppose x1 is in the list:

```
<html>
<script language="JavaScript">
function dummy() {
    x1 = "some text" + some_var + some_function();
}
</script>
</html>
```

will become:

```
<html>
<script language="JavaScript">
function dummy() {
```

```
    x1 =iplanet( "some text" + some_var + some_function());
}
function iplanet(url) {
    var gwhost = 'gateway host';
if (url.charAt(0) == '/') {
        return 'https://' + gwhost + ':443/http://server host:8080' +
 url;
    }
index = url.indexOf('http://127.0.0.1');
    if (index == 0) {
        return url;
    }
index = url.indexOf('https://127.0.0.1');
    if (index == 0) {
        return url;
    }
index = url.indexOf('http://localhost');
    if (index == 0) {
        return url;
    }
index = url.indexOf('https://localhost');
    if (index == 0) {
        return url;
    }
index = url.indexOf('https://' + gwhost + ':443/');
    if (index == 0) {
        return url;
    }
index = url.indexOf('https://' + gwhost + '/');
    if (index == 0) {
        return url;
```

```
    }
index = url.indexOf('://');
    if (index > 0) {
        return ('https://' + gwhost + ':443/redirect/' + url);
    }
return url;
}
</script>
</html>
```

Rewriting JavaScript Function Parameters in HTML

Each entry in this list has the following syntax:

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

The gateway will rewrite the HTML in the parameters of the JavaScript function if there is a match.

Suppose the list has 1 entry:

```
document.write:y
```

```
<html>
<script language="JavaScript">
function dummy() {
    document.write('<html><a href="/index.html">link</a></html>');
}
</script>
</html>
```

The gateway will rewrite the HTML embedded in the function's parameters:

```
<html><a href="/index.html">link</a></html>
```

Rewriting JavaScript Variables in HTML

This entry contains a list of JavaScript variables. The gateway will rewrite HTML in the value that is assigned to the variables.

```
<html>

<script language="JavaScript">

function dummy() {

    varHTML x = "<a
href=http://peregringo.eng.sun.com/appliance/index.html>";

}

</script>

</html>
```

The URL found in:

```
<a href=http://peregringo.eng.sun.com/appliance/index.html>
```

will be rewritten if varHTML is in the list.

Rewriting Applet Parameter Values List

Each entry in this list has this syntax:

```
object_of_appplet_url applet_class applet_parameter_name
[url_pattern]
```

If url_pattern is omitted, the value of the applet parameter is examined be a single URL, and the gateway will rewrite accordingly.

If url_pattern is included, then it contains one or more strings separated by the character that is used in the applet startup code to separate the fields of the value. If the url_pattern matches the start of the string in the specified applet parameter, then the remainder of the parameter value will be considered a URL to be rewritten.

A wildcard (*) in the url_pattern will match any string in all of the above entries.

Suppose 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>
</html>
```

Then, if the list contains this entry, the following URLs will be rewritten as noted in Table.

```
some.html iplanet.class * none         object_of_applet_url
doesn'tmatch object of the requested URL.


/some_dir/some.html iplanet.class  *   url1, url2 but not url3 or
url4, since they are embedded within strings that do not appear tobe
URLs (i.e. they do not start with "/", "http" or "https").


/some_dir/some.html iplanet2.class *   none      iplanet2.class is
not in the applet tag.
* * server* *|*|*|       url3                   *|*|*| matches
0|234|test|
```

Running In HTTP mode

The gateway runs in HTTPS mode after installation, accepting SSL connections from browsers and rejecting non-SSL connections. However, you can configure the gateway to run in HTTP mode using the following steps. The benefits of doing this are performance related since there is overhead involved in managing SSL sessions and encrypting and decrypting the SSL traffic. Eliminating these steps speeds gateway performance.

1. Log in to admin console.
2. Click 'Gateway Management' in left frame.
3. Click 'Manage Gateway Profile' in right frame.
4. Click 'Show Advanced Options' button at the bottom of the page.

5. Locate the 'Gateway Port' attribute and change to the port desired for http protocol.
6. Locate the 'Gateway Protocol' attribute and change it to http.
7. Click the 'Submit' button at the bottom of the page.
8. Click 'Server Management' in left frame.
9. Click 'Manage Server Profile' in right frame.
10. Locate the 'Gateway Port' attribute and change to the port entered in step 5.
11. Click the 'Submit' button at the bottom of the page.
12. From the terminal window, log on as root on the gateway machine.
13. Open the file: /etc/opt/SUNWips/platform.conf.
14. Locate the string 'ips.gateway.protocol' and change the value to http
15. Locate the string 'ips.gateway.port' and change it to the value of the port defined in step 5.
16. Save the file and exit the text editor.
17. From the terminal window, restart the gateway by issuing the command:

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

Configuring The Gateway Proxy

The gateway proxy is essentially a second gateway that can be run on the Server machine. When used, the gateway will send HTTP requests to the gateway proxy instead of directly to the destination host. The gateway proxy will then send the request to destination server. There are two advantages when using the gateway proxy:

- If there is a firewall between the gateway and server, the firewall needs only open one hole.
- The HTTP traffic is now secure between the gateway and the intranet even if the destination server only supports http protocol (no HTTPS).

The gateway proxy doesn't run after installation. Instead, enable the gateway proxy as follows.

1. Login to admin console.

2. Click 'Gateway Management' in left frame.
3. Click 'Manage Gateway Profile' in right frame.
4. Click 'Show Advanced Options' button at the bottom of the page.
5. Click the 'HTTP Proxy Enabled' button to enable the http proxy.
6. Click the 'HTTP Proxy Port' and change to the desired port for gateway proxy listening.
7. Click 'Submit' button.
8. Run /opt/SUNWips/bin/certadmin on the Server to create a certificate for the Gateway proxy.
9. Start the gateway proxy on the Server by typing:

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

NOTE This may be added to init.d so that the proxy will be started whenever the machine is restarted.

10. Restart the gateway by typing:

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

NOTE After changes are made to the Gateway profile, the Gateway must be restarted to cause it to read the new settings. The Gateway can be restarted from the Administration Console's Gateway Management page.

Enabling PDC

This section is described in Chapter 6, "Configuring Personal Digital Certificates (PDCs) and Encoded Devices Authentication" on page 110.

IP Address Validation

IP address validation is an attribute that can be set on or off from a check box on the Admin Console using the link Gateway Profile>Manage Gateway Profile on the admin console. With this attribute enabled, when a user logs in to iPlanet Portal Server, the gateway will store the source IP address of the client that made the login request. The source IP address of the client's subsequent requests will be compared to the IP address stored in the session. If there is a mismatch, the request will be denied.

If the client browser uses a web proxy to connect to the gateway, the source IP address will be the IP address of the web proxy, not the browser. If the web proxy is using load balancing, the source IP address may change during the user's session causing an incorrect session invalidation. Thus, for general purpose deployments, it is recommended to turn off this attribute.

HTTP Basic Authentication

HTTP basic authentication can be set from the Gateway Profile page in the Admin Console. This page is accessed from the Gateway Management link on the left frame.

Web sites may be protected with HTTP Basic Authentication, requiring visitors to enter a username and password before viewing the site (the HTTP response code is 401 and WWW-authenticate: BASIC). iPlanet Portal Server can save the username and password so that users need not re-enter their credentials when they revisit BASIC-protected web sites.

This setting does not determine whether or not a user may visit BASIC-protected sites, but only whether the credentials the user enters will be saved in the user's profile.

This setting applies to all web sites that the user is permitted to access (i.e., HTTP BASIC authentication caching can not be enabled for some sites and disabled for others).

NOTES Browsing to URLs protected by HTTP Proxy Authentication (HTTP response code 407) is not supported by iPlanet Portal Server.

Browsing to URLs served by Microsoft's Internet Information Server (IIS) protected by Windows NT challenge/response (HTTP response code 401, WWW-Authenticate: NTLM) instead of BASIC authentication is not supported.

Forward Cookie Configuration

iPlanet Portal Server utilizes a cookie to track user sessions. This cookie is forwarded to the Server when the Gateway makes HTTP requests to the Server (e.g. when the desktop servlet is called to generate the user's desktop page). Applications on the Server use the cookie to validate and identify the user using the Portal Server's APIs.

The Portal Server's cookie is not forwarded to HTTP requests made to machines other than the server, unless URLs on those machines are specified in the Forward Cookie URL List. Adding URLs to this list therefore enables servlets and CGIs to receive the Portal Server's cookie and use the APIs to identify the user.

URLs are matched using an implicit trailing wildcard. For example, the default entry in the list:

```
http://server:8080
```

causes the cookie to be forwarded to all URLs starting with "http://server:8080".

Adding:

```
http://newmachine.eng.sun.com/subdir
```

will cause the cookie to be forwarded to all URLs starting with that exact string.

NOTE For this same adding scenario, the cookie would not be forwarded to any URLs starting with "http://newmachine.eng/subdir", since this string does not start with the exact string in the forward list. To have cookies forwarded to URLs starting with this variation of the machine's name, an additional entry would have to be added to the forward list.

Similarly, the cookie would not be forwarded to URLs starting with "https://newmachine.eng.sun.com/subdir" unless an appropriate entry were added to the list.

Non-Portal Server Cookie Management

Many web sites use cookies to track and manage user sessions. When the gateway proxies requests to web sites that set cookies in the HTTP header, the gateway will either discard or pass-through those cookies in the following manner:

- discard all cookies if this attribute is set 'false'
- pass-through all cookies to the user's browser and back to the appropriate web site(s) when the user makes subsequent visits to the web site(s) if this attribute is set 'true'

This setting does not apply to the cookie used by the iPlanet Portal Server to track Portal Server user sessions. It is controlled by the 'Forward Cookie URL List' described above.

This setting applies to all web sites that the user is permitted to access (i.e., you cannot choose to discard cookies from some sites and retain cookies from others).

Chapter 9

Expanding The Portal

This chapter has the following topics:

- Adding a gateway after installation
- Adding a server after installation
- Restarting a gateway or server
- Modifying information about a gateway or a server
- Setting up multiple gateways and servers

Adding Servers and Gateways

After setting up your initial server and gateway, you can add additional gateways and servers as required by your site.

You add more gateways and servers at the Platform level of the role tree.

NOTE You must be Super Administrator to perform the tasks in this section. Domain Administrators are denied access to these tasks.

Character Restrictions on Host Names

iPlanet Portal Server has restrictions on the use of special characters in host names. The servers and gateways you add can have names consisting of the following ASCII characters:

- Characters (a-z, A-Z)
- Digits (0-9)
- Minus sign (-)
- Period (.)

Host names must not include special characters such as braces and commas.

To Add a Gateway After Installation

1. Click Gateway Management on the Administration Console menu.
2. Click Manage Gateway Profile.

   The Component Profile: Platform is displayed.
3. Scroll down to the Gateway List attribute box.
4. Type the fully qualified host name of the new gateway in the field below the attribute box.
5. Press the Add button to add the gateway.

   The new gateway uses the default platform values for gateway port number, name of platform profile, retry interval, and default domain.
6. If the added gateway is on a different domain than the iPlanet Portal Server, scroll to the Cookie Domain List window and enter the new gateway domain name in the text box.

   For example, if the new gateway host name is host1.domain1.com and the iPlanet Portal Server host name is host2.domain2.com, then domain1.com is added to the Cookie Domain List attribute.
7. Click the Add button.
8. Click Submit to create the new gateway.

   You receive a message that the profile was successfully updated.

9. The new gateway URLs must now be added to the iPlanet Portal Server so that a user could log in from the gateway. In the admin console, click Manage Domains.
10. Click the domain desired to give access to the new gateway to open its Domain, Role and Users page.
11. Click the Authentication link.
12. Scroll to the Domain URLs List window attribute and type the gateway hostname in the text box.
13. Click the Add button. Additional forms of the URL will also be added to this list as indicated by the following steps.
14. Type the IP address of the new gateway.

    For example, if the IP address is 10.0.0.1, type this value.
15. Click the Add button.
16. Type the URL in the form of gateway_hostname/gateway_domain.

    For example, if the host name is host1 and the domain name is domain1, type host1.domain1.com/domain1.com
17. Click the Add button.
18. Type the URL in the form of gateway_ipaddress/gateway_domain.

    For example, from the above indicated values, type 10.0.0.1/domain1.com
19. Click the Add button.
20. Type the URL in the form of /gateway_domain.

    For example, from the above indicate value, type /domain1.com
21. Click the Add button.
22. Click the Submit button. The message, 'Profile Successfully Updated' will be displayed.
23. Click the Continue button and repeat steps 10 through 22 for any other domains that will have access to the new gateway.
24. From the admin console home page, click the Server Management link from the left frame.
25. Select the Server name associated with the added gateway and click Restart Servers. The prompt, 'Restart request has been sent to servers' will be displayed.

26. Click the Continue button to return to the Server Management page.

To Add a Server After Installation

1. Click Server Management on the Administration Console menu.
2. Click Manage Server Profile.
3. Go to the field beneath the Server List attribute box and type the fully qualified host name of the new server.
4. Press the Add button to add the server.

   The new server uses the default platform values for server port number and protocol.
5. If the added server is on a new domain, scroll down to the Cookie Domain list window and type the new server domain name in the text box.

   For example, if the new server domain is xxx.com, and xxx.com is not on the list, add it.
6. Click the Add button.
7. Click Submit to create the new server.

   You receive a message that the profile was successfully updated.

To Restart a Gateway or Server

A gateway or server will normally not need to be restarted. However when you change a profile server in a way that does not automatically get updated in the applications, or if you have installed new class files, or if the server or gateway is not responding and thus needs restarting, you may need to use the following procedures.

To Restart a Gateway

1. Click on the Gateway Management link in the iPlanet Portal Server Services part of the menu.
2. Click the button to the left of the gateway's name, then click the Restart Gateways button.

NOTE If the checkbox does not appear next to the gateway name, either the administrator does not have permission to restart the gateway, or the server has been restarted more recently than the gateway. For the first condition, the session privileges can be checked in the:

Manage Domain>Default_Domain>AdminRole>Policy>Session

to add the gateway domains to the allow list of the get valid sessions and delete session attributes. For the second condition, restarting the server wipes out the session information stored on that server. This includes the sessions related to the gateway. Without the handle to the gateway session, the administrator cannot restart it.

To Restart a Server

1. Click on Server Management in the iPlanet Portal Server Services part of the menu.
2. Click the button to the left of the server's name, then click the Restart button.

NOTES If the checkbox does not appear, go to Manage Domain>Default_Domain> AdminRole>Policy>Platform, add the server names to the Allow list, and remove the names from the Deny list.

If you restart the server running the Administration Console, you must log in again. All users who were logged into the server before it was restarted must log in again.

Modifying Information About a Server or Gateway

Should include:

- Renaming a machine
- Changing an IP address
- Removing a server or gateway

Setting Up Multiple Gateways and Servers

Your iPlanet Portal Server platform can have multiple gateways communicating with multiple servers. Each gateway must run on a separate host machine. The iPS gateway uses a round-robin algorithm to assign one user session to one specific server.

Figure 9-1 illustrates a configuration of two gateways and three servers. Server1 has the iPlanet Portal Server profile server installed. Server2 and Server3 are configured to resolve all profile requests through Server1. G1 and G2 use the round-robin algorithm to assign client sessions to Server1, Server2, and Server3. Note that clients A, B, and C are connected using the Gateway1.com on G1, and that client D is connected using Gateway2.com on G2.

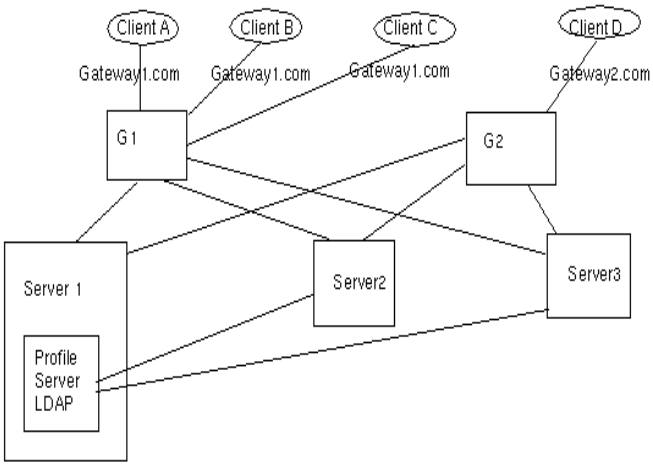

Figure 9-1 iPlanet Portal Server Platform With Multiple Gateways and Multiple Servers

Load Balancing Support in iPlanet Portal Server

If your site requires multiple gateways and servers, consider setting up load balancing and transparent clustering for your iPlanet Portal Server platform. In this scenario, multiple gateways appear to the user to be a single gateway. The iPlanet Portal Server Server supports load balancing, but requires you to configure a single server with the Profile Server for all gateways and servers to share.

To set up load balancing at your site, you must obtain third-party load balancing software. and install it on the gateway identified as the primary contact. This gateway then parcels out the user requests depending on the current load on each gateway.

How Load Balancing Works

Figure 9-2 shows a load balancer installed in front of the iPlanet Portal Server gateways. Each gateway has its own scheduler that allocates service to all four servers.

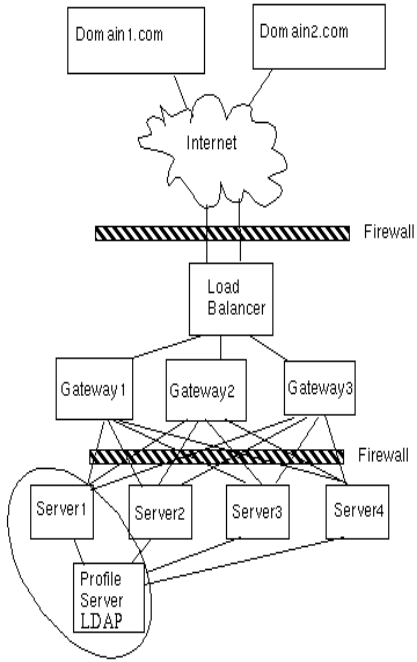

Figure 9-2 iPS Topology With Load Balancer Between Clients and Gateways

Each server in Figure 9-2 has a copy of the iPlanet Portal Serversoftware installed. Only one server is designated as the profile server. Additionally, Server1 was designated the Profile Server during installation. Whenever any server in the platform wants to know about any particular user or application privileges and attributes, it queries the Profile Server on Server1.

Pre-Configuration Issues for Multiple Gateways and Servers

When configuring multiple gateways and servers for your iPlanet Portal Server platform, you have to:

- Configure clients to allow connections to multiple gateways.
- Designate one server as the central Profile Server. When you install the iPlanet Portal Server software on all other servers and gateways of the platform, specify this server when prompted for the name of the Profile Server.
- Decide whether to implement gateway load balancing and transparent clustering.

Chapter 10

Data Logging

Logging

Figure 10-1 Logging Servers: show log files

Any application in iPlanet Portal Server that uses the Logging API can create logs and maintain history log segments. The log files are stored by default in flat files in the directory `/var/opt/SUNWips/logs`, although another location can be specified through the admin console. The product can also be configured to log data to a database. The files can not be deleted manually because the log names are stored in the Profile database.

The log files are maintained by a dedicated log server. Since it operates on the same network as other iPlanet Portal Server components, log server performance may be affected by network traffic.

Manage Logging Profile

Clicking on the Logging link on the Admin Console menu causes the Manage Logging link to appear. Beneath the link is a link for each host. Selecting a host link calls up the Logging Servers: show log files page, as shown in Figure 10-1. From this page, logs can be viewed and deleted.

NOTE Only the Super Administrator can delete logs. A Domain Administrator can only view logs when permissions are set (default). The iwtgateway logs are not viewed by the Domain Administrator.

At the top of the page a logging active or in active status is noted for this particular server. If it is not active, that doesn't mean the log files for that server don't exist, only that logging is turned off. Logging can be turned on or off for a particular server by changing the ACTIVE/INACTIVE log status attribute from the Component Profile: Logging window within the Manage Logging Profile link, as shown in Figure 10-2.

Figure 10-2 Component Profile: Logging

Viewing a Log

Figure 10-3 iwtAuthentication Log

When a particular log file link is clicked, the contents of that file are displayed in a window. For instance, Figure 10-3, shows the current contents of the Authentication log file for a particular server. For this log file, the log information displayed includes:

- Log date and time
- Client domain from where the access to portal server has been made
- Client login id (the userid specified to log in to the portal server)
- Log type (type of log message, such as Auth for authentication)
- Log message

One or all of the log files on a server can be deleted by clicking the checkbox next to the name of the log file and then clicking the Delete Selected Logs button.

Managing the Logging Profile

Clicking on the Manage Logging Profile link on the main Logging window lets you change the server's logging attributes.

Log information can be kept in either a flat ASCII file or in a database. If you want to keep a server's log information in a database, see the section below.

The attributes that you can change for a logging profile are summarized in Table 10-1:

Table 10-1 Logging Attributes

Attribute Name	What it does
DB Driver name	Class name of the JDBC driver (e.g., oracle.jdbc.driver.OracleDriver
DB Password	Password for the database user
DB User	Userid for the database user
Description	Description of the database - usually just “logging”
Log Location	Where the log files are stored in case of file based logging and connection string to connect to the database in the case of databased logging
Log Status	Logs are ACTIVE or INACTIVE for this server
Logging type	Whether logs are stored as files or in a database
Maximum Log Size	Maximum size of a log file on this server
Size of Log Read	Maximum size allowed to be read at one time
Number of Historical Files	Number of backup log files to keep

Attributes for the logging files for a server are normally inherited from the default platform settings, but can be changed to reflect the needs of a particular server. You can also delete a log file by selecting it and clicking the Delete button.

The Show and Hide Read / Write Permissions checkboxes tell you whether administrators or users are allowed to read and write the log files.

Storing Log Information in a Database

If you prefer to store the log information in a database, you can either configure a new installation to do so, or modify your current setup.

Configuring a New Installation

If you are setting up a new iPlanet Portal Server platform, you can directly indicate that log information is to be stored in a database. Follow these steps:

1. At a terminal window, open the */iPS_install_location*/netscape/server4/https-<servername>/config/jvm.conf file and add *jar_file_path* to the CLASSPATH, where *jar_file_path* is the location of the installed JDBC driver (eg: /export/tmp/OraThinDriver_v81.1.6.jar), where <servername> is the name of the machine where iPlanet Portal server has been installed.
2. Save the file.
3. At the terminal window (as root), type the following to restart the server and gateway:

/iPS_install_location/SUNWips/bin/ipsserver start

/iPS_install_location/SUNWips/bin/ipsgateway start

4. In a browser window, log in to the Admin Console. Choose the Logging option on the menu (under Portal Server Services), then click on the Manage Logging Profile link.
5. Choose the Show Advanced Options button at the bottom of the frame. The advanced options will be displayed.
6. Change the Log Location to the connection string the system can use to connect to the database, such as: jdbc:oracle:thin:@ocf8.eng:1521:orcl.

   In this case, it means that we are using *jdbc* to make the connectivity using is Oracle's thin driver, the Oracle instance name is *orcl*, this instance is running on machine ocf8.eng and the listener port is 1521.
7. Change the Logging type to JDBC.
8. Enter the name of the database driver name, in this case, the driver name is oracle.jdbc.driver.OracleDriver.
9. Enter the name of the database user you specified earlier during database installation for Database User Name, and enter the user's database password in the Database User Password field.
10. Click the Submit button. A message will display indicating that the profile was saved successfully. Click the Continue button.
11. If you have specified Log Status as ACTIVE, logging is now being sent to the database. To ensure that this is happening, look for tables with the same names as the logs.

Modifying an Existing Installation

You can modify an existing installation to send logging information to a database by following the same steps as indicated for Configuring a New Installation above. However, since the logging activity begins anew, you may wish to back up your existing data log files to a safe location prior to making this modification.

NOTE When you switch from File to DB logging, logging activities at that point forward take place in the DB, but the old logs are not transferred from File logs to DB logs.

Log Schema in the Database

For database logging, tables are created inside the database to store the logging information. There is one table of information for each log created. Therefore, there will be as many tables inside the database as there are log files created in the portal server. For example, for the iwtGateway log, a log table will appear in the database with the same name. Additionally, the internal table ips_logs is maintained with the list of all existing logs in the database.

The schema for a log file in general is as shown in Table 10-2.

Table 10-2 General Log Database File Schema

Name	Data Type
TYPE	VARCHAR2 (20)
LOGINID	VARCHAR2 (50)
DOMAIN	VARCHAR2 (100)
DATA	VARCHAR2 (300)
TIME	VARCHAR2 (200)

TYPE is the type of the log (e.g., Auth, Gateway, and so forth)

LOGINID is the login id of the client.

DOMAIN is the client domain from where the access is made.

DATA is the message to be logged.

TIME is a string representation of the date-time in yyyy/MM/dd hh:mm:ss format.

All data is stored in Unicode for I18N. The schema should not be changed and is exposed for informational purposes only.

Maintaining iPlanet Portal Server

This chapter describes:

- LDAP backup and restore
- Setting up encrypted communications between the server and the gateway
- Fixing known problems
- Troubleshooting authentication problems

LDAP Backup and Restore

To save and/or restore the current LDAP database before or after re-installing the iPlanet Portal Server product, perform the following steps for both procedures as specified.

NOTE Use absolute path names to specify directory and file names.

LDAP Backup - Procedure 1

1. From the command line, change the directory to the server installation directory:

```
cd /opt/netscape/directory4/slapd-<host name>
```

2. Run the following command to backup the LDAP database:

```
db2bak <backup directory>
```

LDAP Restore - Procedure 1

1. From the command line, change to directory to the server installation directory as shown in step 1 of "LDAP Backup - Procedure 1" on page 193.
2. Run the following command to restore the backed up LDAP database:

   ```
   bak2db <backup directory>
   ```

LDAP Backup - Procedure 2

1. From the command line, change directory as follows:

   ```
   cd /opt/netscape/directory4/slapd-<host name>
   ```

2. Run the following command to back up the LDAP database:

   ```
   db2ldif <ldif file>
   ```

LDAP Restore - Procedure 2

1. From the command line, change directory as follows:

   ```
   cd /opt/netscape/directory4/slapd-<host name>
   ```

2. Run the following command to restore the backed up LDAP database:

   ```
   ldif2db -i <ldif file>
   ```

Setting Up Encrypted Communications Between Server and Gateway

SSL service is used for encrypted communication between the end user and the iPlanet Portal Server gateway, providing greater security for the flow of information between them.

SSL service requires an SSL certificate, which authenticates the user or server. You can use the self-signed certificate created during installation, or you can request and obtain a signed certificate from a Certificate Authority. You then add this certificate to the `rp.keystore` file (the certificate database) on the iPlanet Portal Server gateway.

When you installed the iPlanet Portal Server software, the system created and installed a self-signed SSL server certificate with a default validity of 365 days. At some point after installation, you might want to generate a new self-signed certificate; for example, you might want to change the information for the certificate you entered during the original installation.

To Generate a Self-Signed SSL Certificate on the Gateway

1. Log in to the iPlanet Portal Server gateway as root.
2. Run the `certadmin` script on the iPlanet Portal Server gateway:

```
# /opt/SUNWwt/bin/certadmin
```

The Certificate Administration menu appears.

:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) List Root CA Certificates
6) Quit
choice: [6]
```

3. Type `1` to generate a self-signed certificate.

   The Certificate Administration script prompts for specific information about your organization and a pass phrase for the self-signed certificate:

```
What is the fully qualified DNS name of this host?
[hostname.domainname]
What is the name of your organization? []
What is the name of your organizational unit? []
What is the name of your City or Locality? []
What is the name of your State or Province? []
What is the two-letter country code for this unit? []
...
Enter passphrase []
```

4. Type the information for your organization and a pass phrase for the self-signed certificate.

   The script generates a self-signed certificate with a validity of 365 days and adds it to the file `/etc/opt/SUNWwt/rp.keystore` on the iPS gateway.

5. Stop and restart the reverse proxy server on the iPlanet Portal Server gateway for the certificate to take effect.

   See the procedure “To Restart a Gateway or Server,” on page 180.

6. Make a backup copy of the `rp.keystore` file.

Obtaining SSL Certificates From Vendors

After installation, you have the option to install SSL server certificates signed by vendors who provide official certificate authority (CA) services. iPlanet Portal Server software contains root certificates that can be used with SSL certificates from Verisign, Inc. If you decide to install an SSL certificate from a vendor other than Verisign, you must install a root certificate from that vendor first, and then install the web server certificate.

If you want to use an SSL certificate from a certificate vendor after you have installed the iPlanet Portal Server software, you must run the `certadmin` script to generate an SSL certificate signing request (CSR). The CSR is used to get an SSL certificate from a vendor.

Certificates are stored in the `rp.keystore` file. Once you generate a CSR, make sure you keep a backup copy of the `rp.keystore` file. This file contains your private key, which is associated with the certificate that you purchase. If you lose the file, you cannot use the certificate that you bought.

To Install SSL Certificates From Verisign

1. Log in to the iPlanet Portal Server gateway as root.
2. Run the `certadmin` script on the iPlanet Portal Server gateway:

```
# /opt/SUNWwt/bin/certadmin
```

The Certificate Administration menu appears:

:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) List Root CA Certificates
6) Quit
choice: [6]
```

3. Type 2 on the Certificate Administration menu to generate a certificate signing request (CSR). Either of the following happens:

- If no self-signed certificate exists on this machine, the Certificate Administration script notifies you that you must create one.
- If a self-signed certificate exists on this machine, the information from the certificate appears. The Certificate Administration script asks if the information is correct.

:

```
Is this information correct (y/n)? [n]
```

4. Do the either of the following:

- Type `n` if the information is not correct.

  If you type `n`, the script prompts for information for a new self-signed certificate. Fill in the information as requested.

- Type `y` if the information is correct.

  The script prompts for the name, email address, and phone number of the Web master of the machine for which the certificate is being generated:

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

5. Type the name, the email address, and the telephone number of the administrator or web master for this server.

The `certadmin` script displays the values you typed and asks if the values are correct:

```
Are these values correct (y/n)? [n]
```

6. Type `y` if the information is correct, or `n` if it is not correct.

- If you type `y`, the program generates the CSR and stores it in the file `/tmp/csr.`*hostname*.
- If you type `n`, the `certadmin` script asks you to type the values again.

7. Go to the certificate authority's web site and order your web server certificate.

a. Provide information from your CSR, as requested by the CA.

b. Provide any other information as requested by the CA, such as a pass phrase.

c. Specify your web server type as: `NES Webserver`.

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

The certificate starts with the line:

```
-----BEGIN CERTIFICATE----
```

continues with the certificate itself, and concludes with the line:

```
-----END CERTIFICATE-----
```

Make sure you include both lines with the certificate in the file.

9. Run the `certadmin` script on the iPlanet Portal Server gateway:

```
# /opt/SUNWwt/bin/certadmin
```

The Certificate Administration menu appears:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) List Root CA Certificates
6) Quit
choice: [6]
```

10. Type 4 to install your certificate from the CA.

The Certificate Administration script asks for the path name of the file containing the certificate.

:

```
What is the name (including path) of the file that contains the
certificate? []
```

11. Type the full path to the file containing the certificate from the CA.

The program stores your certificate in the file `/etc/opt/SUNWwt/rp.keystore`.

12. Stop and restart the reverse proxy server on the iPlanet Portal Server gateway for the certificate to take effect.

See the procedure "To Restart a Gateway or Server," on page 180.

13. Make a backup copy of the `rp.keystore` file for the iPlanet Portal Server gateway.

To Install SSL Root Certificates

You must have already generated a self-signed certificate to install a root certificate.

1. Go to the Certificate Authority's web site and download its root certificate.

The web site should contain instructions for downloading the certificate, usually as a file.

2. Become root on the gateway and run the `certadmin` script:

```
# /opt/SUNWwt/bin/certadmin
```

The Certificate Administration menu appears:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) List Root CA Certificates
6) Quit
choice: [6]
```

3. Type 3 to add a root certificate from the CA.

   The script asks for the path name of the file containing the root certificate you want to add to the database.

:

```
What is the name (including path) of the file that contains the
root certificate that you would like to add to your database? []
```

4. Type the full path to the file containing the root certificate.

   The file appears and the `certadmin` script asks if the information is correct.

:

```
Is this information correct (y/n)? [n]
```

5. Type y if the file is correct, or n if it is not.

- If you type y, `certadmin` stores the root certificate in the `/etc/opt/SUNWwt/rp.CAstore` file.
- If you type n, it does not add the root certificate.

To Install SSL Certificates From a Certificate Authority

1. Log in to the iPlanet Portal Server gateway as root.
2. Run the `certadmin` script on the iPlanet Portal Server gateway:

```
# /opt/SUNWwt/bin/certadmin
```

The Certificate Administration menu appears:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) List Root CA Certificates
6) Quit
choice: [6]
```

3. Type 4 on the Certificate Administration menu to install the certificate from the CA.

   The Certificate Administration script asks for the path name of the file containing the certificate:

```
What is the name (including path) of the file that contains the
certificate? []
```

4. Type the full path to the file containing the certificate.

   The program adds your certificate to the `/etc/opt/SUNWwt/rp.keystore` file.

5. Stop and restart the iPlanet Portal Server gateway for the certificate to take effect.

6. Make a backup copy of the `.rppass`, `rp.CAstore`, and `rp.keystore` files for the iPlanet Portal Server gateway. If you ever need to restore a certificate, you can copy these three files back to `/etc/opt/SUNWwt`.

7. Run the `certadmin` script on the iPlanet Portal Server gateway:

```
# /opt/SUNWwt/bin/certadmin
```

The Certificate Administration menu appears:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) List Root CA Certificates
6) Quit
choice: [6]
```

8. Type `5` on the Certificate Administration menu to display all CA certificates installed.

Configuring Encrypted Communications on the Server

1. Go to the NES administration console by typing the following URL:

`http://`*iPlanet Portal Server_server***`:8888`**

2. Type the appropriate administrative ID and password you used during installation in the popup window.

3. Click the Manage button in the frame on the right of the next window that appears.

At this point, the system may warn you that the configuration has been manually edited and the resulting changes have not been loaded. If so:

a. Dismiss the warning window.

b. Click the Apply button in the upper right corner of the screen.

If you are asked to undo the changes, choose to undo them and click Apply again.

c. Choose Load configuration files.

A popup window appears indicating that operation was successful.

d. Click OK to dismiss this window.

NOTE When given a choice, always load the configuration files. If you somehow save the current setup when none has been loaded (because the system does not load manual edits), you will overwrite the web server configuration, thus requiring that you reinstall the iPlanet Portal Server platform software. Read all the dialog boxes and be sure to choose to load the configuration files.

---

4. Select the Security tab.

The “Create a Trust Database” screen appears.

5. Type a database password (twice), and click OK to create the database.

A popup window appears indicating that operation was successful. Click OK to dismiss this window.

6. Select “Request a certificate” on the navigation bar on the left side of the screen

7. Type your email address in the “CA email address” field.

8. Type the same password In the Key Pair File Password field that you typed in step 5.

9. Type your name and telephone number and other data requested.

10. Type the fully qualified name of the iPlanet Portal Server server (such as ipsserver.eng.sun.com) in the Common Name field.

11. Click the OK button to generate a certificate signing request (CSR).

    At this point, the right frame contains your CSR. The CSR will also be mailed to the address you typed. You will need this CSR to request a certificate from the Certificate Authority (CA) you choose.

    NES has server CAs for most of the major vendors. You can view the installed server CAs, as well as any server certificates you have installed, by clicking on the Manage Certificates option in the navigation frame.

12. After you receive your certificate, click the Install Certificate button in the navigation frame

    The certificate begins with the following line:

    -----BEGIN CERTIFICATE----

    continues with the certificate itself, and ends as follows:

    -----END CERTIFICATE-----

    Make sure you include both of these lines with the certificate in the file.

13. Type your SSL pass phrase in the Key Pair File Password field,

    (Optional) If you have saved your certificate in a file, do either of the following:

- Type the file name in the Message in This File: field.
- Select the Message Text button and type the text in the text area.

14. Click the OK button to install the certificate.
15. Click the Add Server Certificate option when asked to confirm the addition of this certificate,
16. (Optional) Click Manage Certificates and verify that your certificate has been installed.
17. Dismiss the resulting popup window indicating the success of this operation.
18. Click the OK button to dismiss the warning window.

    For now, ignore the warning about stopping and starting the server.

19. Click the Preferences tab.
20. Click the Encryption On/Off option in the navigation frame on the left.
21. Type a port number in the Port Number field.

NOTE This will be 443 if you requested SSL, or 8080 otherwise, unless you have specifically picked another port number during the installation of the server.

22. Click the On button if you requested SSL to be used, during the install process.

    If a popup window asking for the server password appears, type anything for the password.

23. Click the OK button to enable encryption on the web server.

    Ignore the warning about stopping and restarting the server. The changes to the configuration are saved, but the server will not be restarted. The server need not be restarted here.

24. Choose the Save and Apply option when you see an error message confirming the changes to the configuration files

    At this point you see a message asking you to restart the web server. Do NOT restart from the administration console.

25. Go to a terminal window and type:

```
/etc/init.d/wtserver start [debug]
```

    Include the optional `debug` argument to confirm that the platform server is not running. This allows you to see two messages from NES, one confirming the startup of the administration console and the other confirming startup of the web server.

26. Verify that the port is correct and that it is running on a URL that starts `https://....` You will see an error message if the port number or URL is incorrect.

Remember to configure the gateway as directed in the *iPlanet Portal Server Installation Guide*.

Fixing Known Problems

Questions that arise during the installation, configuration, or operation of iPlanet Portal Server can include:

- Browser issues involving the Netlet application
- Platform debugging
- Authentication Problems
- Diagnosing and isolating problems related to authentication
- What resources and advice for guidance with common issues

This section provides general guidelines and suggestions for these questions.

Browser Issues Involving the Netlet

After authenticating themselves, users occasionally receive the following message from the Netlet:

```
Netlet was unable to determine your browser proxy settings.
.
.
See your network administrator for the correct setting.
```

This message appears if the user's browser has a `proxy.pac` file specified as the Proxy setting in the Preferences window. The Netlet cannot run with this setting.

To correct the problem, have the users set the proxies manually. They cannot use the automatic setup for proxies along with the Netlet.

Setting Platform Debugging

As Super Administrator, you can turn on platform-wide debugging by using the command line interface to modify value `wtdebug` in the file `/etc/opt/SUNWips/platform.conf`. By default, this value is set to off.

In order to see debugging on `stdout`, you must start the server with the command:

```
ipsserver start debug
```

To see debugging on the gateway, you must start the gateway with the command:

```
ipsgateway start debug
```

Possible values for debug are:

error=error debugging (bugs)
warning=warning debugging (also error)
message=message debugging (also error, warning for all applications)
on = all (error, warning, message) debugging to `stdout (system.out)`
off= debugging disabled

You can use wildcards for individual components only when output is to `stdout`. Debug levels are cumulative, warning displays error and warning, message displays error and warning message.

`iwtAuth*` turns on auth debugging only
`iwtNetlet*` turns on Netlet config debugging

Troubleshooting Authentication Problems

If you do not see the module that you have added as a choice on the login page, return to the Administration Console and confirm your Authentication Module settings at the platform and domain level.

NOTE If you encounter authentication problems that seem to be confined to interaction with the iPlanet Portal Server system or that prove difficult to reproduce or diagnose, use the following sections to manually start and test the authentication modules and helpers.

Modules with Helpers

The RADIUS, SafeWord, SecurID, S/Key, and UNIX authentication methods use both an iPlanet Portal Server Server authentication module and a separate helper process. These helpers communicate with their respective authentication modules over TCP ports. They accept connections originating only from the localhost, or the same system on which they are running. Once the helper successfully receives all its configuration information, it enters its normal authentication mode.

To manually test these authentication helpers, first be sure that the helper is not already running. These helpers reside in `/opt/SUNWips/bin`. For full debug logging, make sure the helper's debug log file exists, then start the helper with the -v (verbose) flag. Use the -c (port number) flag if the helper's default configuration port conflicts with some other process running on the iPlanet Portal Server Server system.

The helper's debug files are located in `/var/opt/SUNWips/debug/auth`, and are named `radius_client.debug`, `safeword_client.debug`, `securid_client.debug`, `skey_client.debug`, and `unix_client.debug`. For example, an easy way to create the RADIUS debug file is as follows:

```
# touch /var/opt/SUNWips/debug/auth/radius_client.debug
```

The SafeWord, RADIUS, UNIX, S/Key, and SecurID authentication modules also include a separate helper component with which the modules communicate over specified ports. At iPlanet Portal Server Server initialization, the helper components are brought up in listening mode on a configuration port. The respective authentication modules send configuration information retrieved from the Profile Server. After successfully receiving its configuration information, each helper component opens the port specified for its authentication requests.

Each of these authentication modules needs the following configuration attributes set before it can work properly:

- Configuration port: where the helper receives configuration information (including the remaining attributes) from its respective authentication module
- Authentication port: where the helper receives authentication requests
- Session timeout: the maximum time in minutes that an authentication request may use for completion, from submission of the authentication parameters to resolution of the request (successful or unsuccessful)
- Maximum number of concurrent authentication requests permitted for that authentication method

Other configuration information specific to each authentication method is passed during the configuration process.

Except for the Windows NT Authentication module, which uses ASCII input, all authentication modules in iPlanet Portal Server are internationalized.

After completing debug sessions and returning to production mode, remove the "-v" flag from any script used to start the helpers.

Debugging SafeWord

Starting Debugging Using the SafeWord Helper

To start the SafeWord helper, follow these steps:

1. As root, enter the following:

```
# touch /var/opt/SUNWips/debug/auth/safeword_client.debug
# /opt/SUNWips/bin/doSafeWord -v
```

2. In another terminal window, type

```
% telnet localhost 8945
```

3. The doSafeWord helper then requests the following configuration information:

```
Enter SafeWord Helper Listen Port [7945]:
Enter SafeWord Helper Session Timeout [5]:
Enter SafeWord Helper Max Sessions [5]:
Enter Domain Name:
This domain has SafeWord enabled: [y]/n:
Enter SafeWord Helper Logging Level [0]:
Enter SafeWord Helper SafeWord Servername:
<safeword_server_hostname>
Enter SafeWord Helper SafeWord Server Port [7482]:
Enter SafeWord Helper SafeWord System [STANDARD]:
Enter SafeWord Helper Log Path
[/var/opt/SUNWips/logs/safehelper/log]:
More SafeWord Servers (y/[n]):
------end if no more servers------
```

```
get_config_info: doSafeWord configured successfully
```

Press the Enter key to accept the default value, shown in brackets, or enter the value you want to use. Default values are usually sufficient for debugging purposes. However, you must supply the Domain Name and the SafeWord Servername, which is the hostname of the system where the SafeWord server resides.

4. The helper is now in normal authentication mode. It has opened port 7945 (the default) or whatever port you have specified, and is waiting for authentication requests. To test SafeWord authentication, type:

```
% telnet localhost 7945
```

The following messages are sent by the doSafeWord helper when authenticating to the SafeWord server:

```
Enter iPlanet Portal Server Domain Name:

Enter m_UserID:

ChallengeText =

InputPrompt = Enter Gold/Platinum Password:

Authentication complete, user passed -- No problems
```

or

```
Authentication complete, user failed -- Failed authentication
```

The iPlanet Portal Server Domain Name is the name entered during configuration. If multiple SafeWord servers are configured to the helper, enter the correct corresponding domain name.

The prompt for m_UserID is the same as an iPlanet Portal Server prompt for your SafeWord userid.

Gold and Platinum Passwords refer to various levels of SafeWord tokens.

Debugging SecurID

Starting Debugging Using the SecurID Helper

To start the SecurID helper, follow these steps:

1. As root, enter the following:

```
# touch /var/opt/SUNWips/debug/auth/securid_client.debug
```

```
# /opt/SUNWips/bin/doSecurid -v
```

2. In another terminal window, type:

```
% telnet localhost 8943
```

3. The doSecurID helper then requests the following configuration information:

```
Enter SecurID Helper Listen Port [7943]:
Enter SecurID Helper Session Timeout [5]:
Enter SecurID Helper Max Sessions [5]:
Enter Webtop Domain Name:
This domain has SecurID enabled? [y]/n:
Enter Config Path for Server #0 [/opt/ace/data]:
Enter User Config Path for Server #0 [/opt/ace/prog]:
More SecurID Servers (y/[n]):
get_config_info: doSecurID configured successfully
```

   Press the Enter key to accept the default value, shown in brackets, or enter the value you want to use. Default values are usually sufficient for debugging purposes.

   Since the doSecurID helper supports multiple ACE/Servers, you supply the directories where the corresponding sdconf.rec files are located. Although the User Config Path may not be used, it should be both specified and exist.

4. The helper is now in normal authentication mode. It has opened port 7943 (the default) or whatever port you have specified, and is waiting for authentication requests. Return to local control by typing:

```
% telnet localhost 7943
```

The following messages are sent by the doSecurID helper when authenticating to the SafeWord server:

```
Enter iPlanet Portal Server domain name:
Enter SecurID login:
Enter passcode:
Authentication passed
```

or

```
Access denied
```

The “iPlanet Portal Server domain name to use” is the same as enforced for this domain combination during configuration.

Debugging RADIUS

Starting Debugging Using the RADIUS Helper

To start the RADIUS helper, follow these steps:

1. As root, enter the following:

```
# touch /var/opt/SUNWips/debug/auth/radius_client.debug
# /opt/SUNWips/bin/doRadius -v
```

2. In another terminal window, type

```
% telnet localhost 8944
```

3. The doRadius helper then requests the following configuration information (default values are shown in brackets):

```
Enter Radius Helper Listen Port [7944]:
Enter Radius Helper Session Timeout [5]:
Enter Radius Helper Max Sessions [5]:
get_config_info: doRadius configured successfully
```

   You can press the Enter key at each prompt to use the default value, or you can supply your own values. The default values are usually sufficient for debugging purposes.

4. The helper is now in normal authentication mode. It has opened port 7944 (the default) or whatever port you have specified, and is waiting for authentication requests. To test RADIUS authentication, type:

```
% telnet localhost 7944
```

5. The doRadius helper sends the following messages when authenticating to a RADIUS server:

```
Enter Radius login:
Enter password:
Enter server 1:
Enter server 2:
Enter shared secret:
```

```
Enter server port:
Authentication passed
```

or

```
Access denied for userid ...
```

You must supply the appropriate login, password, name for server 1, and shared secret. Supplying a name for server 2 is optional; press Enter to skip server 2. Note that if two RADIUS servers are specified, the shared secret is still the same. Press Return to use the default RADIUS server port (1645).

6. The doRadius helper sends the following messages when authenticating to a SafeWord RADIUS server:

```
Enter Radius login:
Enter password:
Enter server 1:
Enter server 2:
Enter shared secret:
Enter server port:
CHALLENGE_MSG:
Enter Challenge Response:
Access challenge passed
```

or

```
Access challenge failed for userid ...
```

7. The doRadius helper sends the following messages when authenticating to an ACE/Server RADIUS server:

```
Enter Radius login:
Enter password:
Enter server 1:
Enter server 2:
Enter shared secret:
Enter server port:
Authentication passed
```

or

```
Access denied for userid ...
```

8. The doRadius helper sends the following messages when authenticating to an ACE/Server RADIUS server in an authentication session that includes “next token mode”:

```
Enter Radius login:

Enter password:

Enter server 1:

Enter server 2:

Enter shared secret:

Enter server port:

CHALLENGE_MSG: (Wait for the tokencode to change, then enter the new
tokencode)

Enter Challenge Response:

Access challenge passed
```

or

```
Access challenge failed for userid ...
```

9. The doRadius helper sends the following messages when authenticating to an ACE/Server RADIUS server in an authentication session that includes “new PIN mode”:

```
Enter Radius login:

Enter password:

Enter server 1:

Enter server 2:

Enter shared secret:

Enter server port:

CHALLENGE_MSG: A new PIN is required. Do you want the system to
generate your new PIN? (y/n):

Enter Challenge Response: (enter N)

CHALLENGE_MSG: Enter a new PIN between 4 to 8 digits:

Enter Challenge Response:

CHALLENGE_MSG: PIN accepted. Wait for the tokencode to change, then
enter the new tokencode:

Enter Challenge Response:
```

```
Access challenge passed
```

or

```
Access challenge failed for userid ...
```

The challenge messages for new PIN generation may vary, depending upon how the user is configured in the ACE/server.

Debugging Windows NT Primary Domain Controller

Configuring Windows NT Aliases

The `iwtAuthNT-authAliases` attribute is set on a per user basis through the Administration Console.

Manually Testing Windows NT Authentication

You can manually check if NT authentication is working from your iPlanet Portal Server by typing:

`#/opt/SUNWips/bin/smbclient -w` <*workgroup*> `-l` <*host*> `-u` <*username*>

%<*password*>

where you substitute the appropriate values for workgroup, host, username, and password. Make sure you have installed third party packages.

Debugging UNIX

Starting Debugging Using the UNIX Helper

To start the UNIX helper, follow these steps:

1. As root, enter the following:

```
# touch /var/opt/SUNWips/debug/auth/unix_client.debug
# /opt/SUNWips/bin/doUNIX -v
```

2. In another terminal window, type:

```
% telnet localhost 8946
```

3. The doUNIX helper then requests the following configuration information (default values are shown in brackets):

```
Enter UNIX Helper Listen Port [7946]:

Enter UNIX Helper Session Timeout [5]:

Enter UNIX Helper Max Sessions [5]:

get_config_info: doUNIX configured successfully
```

Press the Enter key at each prompt to use the default value, or supply your own values. The default values are usually sufficient for debugging purposes.

4. The helper is now in normal authentication mode. It has opened port 7946 (the default) or whatever port you have specified, and is waiting for authentication requests. To test UNIX authentication, type:

```
% telnet localhost 7946
```

5. The following messages are sent by the doUNIX helper when authenticating to a UNIX server:

```
Enter UNIX login:

Enter password:

Authentication passed
```

or

```
Access denied for userid xxx, return = dd
```

Debugging S/Key

Starting Debugging Using the S/Key Helper

To start the S/Key helper, follow these steps:

1. As root, enter the following:

```
# touch /var/opt/SUNWips/debug/auth/skey_client.debug

# /opt/SUNWips/bin/doSKey -v
```

2. In another terminal window, type

```
% telnet localhost 8947
```

3. The doS/Key helper then requests the following configuration information (default values are shown in brackets):

```
Enter S/Key Helper Listen Port [7947]:

Enter S/Key Helper Session Timeout [5]:

Enter S/Key Helper Max Sessions [5]:

get_config_info: doSKey configured successfully
```

Press the Enter key at each prompt to use the default value, or supply your own values. The default values are usually sufficient for debugging purposes.

4. The helper is now in normal authentication mode. It has opened port 7947 (the default) or whatever port you have specified, and is waiting for authentication requests. To test S/Key authentication, type:

```
% telnet localhost 7947
```

5. The following messages are sent by the doSKey helper when authenticating to a S/Key server:

```
Enter SKey UUID:

Enter PIN:

Enter passphrase number dd::

Authentication successful for UUID xxxxx, UNIX UserID xxxx
```

or

```
Authentication unsuccessful for UUID xxxxx
```

or

```
Authentication failed (UUID or PIN does not match)
```

Remember that the passphrases are case-sensitive and always all uppercase.

Administering the Firewall Application

This chapter describes the following:

- How the iPlanet Portal Server firewall application works
- How to configure and administer the iPlanet Portal Server firewall application using the command line

iPlanet Portal Server Firewall Application

In most iPlanet Portal Server applications, a separate firewall is used to restrict external access to the iPlanet Portal Server gateway to traffic on TCP Port 443, or to the port you have configured to carry SSL traffic.

For situations in which an external firewall does not exist, iPlanet Portal Server provides the option of installing an internal firewall, which offers limited configuration options. If you want greater control over the ports and traffic than this firewall application provides, you must install a firewall product like Sun Microsystems' SunScreen EFS.

If you choose not to install the iPlanet Portal Server firewall application, make sure that you configure your existing firewall to restrict external access (access from the Internet) to the iPlanet Portal Server gateway to the SSL port only (port 443 by default), while leaving full access to the iPlanet Portal Server gateway from all machines and all ports on the internal or private network. This assumes that everyone logging in from the Internet to have access to iPlanet Portal Server.

NOTE Port 443 is the usual default port for SSL traffic, and the instructions throughout this chapter assume that you selected port 443 for SSL traffic.

How the Firewall Works

The iPlanet Portal Server firewall application uses proven Sun Microsystems' firewall technology to protect your network with dynamic packet filtering.

Dynamic packet filtering means that firewall examines each packet as it arrives. Based on information in the packet, the state retained from previous events, and a set of rules that implement the security policy for access control, the firewall passes the packet from one network to another (that is, from the Internet to your intranet) or drops it.

The iPlanet Portal Server firewall application uses a set of *ordered rules* to filter packets. When you configure the iPlanet Portal Server firewall application, you translate the security policies for this product into a series of rules that specify which services are to be allowed, what to do with packets for services that are disallowed, and what to do when packets are dropped. You then place these rules in sequence to specify which rules override others.

When the iPlanet Portal Server firewall application receives a packet, it tests the packet against the rules in order. The firewall does not test each packet against each rule; it assumes that the first rule to match the service, source address, or destination address of the packet is the rule that controls the packet. Depending on the settings in the applicable rule, the firewall passes or drops the packet. If the packet does not match any rule that specifically allows it to pass, the firewall drops it.

Configuring the iPlanet Portal Server Firewall Application

The firewall application is the only application in the iPlanet Portal Server software that you configure and administer solely through the command-line user interface. It uses a special version of Sun Microsystems' proven firewall technology.

The `fw.configure` command is the command used to install and minimally configure the firewall application. You usually run this command as part of the installation procedure on the iPlanet Portal Server gateway.

NOTE The commands for the iPlanet Portal Server firewall application are located in `/opt/SUNWsrfw/bin`.

To Configure the iPlanet Portal Server Firewall Application

1. As root, run the following command on the iPlanet Portal Server gateway to bootstrap the firewall to a point where it can filter network packets:

```
# fw.configure
```

2. Respond to the questions to activate and minimally configure the firewall.

   The `fw.configure` process initializes the firewall application.

3. Add or change rules as necessary to configure your firewall fully.

   By default, only packets coming from the external iPlanet Portal Server gateway interface are examined and few rules are installed. `fw.configure` installs the following three default rules that:

   a. Allow external access from the iPlanet Portal Server gateway's Internet interface to the SSL port. (The default port number is 443.)

   b. Allow the iPlanet Portal Server gateway access to anywhere.

   c. Allow routing information from the Internet interface on the iPlanet Portal Server gateway to be updated.

   Everything that is not expressly allowed in these rules is denied.

4. Reboot the iPlanet Portal Server gateway after the command `fw.configure` finishes running for the rules to take effect.

Administering the iPlanet Portal Server Firewall Application

You must administer the firewall application as root (superuser). You administer the iPlanet Portal Server firewall application only from the command-line user interface. There are only four commands used to administer the firewall application:

- `fw.activate`

- `fw.address`
- `fw.rule`
- fw.services

Using `fw.activate` to turn on firewall

This command turns the firewall application off or on. Turning the firewall application off means that it is no longer filtering inbound and outbound packets. Turning the firewall application on reactivates the rules that were active before it was turned off.

1. As root, type the following to turn the firewall application off:

```
# fw.activate off
```

2. As root, type the following to turn the firewall application on:

```
# fw.activate on
```

Using `fw.address` to change address

This command manipulates address definitions that the firewall application's packet filtering rules use. Use this command to:

- Add the IP address for a machine that is located on the Internet. When you add an IP address, you name it; *e.g.*, `sales_office_boston`. You can also include a descriptive comment for the address that you are defining.
- Add a range of IP addresses for machines that are located on the Internet. You only need to specify the beginning IP address and the ending IP address of the range. You name this range when you define it. You can also include a descriptive comment for the range of addresses that you are defining.
- Add a list of IP address that consists of host addresses, ranges of addresses, and other address lists.

- Delete an address by IP address or by name from the address file.
- List a particular address by name or all the address that are currently defined in the address file.

Address Management

The firewall application identifies network elements—networks, subnetworks, and individual hosts—by mapping a named *address object* to one or more addresses. These address objects are used in defining the firewall application's network interfaces and as a source and destination addresses for rules. An address object can represent a single computer or a whole network. You can gather address objects representing individual and network addresses together to form address groups. The firewall application lets you define address objects that specifically include or exclude other address objects (single IP hosts and ranges of contiguous IP addresses).

Individual IP Addresses

The firewall application identifies an individual host by linking its unique IP address to an address object, which can use the name or IP address of the host.

- To add an address, as root type the following. For example:

```
# fw.address add myhost HOST 1.1.1.1 "An example of an added \
address named myhost"
```

Address Ranges

An address range is a set of numerically contiguous IP addresses. Networks and subnetworks are typically identified by an address range name. Use the beginning and ending addresses to identify an IP address range.

- To add a range of addresses, as root, type the following to add a range of addresses. For example:

```
# fw.address add mynet RANGE 1.1.1.1 1.1.1.5 "An example of a \
range of address named mynet"
```

The range represents all the addresses inclusive between the address 1.1.1.1 and 1.1.1.5. It is named mynet.

- To delete an address or a range of addresses that you have named myhome, for example, as root type the following:

```
# fw.address delete myhome
```

- To list an address, as root, type the following to list a single name of an address or a range of addresses, for example:

```
# fw.address list myhome
```

The address range currently defined as myhome is listed.

- To list all addresses, as root, type the following to list all addresses currently defined:

```
# fw.address list
```

All addresses currently defined are listed.

Using `fw.rule` for packet filtering

This command uses various options to manipulate the firewall application's packet filtering rules. You can change the action, service, or both by writing new rules, deleting old rules, and moving rules to the position that you want. Use `fw.rule` to:

- Add a rule with a new action (ALLOW or DENY) or a different service or both. ALLOW means permit the packet that meets the qualifications in the rule through. DENY means reject the packet. You also add new port numbers with this command.
- Delete a rule from the list of rules.
- List the ordered rules governing the firewall application or to list the interface that the firewall application is using.
- Move a rule from one position to another in the ordered list of rules, thus changing the order in which it will take effect.

Rules

The configurations for the basic firewall application are based on sets of *ordered* rules. The default rules that are installed with the basic firewall establish a security policy that works well with iPlanet Portal Server. These rules specify the action to be taken for services between two addresses that are on different interfaces of the firewall.

- To list the rules, as root, type the following to list the rules:

```
# fw.rule list rule
```

The rules (in this case, the default rules) are listed in the order in which they examine incoming packets.

