Administration Guide

i-Planet™ 2.0

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A. 650-960-1300

Part No. 805-7688-10
May 1999, Revision A

Contents

Figures

Tables

Preface

The *i-Planet Administration Guide* is designed to help you configure and administer your i-Planet™ software.

Who Should Use This Manual

The *i-Planet Administration Guide* is written for the system administrator. This book assumes that you have root access, are familiar with administration concepts for Solaris systems, including the use of `pkgadd` to install programs and the use of `admintool` to add users, and are familiar with networking concepts.

How This Manual Is Organized

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

- **Chapter 1, "i-Planet Overview,"** presents an overview of the features, compatibility, hardware and software requirements, and online help and documentation of your *i-Planet* software.
- **Chapter 2, "Administration Console,"** describes how to use *i-Planet*'s Administration Console.
- **Chapter 3, "Other Administrative Tasks,"** describes the scripts and commands as well as what files may need editing for i-Planet.
- **Chapter 4, "i-Planet User Administration Command Line Interface,"** describes the Java™ command line interface that i-Planet administrators can use to create i-Planet users, delete i-Planet users, view the properties of all i-Planet users, and List all i-Planet users.

- **Chapter 5, "SSL Service and Certificates,"** describes how to create self-signed SSL certificates, obtain SSL certificates from Verisign and other vendors, use SSL service between the i-Planet server and i-Planet gateway, and enable SSL service.
- **Chapter 6, "Administering i-Planet Firewall Application,"** describes how to configure and administer the i-Planet firewall application.
- **Chapter 7, "Authentication,"** contains information on authentication and the authentication modules.
- **Chapter 8, "Supporting Remote Users,"** describes what you need to do to set up and prepare your remote users, what issues you can expect, and the resolution to the problems.
- **Appendix A, "Customizing i-Planet HTML Template Files,"** provides instructions for customizing the appearance of the i-Planet Desktop.
- **Appendix B, "Pluggable Authentication APIs,"** contains the instructions for the pluggable authentication application programming interface (API).
- **Appendix C, "Third Party Software,"** describes how to install and configure a pcANYWHERE host on your desktop PC at work, how to install other third-party software for controlling PCs remotely, how to add the package for GO-Joe, how to configure the RPC port for Microsoft Exchange, and how to install NetCon.

Related Books

Other documents in i-Planet 2.0 documentation set are:

- *i-Planet 2.0 Installation Guide*
- *i-Planet 2.0 Installation Install Card*

Ordering Sun Documents

The SunDocs[SM] program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals using this program.

For a list of documents and how to order them, see the catalog section of the SunStore[SM] Internet site at `http://www.sunstore.sun.com`.

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/.

What Typographic Changes Mean

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

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% You have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name%` **`su`** `Password:`
AaBbCc123	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.

TABLE P-2 Shell Prompts

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

i-Planet Overview

This chapter discusses the following topics:

- What is the i-Planet software?
- Features of the i-Planet software
- Compatibility with SunScreen™ products
- Hardware and software requirements
- Online help and documentation

This Guide

This guide assumes that the systems administrator and the i-Planet administrator are the same person or at least persons of the same level of experience, level, and skill, and that have the same access to the network.

The term user, when used, refers to the i-Planet administrator and the systems administrator when they are the same person.

The term end user refers to the employee or business partner who is using the i-Planet product to obtain access over the Internet to the company's private network.

You use the information in this guide to configure and manage, that is, administer the i-Planet product. You do this primarily through the Administration Console, which is a browser-based graphical user interface (GUI). You must also administer parts of this product using the command line and you probably will have to modify some files. In addition to this guide, there is online help for the Administration Console. The only documentation that the end users have is the on-line help. You will have to supply them with certain information, such as passwords for authentication.

What Is The i-Planet Software?

The i-Planet software is a unique solution that provides a company's remote and travelling employees with worldwide remote access to the corporate network over the Internet from any computer with a Java-enabled web browser. The i-Planet software acts as a mediator between users coming in through the Internet to the corporate intranet. It provides secure end-user connectivity across all networks and a uniform, familiar, web browser-based interface.

The i-Planet software lets companies:

- Leverage the public network and Internet service providers (ISPs) to reduce costs.
- Increase productivity with better access to information.
- Simplify remote access for end users.
- Access anytime, anywhere with any computer with a browser. This means that the client could be behind a web proxy or a firewall.

The i-Planet software lets administrators:

- Authenticate Internet-based end users with a convenient, secure one-time password scheme or the plug-in authentication module of your choice.
- Implement access control technology that greatly increases intranet security.
- Allow secure access to electronic mail servers, web servers, and file servers.
- Allow users to have access through a web browser-based interface, sharply reducing learning curve and training time for remote end users.
- Administer the i-Planet software through an easy-to-use browser-based interface.
- Install an optional packet-filtering firewall application based on proven Sun Microsystems' SunScreen technology.

The i-Planet product provides a corporation and its remote and travelling employees with cost-effective, fast, secure access to corporate information, personal email, applications, and internal web sites. It provides this access at anytime, from anywhere, and from any platform that uses Netscape 4.06 with Java Advanced Windowing Toolkit (AWT) 1.1 support (or Netscape 4.04 or 4.05 with the JDK™ 1.1 patch) or greater and Internet Explorer 4.0 or greater. The Java® Developers Kit (JDK) 1.1 patch from Netscape contains AWT 1.1 and greater support for JDK 1.1.

The i-Planet software consists of two main components:

- The i-Planet gateway—contains the software for the i-Planet gateway and the software for the (optional) i-Planet firewall application
- The i-Planet server —contains the software for the i-Planet platform and the software for the i-Planet applications.

You can install the i-Planet software on:

- One machine

- Two machines—With the i-Planet gateway on one machine and the i-Planet server on another. This is the preferred configuration.

How Does the i-Planet Software Work?

The i-Planet software consists of individual components that act as building blocks. Each of these components have a well-defined interface that hides their internal implementation. This allows for them to interact without depending on a particular implementation, and allows you to extend and expand the functionality easily that the i-Planet product offers to clients.

The entire i-Planet architecture is Internet and web based. The communication protocols include both standard HTTP (Hypertext Transfer Protocol) and HTTPS (Secure Hypertext Transfer Protocol, an encrypted version of HTTP that is understood by all newer web browsers and allows secure communication between a web browser and web server across any network). Additional i-Planet applications, in particular remote windowing software and specific communication components, use their native TCP-based communications protocols, encrypted and passed through the configured SSL port.

By relying on these protocols, the i-Planet product lets you use standard web browsers for both secure end-user access to applications and for secure administration of the i-Planet software. All remote-user traffic uses the SSL port for all traffic, while administrative access can be through HTTP or HTTPS, if you are using SSL service for communication between the i-Planet server and the i-Planet gateway.

For simplicity in explanation and discussion, this document assumes that all end users have access to your i-Planet installation from somewhere on the Internet—even though it applies equally to both the Internet and intranet. Depending on the type of authentication used, web-browser-based administrative access to the i-Planet product can come from within your internal network or from a remote host over the Internet.

FIGURE 1-1 shows a basic diagram of the i-Planet product, including the default port numbers, as installed on two machines. SSL is used to encrypt the connection between client to the i-Planet gateway over the Internet. SSL can be used as an option to encrypt the connection between the i-Planet server to the i-Planet gateway.

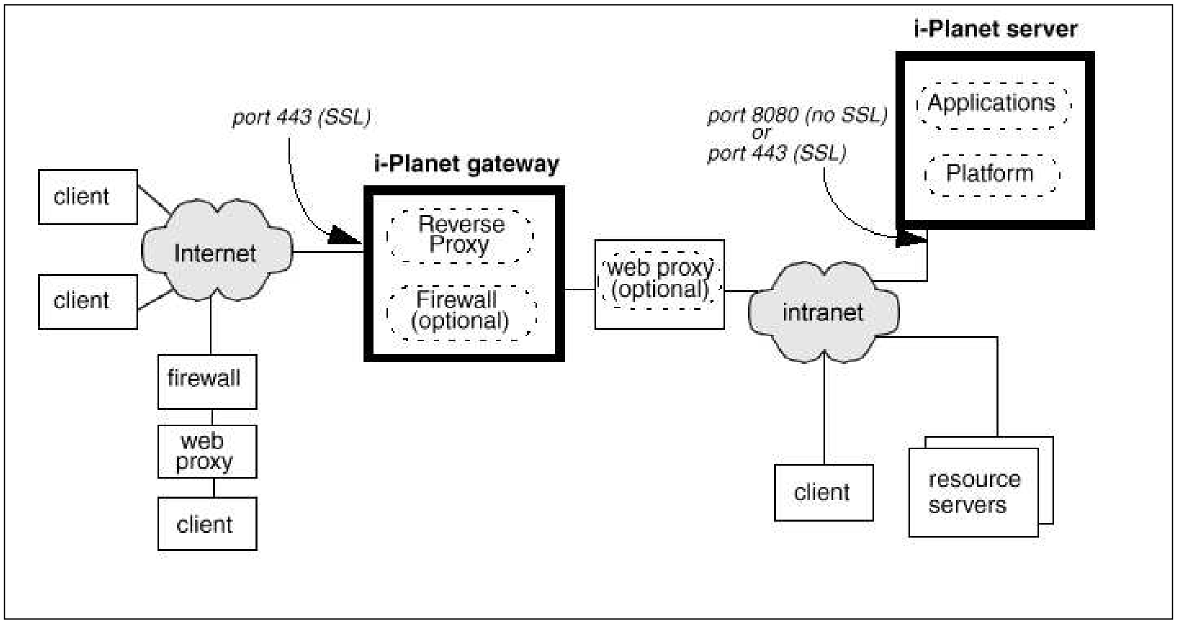

FIGURE 1-1 i-Planet Basic Diagram

The following sections detail each of the main components and their roles in this communication process.

The i-Planet Gateway

The i-Planet gateway forms the boundary between the Internet and the intranet. It has two main responsibilities:

1. It acts as the border guard, establishing identity and allowing access.
2. It also acts as a translator, altering documents served so that links to the intranet content will work on the extranet.

In general, networks "inside" your i-Planet gateway can be considered secure, internal networks, that is your intranet. Networks outside the i-Planet gateway (that is, the Internet) are not secure, and access from those networks must be closely controlled, through encryption and authentication. The i-Planet gateway component provides this control.

To accomplish these goals, the i-Planet gateway relies on three subsystems.

1. **Server subsystem**—Listens for network connections and assigns resources to process these requests.

2. **Connection handler subsystem**—Does the actual processing of the requests. It translates and transmits the response back to the client.

3. **Authentication and profile subsystem**—Handles authorization, authentication, and profile information for the gateway.

The i-Planet gateway also runs the optional i-Planet firewall application that is included with the i-Planet software. Although it is not required for baseline operation of the i-Planet product, it provides greater security.

The i-Planet Server

The i-Planet server handles all of the details of authorization, authentication, policy, and user profile access and management, which compose the i-Planet platform. It also handles the functionality of the i-Planet application server. Communication with the i-Planet server is generally through HTTP. If you have enabled SSL service from the i-Planet server to the i-Planet gateway, communication is through HTTPS. You have administrative access to the i-Planet administration screens through a web browser.

The i-Planet Platform Server

The i-Planet platform server is composed of several subsystems: authentication, authorization, and profile management. These subsystems handle the connections to outside services. Because these subsystems are independent browser links to the overall i-Planet product, you can incorporate many different technologies into your installation of the i-Planet software, without making major changes to the i-Planet server or to other i-Planet components.

The i-Planet server subsystems work together and interface with external data sources to manage the process of identifying users to the system, determining access rights, and providing that access. The platform-server subsystems are:

1. **The authentication subsystem—**deposits, manages, and clears cookies from end user's systems. It describes the physical and virtual connection from the end user's browser to the i-Planet server. In this way, it essentially authenticates each transaction.

2. **The authorization subsystem—**assures that end users have the correct permissions to use particular applications.

3. **The profile-management subsystem—**Stores application profiles and user profiles, as well as interfaces with external data sources, such as files and directory servers. Application profiles and user profiles declare the allowable set

of roles that can be assumed by the authenticated user name. These profiles also contain additional user-specific application and personal information. For example, a user profile contains information about the user's identity.

i-Planet Application Server

The i-Planet application server can link to any TCP/IP accessible application on your intranet. The i-Planet product has a core set of applications that offer baseline remote access functionality, including viewing your group calendar and accessing email. By design, HTTP accessible applications, including any applications already running on your intranet, should work without modification. The i-Planet product has no specific requirements on how additional add-in applications are structured.

The i-Planet product comes with the following applications for end users:

- **i-Planet Desktop**—Provides access to all online help and a central access point for end users to obtain access to all i-Planet applications. Remote users can change their preferences from the i-Planet Desktop.
- **NetMail** —Provides full IMAP mail server access and offline reading capabilities.
- **NetMail Lite**—supports Sun Internet Mail Server (SIMS) without requiring support for Java applets.
- **NetCalendar**—Provides an HTML client calendar that supports CDE and the Sun Calendar server.
- **NetSurf**—Permits end users to look at certain web pages on your intranet.
- **NetFile**—Provides end users with additional, flexible remote access capabilities of your choice (including Telnet and remote X-Windows capabilities).
- **NetFile Lite** —Provides limited remote file system access without requiring a Java applet.
- **Generate SKEYs**—Allows users to generate their own S/Key passwords.

Online Help and Documentation

Online help is available for the i-Planet administration interface as well as for the end-user i-Planet Desktop and all included end-user applications. Access help by clicking the help links, located on every page in the i-Planet interface. From any page within the Administration Help you can navigate to the help index and all other administration help pages. Similarly, your users have access to help for every page of the i-Planet product, and from there can navigate to a help index and all other end-user help pages.

The installation CD-ROM for the i-Planet software contains a documentation directory with administration documentation in HTML and PostScript formats.

Note – You can reach the files directly through the system or through your web server.

Look for:

- HTML files at `http://`*`i-Planet_server`*`/docs/usenglish/manuals/html/`
- The PostScript file at `http://`*`i-Planet_server`*`/docs/usenglish/manuals/ps/`
- Online administration help by clicking the **Help** button
- Online remote-user help by clicking the **Help** button
- Man pages at `/opt/SUNWstnr/man`

CHAPTER **2**

Administration Console

This chapter describes how to use the i-Planet Administration Console.

Administration Console

The Administration Console is a a browser-based graphical user interface (GUI) that you use to view and set the preferences and values that you want end users to have and to see. End users can override some of the values that you set in the Administration Console, others they cannot. You also can view the logs through the Administration Console.

All traffic between the browser that the end user is using and the i-Planet gateway is always encrypted. If, however, you are using SSL service for communication between the i-Planet server and the i-Planet gateway, NetSurf traffic and any other traffic that does not go to the i-Planet server are unencrypted.

Note – If you are not using SSL service for communication between the i-Planet server and the i-Planet gateway, things like authentication information and passwords, such any S/Key passwords that end users generate, will be in clear text between the i-Planet server and the i-Planet gateway. All information from the i-Planet gateway to the end user is encrypted.

To Gain Access to the Administration Console

Note – You cannot use the Administration Console to administer the i-Planet gateway.

You use the Administration Console, an HTML-based tool, for viewing and editing the i-Planet server configuration.

How do I use it?

You can use the Administration Console from the intranet or as an end user over the Internet.

▼ To Reach the Administration Console From the Intranet

1. **To start the console, if you are not using SSL service to communicate between the i-Planet server and the i-Planet gateway, start a browser and type the URL:**

   `http://`*`i-Planet_server`*`:8080/console`

   - **Start the console, if you are using SSL service to communicate between the i-Planet server and the i-Planet gateway and you are using the default port 443, start a browser and enter the URL:**

   `https://`*`i-Planet_server`*`/console`

   - **Start the console, if you are using SSL service to communicate between the i-Planet server and the i-Planet gateway and you are using a port other than port 443, start a browser and type the URL:**

   `https://`*`i-Planet_server:port_number`*`/console`

   The login page appears as shown in FIGURE 2-1.

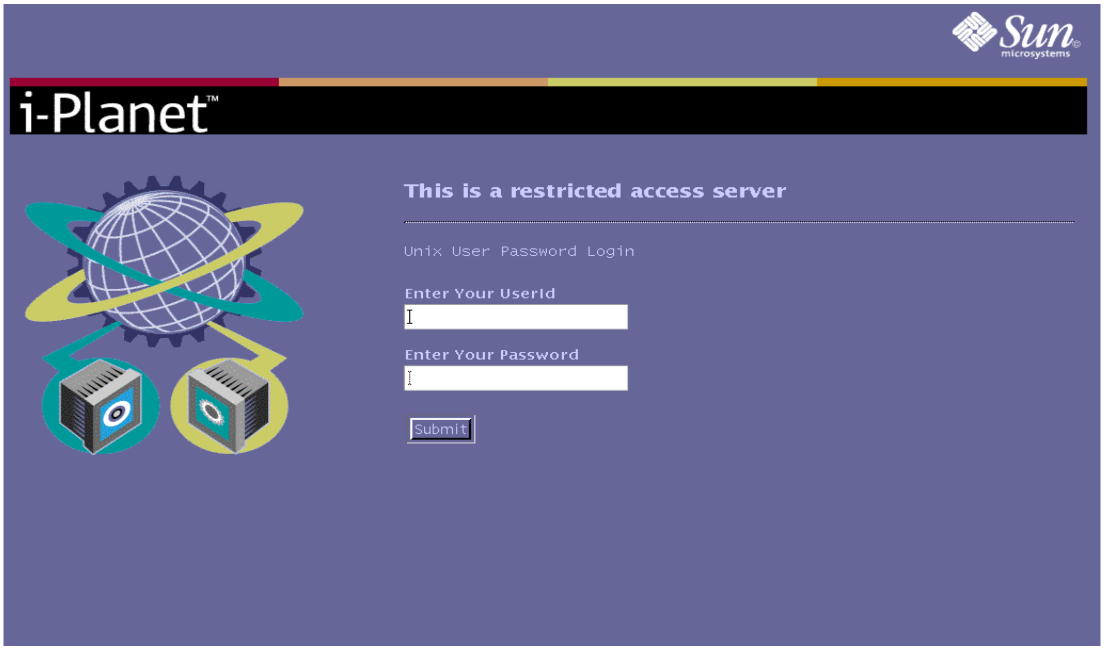

FIGURE 2-1 The Login Page

2. **Type root as your user ID and the UNIX root password on the i-Planet server.**

   Other user names and passwords can be configured to log into the i-Planet server. If your user name has been appropriately configured (as described in the following section), you can provide your name and password rather than root and root's password.

Caution – Any user with the root password on the i-Planet server can log in and control the i-Planet Administration Console.

---

3. **Click the Submit button to complete logging in and to start the Administration Console.**

   The Administration Console has two components shown in FIGURE 2-2: (1) the administration frame and (2) the navigation frame. The administration frame displays the viewable and configurable parameters. The navigation frame lists the applications and the services that are available for configuration or viewing.

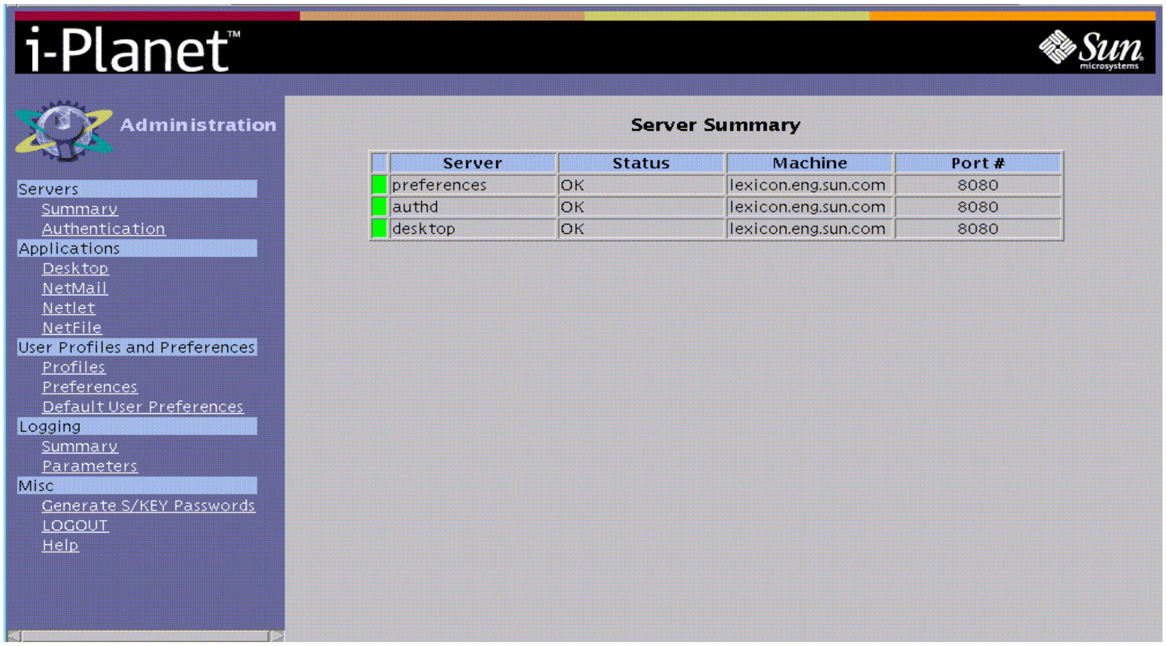

FIGURE 2-2 Server Summary Page—Initial Page of the Administration Console

▼ To Reach the Administration Console From the Internet

1. **Type the URL for the i-Planet Gateway in the location field of a browser to fetch the Authenticator Menu for the i-Planet Desktop:**

```
https://i-Planet_gateway
```

If you have specified only one type of authentication, you will not see the Authenticator Menu.