```
1 ALLOW "ssl" from "le0" to "localhost"
2 ALLOW "common services" from "localhost" to "*"
3 ALLOW "rip" from "*" to "*"
```

- To add a rule, as root, type the following:

```
# fw.rule add ALLOW service from host to host
```

This rule lets you add a service from a named remote host to a local host. Use the `list` option to see the new list of rules.

- To delete a rule, as root, type the following:

```
# fw.rule delete 4
```

Rule number 4 is deleted. Use the list option to see the new list of rules.

- To move a rule, as root, type the following:

```
# fw.rule move 5 4
```

Rules 5 and 4 are reordered. Use the list option to see the new ordering.

Using `fw.services` supplied

The basic firewall application is shipped with a number of predefined network *services*, such `ftp`, `telnet`, `dns`, and `rsh`, as well as predefined service groups.

Standard Services

Besides the basic services, every TCP/IP implementation provides services such as `echo`, `discard`, `daytime`, `charge`, and `time`. Each service use a state engine, a sort of protocol checker. For example, the FTP state engine checks port numbers when the `ftp` service is being used.

Service Groups

In addition to the basics services, the basic firewall application is shipped with predefined service group. One such group is `common services`, which consists of `tcp` traffic on port 0 to 3850 or port 3855 to 65535, `udp` traffic on all ports, `syslog`, `dns`, `rpc`, `nfs`, `icmp`, `route`, `ftp`, `rsh`, `real audio`, `pmap udp all`, `nis`, `archie`, `traceroute`, and `ping`.

- To list all services, type the following:

```
# fw.services list
```

  Use this command with the option `list service` to list the available services and with the option `list interface` to list the interface that the firewall application is using.

- To list the services with the service name, type the following:

```
# fw.services list servicename
```

- To delete the service with the service name, type the following:

```
# fw.services delete servicename
```

- To add a port, as root, type the following:

```
# fw.services add NAME protocol port-number
```

This command adds the service name using the protocol named on the port number specified. For example:

```
# fw.services add MYSERVER TCP 30000
```

adds a new TCP service on port 30000 of MYSERVER.

Firewall Troubleshooting

To avoid problems in configuring and using the iPlanet Portal Server firewall application, follow these suggestions:

- Do not run the command `fw.configure` through the public interface.
- Run the command `fw.rule list interface` to see which network interface is currently enabled or is controlled by the iPlanet Portal Server firewall application.
- Run the command `fw.rule list rule` to display a list of the current filtering rules.
- If you are completely locked out, try one of the following:
  - Run the command `fw.activate off` to turn the iPlanet Portal Server firewall application off (which means that it is no longer working and that all traffic can pass through it unfiltered.)
  - Run the command `fw.rule add ALLOW “common services” from ALL to ALL` to allow all traffic to pass through it.
- With regard to the firewall application, *disabled* means that the firewall will pass all traffic through it unfiltered.

Appendix B

iPlanet Portal Server Attributes

The following tables represent attribute names and descriptions for the indicated component in the table title.

Platform-wide Authentication Attributes

Table B-1, lists the attributes that are platform-wide. You find them by clicking the Manage Platform Settings link on the iPlanet Portal Server page, then the Profiles->Authentication link on the right side of the window. No platform-wide attributes can be overridden at the domain or role level.

Table B-1 Platform-wide Authentication Attributes

Attribute	What it does
UNIX Configuration Port	Port on which the UNIX authentication helper receives its configuration information. Must also be specified in the UNIX helper.port `/etc/opt/SUNWips/platform.conf`.
UNIX Helper's Port	Port on which the UNIX authentication helper listens for UNIX authentication requests.
UNIX Timeout	Number of minutes a UNIX authentication request has to finish a given authentication session.
UNIX Threads	Maximum number of concurrent UNIX authentication requests permitted.

Table B-1 Platform-wide Authentication Attributes *(Continued)*

Attribute	What it does
RADIUS Configuration Port	Port on which the RADIUS authentication helper receives its configuration information. Must also be specified in the radiusHelper.port entry in `/etc/opt/SUNWips/platform.conf`.
RADIUS Helper's Port	Port on which the RADIUS authentication helper listens for RADIUS authentication requests.
RADIUS Timeout	Number of minutes a RADIUS authentication request has to finish a given authentication session.
RADIUS Threads	Maximum number of concurrent RADIUS authentication requests permitted.
S/Key Maximum Passphrases Allows	A hard maximum on the number of S/Key passphrases that can be generated at one time (400 per user).
S/Key Configuration Port	Port on which the S/Key authentication helper receives its configuration information. Must also be specified in the skeyHelper.port entry in `/etc/opt/SUNWips/platform.conf`.
S/Key Helper's Port	Port on which the S/Key authentication helper listens for S/Key authentication requests.
S/Key Timeout	Number of minutes an S/Key authentication request has to finish a given authentication session.
S/Key Threads	Number of concurrent authentication requests permitted.
SecurID Configuration Port	Port on which the SecurID authentication helper receives its configuration information. Must also be specified in the securidHelper.port entry in `/etc/opt/SUNWips/platform.conf`.
SecurID Helper's Port	Port on which the SecurID authentication helper listens for SecurID authentication requests.
SecurID Time-out	Number of minutes a SecurID authentication request has to finish a given authentication session.
SecurID Threads	Maximum number of concurrent authentication requests permitted.

Table B-1 Platform-wide Authentication Attributes *(Continued)*

Attribute	What it does
SafeWord Configuration Port	Port on which the SafeWord authentication receives its configuration information. Must also be specified in the safewordHelper.port entry in `/etc/opt/SUNWips/platform.conf`.
SafeWord Helper's Port	Port on which the SafeWord authentication helper listens for SafeWord authentication requests.
SafeWord Timeout	Number of minutes a SafeWord authentication request has to finish a given authentication session.
SafeWord Threads	Maximum number of concurrent authentication requests permitted.

Super Administrator Authentication Attributes

Table B-2 lists authentication attributes for the Super Administrator profile. These may be found by clicking the links in the order specified:

- Manage Administrators> (*domain of interest*)
- Admin Role (under Super Admins)
- Authentication.
- Click the Show Advanced Options button at the bottom.

Table B-2 Super Administrator Role Authentication Attributes

Attribute	What it does
Admin authentication	Specifies type of authentication being used by Super Administrator.
Authentication modules	Specifies location of class file corresponding to each authentication module.
Default user role	Default role used for a new user. When a user authenticates but does not have a user profile, this is the role they are assigned. Note that this assumes that iwtAuth-requiresProfile is set to false.
Domain URLs	List of URLs a user may use to login to the default iPS domain.

Table B-2 Super Administrator Role Authentication Attributes *(Continued)*

Attribute	What it does
Pluggable authentication page generator class	Class used by pluggable authentication modules to generate authentication screens.
Authentication Requires Profile	Specifies whether a profile for a user is required to login.

Domain Level Authentication Attributes

Some of the authentication attributes are set only at the domain level. B-3 lists the attributes that are domain-wide. Domain-wide attributes, can be customized by either a Domain Administrator or the Super Administrator.

The links used to get to the domain-wide authentication attributes depend upon whether you are a Super Administrator or a Domain Administrator.

If you are a Super Administrator:

1. Click Manage Domains.
2. Click the domain name.
3. Click the Authentication link (under Profiles).

If you are a Domain Administrator:

1. Select Manage Roles and Users.
2. Select the proper Authentication module.
3. Change the attributes as needed.

Table B-3 Domain-wide Authentication Attributes

Attribute	What it does	Comment
Authentication Requires Profile	Requires a user profile to authenticate; may be used to deny access to users who do not already have profiles set.	Authentication Profile

Table B-3 Domain-wide Authentication Attributes *(Continued)*

Attribute	What it does	Comment
Prompt for userid before authentication	Any user trying to authenticate from a specific domain gets the authenticators configured for that domain. You may instead want to ask for a userid and look up the profile for the user's authentication type(s).	Advanced Option of User Profile
Authentication Menu	Shows (highlighted) the modules enabled for this domain.	Authentication Profile
Trusted proxy feature	Enable or disable trusted proxy feature for a user.	Advanced Options of Platform Profile
URL matching domain	List of strings a user may use to signal authentication which domain they are authenticating to.	Authentication Profile
Default user role	When a user authenticates but does not have a user profile, this is the role they are assigned to.	Authentication Profile
RADIUS Server1	First RADIUS server (hostname or IP address) for this domain.	Radius Profile (under Authentication branch)
RADIUS Server2	Second RADIUS server (hostname or IP address) for this domain. Contacted if RADIUS Server1 does not answer. Optional.	Radius Profile (under Authentication branch)
RADIUS Shared Secret	The RADIUS shared secret assigned to the iPlanet Portal Server Server (also configured in the RADIUS server).	Radius Profile (under Authentication branch)
RADIUS Server's Port	The port that the RADIUS Server uses to listen for authentication requests. The most common is 1645 (default), followed by 1812.	Radius Profile (under Authentication branch)
SafeWord Logging Level	The SafeWord logging level (default 0 [none]). Other values: 1 (INFO), 2(ERROR), 4 (DEBUG), 5 (ALL)	SafeWord Profile under Authentication Branch

Table B-3 Domain-wide Authentication Attributes *(Continued)*

Attribute	What it does	Comment
SafeWord Log Path	The SafeWord log path. Default is /var/opt/SUNWips/debug/auth/safehelper.log, if logging level is non-zero.	SafeWord Profile under Authentication Branch
SafeWord Server Identifier	An index indicating which SafeWord server to use for this domain. Set by the system during configuration time.	SafeWord Profile under Authentication Branch
SafeWord Server Hostname	Host name of the SafeWord server serving this domain.	SafeWord Profile under Authentication Branch
SafeWord Server's Port	The port on which the SafeWord server listens (default 7482).	SafeWord Profile under Authentication Branch
SafeWord System Name	The SafeWord System Name (default STANDARD).	SafeWord Profile under Authentication Branch
SecurID User Configuration Path	Path for the ACE/Client API to find the user configuration information (default /opt/ace/prog).	SecurID Profile under Authentication Branch
SecurID Server Identifier (Local)	An index indicating which ACE/Server to use for this domain. Set during configuration time.	SecurID Profile under Authentication Branch
SecurID Server Identifier Name	Name to associate with the SecurID Server Identifier (default Server000).	SecurID Profile under Authentication Branch
SecurID Server's Configuration Path	Path for the ACE/Client API to find the ACE/Server configuration file, sdconf.rec (default /opt/ace/data).	SecurID Profile under Authentication Branch
S/Key Maximum Passphrases to Generate	The maximum number of S/Key passphrases this user may create (default 100).	S/Key Profile under Authentication Branch
User's default URL	When a user is authenticated, they are redirected to this page. The default is the iPlanet Portal Server desktop.	Advanced Options in User Profile.

Table B-3 Domain-wide Authentication Attributes *(Continued)*

Attribute	What it does	Comment
User login state	Allows you to prevent a specific user from authenticating. Note that if a user already has a valid session, changing this attribute will not take effect until the next session. To kick the user off now, go to Manage Sessions in the menu side of the Administration Console and destroy the session.	User Profile
LDAP DN to start search	LDAP Distinguished Name. For example, for sun.com: dc=sun, dc=com	Ldap Profile under Authentication Branch
LDAP DN for root user bind	See the section, *Configuring LDAP Authentication*.	Ldap Profile under Authentication Branch
LDAP Password for root user bind	See the section, *Configuring LDAP Authentication*.	Ldap Profile under Authentication Branch
LDAP Search filter for userId	See the section, *Configuring LDAP Authentication*.	Ldap Profile under Authentication Branch
LDAP scope for the userId search	See the section, *Configuring LDAP Authentication*.	Ldap Profile under Authentication Branch
Enable SSL to LDAP server	See the section, *Configuring LDAP Authentication*.	Ldap Profile under Authentication Branch
Windows NT Primary domain	Name of the NT primary domain	NT Profile under Authentication Branch
Windows NT Authentication server	Listener of the NT authentication server.	NT Profile under Authentication Branch

Appendix C

iPlanet Portal Server 3.0 Third-Party Software CD-ROM

This appendix describes the third-party applications available on the iPlanet Portal Server Third Party CD labeled, “Contains 3rd Party Software Only.” The next sections include procedures for installing and configuring the following third party applications:

- Samba client for NetFile’s connections to Samba file servers
- GO-Joe server-side software
- pcANYWHERE PC-based software

NOTE There is no server-side component for Citrix servers. The Citrix applet connects directly to Citrix-enabled machines.

Samba

Samba is an open source software suite that provides seamless file services to SMB/CIGs clients. If you want to allow end users access to Microsoft Windows networks through the NetFile applet or NetFile Lite (HTML) client), you must install the Samba client on the iPlanet Portal Server. For more information about Samba, see the URL:

`http://us1.samba.org/samba/about.html`

iPlanet Portal Server supports Samba version 2.0.4.

To Install Samba Software

1. Mount the iPlanet Portal Server CD-ROM, “Contains 3rd Party Software Packages Only.”
2. Become root on the iPlanet Portal Server.
3. Change to the directory on the CD-ROM:

```
# cd /cdrom/cdrom0
```

4. Run the `install_3ps` script.