2. **Click the type of authentication that is being used in the Authenticator Menu, shown in** FIGURE 2-3**.**

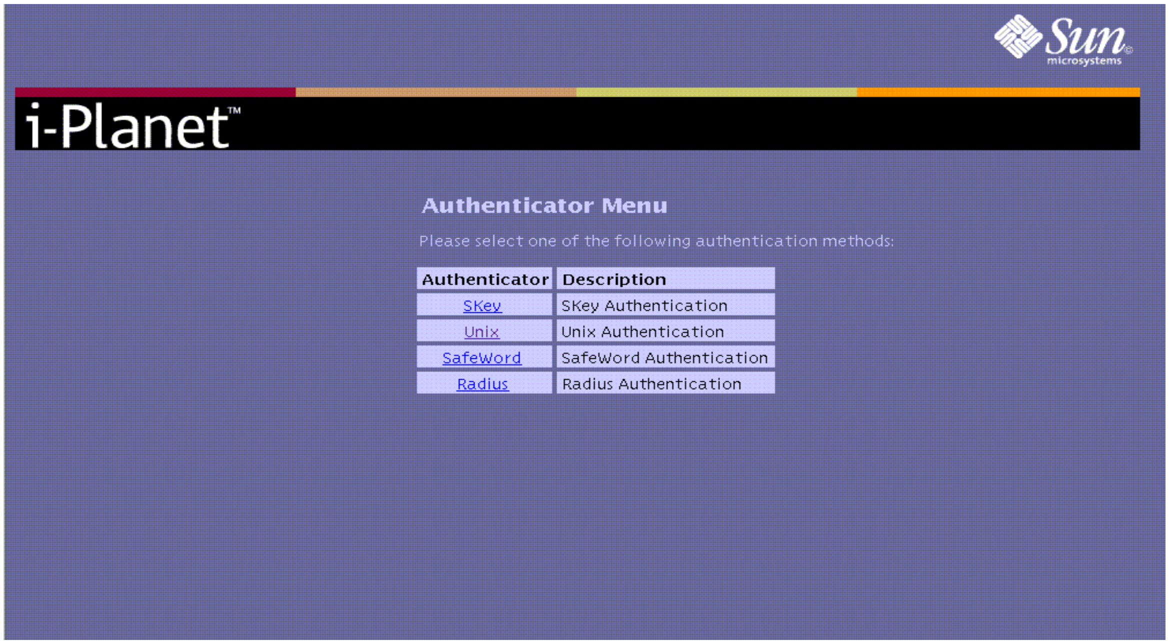

FIGURE 2-3 Authenticator Menu for the i-Planet Desktop

3. **Type your user ID and password as required by the authentication being used.**
4. **Click Submit.**

   FIGURE 2-4 shows the Log in Page for the i-Planet Desktop.

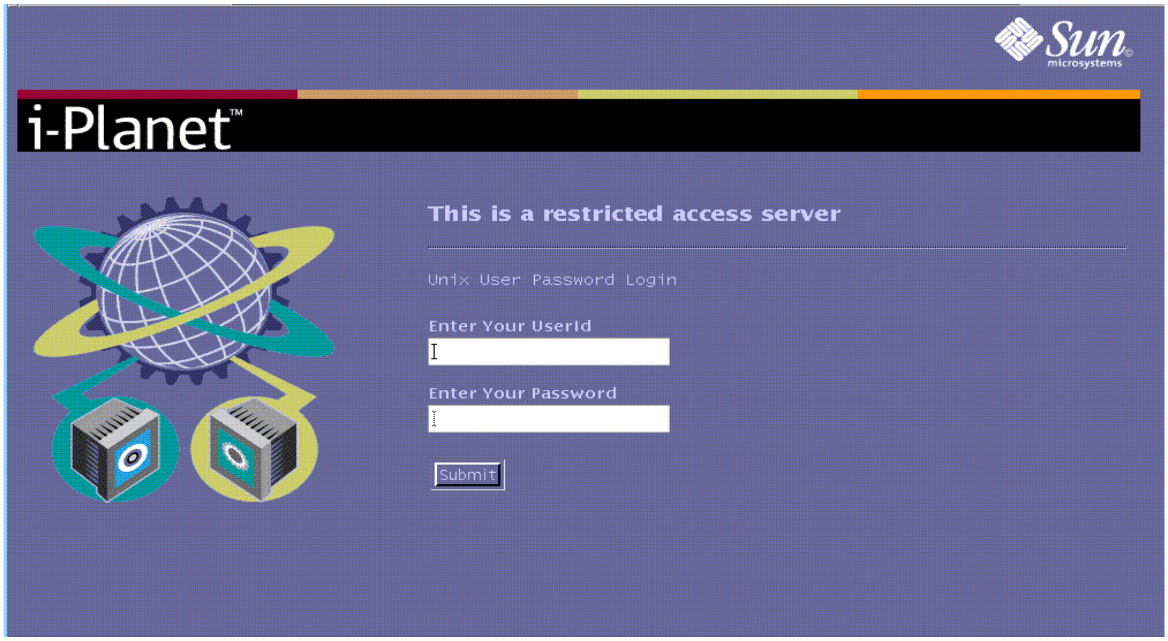

FIGURE 2-4 Log In Page for the i-Planet Desktop

5. **Type the URL to the i-Planet Gateway using https followed by the URL to the i-Planet server using http in the Go To field of the browser to connect to the Administration Console.**

   The form for the URL is:

```
https://i-Planet_gateway/http://i-Planet_server:port_number/
console
```

FIGURE 2-5 shows the Front Page of the i-Planet Desktop with the URL in the Go To field of the browser to connect to the Administration Console.

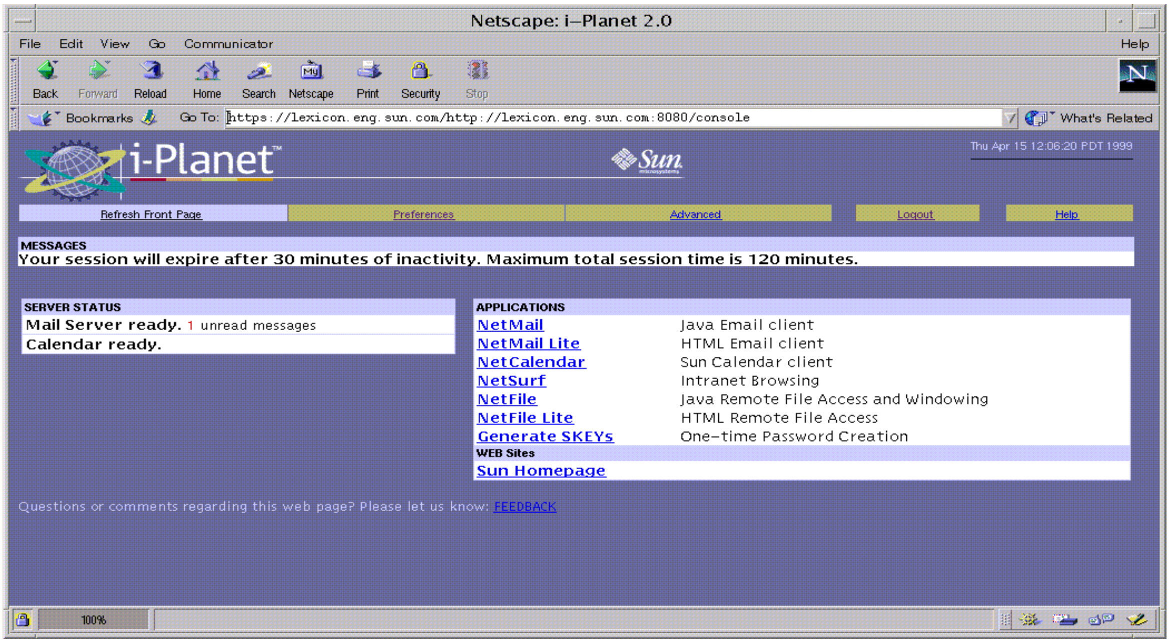

FIGURE 2-5 Front Page of the i-Planet Desktop with the URL to Connect to the Administration Console

The Server Summary page of the Administration Console, shown in FIGURE 2-2, will display.

Using the Administration Console

Once the Administration Console is up and running, you can click the different entries in the navigation frame to display the information in the administration frame. After changing the parameters in the administration frame, click **Enter** to save them.

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure “To Stop and Restart the Web Server on the i-Planet Server” in Chapter 3 "Other Administrative Tasks.”

If you want to cancel your changes and return to the previous settings, click the **Reset** button.

The navigation frame contains five labelled sections, each of which has one or more subsections that consist of links. Clicking a link to a subsection brings up the corresponding subsection in the administration frame.

Servers

Two links are available for servers: Summary and Authentication

Summary

Clicking the Summary link displays the Server Summary table, shown in FIGURE 2-2. This table shows the servers, status of the servers (up or down), the machines on which the servers are running, and the port numbers. You cannot edit this table nor can you reconfigure the settings from the Administration Console.

The i-Planet Server Summary page displays as the default first page for the Administration Console.

Authentication

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3 "Other Administrative Tasks."

Clicking the Authentication link displays the Authentication Parameters page, shown in FIGURE 2-6.

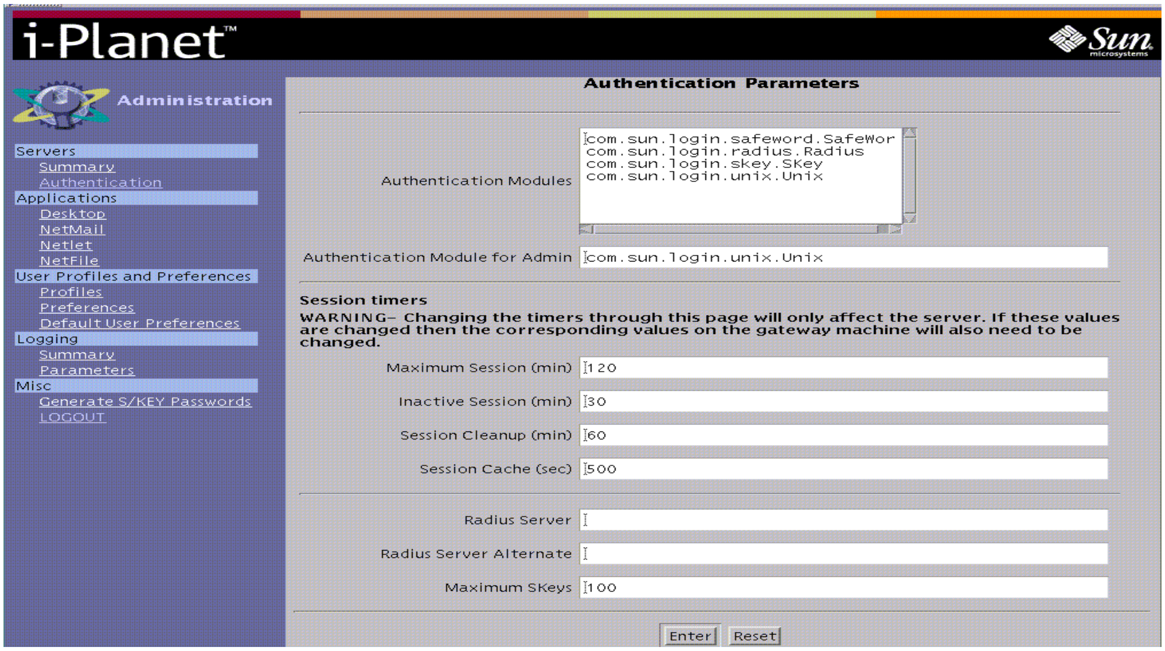

FIGURE 2-6 Authentication Parameters Page

From this page, you can:

- Add the authentication module or modules that you want end users to use.
- Delete the authentication module or modules that you do not want end users to use.
- Change the:
  - Authentication Module for Administration
  - Maximum Session Time (in minutes)
  - Inactive Session Timer (in minutes)
  - Session Cleanup Timer (in minutes)
  - Session Cache Timer (in seconds)

The authentication modules are discussed in Chapter 7 "Authentication."

If you change the default setting in any or all of the four timer fields above, you must edit the file `/etc/opt/SUNWstnr/platform.conf` on the i-Planet gateway so that the i-Planet gateway and the i-Planet server have the same values. You must do this each time you change any setting for a timer.

▼ To Edit i-Planet Gateway's `platform.conf` File

1. **Edit the appropriate line in the file** `/etc/opt/platform.conf` **on the i-Planet gateway, shown in** TABLE 2-1**, to change the default setting to the same value as in the respective field in the Administration Console.**

TABLE 2-1 Timer Field and the Equivalent Line in the `platform.conf` File

Administration Console Field (unit of time)	i-Planet Gateway's `platform.conf` (unit of time)
Maximum Session Timer (minutes)	`limCreate=` `(minutes)`
Inactive Session Timer (minutes)	`limAccess=` `(minutes)`
Session Cleanup Timer (minutes)	`limLogout=` `(minutes)`
Session Cache Timer (seconds)	`cacheSeconds=` `(seconds)`

2. **Stop and restart the reverse proxy server on the i-Planet gateway.**

   See the section "Stopping and Restarting the i-Planet Gateway's Reverse Proxy Server"in Chapter 3 "Other Administrative Tasks."

   On this page you also can:

   - Enter the:
     - Radius Server
     - Radius Server Alternate

     For reasons of security, you set the RADIUS Shared Secret on the i-Planet server in the file `/etc/opt/SUNWstnr/platform.conf`.

▼ To Set the RADIUS Shared Secret

1. **Edit the file** `/etc/opt/SUNWstnr/platform.conf` **on the** i-Planet server **to set the line** `radius.secret=` **equal to the shared secret.**

2. **Set the maximum number of allowable sets of S/Key passwords.**

   The maximum number of allowable sets cannot be greater than 400, which is the absolute maximum number of sets.

3. **Stop and restart the web server on the i-Planet server**

   For information on stopping and restarting the web server, see the section "Stopping and Restarting the Web Server" in Chapter 3 "Other Administrative Tasks."

Applications

This section contains links that allow you to modify or set values for configuring the i-Planet Desktop, NetMail, Netlet, and NetFile applications.

Desktop

Clicking the Desktop link displays the Desktop Configuration page, shown in FIGURE 2-7 and FIGURE 2-8.

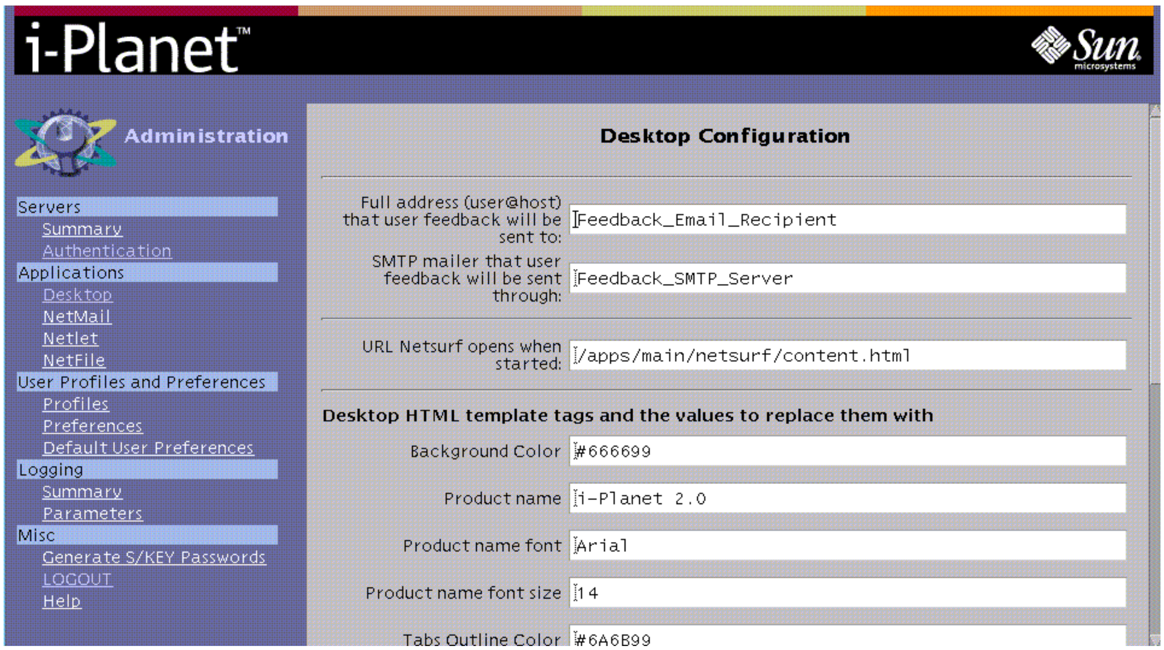

FIGURE 2-7 Desktop Configuration—Upper Half of the Page

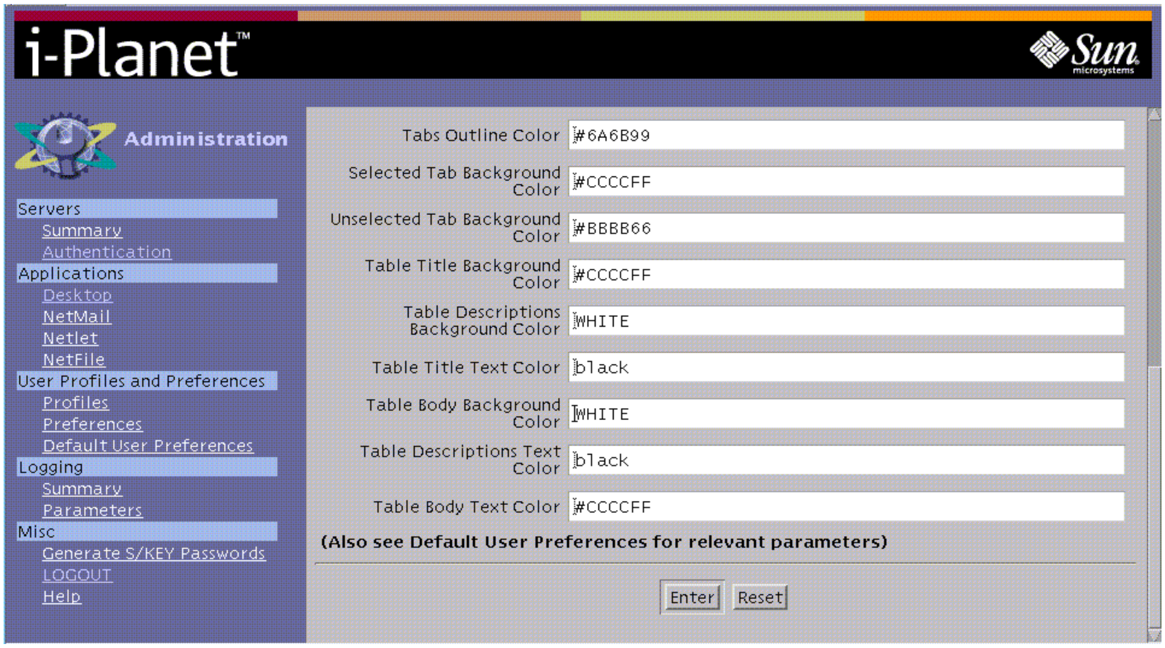

FIGURE 2-8 Desktop Configuration—Lower Half of the Page

You change the user i-Planet Desktop configuration by changing the values on this page. You can specify the:

- Mailer (SMTP_host) that is used to transmit user feedback
- Feedback address to which the end user's feedback will be sent
- Initial URL that NetSurf will open when it starts
- Values for Desktop HTML template tags

Colors can be RGB hexadecimal values (for example, #0000FF for blue), or an approved HTML word for a color. The HTML names and the RGB values are generally listed in any HTML reference.

You can test the changes by making them, stopping and restarting the web server, logging out of the Administration Console and, then logging in to the i-Planet Desktop.

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3 "Other Administrative Tasks."

Also see Default User Preferences in the “User Profiles and Preferences Section.”

NetMail

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure “To Stop and Restart the Web Server on the i-Planet Server” in Chapter 3 "Other Administrative Tasks.”

Clicking the NetMail link displays the NetMail Default Configuration page for new users. It consists of two sections: Default Values for New NetMail Users - Overridden by user preferences and Default Values for New NetMail Users - Not overridden by user preferences.

The mail feature of NetFile from the i-Planet Desktop uses the preferences set by NetMail. Outgoing mail will be sent using the SMTP server that is defined in NetMail. You can change the mail settings through the NetMail preference dialogue or the end user can change them on the Preference page of the i-Planet Desktop.

- Default Values for New NetMail Users - Overridden by user preference is shown in FIGURE 2-9.

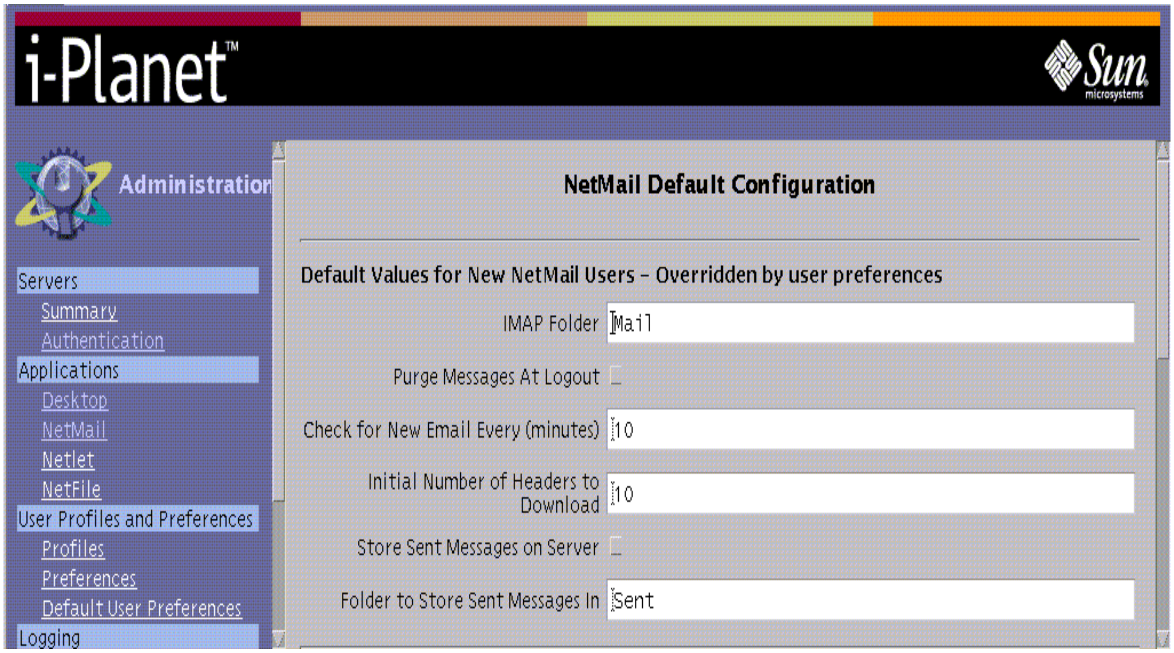

FIGURE 2-9 NetMail Default Values for New NetMail Users - Overridden by User Preferences

End users can override these settings with information that they enter on the Preference dialogue for NetMail.

You can change the default new users settings, including the:

- Name of the default IMAP folder
- Enabling purging messages at logout
- Time in minutes to check for new email

  Set the time to check for new email so that it is greater than the Inactive Session time that you set on Authentication Parameters page. This will prevent failure to time out when the end users are using NetMail and NetFile until the maximum time out for the session is reached.

  If you do not want the end user to be able change the time to check for new mail parameter on the Preference page of the i-Planet Desktop, type the parameter `inactivityinterval` from TABLE 2-4 in the Names of Uneditable Preferences field.

- Initial number of headers to download
- Enabling storing sent messages on the server.
- Setting the folder in which to store sent messages.

- Default Values for New NetMail User - Not Overridden by user preferences is shown in FIGURE 2-10.

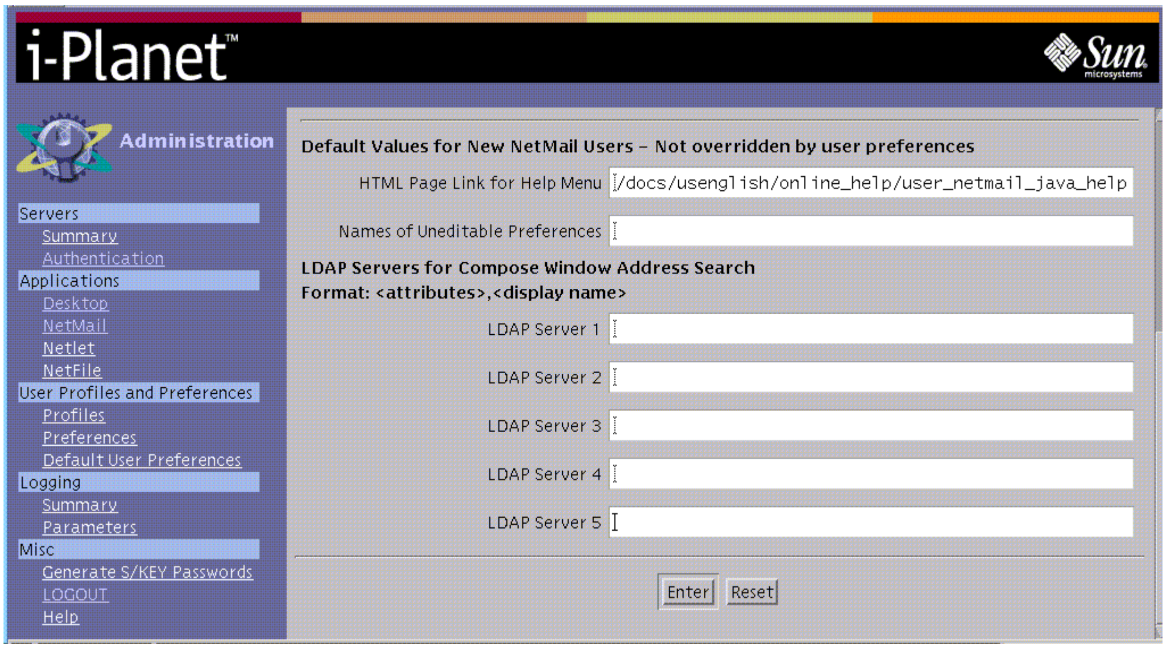

FIGURE 2-10 NetMail Default Values for New NetMail Users - Not Overridden by User Preferences

- HTML page link for help menu
- Folder in which to store sent messages
- LDAP Server —Lightweight Directory Access Protocol (LDAP) is a protocol that allows end users to have access to information from online directory services. By configuring NetMail to use directory services, end users can use the Address Search feature in the Compose Message window of NetMail to search for email addresses.

LDAP Parameters

You configure access to up to five LDAP servers through the Administration Console. Each parameter has the following form:

```
attribute,display name
```

You replace the values in italics as follows:

attribute—Attributes used to connect to the directory server.

Each attribute:

- Has the form `argname=argvalue`.
- Is separated by an ampersand (`&`).
- Is URL encoded.

display name—Name of the directory that shows up in the Address Search tab of the Compose window. This name can be any sequence of characters that does not contain a question mark (?) nor a comma (,).

TABLE 2-2 shows the URL encoding in the attribute value.

TABLE 2-2 Values and Their Encoding

Value	Encoded as
space	+
plus sign (+)	%2B
comma (,)	%2C
percent sign (%)	%25

You can use the arguments shown in TABLE 2-3.

TABLE 2-3 Arguments and Their Descriptions

Argument Names	Descriptions
ldapserver	LDAP server domain name. This argument is required because it specifies the domain name of the LDAP server to be searched.
ldapport	TCP port on which the LDAP server is listening. This parameter defaults to port 389.
timelimit	The maximum time in seconds that the LDAP server should spend searching.
base	The base argument for the search. Use the base argument to narrow the search to a specific area. An example of a base argument that specifies the base LDAP search parameters using URL encoding is: `base=dc=Sun%2cdc=com`
`binddn`	The `dn` (username) to use when accessing the LDAP server.
`passwd`	The password to use when accessing the LDAP server.
`scope`	One of `base`, `one`, or `sub`. This value specifies the type of search. The default value is `sub`.
`alias`	One of `never`, `search`, `find`, `always`. This value specifies how to handle aliases. The default value is `never`.

You must end the last argument with an ampersand (`&`) because the NetMail (Java) applet adds arguments for the search string and the count to the URL before doing the search.

Example One

The following parameter is an example that references the InfoSpace LDAP server:

```
ldapserver=ldap.infospace.com&,Infospace LDAP
```

Because the LDAP parameters are in the Administration Console, every user gets the same LDAP server list.

Example Two

The following parameter is an example that references server x with options.

```
ldapserver=srver.com&ldapport=1449&binddn=username&passwd=password&
alias=find,An LDAP server
```

When you use Netmail's Address Search feature to obtain access to a directory service, the LDAP request is passed to the web server that runs the LDAP CGI program. The CGI program requests information from the LDAP server. The web server must be able to communicate with the LDAP server. If the web server and the LDAP server are both behind a firewall, NetMail users can still search the directory even if they are outside the firewall.

Configuring Names of Uneditable Preferences

You can enter any or all of the parameters shown in TABLE 2-4 in the Names of Uneditable Preferences field on the page for Default Values for New NetMail Users in the Administration Console. The end user cannot change these preferences. Multiple values are separated by commas. The preferences that you enter will not be visible as editable values in NetMail's Preferences dialogue.

TABLE 2-4 Names of Uneditable Preferences for NetMail

Parameter	Possible Value	Default	Preference Field
`autopurge`	Boolean	False	Read | Purge deleted messages from Inbox:
`imapfolder`	Any string	Mail	Read | IMAP folder directory:
`imapinboxserver`	An IMAP server host name or IP address	None	Servers | Incoming mail (IMAP):
inactivityinterval	Integer 5 or greater	0	Read | Check for new mail every minute:
indentprefix	Any string	>	Send | Quote prefix for replies:
`initialheaders`	Any positive number	10	Read | Initial headers:
`logmessages`	Boolean*	True	Send | Keep copy of sent messages:
`multiplereadwindows`	Boolean	False	Read | Multiple read windows:
record	Any string	Sent	Send | Sent Messages Folder:
`replyfields`	Any combination of author, body, or date	Body	Send | Include in reply:
replytoaddress	Any string	None	Send | Reply to address:
`smtpmailserver`	An SMTP server host name or IP address	None	Servers | Incoming mail (SMTP):

* A Boolean value is considered true if the value is yes or true. Anything else is considered false. The value is not case sensitive.

Note – The values you specify for the parameters in the NetMail of the Administration Console override the default values.

Netlet

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure “To Stop and Restart the Web Server on the i-Planet Server” in Chapter 3 "Other Administrative Tasks.”

This is the client program that works together with the reverse proxy server on the i-Planet gateway to allow secure access from the Internet to TCP/IP application on your intranet. You can specify which predefined application rules will be enabled as well create rule for your own TCP/IP applications that you want to access through the Netlet.

Clicking the Netlet link displays the Netlet Administration page, shown in FIGURE 2-11.

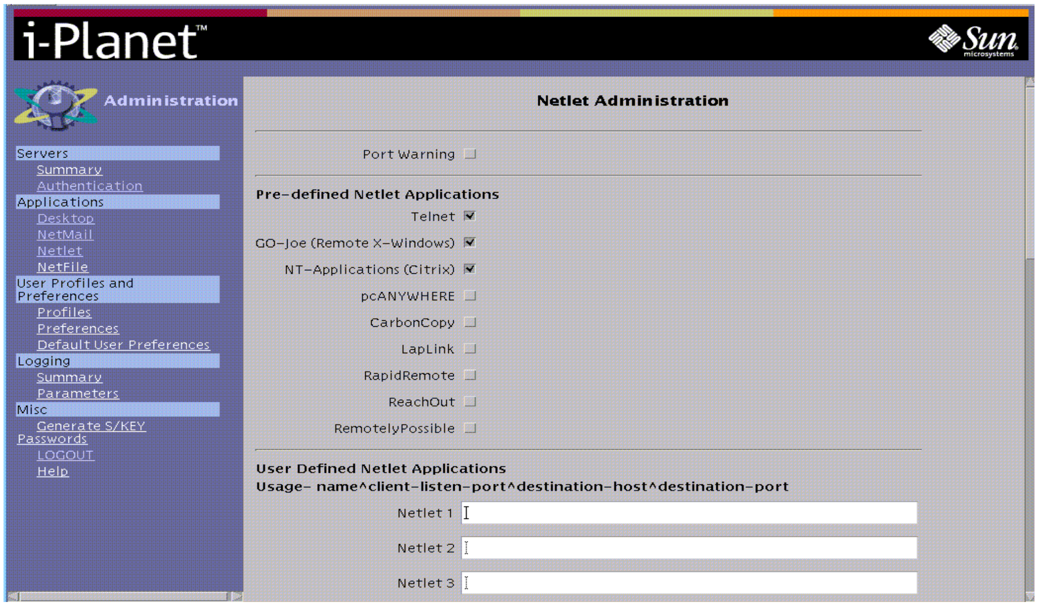

FIGURE 2-11 Netlet Administration Page

Note – The predefined Netlet rules work in conjunction with NetFile. For them to be active, you must enable them on this page and on the NetFile Configuration page.

The Netlet Administration page shows the predefined applications and provides a the place and the means for writing user-defined Netlet rules (up to a limit of 30).

The predefined function and rules are:

- **Port Warning**—Enables or disables support for a warning window that displays from the NetFile page of the i-Planet Desktop application when a connection to a Netlet port is being attempted. The Netlet Connection Attempt window also shows the number of the port. The end user can then decide to:
  - Click OK to continue
  - Cancel to stop the connection
  - Choose not to see this warning again, which disables the port warning for the current session *only*.
- **Predefined Netlet Rules**—Enables or disables support for the applications listed.

  The destination system is given at runtime through the NetFile application. You must also enable the Netlet functions on the NetFile Configuration page. The defined applications are:

- **Telnet**—allows end users to use Telnet to have access to systems on the intranet. Addresses for Telnet are established dynamically, if you are using NetFile. The Telnet client is the one that is configured in the client browser.
- **GO-Joe** (remote X-Windows)—allows end users to use GO-Joe for remote X-Window control for the Solaris operating environment. GO-Joe is a thin client X server that uses a three-star, distributed client-server architecture (X server, X client, and display applet). The GO-Joe server must be installed on the destination machine. Information on the requirements for installing GO-Joe is in the section "GO-Joe" in Appendix C "Third-Party Software."
- **NT-Applications** (Citrix)—allows end users to use Citrix-based applications over the Internet. Citrix reserves port 1494. Citrix has Java and non-Java clients that support TCP/IP. i-Planet is customized to start the Citrix client (Java applet) and a Citrix-based proxy when you configure it appropriately.

Note – If your end users will be connecting to any a Microsoft Windows-based machine using NetFile, you must first install the Samba software that is on the i-Planet CD-ROM, "Contains 3rd Party Software Packages Only," on the i-Planet server.

- **pcANYWHERE** (a Windows 95, 98, and NT remote-control product)—Allows users to have remote PC Microsoft Windows control. Information on installing and configuring pcANYWHERE is in the section "pcANYWHERE" in Appendix C "Third-Party Software." The pcANYWHERE client (Java applet) software is installed with i-Planet. A demonstration copy of the pcANYWHERE server software is on the i-Planet CD-ROM, "Contains 3rd Party Software Packages Only." If you enable this option, you must buy a copy of the server software and install it on the computer that your end users want to control remotely.

  The i-Planet product also supports the software CarbonCopy, LapLink, RapidRemote, ReachOut, RemotelyPossible (all Microsoft Windows 95, 98, and NT remote-control products). If you want to use them, you must buy these products separately.

  TABLE 2-5 shows the ports that are reserved for the predefined Netlet rules. Do not use these reserved ports in writing your own Netlet rules.

TABLE 2-5 Reserved Listen Ports for Predefined Netlet rules

Predefined Netlet rule	Reserved Ports
Telnet	30000
GO-Joe	10491
Citrix	1494
pcANYWHERE	4631, 5632

TABLE 2-5 Reserved Listen Ports for Predefined Netlet rules

Predefined Netlet rule	Reserved Ports
CarbonCopy	1138
LapLink	51547
RapidRemote	45414
ReachOut	43188
RemotelyPossible	799
loopback*	8000

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

`loopback` is required because of the Java security model. Applets are only allowed to make connections back to the server from which they were loaded. In order to make the included client applets work with the Netlet, they must appear to be downloaded from server `localhost`. This is accomplished by telling the Netlet to fetch the desired applet. Traffic requests on the `loopback` port are requests to the Netlet to go back to the i-Planet server and download the object whose path is given in the URL.

- **User-Defined Netlet rules**—You define the user-defined Netlet rules in the lower half of the Netlet Administration page, shown in FIGURE 2-11. The end user cannot dynamically specify a destination server at run time. The destination server is fixed. You must define the whole path for them.

Note – You are limited to 30 user-defined rules.

The syntax for defining these applications is: *`name^client-listen-port^destination-host^destination port,`* in which:

- The symbol "^" is the field separator in this syntax.
- *`name`*—some identifier for this entry. It is only used to track the application.
- *`client-listen`*—the port for which the Netlet listens on the end user's client machine.There can be only one entry or rule for each `client-listen` port
- *`destination-host`*—the name or IP address of the destination host to which traffic will be directed.
- *`destination-port`*—the port on the destination host to which all traffic will be directed.

Note – You cannot assign a port number greater than 64000 when you are defining your own Netlet rules.

For example, the following procedure shows how to write a Netlet rule that will allow telnet traffic to a specific system.

▼ To Write a Netlet for Special Telnet Handling

1. **Write a Netlet rule for special handling of Telnet in one of the fields for writing user-defined Netlet rules, as follows:**

```
telnetspecial^23^machine-on-the intranet^23
```

2. **Click the Enter button at the bottom of the page to save this Netlet rule.**

   This Netlet allows Telnet traffic from any remote machine and directs it to `machine-on-the-intranet`. Any normal Telnet traffic on port 23 (the destination Telnet port) to the machine on which the netlet is running will be redirected to `machine-on-the-intranet`. You can specify different names or port numbers, depending on your requirements. You must not have any other handler for port 23 for this to work (that is, no Telnet service/daemon specified).

3. **As root on the i-Planet server, stop and restart the web server so that the Netlet rule you just defined will take effect.**

   See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3 "Other Administrative Tasks."

Note – If you monitor incoming or outgoing traffic through your firewall, you will see that all Netlet traffic on the outside actually passes on your SSL port (likely 443). The TCP protocols used by the Netlet rules are tunnelled through your SSL port.

See Appendix D "Configuring TCP/IP Client/Server Products to Work With the Netlet" for more information on configuring user-defined Netlet rules.

NetFile

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3 "Other Administrative Tasks."

Clicking the NetFile link displays the NetFile Configuration page shown in FIGURE 2-12.

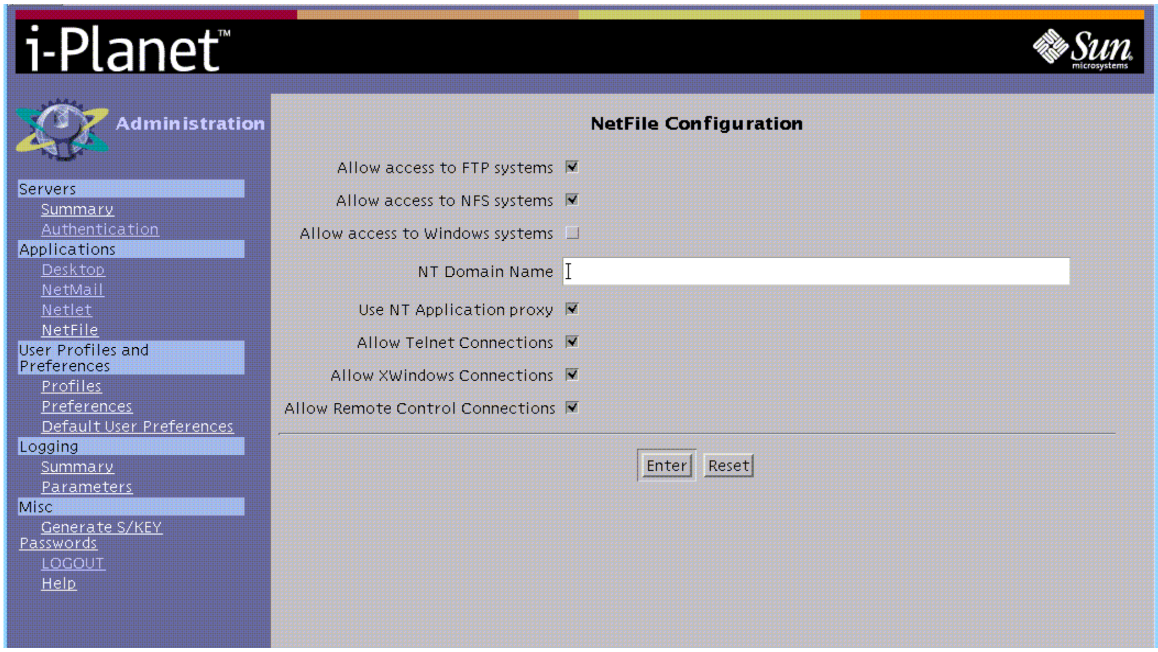

FIGURE 2-12 NetFile Configuration Page

Note – For defined applications on the Netlet Administration page to be active, they must be turned on here and on the Netlet Administration page.

Allow Access to FTP, NFS, Microsoft Windows, and NetWare Systems

These options enable or disable support for access to FTP, NFS, Microsoft Windows, and NetWare systems. You must obtain the NetWare software separately. NetFile will automatically detect the type of file system for a selected system. Access to a system that supports multiple access types is assigned in the following order:

- Allow access to Windows systems
- Allow access to FTP systems
- Allow access to NFS systems
- Allow access to NetWare systems

Note – The information for NetWare will only appear on the NetFile Configuration page, if you have installed NetCon 7.0 from the NetCon Corporation on the i-Planet server. You can use NetCon 7.0 only with Solaris 2.5.1. and 2.6.

The machine type is determined by seeing if a connection can be established to well-known ports. For example, 139 is used for Microsoft Windows networking (for Windows '95, '98, and NT), 21 is used for FTP, and 2049 is used NFS.

If, for example, a system can be reached through Microsoft Windows networking, then it will treated as a Microsoft Windows system, regardless of whether or not it can also be reached through FTP.

Note – If you have not installed the Samba software to allow access to a Microsoft Windows network, then enabling Microsoft Windows system setting on the NetFile Configuration page will not provide end users access. The Samba software is on the i-Planet CD-ROM, "Contains 3rd Party Software Packages Only."

- **NT Domain Name**—Enter the name of the NT domain that provides authentication to your Microsoft Windows network.

All of the remote windowing functions and applications below are only available through the Java version of NetFile.

- **Use NT Application proxy**—Enables or disables Netlet support for a Citrix-based proxy.
- **Allow Telnet Connections**—Enables or disables Netlet support for Telnet access to the hosts that the end users select.
- **Allow X Windows Connections**—Enables or disables Netlet support for X Windows. It allows an end user to run an X Window session over the Internet. The GO-Joe client software is included with the i-Planet server. For more information on GO-Joe, see Appendix C "Third-Party Software.".
- **Allow Remote Control Connections**—Enables or disables Netlet support for remotely controlling Microsoft Windows Desktop systems. The supported remote control products are listed in "Netlet" section of this chapter.

  All remote control software (except pcANYWHERE) must be configured to send all traffic to `localhost`. The Netlet will intercept this local traffic, encrypt it, and route it through the i-Planet proxy. If end users want to use pcANYWHERE software, they must install the pcANYWHERE host on the PCs that they want to control remotely on the private network. See the section "pcANYWHERE" in Appendix C "Third-Party Software" for instructions on installing and configuring pcANYWHERE.

Note – With pcANYWHERE's Java client, you do not need to install client software.

End users must install the appropriate client remote-control software on their local PC and appropriate server software on remote systems, if they want to use a remote-control application. (The GO-Joe server software is included on the i-Planet CD-ROM, “Contains 3rd Party Software Packages Only.”) They should check the documentation of the remote-control application for any requirements.

Caution – End users should verify that the remote-control software is working properly before attempting to use it through i-Planet.

User Profiles and Preferences Section

This section contains links to the profiles of the users and their preferences as well as allowing you to edit the default preferences and parameters.

Profiles

Clicking the Profiles link displays the User Profile Summary table shown in FIGURE 2-13. It shows user ID, available roles (admin or web or both) for each user ID, and the default user page.

You can only view the information in the User Profile Summary page.

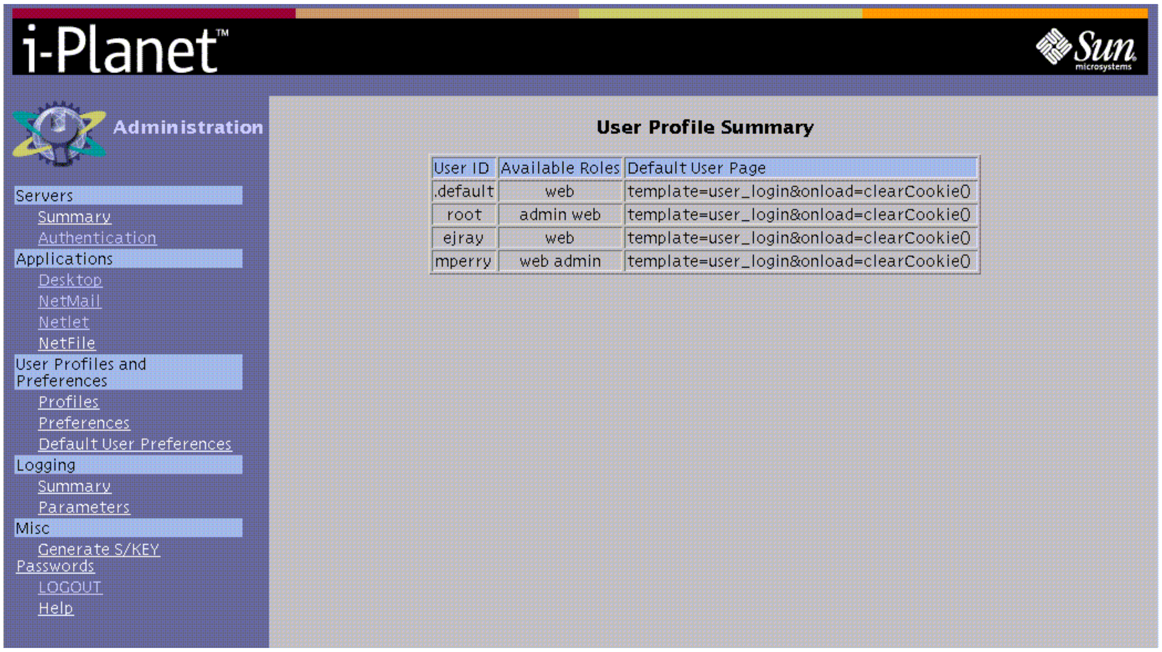

FIGURE 2-13 User Profile Summary Table

Preferences

You can only view the information in the Preference page.