```
# install_3ps
```

   This adds the package `SUNWsrsmb` to the iPlanet Portal Server platform server.

5. Eject the CD-ROM:

```
# cd /
# eject dcrom0
```

   Any process started when the current working directory is `/cdrom/cdrom0` must be stopped before you can eject the CD-ROM.

GO-Joe

GO-Joe is a thin client X server for all Java-enabled displays. It provides access to UNIX/X without software rewriting or a fat X server on the desktop. It is available from the GraphOn Corporation.

After you have installed the GO-Joe server software, you can control a desktop UNIX machine remotely over the Internet. You can find more information on GO-Joe at the URL:

`http://www.graphon.com/`

Five licenses are included in the package that is supplied. If you want more than five licenses or have any question about the licensing, you must contact the GraphOn Corporation.

NOTE You must purchase a copy of GO-Joe for each desktop that you want to control remotely with more than five users.

GO-Joe consists of a client-side and server-side component. The client-side component is an applet that iPlanet Portal Server downloads through a pre-configured Netlet rule. The applet is installed on the iPlanet Portal Server when you install iPlanet Portal Server 3.0. The Netlet is also pre-configured to proxy connections from the applet to target machines running Solaris. The target Solaris machines must have the `SUNWgjvxs` package installed on them to be controlled by the applet.

iPlanet Portal Server end users are given access to Solaris machines through the Netlet provider on the iPlanet Portal Server Desktop. To add Solaris machines to a user's list, you edit the user's Netlet targets. Or, the users can add Solaris machines by editing the Netlet provider window.

Installing GO-Joe on the Machine You Want to Control

If your end users want to have remote X-Window control of a machine, you or they must install the package `SUNWgjvxs` from the iPlanet Portal Server Third Party CD-ROM on the machines that they want to control.

To Add the `SUNWgjvxs` Package

1. Mount the iPlanet Portal Server CD-ROM, "Contains 3rd Party Software Packages Only," on the machine that you want to control remotely.
2. Become root and go to the directory on the CD-ROM for your OS:

```
#cd /cdrom/cdrom0
```

3. Add the package `SUNWgjvxs`:

```
#pkgadd -d . SUNWgjvxs
```

4. Eject the CD-ROM:

```
# cd /
# eject cdrom0
```

You must stop any process started when the current working directory is `/cdrom/cdrom0` before you can eject the CD_ROM.

Using GO-Joe With Browsers

GO-Joe has no known problems with Netscape. Internet Explorer may hang if you are using it with GO-Joe. The following procedure may prevent this difficulty.

To Use GO-Joe With Internet Explorer

1. Press the Tab key until you reach the Start Session button.
2. Press Space bar, Enter key, or click the Start Session button.

NOTE More recent versions of Internet Explorer may not have this problem.

By default, the startup file for the GO-Joe client sets the virtual display size to 100 percent of the width and height of the browser when end users start the applet.

Because the browser's resolution size for the virtuality display has already been negotiated with the window server, resizing the window will not help.

End users should set the fonts for the window manager to a small font size, if they use this feature often from systems that have lower resolutions so as not to limit the screen real estate in which to operate.

pcANYWHERE

Symantec's pcANYWHERE provides fast, easy access to office PCs from remote locations. After you have installed pcANYWHERE on an office system, you can control that system remotely from the Internet.

pcANYWHERE consists of a client-side component and a PC-based component. The client-side component is an applet that iPlanet Portal Server downloads through a pre-configured Netlet rule. The applet is installed on the iPlanet Portal Server when you install iPlanet Portal Server 3.0. The Netlet is also pre-configured to proxy connections from the applet to target PCs. The target PCs must have the PC side component installed on them to be controlled by the applet.

iPlanet Portal Server end users are given access for PCs through the Netlet provider on the iPlanet Portal Server Desktop. To add PCs to a user's list, you edit the user's Netlet targets. Or, the users can add PCs by editing the Netlet provider window.

An evaluation version of pcANYWHERE 32 version 8.0 software for PCs is included in the iPlanet Portal Server software distribution on the "Contains 3rd Party Software Only" CD. You can purchase the full version from Symantec or through commercial software dealers, and can find more information on pcANYWHERE at the URL `http://www.symantec.com/pcANYWHERE`.

NOTE If you want to use pcANYWHERE after the trial version on the CD expires, you must purchase a copy of pcANYWHERE for each desktop that you want to control remotely.

To install the Trial Version of pcANYWHERE on the CD

The iPlanet Portal Server third part CD includes a 30-day trial version of pcANYWHERE.

1. Insert the iPlanet Portal Server CD-ROM "Contains 3rd Party Software Only" in the CD-ROM drive of the computer to be controlled remotely.
2. Follow the instructions given by the pcANYWHERE wizard.

To Configure the Trial Version of pcANYWHERE

Follow the procedure below to configure the trial version of pcANYWHERE.

1. Restart your computer.

2. Choose Start | Programs | pcANYWHERE32 | pcANYWHERE.

   pcANYWHERE starts.

3. Click the I Agree button to accept the evaluation license agreement.pcANYWHERE Evaluation Agreement

4. Click Cancel to exit from the Smart Setup Wizard.

   The Smart Setup Wizard starts when you first run pcANYWHERE and configures items that are not necessary to run pcANYWHERE with the iPlanet Portal Server product.

5. Choose Quick Start | Add Be a Host PC Item shown in Figure C-1.

   The Quick Start wizard walks you through the configuration steps.

Figure C-1 Quick Start with Add Be a Host PC Item

6. Provide a name (for example, iPlanet Portal Server) for the connection as shown in Figure C-2 and click Next.

Figure C-2 Provide a Name for the Connection

7. Select TCP / IP for the connection device shown in Figure C-3 and click Next.

Figure C-3 Specify TCP / IP for the Connection Device

You *must* select TCP / IP from the drop down list to use pcANYWHERE with iPlanet Portal Server.

8. Click Finish as shown in Figure C-4 to complete the pcANYWHERE Wizard.

Figure C-4 Last Screen of the Quick Start Wizard

CAUTION Do **NOT** check the option "Automatically launch after wizard."

The installation program returns you to the pcANYWHERE Main Window. You now must configure the properties for iPlanet Portal Server.

9. Right-click the iPlanet Portal Server icon, and choose Properties from the pop-up menu.

CAUTION Do **NOT** double-click the iPlanet Portal Server icon.

The iPlanet Portal Server Properties window appears, as shown in Figure C-5.

Figure C-5 iPlanet Portal Server Properties Window

10. Verify that TCP/IP is checked and highlighted in the Device List.

If it is not checked and highlighted, click the box before TCP/IP to check and highlight it.

11. Click the Settings tab at the top of the iPlanet Portal Server Properties window to move to the next set of options.

12. Configure the Settings shown in Figure C-6 according to the table belowTable C-1.

Figure C-6 Specify the Settings for Your Connection

Table C-1 Required Choices for **iPlanet Portal Server** Options (Only the possible choices are shown)

Section	Option	Value
Host Startup	• Launch with Windows	Yes
	• Use Windows screen saver	No
	• Run Minimized	Yes
Abnormal End of Session	• Wait n Minutes for User to Reconnect	1
Then	• Wait for Anyone	Yes
In Session	• Keyboard / Mouse Active During Session	Host and Remote
After A Normal End of Session	• Wait For Anyone	Yes

13. Click the Callers tab at the top of the iPlanet Portal Server Properties window shown in Figure C-7 to move to the next tab.

14. Choose Specify individual caller privileges.

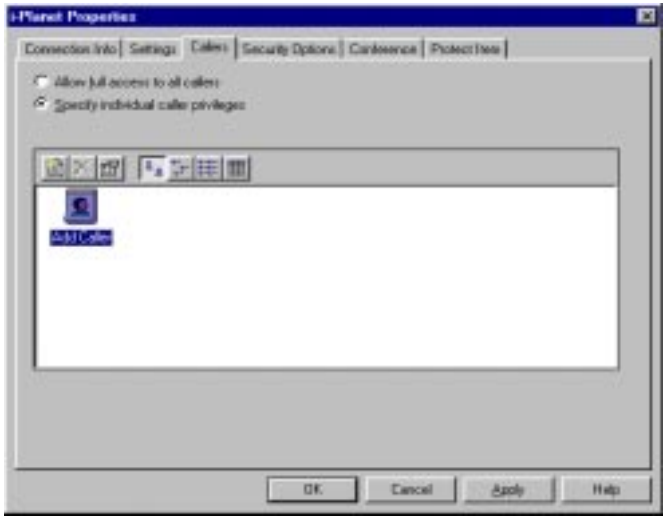

Figure C-7 Callers Tab for Individual Caller Privileges.

15. Double-click the Add Caller icon to start the Add Caller Wizard.

16. Type the caller's name as shown in Figure C-8.

    This is typically your user name for your system. It identifies you when you connect from the Internet.

Figure C-8 Specify the Name for the Caller.

17. Click Next.

18. Specify the caller's login name as shown Figure C-9.

Figure C-9 Specify the Login name and Password.

This is the same name or user ID that you typed in the previous screen shown in Figure C-8.

19. Type the password that you want to use, and then confirm the password by typing it again in the next field as shown in Figure C-9.

20. Click Next when you have finished.

21. Click Finish to complete the New Caller Wizard as shown in Figure C-10.

Figure C-10 Last Screen of the New Caller Wizard.

22. Click the Security Options tab at the top of iPlanet Portal Server Properties window.
23. Configure the Security Options as shown in Figure C-11 according to Table C-2.

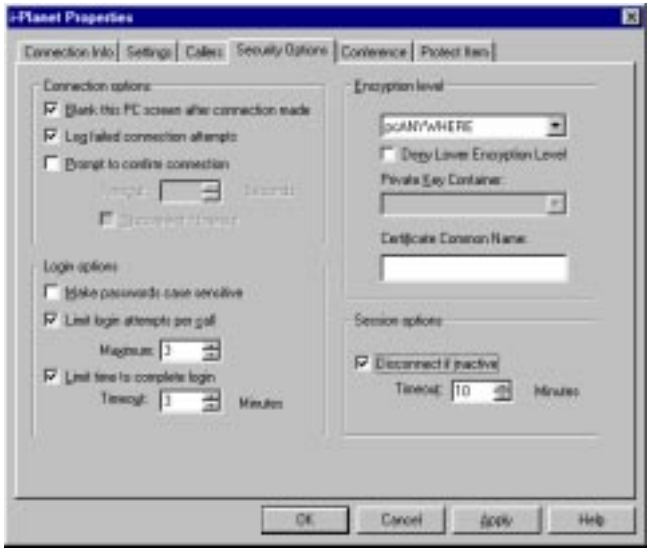

Figure C-11 Specify the Security Options for the Connection.

Table C-2 Required Choices for Security Options (Only the possible choices are shown)

Section	Option	Value
Connection Options	• Blank This PC Screen After Connection	Yes
	• Log Failed Connection Attempts	Yes
	• Prompt To Confirm Connection	No
Login Options	• Make Passwords Case Sensitive	No
	• Limit Login Attempts Per Call	Yes
	• Maximum	3
	• Limit Time To Complete Login	Yes
	• Time-out *n* Minutes	3
Encryption Level	• pcANYWHERE	pcANYWHERE
Session Options	• Disconnect if Inactive n Minutes	any value; value required, but not restricted.

You *must* type a value for the Disconnect if Inactive n Minutes option. You can, however, type whatever value you want. A good value for this option is typically five to ten minutes. There is a trade-off between typing a value that is too large or too small. If you specify a large value and are unexpectedly disconnected from the Internet, you cannot connect back to your PC for remote control until the time expires. If, on the other hand, you choose a value that is too small, you may be unexpectedly disconnected, for example, while you are reading a long document

24. Click OK.

25. Double-click the new iPlanet Portal Server icon to start host mode on your PC and wait for connections.

TIP Turn off any animated screen saver on the desktop PC. Using an animated screen saver delays logging in because the PC has to send all the image data from it over the network.

Glossary

access control Implements the privileges granted by authorization.

address In networking, a unique code that identifies a *node* to the *network*. Names like i-planet.demo.sun.com are translated to "dotted quad" addresses (10.0.24.15) by the Domain Name Service. (DNS).

administration console The administrator's GUI interface to iPlanet Portal Server.

API Application Program Interface, a set of calling conventions or instructions defining how programs invoke services in existing software packages.

applet A program written in the Java™ programming language to run within a Web browser. An example would be the Java front ends to iPlanet Portal Server's NetMail and NetFile applications.

attribute A configurable parameter of a profile.

ASP Access Service Provider. A company that, for a fee, provides access to applications that users can run without owning their own copies. See *ISP*.

authentication The process of verifying a user's identity.

authentication module An authentication module controls a specific authentication process. For example, iPlanet Portal Server provides authentication modules for Microsoft Windows NT, UNIX, S/key, and others, as well as opening the authentication API so other authentication modules can be written as needed.

authorization The process of granting specific access privileges to a user. Authorization is based on authentication and enforced by access control.

CA See *Certificate Authority*.

cache In Web browsers, the archive of recently visited Web pages, graphics, or other files that is stored in memory or on users' disks.

CDP Certificate Discovery Protocol. Request and response protocol used by two parties to transfer certificates.

certificate A set of data that identifies a person, machine, or application.

certificate identifier (ID) Generic naming scheme term used to identify a particular self-generated or issued certificate. It effectively decouples the identification of a key for purposes of key lookup and access control from issues of network topology, routing, and IP addresses.

Certificate Authority (CA) Trusted network entity that digitally signs a certificate containing information identifying the user; such as the user's name, the issued certificate, and the certificate's expiration date. Verisign is one of the best known CA's.

component An application or a service in iPlanet Portal Server. Components have attributes and privileges, much like users.

content filtering Practice of allowing or disallowing traffic based on the content of the data being sent.

cookie General mechanism that server-side connections can use to store and retrieve information on the client side of the connection. Cookies are small data files written to a user's hard drive by some Web sites when viewed in a Web browser. These data files contain information the site can use to track such things as passwords, lists of pages visited, and the date when a certain page was last looked at.

data compression Application of an algorithm to reduce the space required to store or the bandwidth required to transmit data.

decryption Process of decrypting information that has been encrypted. See *encryption*.

demilitarized zone (DMZ) Small protected network between the public Internet and a private intranet, usually demarcated with firewalls on both ends. This area is used to provide limited public access to resources such as Web servers, FTP servers, and other information resources.

desktop What the user sees on the screen. This usually includes a preferred set of applications and access privileges.

digital signatures Data added to a document to identify the sender using a public-key encryption scheme.

DMZ See *demilitarized zone*.

DNS Domain Name Service is a distributed name and address lookup mechanism used to translate domain names (ips.demo.sun.com) to IP addresses (10.23.134.24). It also allows reverse lookup, to translate IP addresses back into names.

domain The last part of a *fully qualified domain name* that identifies the company or organization that owns the domain name (for example, sun.com, sun.co.uk).

encryption Process of protecting information from unauthorized use by making the information unintelligible. Some encryption methods employ codes, called keys, which are used to encrypt the information. Contrast with *decryption*.

firewall Computer situated between an internal network and the rest of the network that filters packets as they go by according to user-specified criteria. Firewalls are normally used to protect systems on one side from unauthorized access by users on the other side.

File Transfer Protocol (FTP) A file transfer protocol often used on TCP/IP networks to copy files to and from remote computers.

fully qualified domain name The complete domain name of a system, including the hostname, network name if applicable, and domain; for example west.sun.com.

gateway A system that provides and controls connections to another network. See *VPN*.

host Name of a device on a TCP/IP network that has an IP address.

HTML Hypertext Markup Language. A file format, based on SGML, for hypertext documents on the Internet.

HTTP Hypertext Transfer Protocol, which describes how Web browsers and Web servers exchange information. See *URL*.

HTTPS Hypertext Transfer Protocol Secure, which describes the use of HTTP over an SSL connection, usually on port 443.

ICMP Internet Control Message Protocol. IP protocol that handles errors and control messages, to enable routers to inform other routers (or hosts) of IP routing problems or make suggestions of better routes. See *ping*.

IMAP Internet Message Access Protocol allows remote access to mailboxes and folders. IMAP clients usually leave some or all messages and folders on the server, unlike POP, in which all messages are downloaded.

Internet Protocol Protocol within TCP/IP suite used to link networks worldwide, developed by the United States Department of Defense and is used on the Internet. The prominent feature of this suite is the IP protocol.

IP See *Internet Protocol*.

ISP Internet Service Provider. A company providing Internet access. This service often includes a phone number access code, username, and software—all for a provider fee.

issued certificate Certificate that is *issued* by a *Certificate Authority*. See *self-generated certificate*.

ISV Independent Software Vendor. Third-party software developer.

Java™ Object-oriented, platform independent programming language developed by Sun Microsystems to solve a number of problems in modern programming practice.

JDK Java Development Kit. Software tools used to write Java applets or application programs.

key Code for encrypting or decrypting data.

LAN Local area network, a private network at a single location. Multiple LANs can be interconnected to form a WAN.

LDAP Lightweight Directory Access Protocol. One of the protocols used in iPlanet Portal Server to resolve profile attributes and privileges.

load balancer A load balancer controls connections to multiple gateway machines to allow approximately equivalent loads on each of the available systems.

NAT See *network address translation*.

Netlet A Java applet used in iPlanet Portal Server to allow any TCP/IP-based applications to securely connect to servers through an authenticated iPS connection.

network address translation (NAT) Function used when packets passing through a firewall have their addresses changed (or translated) to different network addresses. Address translation can be used to translate unregistered addresses into a smaller set of registered addresses, thus allowing internal systems with unregistered addresses to access systems on the Internet.

network mask Number used by software to separate the local subnet address from the rest of a given IP address.

NFS™ Network File System. A file system distributed by Sun Microsystems that enables a set of computers to cooperatively access each others files in a transparent manner.

NIS and NIS+ Network Information Service. NIS+ is a newer version (with a lookup service) for Solaris 2.x, with enhanced security.

node A transfer point within a network. Data is passed from node to node in a network until the data reaches its final destination.

passphrase Collection of characters used in a similar manner to, although typically longer than, a password. See *password*.

password Unique string of characters that a user types as an identification code; a security measure to restrict access to computer systems and sensitive files.

personal digital certificate (PDC) An electronic certificate attached to a message that authenticates a user. A personal digital certificate can be created by correctly entering a userID and password, or by using an SSL certificate request that in turn uses the security certificate of the server through which the user is connected.

PDC See *personal digital certificate*.

ping A TCP/IP command that verifies a connection to another host.

plaintext Unencrypted message.

Point-to-Point Protocol (PPP) PPP (the successor to SLIP) provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. Used for TCP/IP connectivity, usually for PC's over a telephone line. Also known as PPTP.

POP Post Office Protocol; defines a mechanism with which Internet users can connect to and download their waiting email messages.

PPP See *Point-to-Point Protocol*.

port The location (or socket) to which TCP/IP connections are made. Web servers traditionally use port 80, while FTP uses port 21 and telnet uses port 23. iPlanet Portal Server uses some special ports, particularly on client systems, to securely communicate through the iPS session to servers.

preference A user-specified choice about what appears or doesn't appear on the desktop, and how it appears, or other traits such as timeout settings.

private network A network of computers that is inaccessible unless you have appropriate access privileges. Private networks may be as small as a one-office LAN or as large as a multi-country enterprise network. See also *public network*.

privilege A type of access right that is granted to a user, a set of users, or a resource that is specified by the particular type of authorization implemented.

profile The attributes and privileges for an iPS entity, such as user, role, domain, or component.

profile server A special segment of iPlanet Portal Serverthat is devoted to storing profile information.

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provider A Java class that can write HTML content to a mini-frame in the desktop. Providers (also called *content providers*) are used to create information in specific areas of a user's desktop.

proxy A proxy is an intermediary program that makes and services requests on behalf of clients. Proxies act as servers and clients in turn, and are used to control the content of various network services. See *reverse proxy*.

public-key certificate A data structure containing a user's public key, as well as information about the time and date during which the certificate is valid.

public-key cryptography Also known as *asymmetric* key cryptography. In public-key cryptosystems, everyone has two related complementary keys: a publicly revealed key and a *secret* key (also frequently called a *private* key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the secure channels that a conventional cryptosystem requires.

public network Like the Internet, a public network carries traffic from a variety of companies, individuals, and sources and is inherently insecure. Contrast with *private network*.

query Process for extracting particular data.

reverse proxy A proxy which performs bi-directional URL rewriting and translation between clients and servers. Unlike a proxy, which exists at the client side, a reverse proxy exists at the server side of the network. In iPlanet Portal Server, the reverse proxy exists on theiPS gateway.

role A role defines all aspects of a user's experience when running in the iPlanet Portal Server environment. A role can, for instance, correspond to a job title (manager, engineer, sales, etc.) or can be defined other ways, such as a full member of a working group or an observer. A role determines what a user sees and can use.

router Intermediary device responsible for deciding which of several paths network (or Internet) traffic will follow.

secret key In public-key cryptography, a private key that is never disclosed to the public. See *public-key cryptography*.

Secure Socket Layer (SSL) A form of secure, low-level encryption that is used by other protocols like HTTP and FTP. The SSL protocol includes provisions for server authentication, encryption of data in transit, and optional client authentication. The version used in iPlanet Portal Server uses RSA's public and private key encryption, as well as a digital certificate.

self-generated certificate Public key value only used when entities are named using the message digest of their public value, and when these names are securely communicated. See *issued certificate*.

session An iPlanet Portal Server session is a sequence of interactions between a user and one or more applications, starting with login and ending with logout or timeout.

session key Common cryptographic technique to encrypt each individual conversation between two people with a separate key.

SGML Standard Generalized Markup Language. Method of tagging a document to apply to many format elements.

shared-key cryptography Also known as *symmetric key cryptography*. Cryptography where each party must have the same key to encrypt or decrypt *ciphertext*.

smart card A plastic card with a magnetized strip that is used for authentication.

SMTP Simple Mail Transfer Protocol. Used on the Internet to route email.

SMTP proxy A variant of SMTP that sends messages from one computer to another on a network and is used on the Internet to route email.

SNMP Simple Network Management Protocol. Network management protocol that enables a user to monitor and configure network hosts remotely.

SSL See Secure Socket Layer.

SSL Certificate An electronic token that means you or a vendor have given approval to encrypt and decrypt your secure transactions, using PKI. You create a self-signed SSL Certificate when you install iPlanet Portal Server software. However, you can also obtain an SSL Certificate from a certificate vendor who authorizes secure communications services over the Internet.

subdomain The next-to-last part of a *fully qualified domain name* that identifies the division or department within a company or organization that own the domain name (for example, eng.sun.com, sales.sun.co.uk); not always specified.

subnet Working scheme that divides a single logical network into smaller physical networks to simplify routing.

subnet mask Specifies which bits of the 32-bit IP address represent network information. The subnet mask, like an IP address, is a 32-bit binary number: a 1 is entered in each position that will be used for network information and a 0 is entered in each position that will be used as node number information. See *node*.

symmetric key cryptography See shared-key cryptography.

TCP See transmission control protocol.

TCP/IP Transmission Control Protocol / Internet Protocol. Protocol suite originally developed for the Internet. It is also called the *Internet* protocol suite. Solaris networks run on TCP / IP by default.

telnet Virtual terminal protocol in the *Internet* suite of protocols. Enables users of one *host* to log in to a remote host and interact as normal terminal users of that host.

telnet proxy An application which sits between the telnet client and telnet server and acts as an intelligent relay.

transmission control protocol (TCP) Major transport protocol in the Internet suite of protocols providing reliable, connection-oriented, full-duplex streams. Uses IP for delivery. Encrypts only IP packet data, but not the headers. Corresponds to the transport layer, which is the fourth of the seven ISO layers. See *TCP/IP*.

transparent clustering A condition whereby multiple machines will appear to the user to be a single machine. In iPlanet Portal Server, the condition where multiple gateways appear to the user to be a single gateway.

tunneling Process of encrypting an entire IP packet, and wrapping it in another (unencrypted) IP packet. The source and destination addresses on the inner and outer packets may be different.

tunnel address Destination address on the outer (unencrypted) IP packet to which tunnel packets are sent. Generally used for encrypted gateways where the IP address of the host serves as the intermediary for any or all hosts on a network whose topology must remain unknown or hidden from the rest of the world.

URL Uniform Resource Locator. A code that searches for the location of a specific address on the Internet.

user ID Name by which a user is known to the system.

Virtual Private Network A network with the appearance and functionality of a regular network, but which is really like a private network within a public one.

The use of encryption in the lower protocol layers provides a secure connection through an otherwise insecure network, typically the Internet. VPN's are generally cheaper than true private networks using private lines, but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or possibly by routers.

VPN gateway The entry point to a VPN. Typically protected by a firewall.

VPN See *Virtual Private Network.*

WAN Wide area network, a private network (intranet) spanning more than one physical location.

Watchdog A process that monitors a gateway and restarts the gateway if its processes fail.

Web See *World Wide Web.*

Web page Document on the Web.

web server An application that responds to web requests such as HTTP, FTP, etc.

World Wide Web Network of servers on the Internet that provide information and can include hypertext links to other documents on that server and often other servers as well.

Index

NUMERICS

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X