To view an end user's preference, you move through a series of administration pages for the initial letter or character for the end user's name, then the name of the end user at whose preferences you want to look.

- Clicking the Preferences link displays the User Preference Directories page shown in FIGURE 2-14.

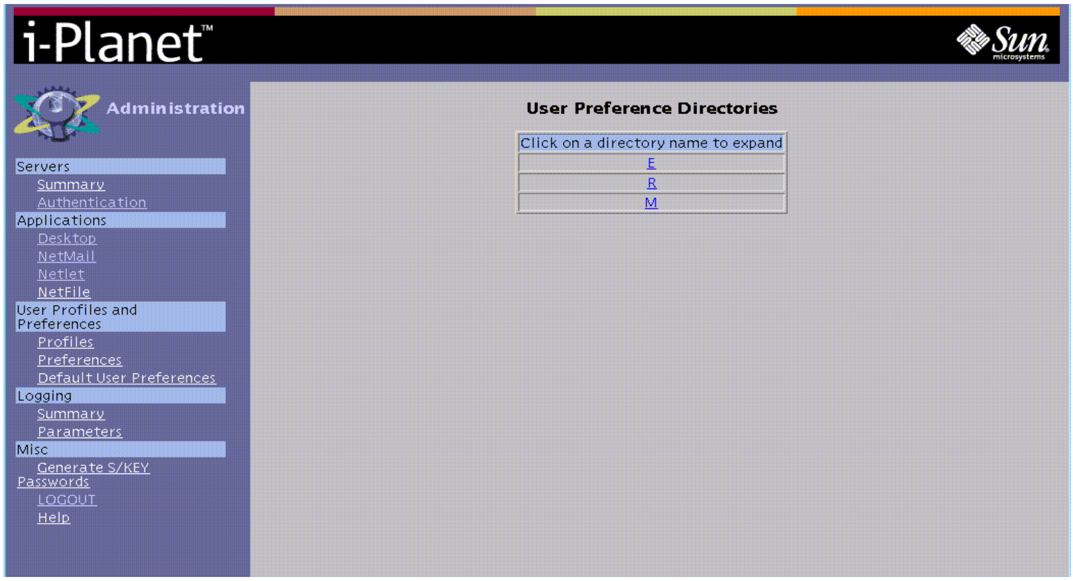

FIGURE 2-14 User Preference Directories Page

- Clicking a letter (or character) displays the login names that start with that letter (or character) shown in FIGURE 2-15.

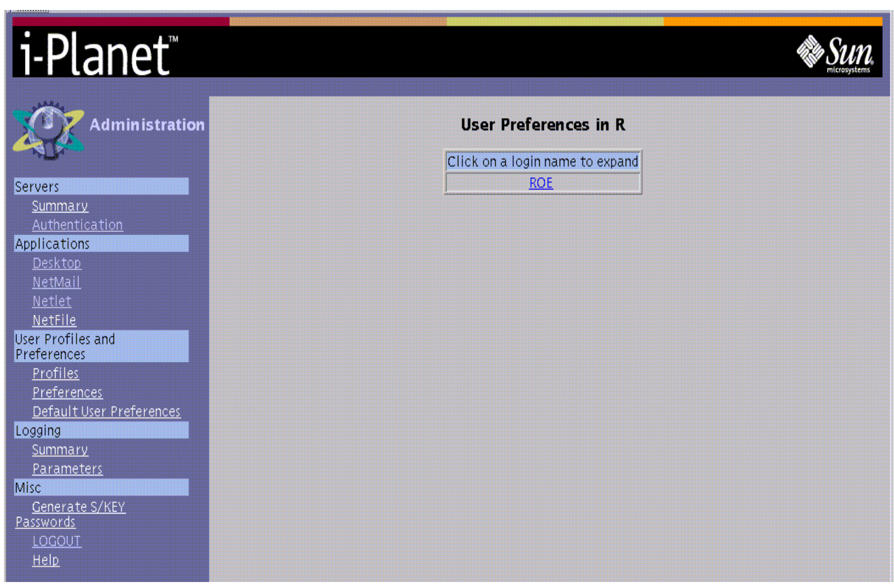

FIGURE 2-15 User Preferences for Login Names Starting With the Letter ”R”

- Clicking a user's name displays a table showing the preferences for that user shown in FIGURE 2-16.

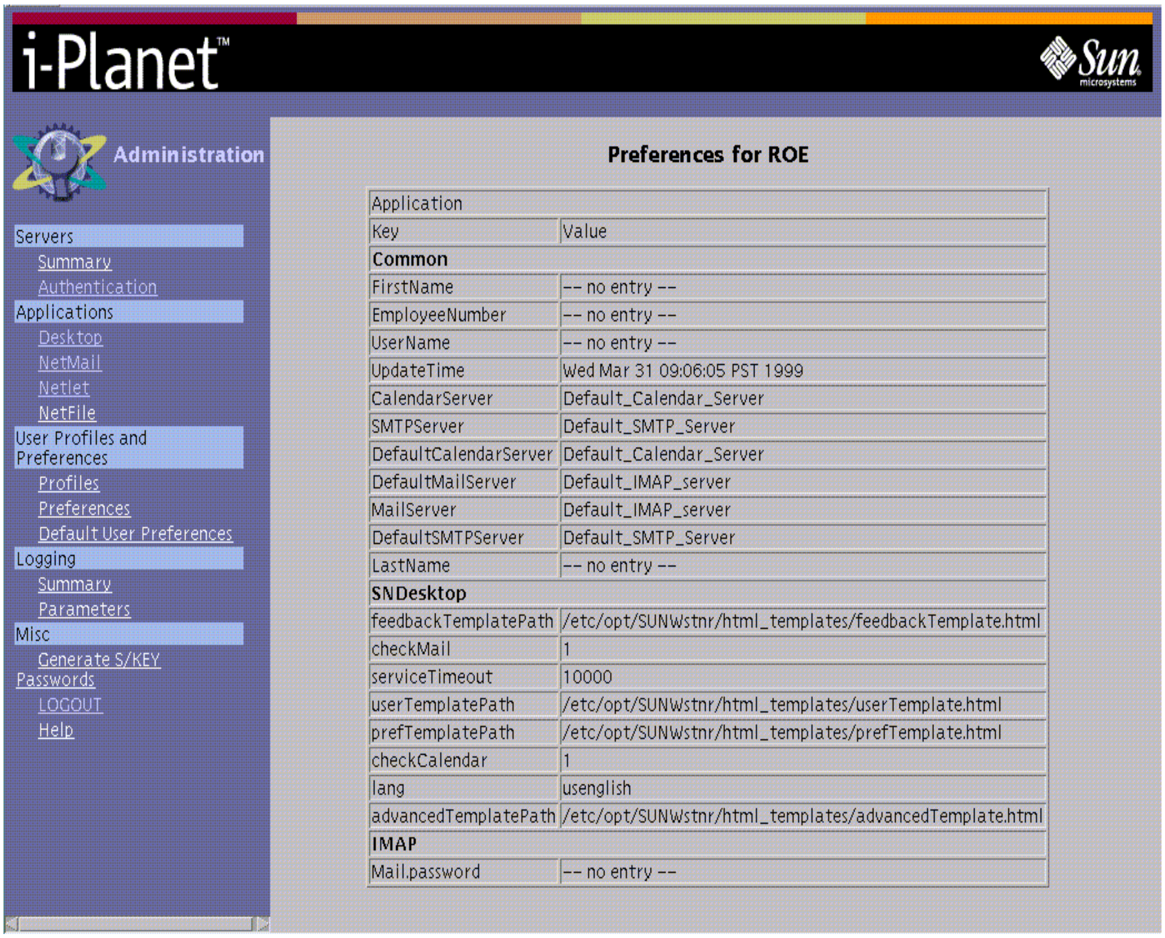

FIGURE 2-16 User Preferences for ROE Table

Preferences page shows the current configuration settings for each end user (both those that are controlled through the i-Planet Administration Console and those that end users can configure through their i-Planet Desktop). You can use the information contained here in debugging problems in connecting to the various applications over the Internet.

Default User Preferences

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3 "Other Administrative Tasks."

Clicking the Default User Preferences link displays the Default User Preferences and Profiles, shown in FIGURE 2-17 and FIGURE 2-18.

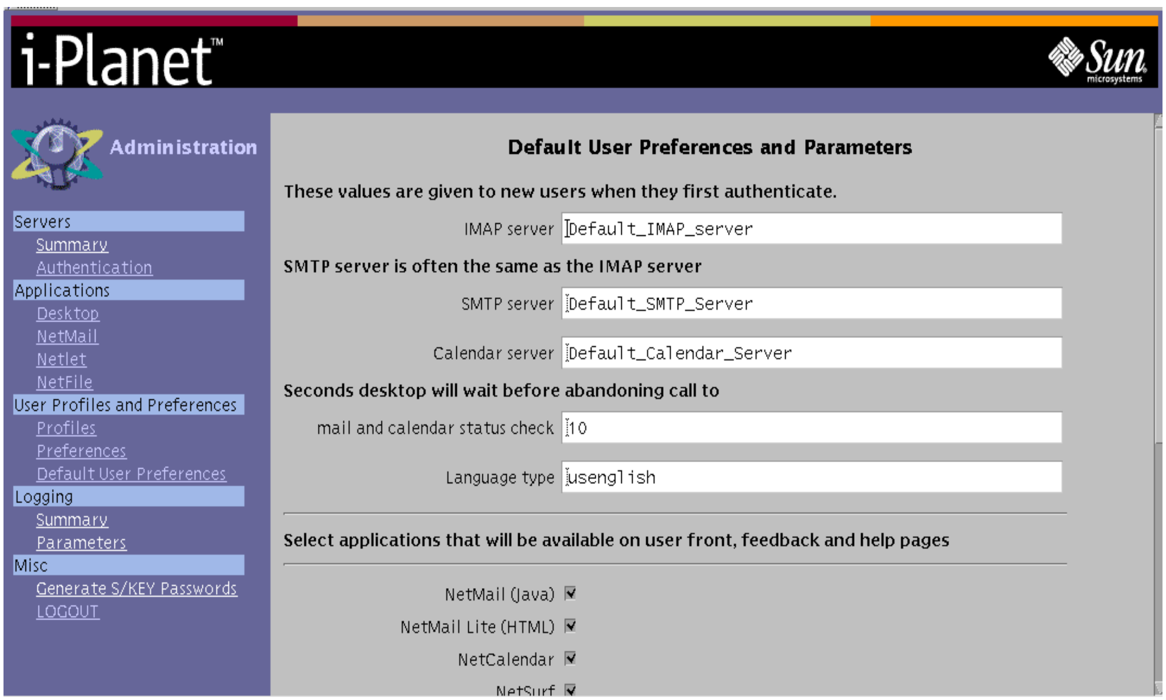

FIGURE 2-17 Default User Preferences and Parameters Page—Upper Half of the Page

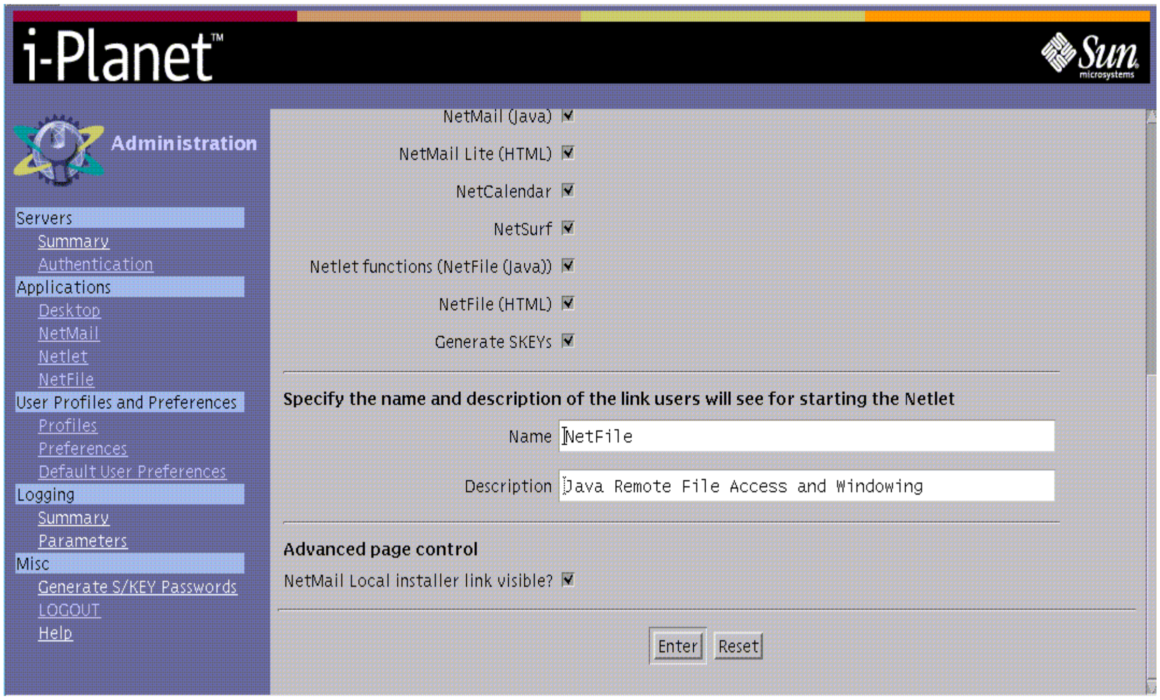

FIGURE 2-18 Default User Preferences and Parameters Page—Lower Half of the Page

These are the values that new end users have when they first authenticate. They are reflected in the fields of the Preferences page of the i-Planet Desktop when the end users first log in. End users can edit some values on the Preferences page of the i-Planet Desktop, but not all. If an application is visible, end users have access to it.

On this page, you specify:

- The time in seconds that the i-Planet Desktop will wait before abandoning a call to the mail and calendar servers
- The Preferred language. The default is US English.
- The Applications that appear on the front page of the i-Planet Desktop that end users see. Enabling an application also enables the help and the feedback pages for that application.
- That the NetMail Local Installer Link is to be visible on advanced page control. This makes the NetMail Local Installer visible on the Advanced Options page of the i-Planet Desktop. When the end users click on the NetMail Local Installer link, a browser window appears. As explained in this window, the functionality allows end users to install the NetMail applet on their local disk so that they can use NetMail to read and compose email without being connected to the Internet. This is known as *disconnected mode*.

Once end users have installed the NetMail applet locally, they can connect and read their email without having to download the applet each time. They also can save their email to an encrypted file on disk, so that they can continue working while they are disconnected from the server. When they reconnect, all their changes to the local email cache will be made to the server, synchronizing their states. Any email that they have composed and want sent will also be sent when they reconnect. The end users are guided through the installation of this feature.

You can test the changes by making the changes using one browser, then viewing the results in another browser instance.

Logging Section

This section contains links to log files, allows you to turn logging on or off, and to change the log server parameters

Summary

Clicking the Summary link displays a table that contains links to the current and previous revisions of the Netlet, NetMail, Authentication, and Master Log files, as shown in FIGURE 2-19. The previous revisions are the most recently archived versions.

Note – You turn logging on or off on this page. If you change the status of the logging, you must click **Enter** so that this change will save your changes. You must stop and restart the web server for the changes to take effect. See the procedure “To Stop and Restart the Web Server on the i-Planet Server” in Chapter 3 "Other Administrative Tasks.”

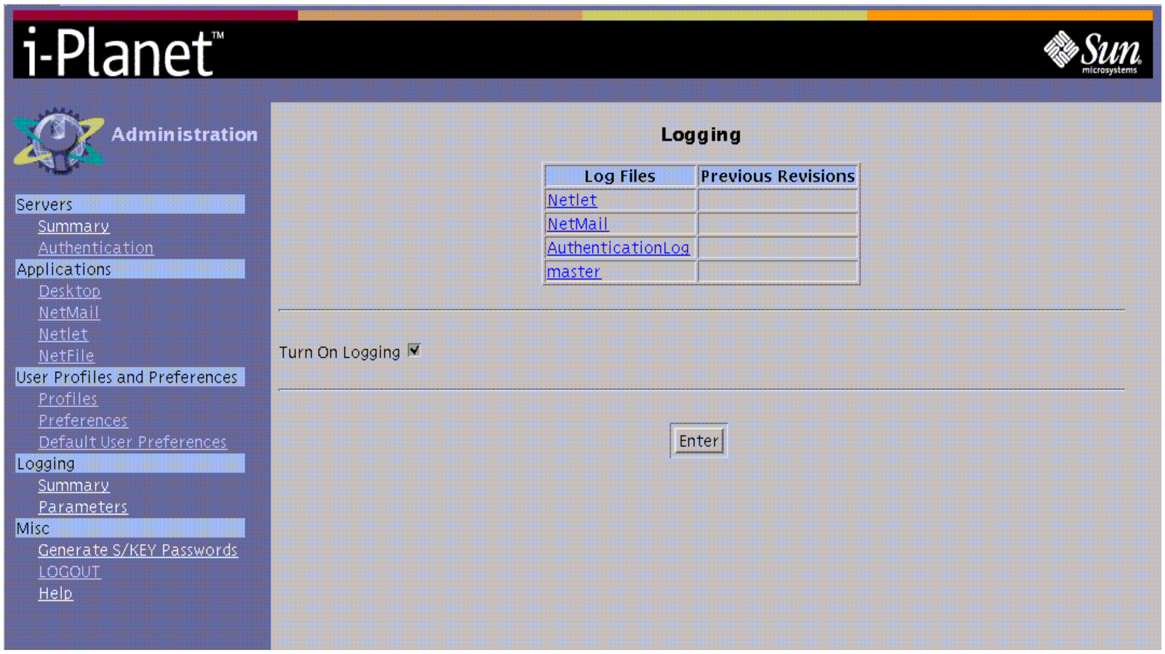

FIGURE 2-19 Links to the Various Log Files

The log files are displayed for viewing only when you click the link to them. The log files are in `/var/opt/SUNWstnr/logs`. The log files are flat files that you can manipulate with the usual UNIX tools.

Parameters

Clicking the Parameters link displays the Log Server Parameters page, shown in FIGURE 2-20. You can change the location of the log files, the maximum size of the log files, and the number of the history files from this page. The location of the log file is relative to the root of the server (host). The size of the log file is in bytes.

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3 "Other Administrative Tasks."

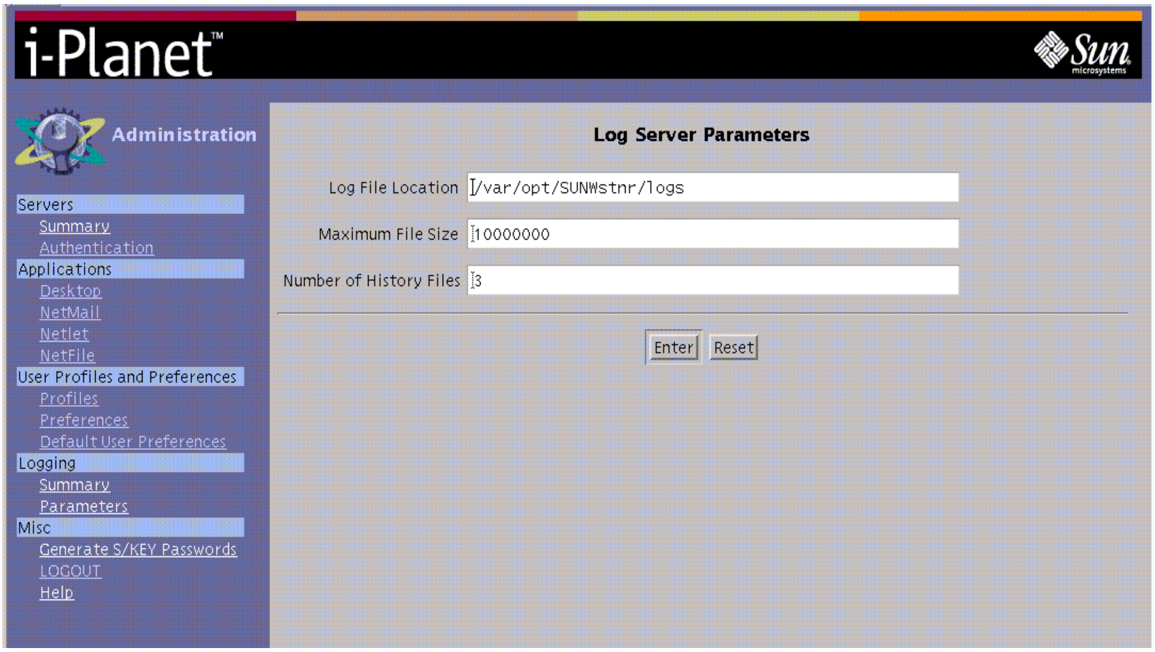

FIGURE 2-20 Log Server Parameters Page

Miscellaneous Section

This section contains the links for generating S/Key passwords for your users, logging out of the Administration Console, and displaying the online help for the Administration Console.

Note – If you change any of the parameters on this page, before you leave the page, you must click **Enter** to save your changes. After you have made all the changes in your editing session, you must stop and restart the web server for the changes to take effect. See the procedure “To Stop and Restart the Web Server on the i-Planet Server” in Chapter 3 "Other Administrative Tasks.”

Generating S/KEY Passwords

Clicking the Generate S/Key Passwords link displays the Create S/Key Passwords page, shown in FIGURE 2-21. Use this page to generate new S/Key passwords for users before they become end users.

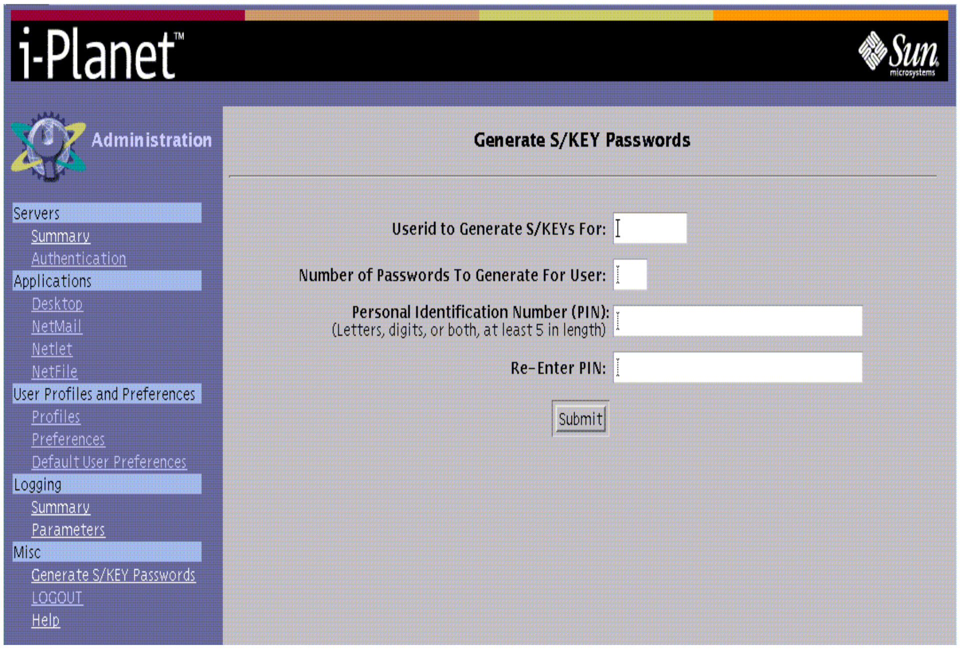

FIGURE 2-21 The Generate S/Key Passwords Page

The name you enter in the Userid to Create S/Key for box must be a valid UNIX user name for the i-Planet server or the server on which the Administration Console is running.

▼ To Generate the S/Key Passwords

1. **Type the user name (Userid),**
2. **Type the number of passwords that you want generated.**

   (The maximum number of allowable sets of S/Key passwords is displayed on the Authentication Parameters Page.)
3. **Type the personal identification number (PIN).**

   The PIN must be at least five alpha-numeric characters long.
4. **Type the PIN again for confirmation.**
5. **Click the Submit button to generate the list of passwords for the end user**

   The list of passwords generated for the end user is displayed as shown in FIGURE 2-22.

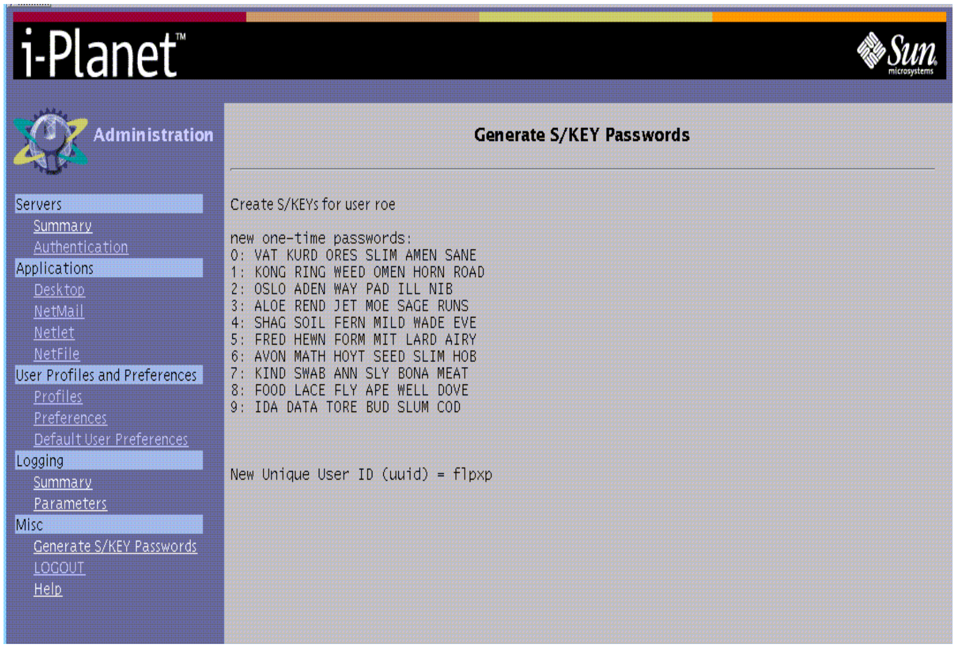

FIGURE 2-22 List of S/KEY Passwords Generated

6. **Give the end user the generated list of passwords, the unique user ID (uuid), and, separately, the PIN that you used in generating the list.**

   The end user will need the unique user ID and PIN as well as the list of passwords, in order to log in remotely.

7. **Remind the end user to keep the PIN separate from the unique user ID and the list of passwords.**

Logout

Clicking the LOGOUT link logs you out and displays the Logout Confirmation page, shown in FIGURE 2-23.

FIGURE 2-23 The Logout Confirmation Page

Help

Clicking the Help link displays the HTML page for the Administration Help Topics shown in FIGURE 2-24. Use the links to navigate through the online help. The help page also has links to the PostScript files of the documentation.

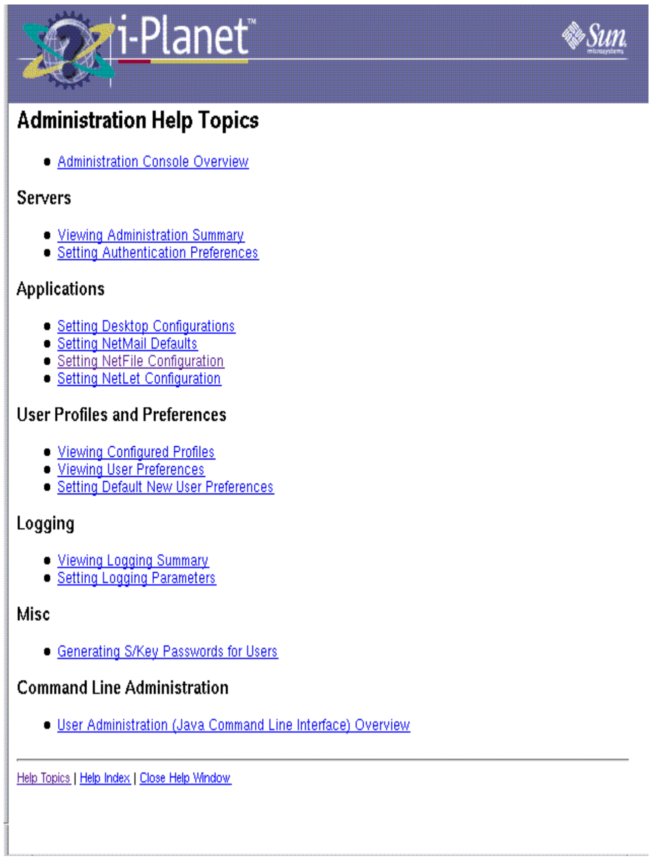

FIGURE 2-24 Administration Help Topics

CHAPTER 3

Other Administrative Tasks

This chapter describes how to:

- Modify choices that were made during the installation procedure
- Modify files for special circumstances
- Stop and restart the i-Planet gateway's reverse proxy
- Stop and restart the i-Planet server's web server
- Find and install certificates from a certificate authority

Subdomains

If, after you have installed the i-Planet software, you want to add, delete or change subdomains on your network, you must edit the file `/opt/SUNWsnrp/config/HTMLTranslator.config` on the i-Planet gateway.

▼ To Add a Subdomain or Subdomains

1. **As root, add the new domain or domains to (or delete the domain or domains from) the line `Domains=Eng` in the file** `/opt/SUNWsnrp/config/HTMLTranslator.config` **on the** i-Planet gateway. **Use the vertical line (or pipe) (|) character to separate the subdomains.**

   For example, if you defined the `eng` subdomain during installation and you now want to include the `corp` domain, add `|corp` to the line `Domains=eng`. The name for the subdomain is not case sensitive.

   The file should now look like the following:

```
Host=https://i-Planet_server.eng.company.com/
Domains=Eng|corp
…
```

2. **Stop and restart the reverse proxy on the** i-Planet gateway **for the change to take effect.**

   See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in this chapter.

Web Proxy

Adding a Web Proxy

If you opted not to define a web proxy during the installation procedure, you can add one by the following procedure.

▼ To Add a Web Proxy

1. **As root, on the** i-Planet gateway**, modify the file** `/opt/SUNWsnrp/config/ReverseProxy.config` **so that the line** `Proxy=` **reads** `Proxy=`*`fully_qualified_name_of_web_proxy_machine`*`:`*`port_number`***, if the port number is required.**

   You can also use this procedure to change the web proxy. For example, if you want to change the `webproxy2.corp.company.com` as the web proxy and you want to use port from 8000 to 8080. Change the line `Proxy=` in the file `/opt/SUNWsnrp/config/ReverseProxy.config` to `Proxy=webproxy2.eng.company.com:8080`.

   The line in the file should now look like the following:

   ```
   Proxy=webproxy2.corp.company.com:8080
   ```

2. **Stop and restart the reverse proxy on the i-Planet gateway for the change to take effect.**

   See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in this chapter.

Fine Tuning the Web Proxy

If you have installed a web proxy either during installation or after install, you can fine tune the web proxy by modifying the file `/opt/SUNWsnrp/config/ReverseProxy.config` and the files `/etc/opt/SUNWstnr/gateway/UseWebProxyURL.conf` and `/etc/opt/SUWNstnr/gateway/DontUseWebProxyURL.conf`. This permits you to specify:

- URLs that must be passed to the web proxy.
- URLs that are not to be passed to the web proxy.

If the line `Proxy=` does not contain a web proxy, no web proxy is used, no matter what value is set for `UseProxy=`. If a web proxy is specified in the line `Proxy=`, then that web proxy is used or not, depending on the value, `true` or `false`, to which you have set the line `UseProxy=`:

- `true` means that you want to use the web proxy for any URL, except for those listed in the file `DontUseWebProxyURL.conf` file.

  If you want a URL to be passed to the web proxy, the request header is checked against the entries in the `DontUseWebProxyURL.conf` file. If it matches, the request is not passed to the web proxy. If it does not match any of the entries, it is passed to the web proxy.

- `false` means that you do not want to use the web proxy for any URL, except for those listed in the file `UseWebProxyURL.conf` file.

  If you do not want a URL to be passed to the web proxy, the request header is checked against the entries in the `UseWebProxyURL.conf` file. If it matches, the request is passed to the web proxy. If it does not match any of the entries, it is not passed to the web proxy.

Use the following procedure to tune the web proxy and to set which URLs must pass through the web proxy and which do not.

▼ To Tune the Web Proxy

1. **As root, on the i-Planet gateway, modify the** `ReverseProxy.config` **file in the directory** `/opt/SUNWsnrp/config` **so that the line** `UseProxy=true`**, if you want to use the web proxy for all URLs or so that the line** `UseProxy=false`**, if you do not want to use the web proxy for all URLs.**

2. **As root, on the i-Planet gateway, type the URLs for which you want to use the web proxy in the file** `/etc/opt/SUNWstnr/gateway/UseWebProxyURL.conf`**.**

   The form for the URLs is `http://`*`hostname:port_number`*, where the `hostname` and `port_number` must match the name of the host and the port number where it is used in any other file or in the Administration Console.

3. **As root, on the i-Planet gateway, type the URLs for which you do not want to use the web proxy in the file** `/etc/opt/SUNWstnr/gateway/DontUseWebProxyURL.conf`**.**

   The form for the URLs is `http://`*`hostname:port_number`*, where the `hostname` and `port_number` must match the name of the host and the port number where it is used in any other file or in Administration Console.

4. **Stop and restart the reverse proxy on the** i-Planet gateway **for the change to take effect.**

   See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in this chapter.

Stopping and Restarting the i-Planet Gateway's Reverse Proxy Server

If you modify any of the configuration files manually, you must restart the i-Planet gateway's reverse proxy server for it to recognize the changes. It is generally a good idea to first stop the reverse proxy, to ensure that it is not running, then to restart the reverse proxy.

Note – Restarting the reverse proxy on the i-Planet gateway should not affect an application, if it is not using a Netlet other than the time it takes to restart the reverse proxy server on the i-Planet gateway. Any connection through the Netlet will be lost when you restart the reverse proxy server.

If you have to reboot the i-Planet gateway, the reverse proxy server will start automatically.

▼ To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway

- **As root on the** i-Planet gateway**, stop and restart the reverse proxy server:**

```
# /opt/SUNWsnrp/bin/iplanet_gw stop
# /opt/SUNWsnrp/bin/iplanet_gw start
```

URL Rewriting for HTML Files

Within HTML files, URLs can exist anywhere in JavaScript™. The URL rewriter must be able to open the page to which the URLs in the JavaScript statements refer. For the Java rewriter to be able to do this, you must modify the file /opt/SUNWsnrp/config/HTMLTranslator.config on the i-Planet gateway.

▼ To Modify the File HTMLTranslator.config

1. **As root on the i-Planet gateway, add the following lines to the file** /opt/SUNWsnrp/config/HTMLTranslator.config:

```
JavaScriptRewrite=openNewWindow:y|parent.openNewWindow:y
JavaScriptVariables=location.href|_fr.location|mf.location\
|parent.location|self.location
```

JavaScriptRewrite variable is set equal to the function openNewWindow or parent.openNewWindow and its flag set to y. Functions have the form func1:y, ,y, where func1 is the name of the function, the colon separates the name from the flags, and the flags are separated by commas. A flag is an instruction to translate a corresponding argument or not.

The statement JavaScriptRewrite=func1:y, ,y|func2:,y,y means that if the variable JavaScriptRewrite finds func1 or func2 in an HTML page, it will rewrite it according to the flags set for the arguments to that function. If it finds func1, it will rewrite the first and third arguments because the flags for those arguments are set to y for yes, but not to the second argument. If it finds fun2, it will rewrite the second and third arguments because the flags for those arguments are set to y to yes, but not the first argument.

The URL rewriter sets the JavaScriptVariables listed equal to the values for these variables that it finds in the JavaScript in an HTML page.

For example, the variable JavaScriptVariable is set so that the line in the file reads JavaScriptVariables=location.href|_sr.href and an HTML page contains the following JavaScript:

```
<script language=javascript>
loc = "/cgi-bin/aaa.cgi";
location.href = "/cgi-bin/bbb.cgi";</script>
```

The URL rewriter looks through the JavaScript for the variables location.href and _sr.href. It finds a match for location.href, and it does not find a match for the variable loc (because the variable loc does not appear in the JavaScriptVariables statement). It also does not find a match for _sr.href.

The URL rewriter then sets the value of location.href equal to "/cgi-bin/bbb.cgi", and the HTML page becomes:

```
<script language=javascript>
loc = "/cgi-bin/aaa.cgi";
location.href =
"https://i-Planet_gateway/http://destination_host/cgi-bin
/bbb.cgi";</script>
```

The variable loc remains unchanged since there are no instructions in the JavaScriptVariables statement for rewriting it.

2. **Stop and restart the reverse proxy on the i-Planet gateway for the change to take effect.**

   See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in this chapter.

Enabling or Disabling UNIX Login to The i-Planet Desktop for the End User

You can enable or disable UNIX login for the end user to the i-Planet Desktop on the i-Planet gateway.

▼ To Enable UNIX Login for the End User

1. **As root on the i-Planet gateway, type the following command to enable the end user to use UNIX to log in to the i-Planet Desktop.**

```
# /opt/SUNWsnrp/bin/iplanet_gw unix on
```

2. **Stop and restart the reverse proxy on the i-Planet gateway for the changes to take place.**

   See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in this chapter.

3. **As root on the i-Planet server, type the following command to enable the end user to use UNIX to log in to the i-Planet Desktop.**

```
# /opt/SUNWjeev/bin/iplanet_serv unix on
```

4. **Stop and start the web server on the i-Planet server.**

   See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in this chapter.

▼ To Disable UNIX Login for the End User

1. **As root, type the following command on the i-Planet gateway to disable UNIX login.**

```
# /opt/SUNWsnrp/bin/iplanet_gw unix off
```

2. **Stop and restart the reverse proxy on the i-Planet gateway for the changes to take place.**

   See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in this chapter.

3. **As root on the i-Planet server, type the following command to disable the end user to use UNIX to log in to the i-Planet Desktop.**

```
# /opt/SUNWjeev/bin/iplanet_serv unix off
```

4. **Stop and start the web server on the i-Planet server.**

   See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in this chapter.

Adding Users for the Administration Console

Use the following procedure to enable users to administer i-Planet through the Administration Console.

▼ To Add a User Who Has Not Logged In

1. **If a regular user has not previously logged into the i-Planet Desktop and you want to enable a regular user to run the Administration Console, as root on the i-Planet server, change to the directory** `profiles` **and copy the file** `root` **to the name of the new user:**

```
# cd /opt/SUNWjeev/profiles
# cp root new-user
```

2. **Edit the file for the new user and replace the lines:**

   `role=web with role=`**`web admin`**

   `session.uid=root` with `session.uid=`***`new-user`***.

   The file for the new user should now look like the following:

```
role=web admin
user.url=http://fully_qualified_server_host_name:8080/\
servlet/SNDesktop?template=user_login
session.uid=new-user
```

▼ To Add a User Who Has Logged In

- **If the user has logged in, as root on the i-Planet server, edit the file for the user in** `/opt/SUNWjeev/profiles` **and add admin to the line** `role=web`**.**

  The file for the user should now look like the following:

```
role=web admin
user.url=http://fully_qualified_i-Planet_server_host_name:808
0/\
servlet/SNDesktop?template=user_login
session.uid=new-user
```

Note – If users want to run the Administration Console from outside the i-Planet gateway or firewall or both, they must have `admin` privileges. They must either log in as root or log in as a regular user with the admin role.

Web Server

The web server is located on the i-Planet server.

Restarting the Web Server

Caution – You must restart the web server manually after the i-Planet server fails. You must also restart the web server manually, if it fails.

You restart the web server with the following procedure:

▼ To Restart the Web Server

- **As root on the i-Planet server, type the following to restart the web server:**

```
# /opt/SUNWjeev/bin/iplanet_serv start
```

Stopping and Restarting the Web Server

If you make any changes, whether through the Administration Console or by editing files, you must stop and restart the web server on the i-Planet server before the changes will take effect.

If you have to reboot the i-Planet server, the web server will start automatically.

▼ To Stop and Restart the Web Server on the i-Planet Server

● **As root on the i-Planet server, type the following to stop and restart the web server:**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

Note – End users must start their session over because all the session information is contained in the i-Planet server. No warning message is sent to the end users.

Tuning the Web Server

Overview

This section provides information on tuning the web server for more efficient operation within the operating environment.

As root, you can:

- Add these settings to the file containing the shell script in `/etc/rc3.d` for settings like these
- Create a new file for these settings in `/etc/rc3.d`

The shell script in this file should run before the shell script in file `S42rp`, which contains the script that starts the Java Web Server™.

TCP/IP Settings

The following TCP/IP settings have been identified as beneficial to servers running web servers.

```
ndd -set /dev/tcp tcp_close_wait_interval 45000
ndd -set /dev/tcp tcp_mss_max 6000
ndd -set /dev/tcp tcp_fin_wait_2_flush_interval 16000
ndd -set /dev/ip ip_path_mtu_discovery 0
ndd -set /dev/tcp tcp_conn_req_max_q 1024
ndd -set /dev/tcp tcp_conn_req_max_q0 1024
```

```
ndd -set /dev/tcp tcp_conn_req_min 1
ndd -set /dev/tcp tcp_xmit_hiwat 65535
ndd -set /dev/tcp tcp_recv_hiwat 65535
ndd -set /dev/tcp tcp_cwnd_max 65534
ndd -set /dev/tcp tcp_keepalive_interval 90000
ndd -set /dev/tcp tcp_ip_abort_interval 60000
ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
ndd -set /dev/tcp tcp_rexmit_interval_initial 3000
ndd -set /dev/tcp tcp_rexmit_interval_min 3000
ndd -set /dev/tcp tcp_rexmit_interval_max 10000
ndd -set /dev/tcp tcp_conn_grace_period 500
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/tcp tcp_slow_start_initial 2
```

Using the Java Web Server Administration Tool

It should be unnecessary to administer the Java web Server through the Java Web Server Administration tool. But should it be necessary, use the following procedure to enable the password and log in to the Java Web Server.

The default setting for logging in to the Java Web Server Administration tool is set to **admin** as the login. The default password, admin, as the password is disabled when the Java web server is installed.

If you need to run the Java Web Server Administration tool, you must

- Enable the default password
- Run the administration tool
- Change the password for reasons of security

Note – Do not use the Java Web Server Administration tool to start and stop the Java Web Server. Use the command in the procedure below or in the section “Stopping and Restarting the Web Server” in this chapter.

▼ To Enable the Password and Log In to the Java Web Server Administration Tool

1. **Enable the default password for the Java Web Server Administration tool:**

```
# cp /opt/SUNWjeev/realms/data/defaultRealm/keyfile \
/opt/SUNWjeev/realms/data/adminRealm/keyfile
```

2. **Stop and restart the web server on the i-Planet server**

   For information on stopping and restarting the web server, see the section "Stopping and Restarting the Web Server" in this chapter.

Caution – The default login is **admin** and the default password is **admin**. This is a security risk. Please log in to the Java Web Server Administration tool and change the password.

---

3. **In a browser, type the following URL to run the Java Web Server Administration tool:**

```
http://i-Planet_server:9090/
```

Port 9090 is the administration port for the Java Web Server.

Denying NetFile End Users Access to Hosts

You can edit the `netfile.denyhosts` field in the `/etc/opt/SUNWstnr/platform.conf` file to deny end users access to hosts such as the i-Planet gateway. You do this by editing the `platform.conf` file on the i-Planet server. You cannot do this using the Administration Console.

If end users try to add a machine whose IP address is one of those in `netfile.denyhosts` field, they will receive an error message and they will not be allowed access to that machine.

NetFile always denies access to the host on which it is running. NetFile gets this address itself. You do not need to add its address to the `platform.conf` file manually.

▼ To Deny Hosts Access to i-Planet NetFile Application

- **Add the IP addresses of the machines to which you want to deny access in the** `netfile.denyhosts` **field of the** `/etc/opt/SUNWstnr/platform.conf` **file on the i-Planet server, for example:**

```
netfile.denyhosts=129.123.1.1 123.123.1.2
```

Separate the addresses in this field by spaces. Use the form in the example.

Licensing

General Information About Licensing

i-Planet requires that the number of end users in the file `/opt/SUNWjeev/profiles` be equal or less than the number of Right To Use (RTU) tokens that is available under your licensing agreement. You can remove end users who are no longer with your company, but you cannot have more users than your allotted RTUs. If you have more names in the `profile` file, no one will be able to log in.

If the license server should stop or if you stop the license server, end users will not be able to log into the i-Planet Desktop until it is started.

Stopping and Starting the License Server

If the i-Planet server should go down, the license server should automatically start at reboot. If the license server does not automatically start up, use the following commands to stop and start the license server. In the unlikely event that your end users receive an error message that they cannot log in, it may be that you must restart the license server

▼ To Stop and Start the License Server

1. **As root, on the i-Planet server, stop and start the license server:**

```
# /etc/rc2.d/S85lmgrd stop
# /etc/rc2.d/S85lmgrd start
```

2. **Stop and restart the web server on the i-Planet server.**

   For information on stopping and restarting the web server, see the section "Stopping and Restarting the Web Server" in this chapter.

Configuring the Browsers

i-Planet works with Netscape and Internet Explorer. This section contains information about using these browsers.

Netscape

This section contains information on tuning various versions of Netscape browsers.

Warnings with Netscape 4.05

When using Netscape 4.05 with the Solaris 2.6 Operating Environment, warnings that you get when Java windows comes up appear whenever you start a new window.

To prevent this behavior, use the following procedure to create the file.

▼ To Add the File `.Xdefaults`

1. **Create a file called** `.Xdefaults` **in your home directory.**
2. **Put the following lines in this file:**

```
Netscape.useStderrDialog:       false
Netscape.useStdoutDialog:       false
```

To prevent this behavior, follow the procedure below, if the file `.Xdefaults` already exists in your home directory.

▼ To Modify the File `.Xdefaults`

- **If this file already exits in your home directory, add the lines:**

```
Netscape.useStderrDialog:       false
Netscape.useStdoutDialog:       false
```

Netscape and Applications from the Desktop

For all versions of Netscape, the preferences must be set to accept all cookies. Use the following procedure to do this.

▼ To Set Netscape Browsers to Accept All Cookies

1. **Start Netscape.**
2. **From the Edit menu, choose Preferences.**
3. **On the Category frame of the Netscape: Preferences window, click Advanced.**
4. **On the Cookies panel of the Advanced Change preferences that affect the entire product, click the radio button before "accept all cookies."**
5. **Click OK at the bottom of the Netscape: Preferences window.**

Netscape `tmp/` File Size

The amount of space available for `tmp/` files on the server determines the size of files that end users can download or have access.

Internet Explorer

If end users look at sensitive or classified documents through Internet Explorer, they must be sure to exit the browser when they have finished. Copies of all files that they have looked at are stored on the computer that they are using until they close all Internet Explorer windows.

CHAPTER 4

i-Planet User Administration Command Line Interface

This chapter describes the Java command line interface that i-Planet administrators can use to:

- Create i-Planet users
- Delete i-Planet users
- View the properties of all i-Planet users
- List all i-Planet users

Configuring and Testing Classpath Settings

The command-line utility is a Java class called `UserAdminCL`. Before you can run `UserAdminCL`, you must be root on your i-Planet server and have the classes shown in TABLE 4-1 in your classpath:

TABLE 4-1 Classes for `UserAdminCL`

Package	Default Location
`com.sun.stnr.useradmin.UserAdminCL`	`/opt/SUNWstnr/lib/useradmin.jar`
`com.sun.sunnet.SNUtils`	`/opt/SUNWjeev/classes/SNUtils.jar`
`com.sun.sunnet.preferences`	`/opt/SUNWjeev/classes/preference_servlet.jar`
`com.sun.stnr.common`	`/opt/SUNWjeev/classes/common.jar`
Java 1.1 JDK	`/usr/java/lib/classes.zip`

Setting Your Classpath

Use the following procedure to set your classpath so you can use `UserAdminCL`.

▼ To Set Your Classpath

1. **As root, type the following command to set your classpath:**

```
# CLASSPATH=/opt/SUNWjeev/classes/SNUtils.jar:/opt/SUNWjeev/classes\
/preference_servlet.jar:/opt/SUNWjeev/classes/common.jar:/usr/java/lib\
/classes.zip:/opt/SUNWstnr/lib/useradmin.jar
```

2. **Type the following command to export your classpath:**

```
# export CLASSPATH
```

Verifying the Settings to Use `UserAdminCL`

Use the following procedure to verify the settings to use `UserAdminCL`:

▼ To Verify Settings to Use `UserAdminCL`

- **As root, type the following command to run** `UserAdminCL`:

```
# java com.sun.stnr.useradmin.UserAdminCL
```

If you see the following usage message, you are ready to use `UserAdminCL`.

```
com.sun.stnr.common.CommandLineException: missing switch: +action
usage: [jre|java] com.sun.stnr.useradmin.UserAdminCL +action
[create|delete|get|list] [-srclogin] [-destlogin] [-usersfile]
[-defsfile] [-older] [-nologin] [-debug] [-interactive]
```

If you see other error messages, verify your classpath and try again.

Using UserAdminCL

The `UserAdminCL` supports several actions:

- Listing i-Planet users
- Getting specific information about i-Planet users, such as their role
- Creating a new i-Planet user
- Deleting an i-Planet user.

You must use the `+action` command-line switch and one of the actions listed above. Depending on the action, other optional switches provide additional information. Each switch is described below and illustrated with an example.

Using UserAdminCL Summary

The actions and switches available are summarized as follows:

- `-srclogin` *LOGINID*—Specifies the user ID of an existing i-Planet user for use with the delete, create, and get actions.
- `-destlogin` *LOGINID*—Specifies the user ID of a new i-Planet user that is used with the `create` action.
- -`usersfile` *FILENAME*—Specifies the file name for the i-Planet user properties file. Use this with the `create` and `delete` actions.
- `-defsfile` *FILENAME*—Specifies the file name for i-Planet's default file. Use this with the `create` action.
- `-older` *N*—Specifies i-Planet users who have last logged in *N* or more days ago. Use this with `delete` and `list` actions.
- `-nologin`—Specifies i-Planet users who have not yet logged in. Use this with the list and delete actions.
- `-interactive`—Turns off all user interaction for use with the delete action.
- `-debug`—Turns on debugging. Use this with all actions.

Listing i-Planet Users

You can list all i-Planet users who have logged in or for whom profiles have been created in standard output (one line per user).

You can use two optional switches with the `list` action:

- `-older` *N*—Lists the i-Planet users who have not logged in for more than *N* days. If you specify `-older 0`, all i-Planet users will be listed.
- `-nologin`—Lists the i-Planet users who have never logged in. If neither switch is present, all i-Planet users are listed.

▼ To List i-Planet Users Without Any Switch

- **Type the following command to list all i-Planet users without any optional switch, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action list
```

This command lists all i-Planet users who have logged in or for whom profiles have been created:

```
root
abc
jdoe
def
```

▼ To List i-Planet Users With the `-nologin` Switch

Type the following command to list all i-Planet users with the `-nologin` switch, for example:

```
# java com.sun.stnr.useradmin.UserAdminCL +action list -nologin
```

This command lists all i-Planet users who have not logged in:

```
root
```

▼ To List i-Planet Users With the `-older N` Switch

- **Type the following command to list all i-Planet users with the** `-older N` **switch, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action list -older 30
```

This command lists all i-Planet users whose last login was more than 30 days ago:

```
root
abc
```

Viewing an i-Planet User's Properties

Use the following procedure to view an i-Planet user's properties through standard output. Key-value pairs are separated by a new line.

▼ To View an i-Planet User's Properties

● **Type the following command to view an i-Planet user's configuration, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action get -srclogin jdoe
```

This command displays the properties of the i-Planet user specified after the switch `-srclogin`:

```
+ properties for login=jdoe
Common.MailServer=mail.sun.com
Common.CalendarServer=calendar.sun.com
SNDesktop.userTemplatePath=/etc/opt/SUNWstnr/html_templates/
userTemplate.html
SNDesktop.prefTemplatePath=/etc/opt/SUNWstnr/html_templates/
prefTemplate.html
user.url=http://memnoch.eng.sun.com:8080/servlet/SNDesktop?
template=user
role=web
Common.EmployeeNumber=12345
Common.UserName=jdoe
SNDesktop.feedbackTemplatePath=/etc/opt/SUNWstnr/html_templates/
feedbackTemplate.html
SNDesktop.checkCalendar=1
SNDesktop.serviceTimeout=5000
SNDesktop.checkMail=1
SNDesktop.lang=usenglish
session.uid=jdoe
IMAP.Mail.password=f6006d14cafef5faa
Common.LastName=Doe
Common.FirstName=Jane
SNDesktop.advancedTemplatePath=/etc/opt/SUNWstnr/html_templates/
advancedTemplate.html
Common.DefaultMailServer=mail.sun.com
```

Creating a New i-Planet User

You can create a new i-Planet user using the properties of an existing i-Planet user, using the configuration files that you specify, or using system defaults as the basis:

- If you specify both `-srclogin` *`SRCID`* and `destlogin` *`DESTID`*, `create` creates a login ID *`DESTID`* that is based on the properties of the existing i-Planet user named *`SRCID`*.

- If you specify only `-destlogin` *`DESTID`*, the new i-Planet user *`DESTID`* is based on the system default settings.
- If you specify neither `-srclogin` nor `-destlogin`, the information for one or more new i-Planet users is gathered from default configuration files.

Creating a New i-Planet User Using an Existing i-Planet User As the Basis

If you provide both the `-srclogin` *`SRCID`* and `-destlogin` *`DESTID`* switches, the `create` action makes a new i-Planet user based on the properties of the existing i-Planet user that you specified. The new i-Planet user has the login ID of *`DESTID`* and has each property of the i-Planet user with login ID *`SRCID`* (except the IMAP password).

▼ To Create a New i-Planet User Using an Existing i-Planet User As the Basis

- **Type the following command to create a new i-Planet user using an existing i-Planet user as a basis, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action create -srclogin olduser \
-destlogin newuser
```

This command returns the confirmation that the user indicated in the command was created:

```
# + created user=bc81306
```

Creating an i-Planet User from System Defaults

If you provide only the `-destlogin` *`DESTID`* switch, then you create a new i-Planet user based on system defaults. The system defaults for creating a i-Planet user in this fashion are stored in the default i-Planet user configuration file and the default profile file.

The following properties are in i-Planet's default user configuration file `/etc/opt/SUNWstnr/defaultUser.conf`:

- `Common.UserName`
- `Common.FirstName`
- `Common.LastName`
- `Common.MailServer`

- Common.CalendarServer
- Common.EmployeeNumber
- Common.DefaultMailServer
- SNDesktop.userTemplatePath
- SNDesktop.prefTemplatePath
- SNDesktop.feedbackTemplatePath
- SNDesktop.advancedTemplatePath
- SNDesktop.checkCalendar
- SNDesktop.checkMail
- SNDesktop.lang
- SNDesktop.serviceTimeout

The following properties are stored in i-Planet's `/opt/SUNWjeev/profiles/.default` file:

- role
- user.url

Note – You can edit these files directly to set defaults for all new i-Planet users in the system. Each file consists of key value pairs separated by an `=`, with one pair on each line.

▼ To Create a New i-Planet User Using System Defaults As a Basis

- **Type the following command to create a new i-Planet user using system defaults as a basis, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action create -destlogin bc81306
```

This command returns the confirmation that the user indicated in the command was created:

```
+ created user=bc81306
```

Creating New i-Planet Users From a Text File

If you specify neither `-srclogin` nor `-destlogin` switches with the `create` action, then `UserAdminCL` reads data for the new i-Planet user from text files. You can create multiple identical i-Planet users using predefined defaults that are set up in a `defaults` file, or by specifying the per i-Planet user configuration in a flat file, or both. You can specify two command line switches:

- `usersfile`—Specifies the users file, and defaults to `./users` if not specified.
- `defsfile`—Specifies the `defaults` file, and defaults to `./defaults`, if not specified.

Each line in the users file contains information for a single user in the form of one or more key-value pairs. Keys and values are separated by an = (equals sign), and key-value pairs are separated by a ; (semicolon); see the example for the Procedure "To Create New Users From a Text File" below. Only the key `session.uid` is required—any other pairs are optional.

The `defaults` file format is identical to that of the i-Planet `users` file, except that it contains only a single line of properties. The properties specified in the defaults are applied to each i-Planet user named in the i-Planet `users` file for any values not explicitly specified in the i-Planet user's file.

Note – i-Planet stores an i-Planet user's IMAP mail password as an encrypted value. It is encrypted with a proprietary algorithm. If you wish to specify a mail password for each i-Planet user in the `users` file, you can do so, but it must be in plain text. The password will be encrypted before it is saved.

For example, to add three i-Planet users and specify an IMAP password, a mail server, and calendar server for each, you can use the following procedure.

▼ To Create New Users From a Text File

1. **Create a `./users` file, for example.**

   This file should contain the following information:

```
session.uid=bob;IMAP.Mail.password=gimme
session.uid=bill;IMAP.Mail.password=bokbok
session.uid=jan;IMAP.Mail.password=joshua
```

   This file is used to specify information that is different for each i-Planet user that is being created. At a minimum, each i-Planet user's login name (`session.uid`) and the IMAP mail password (`IMAP.Mail.password`) falls into this category.

2. **Because the mail and calendar server are constant among all the i-Planet users, create a `./defaults` file with a single line to populate the mail and calendar server values for all users, for example:**

```
Common.MailServer=foo.bar.com;Common.CalendarServer=farble.bar.com
```

3. **With these files in place, type the following command to run `UserAdminCL`:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action create
+ created login=bob
+ created login=bill
+ created login=jan
```

This command returns the confirmation that the user or user indicated in the command were created:

```
+ created login=bob
+ created login=bill
+ created login=jan
```

Deleting i-Planet Users

You can remove i-Planet users from the system in three different ways: by user ID, by user's last `login` time (if any), or by reading a list of login IDs from a text file.

- If you provide the `-srclogin` *`LOGINID`* switch, the login ID *`LOGINID`* will be deleted.
- If you specify the `-older` *N* switch, then users who have not logged in for *N* days will be deleted.
- If you specify the `-nologin` switch, then users who have never logged in will be deleted.
- If you provide none of the above switches, `UserAdminCL` reads a list of users to delete from a text file.
- If you specify the `-interactive` switch, you will not be asked if you want to delete the user first.

In addition to any specific i-Planet user being deleted, all i-Planet users "aliased" to this user are also removed.

Deleting a Specific i-Planet User by `Userid`

If you specify the `-srclogin` *`LOGINID`* switch after the `delete` action, then the login ID *`LOGINID`* will be removed from the i-Planet database.

▼ To Delete a Specific i-Planet User by `Userid`

- **Type the following command to delete a specific i-Planet user, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action delete -interactive \
-srclogin jb34290
```

This command returns the confirmation that the user indicated in the command was deleted:

```
+ deleted login=jb34290
```

Deleting i-Planet Users Based on Last Login Time

If you specify either the `-nologin` or `-older` *N* switches, i-Planet users are removed based on their last update time (stored as the value for the i-Planet user's `Common.UpdateTime` property). You can view this property with the `get` action.

- If you specify `-nologin`, then users who have not yet logged in will be deleted (`Common.UpdateTime` property is null).
- If you specify `-older` *N*, then users with an update time of more than *N* days from the present are deleted.

Note – Any user that is deleted with the `-nologin` switch is also removed by the `-older` *N* switch. Specifying `-older 0` selects all users.

▼ To Delete i-Planet Users Based on Last Login Time Using the `-older` *N* Switch

1. **Type the following to delete i-Planet users based on last login time using the `-older` *N* switch, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action -interactive delete -older 30
```

2. **Confirm that you want the user indicated deleted by typing y or n:**

```
+ delete login=bob [yes/no] y
+ deleted login=bob
+ delete login=bill [yes/no] y
+ deleted login=bill
+ delete login=bob [yes/no] n
+ no action for login=jan
```

▼ To Delete i-Planet Users Based on Last Login Time Using the `-nologin` Switch

1. **Type the following to delete i-Planet users based on last login time using the** `-nologin` **switch, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action delete -interactive -nologin
```

2. **Confirm that you want the user indicated deleted by typing y or n:**

```
+ delete login=bob [yes/no] y
+ deleted login=bob
```

Deleting i-Planet Users According to a List

If you do not specify `-older N`, `-nologin`, or `-srclogin` switches with the `delete` action, a list of i-Planet users to be removed will be read from a text file. You can provide the file name on the command line to identify the file to be used. If you do not specify a file, `./users` will be used.

`UserAdminCL` reads a list of login IDs from the users file and deletes each one from the system.

The format of this users file is identical to the users file described in the section "Creating New i-Planet Users From a Text File." However, only the `session.uid` property is used and all other content is ignored.

To Delete i-Planet Users According to a List

- **Type the following to delete i-Planet users according to a list, for example:**

```
# java com.sun.stnr.useradmin.UserAdminCL +action delete -interactive
```

This command returns confirmation that the user who meet the criterion in the command are deleted:

```
+ deleted login=bob
+ deleted login=bill
+ deleted login=jab
```

Note – You can specify the `-interactive` switch to prevent prompting.

CHAPTER 5

SSL Service and Certificates

This chapter describes how to

- Create self-signed SSL certificates
- Obtain SSL certificates from Verisign and other vendors
- Use SSL service between the i-Planet server and i-Planet gateway
- Enable SSL service

SSL Service

SSL service is used for encrypted communication between the end user and the i-Planet gateway. You can use the self-signed certificate that you created during installation or you can create a certificate signing request, obtain a signed certificate from a Certificate Authority, and add it to the `rp.keystore` file (the certificate database) on the i-Planet gateway.

Using SSL service between the i-Planet server and the i-Planet gateway provides greater security for the information that must flow between them. SSL service requires an SSL certificate.

SSL Certificates for the i-Planet Gateway

The SSL certificates, either self-signed or from a certificate vendor, who provides authority (CA) services, are used for secure communication over the Internet with the end user. SSL certificates provide a way to authenticate users. When you installed the i-Planet software, you automatically created a self-signed SSL certificate. In creating this certificate, you entered specific information about your organization, such as company name and address, and a passphrase. This information is used in creating a certificate.

If you want to use an SSL certificate that is signed by a certificate vendor after you have installed the i-Planet 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.

Self-Signed SSL Certificate on the i-Planet Gateway

When you installed the i-Planet software, you created and installed a self-signed SSL certificate. At some point after installation, you might want to generate a new self-signed certificate; you might want to change the information for the certificate you entered during the original installation, for example.

▼ To Generate a Self-Signed SSL Certificate for the i-Planet Gateway

1. **As root, run the `certadmin` script on the i-Planet gateway:**

```
# /opt/SUNWsnrp/bin/certadmin
```

The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

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

The Certificate Administration script prompts you to enter specific information about your organization and a passphrase 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 []
```

3. **Enter the information for your organization and a passphrase for the self-signed certificate.**

   A self-signed certificate is generated and added to the file `/etc/opt/SUNWstnr/rp.keystore` on the i-Planet gateway. Your prompt returns.

4. **Stop and restart the reverse proxy server on the i-Planet gateway for the certificate to take effect.**

   See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in Chapter 3, "Other Administrative Tasks."

5. **Make a backup copy of the** `rp.keystore` **file.**

SSL Certificates From Vendors

During i-Planet software installation, you created and installed a self-signed SSL certificate. At some point after installation, you have the option to install SSL certificates signed by vendors who provide official certificate authority (CA) services.

i-Planet 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.

Certificates are stored in the `rp.keystore` file. Once you generate a certificate signing request (used to request a certificate from a third-party vendor), 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 will not be able to use the certificate that you bought.

▼ To Install SSL Certificates From Verisign

1. **As root, run the** `certadmin` **script on the i-Planet gateway.**

   ```
   # /opt/SUNWsnrp/bin/certadmin
   ```

   The Certificate Administration menu is displayed:

   ```
   1) Generate Self-Signed Certificate
   2) Generate Certificate Signing Request (CSR)
   3) Add Root CA Certificate
   4) Install Certificate from Certificate Authority (CA)
   5) Quit
   choice: [5]
   ```

2. **Enter `2` on the Certificate Administration menu to generate a certificate signing request (CSR).**

   The information from your current self-signed certificate is displayed. You are asked if this information is correct.

   - If no self-signed certificate exists on this machine, the Certificate Administration script notifies you that you must create one. Refer to the procedure "To Generate a Self-Signed SSL Certificate for the i-Planet Gateway" earlier in this chapter.
   - If a self-signed certificate exists on this machine, the information from the certificate is displayed. The Certificate Administration script asks the question:

```
Is this information correct (y/n)? [n]
```

   a. **Enter `y` if the information is correct, or enter `n` if it is not correct.**

   - If you enter `n`, you are asked to enter information for a new self-signed certificate. See the procedure "To Generate a Self-Signed SSL Certificate for the i-Planet Gateway" in this chapter.
   - If you enter `y`, you are asked to enter some contact information for the webmaster 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? []
```

   b. **Enter the name, the email address, and the telephone number of the administrator or webmaster for this server.**

   The Certificate Administration script displays the values you enter and asks the question:

```
Are these values correct (y/n)? [n]
```

   c. **Enter `y` if the information is correct, or enter `n` if it is not correct.**

   - If you enter `y`, the CSR is generated and stored in the file `/tmp/csr.`*hostname*.
   - If you enter `n`, the Certificate Administration script asks you to enter the values again.

3. **Go to the certificate authority's website 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 passphrase.**

c. **Specify your web server type as:** `Java Webserver`**.**

Specifying `Java Webserver` means that you want your certificate in privacy enhanced mail (PEM) format.

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

The certificate begins with a line that reads:

`-----BEGIN CERTIFICATE----`

continues with the certificate itself, and ends with a line that reads:

`-----END CERTIFICATE-----`

Make sure you include both of these lines with the certificate in the file.

5. **As root, run the** `certadmin` **script on the i-Planet gateway:**

```
# /opt/SUNWsnrp/bin/certadmin
```

The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

6. **Enter** `4` **on the Certificate Administration menu to install your certificate from the CA.**

The Certificate Administration script asks the question:

```
What is the name (including path) of the file that contains the
certificate? []
```

7. **Enter the full path to the file containing the certificate from the CA.**

Your certificate is stored in the file `/etc/opt/SUNWstnr/rp.keystore` and your prompt returns.

8. **Stop and restart the reverse proxy server on the i-Planet gateway for the certificate to take effect.**

See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in Chapter 3, "Other Administrative Tasks."

9. **Make a backup copy of the** `rp.keystore` **file for the i-Planet gateway.**

▼ To Install SSL Root Certificates and SSL Certificates From Other Vendors

You must have already generated a self-signed certificate to install a root certificate. See the procedure “To Generate a Self-Signed SSL Certificate for the i-Planet Gateway” in this chapter.

1. **Go to the Certificate Authority’s website and download its root certificate.**

   The website should contain instructions for downloading the certificate, usually as a file.

2. **As root, run the `certadmin` script on the i-Planet gateway:**

```
# /opt/SUNWsnrp/bin/certadmin
```

   The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

3. **Enter `3` on the Certificate Administration menu to add a root certificate from the CA.**

   The Certificate Administration script asks the question:

```
What is the name (including path) of the file that contains the
root certificate that you would like to add to your database? []
```

   a. **Enter the full path to the file containing the root certificate.**

      The file is displayed and the Certificate Administration script asks the question:

```
Is this information correct (y/n)? [n]
```

   b. **Enter `y` if the file is correct, or `n` if it is not.**

      - If you enter y, the root certificate is stored the `/etc/opt/SUNWstnr/rp.CAstore` file and your prompt returns.
      - If you enter `n`, the root certificate is not added and your prompt returns.

4. **As root, run the** `certadmin` **script on the i-Planet gateway.**

```
# /opt/SUNWsnrp/bin/certadmin
```

5. **Enter** `2` **on the Certificate Administration menu to generate a certificate signing request (CSR).**
   - If no self-signed certificate exists on this machine, the Certificate Administration script notifies you that you must create one. Refer to the procedure, "To Generate a Self-Signed SSL Certificate for the i-Planet Gateway," earlier in this chapter.
   - If a self-signed certificate exists on this machine, the information from the certificate is displayed. The Certificate Administration script asks the question:

```
Is this information correct (y/n)? [n]
```

   a. **Enter** `y` **if the information is correct, or enter** `n` **if it is not correct.**
      - If you enter `n`, you are asked to enter information for a new self-signed certificate. See the procedure, "To Generate a Self-Signed SSL Certificate for the i-Planet Gateway," in this chapter.
      - If you enter `y`, you are asked to enter some contact information for the webmaster 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? []
```

   b. **Enter the name, the email address, and the telephone number of the administrator or webmaster for this server.**

      The Certificate Administration script displays the values you enter and asks the question:

```
Are these values correct (y/n)? [n]
```

   c. **Enter** `y` **if the information is correct, or enter** `n` **if it is not correct.**
      - If you enter `y`, the CSR is generated and stored in the file `/tmp/csr.`*hostname*.
      - If you enter `n`, the Certificate Administration script asks you to enter the information again.

6. **Return to the Certificate Authority's website and order your web server certificate.**

   a. **Provide information from your CSR, as requested by the CA.**

b. **Provide other information as requested by the CA, such as a passphrase.**

c. **Specify your web server type as:** `Java Webserver`**.**

Specifying `Java Webserver` means that you want your certificate in privacy enhanced mail (PEM) format.

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

The certificate begins with a line that reads:

`-----BEGIN CERTIFICATE----`

continues with the certificate itself, and ends with a line that reads:

`-----END CERTIFICATE-----`

Make sure you include both of these lines with the certificate in the file.

8. **As root, run the** `certadmin` **script on the i-Planet gateway:**

```
# /opt/SUNWsnrp/bin/certadmin
```

The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

9. **Enter** `4` **on the Certificate Administration menu to install the certificate from the CA.**

The Certificate Administration script asks the question:

```
What is the name (including path) of the file that contains the
certificate? []
```

10. **Enter the full path to the file containing the certificate.**

Your certificate is added to the `/etc/opt/SUNWstnr/rp.keystore` file and your prompt returns.

11. **Stop and restart the i-Planet gateway for the certificate to take effect.**

See the procedure “To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway” in Chapter 3, “Other Administrative Tasks.”

12. **Make a backup copy of the** `rp.keystore` **file for the i-Planet gateway.**

Using SSL Service for Encrypted Communication Between the i-Planet Server and the i-Planet Gateway

To use SSL service for encrypted communication between the i-Planet server and the i-Planet gateway, you must:

- Create a self-signed certificate
- Create a certificate signing request on the i-Planet server
- Obtain a signed certificate from the Certificate Authority
- Add the signed certificate to the `rp.keystore` file for the i-Planet server (the certificate database)
- Configure SSL service on the i-Planet gateway
- Configure SSL service on the i-Planet server

Self-Signed SSL Certificate on the i-Planet Server

You cannot use self-signed certificates for SSL service between the i-Planet server and the i-Planet gateway. You must use an SSL certificate from a certificate vendor.

You must generate a self-signed certificate in order to obtain an SSL certificate from certificate vendor who provides authority (CA) services.

▼ To Generate a Self-Signed SSL Certificate for the i-Planet Server

1. As root, run the `certadmin` script on the i-Planet server:

```
# /opt/SUNWsnrp/bin/certadmin
```

The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

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

   The Certificate Administration script prompts you to enter specific information about your organization and a passphrase 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 []
```

3. **Enter the information for your organization and a passphrase for the self-signed certificate.**

   A self-signed certificate is generated and added the file `/etc/opt/SUNWstnr/rp.keystore` on the i-Planet server. Your prompt returns.

4. **Make a backup copy of the `rp.keystore` file on the i-Planet server.**

SSL Certificates for the i-Planet Server

Using SSL service between the i-Planet server and the i-Planet gateway provides greater security for the information that must flow between them. SSL service requires a SSL certificate. In creating a self-signed certificate as part of this process for an SSL certificate for the i-Planet server, you enter specific information about your organization, such as company name and address, and a passphrase.

If you decide to enable SSL service so that you have secure communication between the i-Planet server and the i-Planet gateway after you have installed the i-Planet software, you must to run the `certadmin` script to install an SSL certificate that is signed by a certificate vendor who provides authority (CA) services.

SSL Certificates from Vendors

If you decide to enable SSL services between the i-Planet server and the i-Planet gateway after you have installed the i-Planet software, you must generate a self-signed certificate.

i-Planet 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.

Certificates are stored in the `rp.keystore` file. Once you generate a certificate signing request (used to request a certificate from a third-party vendor), 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 will not be able to use the certificate that you bought.

▼ To Install SSL Certificates From Verisign

1. **As root, run the `certadmin` script on the i-Planet server:**

```
# /opt/SUNWsnrp/bin/certadmin
```

The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

2. **Enter `2` on the Certificate Administration menu to generate a certificate signing request (CSR).**

- If no self-signed certificate exists on this machine, the Certificate Administration script notifies you that you must create one. Refer to the procedure, "To Generate a Self-Signed SSL Certificate for the i-Planet Server," earlier in this chapter.
- If a self-signed certificate exists on this machine, the information from the certificate is displayed. The Certificate Administration script asks the question:

```
Is this information correct (y/n)? [n]
```

a. **Enter `y` if the information is correct, or enter `n` if it is not correct.**

- If you enter `n`, you are asked to enter information for a new self-signed certificate. See the procedure, "To Generate a Self-Signed SSL Certificate for the i-Planet Server" in this chapter.
- If you enter `y`, you are asked to enter some contact information for the webmaster 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? []
```

b. **Enter the name, the email address, and the telephone number of the administrator or webmaster for this server.**

The Certificate Administration script displays the values you enter and asks the question:

```
Are these values correct (y/n)? [n]
```

c. **When prompted, enter** `y` **if the information is correct, or enter** `n` **if it is not correct.**

- If you enter `y`, the CSR is generated and added to the file `/tmp/csr.`*hostname on* the i-Planet server.
- If you enter `n`, the Certificate Administration script asks you to enter the values again.

3. **Go to the Certificate Authority's website and order your web server certificate.**

a. **Provide information from your CSR, as requested by the CA.**

b. **Provide other information as requested by the CA, such as a passphrase.**

c. **Specify your web server type as:** `Java Webserver`**.**

Specifying `Java Webserver` means that you want your certificate in privacy enhance mail (PEM) format.

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

The certificate begins with a line that reads:

```
-----BEGIN CERTIFICATE----
```

continues with the certificate itself, and ends with a line that reads:

```
-----END CERTIFICATE-----
```

Make sure you include both of these lines with the certificate in the file.

5. **As root, run the** `certadmin` **script on the i-Planet server.**

```
# /opt/SUNWsnrp/bin/certadmin
```

6. **Enter** `4` **on the Certificate Administration menu to install your certificate from the CA.**

The Certificate Administration script asks the question:

```
What is the name (including path) of the file that contains the
certificate? []
```

7. **Enter the full path to the file containing the certificate from the CA.**

   Your certificate is stored in the file `/etc/opt/SUNWstnr/rp.keystore` on the i-Planet server.

8. **Enable SSL service on the i-Planet server.**

   See the procedure "To Enable SSL Service on the i-Planet Server" in Chapter 3, "Other Administrative Tasks."

9. **Make a backup copy of the** `rp.keystore` **file on the i-Planet server.**

10. **Enable SSL service on the i-Planet gateway.**

    See the procedure "To Enable SSL Service on the i-Planet Gateway" in Chapter 3, "Other Administrative Tasks."

▼ To Install SSL Root Certificates and SSL Certificates From Other Vendors

You must have already generated a self-signed certificate to install a root certificate. See the procedure "To Generate a Self-Signed SSL Certificate for the i-Planet Server" in this chapter.

1. **Go to the Certificate Authority's website and download its root certificate.**

   The website should contain instructions for downloading the certificate.

2. **As root, run the** `certadmin` **script on the i-Planet server:**

```
# /opt/SUNWsnrp/bin/certadmin
```

The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

3. **Enter** `3` **on the Certificate Administration menu to add a root certificate.**

   The Certificate Administration script asks the question:

```
What is the name (including path) of the file that contains the
root certificate that you would like to add to your database? []
```

a. **Enter the full path to the file containing the root certificate from the CA.**

The file is displayed and the Certificate Administration script asks the question:

```
Is this information correct (y/n)? [n]
```

b. **Enter** `y` **if the file is correct, or** `n` **if it is not.**

- If you enter `y`, the root certificate is stored in the `etc/opt/SUNWstnr/rp.CAstore` file and your prompt returns.
- If you enter `n`, the root certificate is not added and your prompt returns.

4. **As root, run the** `certadmin` **script on the i-Planet server.**

```
# /opt/SUNWsnrp/bin/certadmin
```

5. **Enter** `2` **on the Certificate Administration menu to generate a certificate signing request (CSR).**

- If no self-signed certificate exists on this machine, the Certificate Administration script notifies you that you must create one. Refer to the procedure, “To Generate a Self-Signed SSL Certificate for the i-Planet Server,” earlier in this chapter.
- If a self-signed certificate exists on this machine, the information from the certificate is displayed. The Certificate Administration script asks the question:

```
Is this information correct (y/n)? [n]
```

a. **Enter** `y` **if the information is correct or enter** `n` **if it is not correct.**

- If you enter `n`, you are asked to enter information for a new self-signed certificate. Refer to the procedure, “To Generate a Self-Signed SSL Certificate for the i-Planet Server,” earlier in this chapter.
- If you enter `y`, the Certificate Administration script asks you to enter specific information about your organization:

```
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? []
```

b. **Enter your specific information about your organization.**

The Certificate Administration script displays the values you enter and asks the question:

```
Are these values correct (y/n)? [n]
```

c. **Enter** `y` **if the information is correct or enter** `n` **if it is not correct.**

- If you enter `y`, a CSR is generated and stored in the file `/tmp/csr.`*hostname*.
- If you enter `n`, the Certificate Administration script asks you to enter the values again.

6. **Go to the Certificate Authority's website and order your web server certificate.**

a. **Provide information from your CSR, as requested by the CA.**

b. **Provide other information as requested by the CA, such as a passphrase.**

c. **Specify your web server type as:** `Java Webserver`**.**

Specifying `Java Webserver` means that you want your certificate in PEM format.

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

The certificate begins with a line that reads:

`-----BEGIN CERTIFICATE----`

continues with the certificate itself, and ends with a line that reads:

`-----END CERTIFICATE-----`

Make sure you include both of these lines with the certificate in the file.

8. **As root, run the** `certadmin` **script on the i-Planet server:**

```
# /opt/SUNWsnrp/bin/certadmin
```

The Certificate Administration menu is displayed:

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate from Certificate Authority (CA)
5) Quit
choice: [5]
```

9. **Enter** `4` **on the Certificate Administration menu to install your certificate from the CA.**

   The Certificate Administration script asks the question:

   ```
   What is the name (including path) of the file that contains the
   certificate? []
   ```

10. **Enter the full path to the file containing the certificate from the CA.**

    Your certificate is added to the `/etc/opt/SUNWstnr/rp.keystore` file on the i-Planet server.

11. **Enable SSL service on the i-Planet server.**

    See the procedure "To Enable SSL Service on the i-Planet Server" Chapter 3, "Other Administrative Tasks.".

12. **Stop and restart the web server on the i-Planet server for the certificate to take effect.**

    See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3, "Other Administrative Tasks."

13. **Make a backup copy of the** `rp.keystore` **file on the i-Planet server.**

14. **Enable SSL service on the i-Planet gateway.**

    See the procedure "To Enable SSL Service on the i-Planet Gateway" Chapter 3, "Other Administrative Tasks.".

Configuring SSL Service on the i-Planet Gateway

Use the following procedures to configure SSL service if you want to use it in communicating with the i-Planet server or if you want to disable SSL service and communicate with i-Planet server in the clear.

If you enable or disable SSL service on the i-Planet gateway, you must also enable and disable it on the i-Planet server.

If you are enabling SSL service after you have installed i-Planet, the default port 443 will be used if you used the default installation. If you used the custom installation, the port that you specified during the installation will be used.

▼ To Enable SSL Service on the i-Planet Gateway

1. **As root on the i-Planet gateway, type the following to enable SSL service if you want encrypted communication with the i-Planet server:**

```
# /opt/SUNWsnrp/bin/iplanet_gw ssl on r
```

If you installed the i-Planet software using the default installation, the default SSL port 443 will be used. If you used the customized installation and specified another port for SSL, that port will be used.

2. **Stop and restart the reverse proxy on the i-Planet gateway for the change to take effect.**

See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in Chapter 3, "Other Administrative Tasks."

▼ To Disable SSL Service on the i-Planet Gateway

1. **As root on the i-Planet gateway, type the following to disable SSL service, if you want to communicate with i-Planet server in the clear:**

```
# /opt/SUNWsnrp/bin/iplanet_gw ssl off
```

2. **Stop and restart the reverse proxy on the i-Planet gateway for the change to take effect.**

See the procedure "To Stop and Restart the Reverse Proxy Server on the i-Planet Gateway" in Chapter 3, "Other Administrative Tasks."

Configuring SSL Service on the i-Planet Server

The default installation configures the i-Planet server for communication with the gateway so that it can use both SSL service and clear (plaintext) communication. By default SSL from the i-Planet server to the i-Planet gateway is disabled.

If you enable or disable SSL service on the i-Planet server, you must also enable or disable it on the i-Planet gateway.

If you are enabling SSL service after you have installed the i-Planet software, you must use the default port 443. Both the i-Planet server and the i-Planet gateway must use the same port number for SSL service.

When you are using SSL service for communication between the i-Planet server and the i-Planet gateway, use the URL below to connect to the Administration Console, if you are using the default port 443:

`https://`*`i-Planet_server.domain`*`/console`

Use the URL below to connect to the Administration Console, if you are using a port other than port 443:

`https://`*`i-Planet_server.domain`*`:`*`port`*`/console`

The port number that you use here must be the one that you specified in the custom installation. Both the i-Planet server and the i-Planet gateway must use the same port number for SSL service.

You can switch between communicating with the i-Planet server and the i-Planet gateway using SSL service and communicating in the clear. If you switch the i-Planet server so that it is communicating using SSL (or in the clear), you must also switch the i-Planet gateway so that it is using the same mode of communication as the i-Planet server. The default installation configures the Java web server for both http and https services, but the https service is disabled.

Note – If you used the default installation settings and then decide to turn on SSL service for communication between the i-Planet gateway and the i-Planet server using the command below, the default port 443 is used. If you want to use a different port, you must have specified that port when you installed the i-Planet software using the custom installation.

▼ To Enable SSL Service on the i-Planet Server

1. **As root, type the following command to enable encrypted communication using SSL service from the i-Planet server with the i-Planet gateway.**

```
# /opt/SUNWjeev/bin/iplanet_serv ssl on
```

If you installed the i-Planet software using the default installation, the default SSL port 443 will be used. If you used the customized installation and specified another port for SSL, that port will be used.

2. **Stop and restart the web server before the SSL service will be started.**

See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3, "Other Administrative Tasks."

▼ To Disable SSL Service on the i-Planet Server

1. **As root, type the following command to disable SSL service if you want to communicate with the i-Planet gateway in the clear.**

```
# /opt/SUNWjeev/bin/iplanet_serv ssl off
```

2. **Stop and restart the web server before the SSL service will be stopped.**

   See the procedure "To Stop and Restart the Web Server on the i-Planet Server" in Chapter 3, "Other Administrative Tasks."

CHAPTER 6

Administering the i-Planet Firewall Application

This chapter describes the following:

- How the i-Planet firewall application works.
- How to configure and administer the i-Planet firewall application using the command line.

i-Planet Firewall Application

In most i-Planet applications, a separate firewall is used to restrict the external access to the i-Planet 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, i-Planet 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 i-Planet firewall application, make sure that you configure your existing firewall to restrict external access (access from the Internet) to the i-Planet gateway to the SSL port only (port 443 by default), while leaving full access to the i-Planet gateway from all machines and all ports on the internal or private network.

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 i-Planet 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, 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 i-Planet firewall application uses a set of *ordered rules* to filter packets. When you configure the i-Planet 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 i-Planet 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 i-Planet Firewall Application

The firewall application is the only application in the i-Planet 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 i-Planet gateway.

Note – The commands for the i-Planet firewall application are located in `/opt/SUNWsrfw/bin`.

▼ To Configure the i-Planet Firewall Application

1. **As root, run the following command on the** i-Planet 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 i-Planet gateway interface are examined and few rules are installed. `fw.configure` installs the following three default rules:

   1. Allow external access from the i-Planet gateway's Internet interface to the SSL port. (The default port number is 443.)
   2. Allow the i-Planet gateway access to anywhere.
   3. Allow routing information from the Internet interface on the i-Planet gateway to be updated.

   Everything that is not expressly allowed in these rules is denied.

4. **Reboot the** i-Planet gateway **after the command** `fw.configure` **finishes running for the rules to take effect.**

Administering the i-Planet Firewall Application

You must administer the firewall application as root (superuser). Before you can begin, ensure that the following directories are included in root's default path on the i-Planet gateway:

- `/usr/bin`
- `/usr/sbin`

You administer the i-Planet firewall application only from the command-line user interface. There are only three commands used to administer the firewall application:

- `fw.activate`
- `fw.address`
- `fw.rule`

Using `fw.activate`

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.

▼ To Use `fw.activate`

- **As root, type the following to turn the firewall application off:**

```
# fw.activate off
```

- **As root, type the following to turn the firewall application on:**

```
# fw.activate on
```

Using `fw.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 to add an address, 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. You 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

- **As root, type the following to delete the range of addresses that you have named** `myhome`**, for example:**

```
# 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`

This command uses various options to manipulate the firewall application's packet filtering rules. You can change the action or 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.

Services and Service Groups

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`, `chargen`, 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, for example, 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 the Services

- **Type the following to list the services:**

```
# fw.rule list service
```

You 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 Add a Port

- **As root, type the following to add a new port:**

```
# fw.rule add ALLOW port-number from host to host
```

This rule allows to add a new port from a remote host to a local host. if a service is not defined, tcp is the service used. If the new port is not in the `services` file, it is added.

For example, if you use this rule to add port 3000 from `a-remote-host` to `ALL`, a new *`tcp`* service on port `30000` is added to the service table and the i-Planet gateway would accept communication on port 30000 from a named remote host.

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 i-Planet. 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 to add a rule:**

```
# fw.rule add ALLOW service from host to host
```

This rule allows you to 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 to delete a rule:**

```
# 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 to move a rule:**

```
# fw.rule move 5 4
```

Rules 5 and 4 are reordered. Use the list option to see the new ordering.

Troubleshooting

Several things that often cause problems in configuring and using the i-Planet firewall application are listed below:

- 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 i-Planet firewall application.
- Run the command `fw.rule list rule` to display a list of the current filtering rules.
- If you are completely locked out, you can do one of the following:
  - Run the command `fw.activate off` to turn the i-Planet 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 it will pass all traffic through it unfiltered.

CHAPTER 7

Authentication

This chapter describes:

- Authentication
- Authentication modules

Authentication

Overview

When end users first access the i-Planet URL, they are presented with an HTML authentication page. If the **i-Planet** server is configured with multiple authentication modules, end users are presented with a menu of authentication types. If only one is configured, they are sent directly to that authentication page.

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. This information is only provided to the system administrator or the administrator for i-Planet, if they are the same, through the authentication log of the Administration Console.

After a successful authentication, end users are redirected to the i-Planet Desktop.

Authentication Modules

Several authentication modules are provided with i-Planet. These are UNIX/NIS, RADIUS, S/Key, SafeWord, and SecurID.

UNIX

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 UNIX username and password (local file, NIS, or both) for authentication, then you, the systems administrator, must make sure that the `passwd:` entry in the `/etc/nsswitch.conf` file is set up correctly.

RADIUS

The RADIUS module is a client implementation of Remote Authentication Dial In User Service (*RFC 2138*). This module supports the i-Planet administrator and sets the RADIUS server or servers on the Authentication Parameters page of the Administration Console. You get to this page by clicking the Authentication link under the Servers section of the navigation frame of the Administration console. Fill in the fields labelled Radius Server and Radius Server Alternate.

The RADIUS shared secret must always be in the file `/etc/opt/SUNWstnr/platform.conf`, which you edit manually. You cannot specify it on the Authentication Page for the i-Planet Desktop.

▼ To Set the RADIUS shared secret

- **Edit the file** `/etc/opt/SUNWstnr/platform.conf` **to set the line** `radius.secret=` **equal to the shared secret.**

If you want the end users to type in the RADIUS server along with user name and password, use the following procedure to modify the `/etc/opt/SUNWstnr/Radius.properties` file on the i-Planet server to add another field on the RADIUS Authentication Page for the i-Planet Desktop.

▼ To Modify the File `Radius.properties` File

1. **Add an additional input field for the RADIUS server on the RADIUS Authentication Page for the** i-Planet Desktop **by adding the following line to the end of the** `/etc/opt/SUNWstnr/Radius.properties` **file:**

   `TOKEN Radius Server:`

   CODE EXAMPLE 7-1 shows what the new `.properties` file will look like.

CODE EXAMPLE 7-1 Sample `Radius.properties` File

```
SCREEN
TIMEOUT 60
TEXT RADIUS Authentication
TOKEN User Name:
PASSWORD Password:
TOKEN Radius Server:
```

2. **If you want end users to be able to type in the alternate RADIUS server, then just add another** `TOKEN`**.**

   The i-Planet server must be able to resolve the RADIUS server host name or names specified.

S/Key

S/Key is the one-time password system developed by Bellcore. S/Key users must be valid UNIX/NIS users on the i-Planet server. 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).

Before an end user attempts remote access for the first time, a list of S/Key one-time passwords must be generated for that end user.

For the System Administrator to Generate Passwords for Remote Users

You can generate passwords for end users with the following procedure.

▼ To Generate Passwords for a Remote User

1. **Start the web browser that you want to use.**
2. **Start the Administration Console**
3. **Click the Generate S/KEY Passwords link in the Misc section in the navigation frame of the Administration Console.**
4. **Follow the instructions in the administration frame of the Administration Console.**

   When you generate the passwords on behalf of end users, give them the 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.

For Users to Generate Their Own Passwords

End users can generate their own set of passwords over the intranet before they become remote so that they can use S/Key authentication. They can only use the following procedure over the intranet.

▼ For Users to Generate Passwords

End users use this procedure to generate their own S/Key passwords over the intranet before they become remote.

1. **They start the web browser that they want to use.**

2. **They type the following as the URL in the browser:**

   `http://`*`i-Planet_server`*`:default-port/cgi-bin/skey/skeylogin.cgi`

   8080 is the default port for the i-Planet server.

   Once they have remotely logged into the i-Planet system, end users can generate more one-time passwords by clicking the Generate S/KEY Passwords link on the i-Planet Desktop.

Note – When end users generate more S/Key passwords, the new list of passwords supersedes the previously generated list and UUID for the end users will change.

Removing the i-Planet software will delete all S/Key password information for the end users.

Note – If an end user uses the last password and logs out before generating a new list of passwords, then a new list for that user can only be generated using one of the other two methods.

SafeWord

This module is a client implementation for authenticating using the SafeWord system from Secure Computing. The module is written for a SafeWord configuration that uses X9.9, asynchronous device mode for X9.9, a challenge length of four decimal digits, and a password length of eight digits. The SafeWord server must be installed locally on the i-Planet server.

SecurID

The SecurID module is a client implementation for authenticating the ACE/Server from Security Dynamics Technologies, Inc. The module's interface only provides for authentication. It does not provide for any other functions, such as "new PIN mode." The ACE/Server does not have to be installed locally to the i-Planet server, although the i-Planet software checks at installation for evidence that the ACE/Client has previously been installed. (In particular, it checks for the existence of the file `/etc/sdace.txt`). If you install the ACE/Client subsequently to installing the i-Planet server, you can add SecurID to the list of authenticators through the Authentication Parameters page in the Administration Console.

▼ To Add SecurID to the List of Authenticator Through the Administration Console

1. **Log into the Administration Console.**
2. **Click the Authentication link under the Server section.**
3. **In the Authentication Modules field at the top of the Authentication Parameters frame, add the following line:**

   `com.sun.login.securid.Securid`

4. **Click the Enter button at the bottom of the frame.**
5. **As root, on the i-Planet server, restart the web server, by typing:**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

General

Each authentication module has a properties file that can be used to customize the HTML pages that are displayed to the end user. The properties file for each module is located in `/etc/opt/SUNWstnr` on the i-Planet server. For example, the UNIX authentication modules properties file is `/etc/opt/SUNWstnr/Unix.properties`.

Each authentication module has a `TIMEOUT` parameter that can be modified in the corresponding `/etc/opt/SUNWstrnr/`*`authenication_module`*`.properties` file. 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 UNIX login have two minutes (120 seconds) to login, change the TIMEOUT parameter in the `/etc/opt/SUNWstnr/Unix.properties` from 60 to 120.

For each HTML page that is sent for the authentication module, there is a keyword `SCREEN` followed by keyword TEXT, followed by any number of the keywords `TOKEN` and `PASSWORD`. Each screen may also contain an optional `TIMEOUT` keyword. For example, the `Unix.properties` file contains the following entries as shown in CODE EXAMPLE 7-2.

CODE EXAMPLE 7-2 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.

`TIMEOUT`—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.

`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 i-Planet image with the image following the keyword. The image should be placed in `/opt/SUNWjeev/public_html/images`. This image should be a `gif` file.

`HTML`—This keyword tells the authentication module that you want 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.

CODE EXAMPLE 7-3 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 user ID 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

By default all modules except the UNIX module are enabled. 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 and 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.

Follow these steps to add or remove login modules from i-Planet. (In this example, a RADIUS authentication module is being added, but you use the same steps to add or remove any of the modules.)

▼ To Add (Remove) a Module to (from) the List of Authentication Modules

1. **On the i-Planet gateway in the file named** `reverseproxy.policy` **in the directory** `/opt/SUNWsnrp/policy`**, add the line:**

   ```
   * http://i-Planet _server.eng.sun.com:8080/login/Radius
   ```

   This line tells the **i-Planet** gateway to allow a URL to reach the RADIUS authentication module to start the authentication process. You can add it anywhere in the file. The **i-Planet** gateway uses this file to decide which URLs will be forwarded to the **i-Planet** server.

   If you were removing the RADIUS module, you would delete that line.

2. **As root, type the following to stop and restart the reverse proxy on the i-Planet gateway for it to recognize the changes:**

```
# /opt/SUNWsnrp/bin/iplanet_gw stop
# /opt/SUNWsnrp/bin/iplanet_gw start
```

3. **On the i-Planet server, start the web browser that you are going to use.**
4. **Type the URL for the Administration Console:**

   `http://`*`fully_qualilfied_name_of_i-Planet_server_host`*`:8080/console.`
5. **Click the Authentication link.**
6. **Add the following information to the Authentication Modules list:**

   `com.sun.login.radius.Radius`

   If you were removing a module, you would delete the line.
7. **Click the** Enter **button at the bottom of the page when you have added or removed a module to save your changes.**
8. **As root, on the i-Planet server, type the following to stop and restart the web server:**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

Troubleshooting

The following are some of the areas in which problems often occur:

- **The i-Planet server must be able to resolve whether the** `userid` **is a local or NIS** `userid`**. For example, if the** `passwd` **entry in the** `/etc/nsswitch.conf` **file specifies something like**
  `nis [NOTFOUND=return] files`
  then the system will not find a local userid.
- **If you click on the module link in the login page and keep receiving the same page back, check the file** `reversepolicy.policy` **on the i-Planet gateway.**
- **Also make sure that you restarted the reverse proxy server on the i-Planet gateway.**
- **If you do not see the module that you have added as a choice on the login page, start the Administration Console again.**
- **Make sure the authentication module that you have added (in this example,** `com.sun.login.radius.Radius`**) is listed under the Authentication Modules.** You may have forgotten to click the Enter button at the bottom of the page to save your changes, or you did not stop and restart the web server for the changes to take effect.

The Default URL

When end users successfully authenticate, they are redirected to the default i-Planet Desktop. If they want (or you want them to have) redirection to a page other than the i-Planet Desktop, you must modify the file `/opt/SUNWjeev/profiles/.default`.

▼ To Modify the `/opt/SUNWjeev/profiles/.default` File

- **Set the `user.url` to the URL to which you want all your users redirected after authentication. For example, if you want all your users to go to `www.sun.com` after authentication, type:**

  `user.url=http://www.sun.com`

Note – There is only one default for all users.

---

1. **If you want a different URL for individual end users, you must add the desired URL for each user in the file that corresponds to the authenticated name for that user.**

2. **For example, if a user authenticates as `user123`, the file should be called `/opt/SUNWjeev/profiles/user123` and should contain the following information:**

```
role=web
user.url=http://user_default_url
session.uid=user123
```

CHAPTER **8**

Supporting End Users

The chapter describes the following:

- What you need to do to setup and prepare your end users
- What issues you can expect
- The resolution to the problems

Setting up End Users

Providing support for remote or travelling users will likely occasionally be required, although i-Planet's design and browser-based interface will keep your support requirements to a minimum. Setting up end users involves both the technical setup process and providing your users with the information they need to access the system remotely.

▼ To Set Up an End User

1. **Verify that the user is correctly set up and fully functional on your local network.**
2. **Verify that each end user has a UNIX password.**

   End users must have a UNIX password so that they can use i-Planet.
3. **Add S/Keys for the end user or activate any other authentication module you chose to use.**

   At this point, the end user is technically set up and ready to go. Before the end user can access the system and use it effectively, you must provide several key pieces of information:

   a. **Fully qualified URL for the i-Planet system. For example, this will look something like:**

   ```
   https://i-Planet.acmecorp.com/
   ```

b. **If your end users are new to remote access to your corporate system, you will likely need to remind them that the protocol is https, not http.**

c. **You will likely have to tell them that they must provide a fully qualified domain name—that is, xyz.acmecorp.com, not just xyz, as they can likely do from within the local network. You can use available redirection technology.**

End users can generate their own set of passwords so that they can use the S/Key authentication module before they become remote. They can only use this procedure over the intranet.

▼ For End Users to Generate Passwords

End users can use this procedure to generate their own S/Key passwords over the intranet before they become remote.

1. **They start the web browser that they want to use.**

2. **They type the following as the URL in the browser:**

   `http://i-Planet_`*`server`*`:8080/cgi-bin/skey/skeylogin.cgi`

   8080 is the (default) port for the i-Planet server.

   If SSL is being used between the i-Planet server and the i-Planet gateway, they must type the following as the URL in the browser:

   `https://i-Planet_`*`server`*`/cgi-bin/skey/skeylogin.cgi`

   Once remotely logged into the i-Planet Desktop, end users can generate more one-time passwords by clicking the Generate SKEYs link on the i-Planet Desktop.

Note – If an end user uses the last password and logs out before generating a new list of passwords. then a new list for that user can only be generated using one of the other two methods. Generating more S/Key passwords supersedes the previously generated list. Also, their UUID will change.

Reinstalling the i-Planet software will delete all S/Key user password information.

Access information. The remote end user access information could be:

- Secure Computing's SafeWord token
- Security Dynamics' SecurID token
- RADIUS login and password
- S/Key list of passwords, unique userid, and PIN
- Other authentication tools that you have configured for your users

Connectivity requirements—End users must have full TCP/IP connectivity, either through their own ISPs, through a corporate dialup modem pool, or through some other means (Kinko's, hotels, or any other TCP/IP hookup). Your remote end users will not be able to access your i-Planet installation through non-TCP/IP networks.

Browser requirements—End users must access i-Planet through Internet Explorer 4.0 or higher, Netscape Navigator 4.04 or higher with equivalent SSL, JavaScript, and Java support. Your end users can check their browser versions by choosing Help | About in any browser and reading the version number in the resulting dialog box. Netscape browsers must be set to accept all cookies on the Edit | Preference | Advanced window.

Note – Netscape 4.04 and 4.05 require AWT 1.1 support provided by the JDK 1.1 patch available from Netscape. All versions of Netscape 4.06 and later include the patch.

Caution – If end users look at sensitive or classified documents through Internet Explorer, they must be sure to exit the browser when they have finished. Copies of all files that they have looked at are stored on the computer that they are using until they close all Internet Explorer windows.

Information specific to your i-Planet installation—Provide any special information that the end user will require, if you have added new applications to your i-Planet installation, or if your end users must use specific software in a particular way to gain access to the information they need, or if there are other special settings.

This is the only information your remote end users should require to access and use your i-Planet installation and to be able to work productively.

Troubleshooting

The following selection of Frequently Asked Questions anticipates many of the most likely issues that your users would have.

- I am unable to start the Netlet. The Java console shows something like:

```
# Applet exception: class SServer not found
java.lang.ClassNotFoundException: java/awt/event/ActionListener
    at java.lang.ClassLoader.defineClass(ClassLoader.java)
    at netscape.applet.AppletClassLoader.findClass(AppletClassLoader.java)
    at netscape.applet.AppletClassLoader.loadClass1(AppletClassLoader.java)
* at netscape.applet.AppletClassLoader.loadClass(AppletClassLoader.java)
```

```
at netscape.applet.AppletClassLoader.loadClass(AppletClassLoader.java)
at netscape.applet.DerivedAppletFrame.run(DerivedAppletFrame.java)
at java.lang.Thread.run(Thread.java)
```

The cause is that the browser does not support Java AWT 1.1. Netscape did not support this until version 4.06. There is an AWT 1.1 patch for the earlier 4.xx version of Netscape.

The solution is to use Netscape, version 4.06 or later or to install the AWT 1.1 patch for the version of Netscape being used. Check the Netscape web site for more information.

- When I try to start NetFile, I get the message: "Incorrect URL to Apps server."

  The end user is not connecting through the gateway. End users must connect through the gateway using https to the i-Planet Desktop.

- When I try to use an application on the i-Planet Desktop, I get the message: "You do not have a valid user name. You must EDIT preferences on the i-Planet Desktop."

  The cause is that there is no valid UNIX user ID for the end user in the user name field on the Edit Preferences page of the i-Planet Desktop.

  The solution is to have the end user add the valid UNIX user ID in the user name field on the Edit Preference page of the i-Planet Desktop.

- I cannot access the server. I get only a "No response" message, error messages, or nothing at all.

  Assuming that you have verified that the server is up and that you can log into the server as an end user, the following process may be helpful.

1. Verify that your end user is using the correct URL. In particular, make sure that the URL uses `https://` as the protocol, not `http://`, and that they are entering a fully-qualified domain name. If the problem persists, continue through this process.

2. Verify that the web browser is working correctly by surfing to a popular and consistently responsive site. If the alternative sites do not come up, they likely have a TCP/IP issue and should check with their local support staff for their ISP or other TCP/IP access provider. If the alternative sites do come up, continue through the process.

3. Verify that the user is using the correct version of the browser by looking at Help|About and checking the version number provided there. If the user is using the correct version (Internet Explorer 4.0 or Netscape Navigator 4.04 with AWT 1.1 support or better), continue through the process.

4. Verify security settings in the browser (Edit | Preferences | Advanced in Navigator, and View | Options | Security in Internet Explorer). Cookies must be accepted (with or without warnings) for i-Planet to work properly. Enabling Java and JavaScript is strongly recommended, but not essential.

- How do I use this application?

  Online help is available for every application and every screen delivered with i-Planet. Clicking the help link on any page will access help about that particular application or page, and your users can then navigate back to the main help page and then to any other i-Planet help pages.

  If you have added other applications to your i-Planet installation, add the online help links and files to the existing help pages.

- When systems are added in the HTML or Java user interfaces of NetFile, they do not appear in the following session, the cause is that the HTML UI or the Java GUI do not "end" correctly.

  For the HTML UI, the end user must end the session by clicking the **End Session** button. This is the action that actually writes the preferences.

  For the Java GUI, the end user must choose the End Session option in the menu. However, for the Java GUI only, if the end user shuts down the small window (Netlet page) in which the NetFile link resides too quickly, the NetFile applet cannot connect to the server anymore and the preferences may not be stored.

- Why do I keep timing out and having to log back in?

  i-Planet default settings call for a very short time-out to ensure that open (authenticated) sessions are not left running and unattended because of the particular danger of intrusions into the network. If you are, for example, checking mail, then return to work on a document in a word processor, you will almost inevitably timeout. End users could use the offline NetMail (Java) client to avoid part of this issue, but in general the inconvenience is required to ensure proper corporate security.

Note – As an administrator, you can increase the system-wide time-out interval.

- When using NetFile, what does the error message `Error: Session request failed (131,130) with myname-=SKWASH destname=<machine>` mean?

  This error message means that you are trying to add a windows machine and the name for that machine does not match the DNS or Host file entry.

- What can I do if the browser Internet Explorer hangs when I choose X-Windows on NetFile?

  If Internet Explorer hangs after you click Enter after typing the password when you are using X windows on NetFile, click the login button.

- How can I read and compose my email without being connected to the Internet all the time?

  If the NetMail Local Installer is visible on the Advance Options page of the i-Planet Desktop, you can install the NetMail applet on your local disk. (Click the Advanced link on the navigation bar on the front page of the i-Planet Desktop to move to the Advanced Options page.)

  When you click on the NetMail Local Installer link, a browser window appears that explains that this functionality allows you to install the NetMail applet on your local disk so that you can use NetMail to read and compose email without being connected to the Internet. This is known as *disconnected mode*.

  Once you have installed the NetMail applet locally, you can connect and read your email without having to download the applet each time. You also can save your email to an encrypted file on disk, so that you can continue working while you are disconnected from the server. When you reconnect, all your changes to the local email cache will be made to the server and their states synchronized. Any email that you have composed and want sent will be sent when you reconnect.

- What do I do when I get an error message saying that a license is not available?

  You should contact your i-Planet administrator who may have to restart the license server.

- When I log in using Netscape and click the NetMail or NetFile link, the correct page comes up but it contains the i-Planet Desktop, not the correct page, and it does not open the applet.

  This typically happens when the user preferences for Netscape are set to "Only accept cookies originating from the same server as the page being viewed." The user preferences for Netscape must be set to "Accept all cookies."

- The dialog boxes often appear to be empty. I am using Netscape as my browser.

  When using Netscape as your browser, if your dialog boxes appear to be empty, move your mouse slightly to cause Netscape to display properly.

APPENDIX **A**

Customizing i-Planet HTML Template Files

This chapter describes how to use the HTML templates to customize the authentication pages and the i-Planet Desktop.

HTML Templates

Caution – The classification of these templates and URLs is Unstable. For an explanation of this classification, see the manpage attributes(5) in Solaris 2.6. The likelihood that these templates and URLs will change is very high. Make a backup copy of any template file that you are going to edit.

Generally, you modify the appearance of and the information on the i-Planet Desktop through the Administration Console and through the Edit Preferences page of the end user's i-Planet Desktop. Additionally, however, you can edit template files to control the appearance of the pages in the end user's i-Planet Desktop.

In general, you use the Administration Console to change color settings and certain predefined values. You edit the HTML templates to make substantive changes to layout or design of pages or to add extra functionality, beyond the services possible through the Administration Console.

Caution – You must have strong HTML skills as well as a thorough understanding of web servers and server-side includes to edit template files. If you corrupt a template file, you may have to restore the original files from your i-Planet CD-ROM to recover and gain access to the system.

How Templates Work

HTML template files control the layout and source of the i-Planet Desktop and of the login, logout, and time-out screens. The templates are located on the i-Planet server in the directory `/etc/opt/SUNWstnr/html_templates`.

Note – If you edit these templates, you must stop and restart the web server. To restart the web server, as root type the following commands on the machine on which you have installed the i-Planet server.

▼ To Stop and Restart the Web Server on the i-Planet Server

● **As root, type the following commands to stop and restart the web server:**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

Templates for Customizing the Authentication Pages

These templates allow you to customize the login, logout, and time-out screens. Make sure the pages still contain the sections that the authentication daemon needs to implement the authentication process.

In general any JavaScript or text segment that is of the form `<subst data="rows"></subst>` must exist somewhere in the HTML page after you have modified it.

The `subst` segments are important sections of text that the authentication module dynamically replaces during the login process.

- **login_menu.html**—Is sent when more than one authentication module is configured. This gives the i-Planet end user a choice of which module to use for authentication. The text `<subst data="rows">No menu?</subst>` must be somewhere in the document. It generates a list of URLS to the authentication modules.
- **login_fail_template.html**—Is sent when authentication has failed. This page contains no required sections.

- **login_license_fail.html**—Is sent when there are no more licenses. This page contains no required sections.
- **login_reauth_menu.html**—Is sent when an i-Planet end user's session has been inactive for the time set in the Administration Console. It contains a link for reauthentication. You must not change the JavaScript in this page. You can modify all other HTML.
- **login_trustProxy_warning.html**—Is presented to i-Planet end users who log in to the i-Planet Desktop using Netscape and do not have the browser configured to accept all cookies. In this case the end user cannot start the i-Planet Java applets. If you do not want to display this page because you do not allow the end user to run Java applets, replace the contents of this page with an HTML refresh tag that contains zero time-out and is redirected to `/login/default`.
- **login_template.html**—Is sent for individual authentication modules such as RADIUS or UNIX. The six `subst` text segments must remain after you have modified it. This page is also sent when you log in to the i-Planet Administration Console.
- **logout.html**—Is called after the i-Planet end user selects the logout link on the i-Planet Desktop. It contains no required sections.
- **login_timeout_template.html**—Is called during an authentication session if the i-Planet end user does not submit the login form within the specified time. It has no required sections.
- **login_reauth_admin.html**—Is sent when your administration session has expired. It contains a link for reauthentication. You must not change the JavaScript in this page. You can modify all other HTML.
- **login_timeout_admin.html**—Is called during an administration session if you do not enter anything within the specified time. It has no required text.
- **login_fail_admin.html**—Is sent when authentication has failed. This page contains no required text.
- **logout_admin.html**—Is called after the i-Planet administrator selects the logout link on the i-Planet Administration Console. It contains no required sections.
- **session_terminated.html**—Is displayed if the i-Planet Desktop servlet cannot process the i-Planet end user's request. If the i-Planet server is rebooted while i-Planet end users are logged in, for example, their next request will cause this page to be presented.

Templates for Customizing the i-Planet Desktop

HTML template files control the layout and source of the i-Planet Desktop. The templates are:

- **advancedTemplate.html**—Controls the Advanced page in the end user's i-Planet Desktop. By default, it is set to allow an applet that downloads NetMail and installs it on a local client, but you can add other functionality of your choice.
- **feedbackTemplate.html**—Controls the appearance and layout of the feedback form in the end user's i-Planet Desktop.
- **prefTemplate.html**—Controls the appearance and layout of the Edit Preferences page in the end user's i-Planet Desktop.
- **userTemplate.html**—Controls the Front Page in the end user's i-Planet Desktop.

You can edit these files to change the appearance, the information presented, and the links. You can add or remove various features according to your corporate policy or your security policy. You can also copy these files to build new templates.

URLs for Displaying i-Planet Desktop Templates, Help, and Starting Applications

Where not shown, the gateway prefix https://gw.sun.com/ is optional, since these pages and applications can be used from within the intranet.

Desktop

The `template=` parameter to the i-Planet Desktop Servlet can be used to display any of the four predefined template files, or an arbitrary file using `http://`*`file-to-display`*. Tag-swapping is applied to all tags (if any) found in the source file. See below for a description of the tags:

- `http://apps.sun.com:8080/servlet/SNDesktop?template=user`
  Displays `/etc/opt/SUNWstnr/html_templates/userTemplate.html`
- `http://apps.sun.com:8080/servlet/SNDesktop?template=user_login`
  Displays same template file as above after recording user's login time (visible in admin console under User Preferences)
- `http://apps.sun.com:8080/servlet/SNDesktop?template=pref`
  Displays `/etc/opt/SUNWstnr/html_templates/prefTemplate.html`
- `http://apps.sun.com:8080/servlet/SNDesktop?template=advanced`
  Displays `/etc/opt/SUNWstnr/html_templates/advancedTemplate.html.`
- `http://apps.sun.com:8080/servlet/SNDesktop?template=feedback`
  Displays `/etc/opt/SUNWstnr/html_templates/feedbackTemplate.html`
- `http://apps.sun.com:8080/servlet/SNLogout`
  Ends user's session and displays
  `/etc/opt/SUNWstnr/html_templates/logout.html`
- `http://apps.sun.com:8080/servlet/SNDesktop?template=feedback`
  Displays `/etc/opt/SUNWstnr/html_templates/feedbackTemplate.html`

Help

- `http://apps.sun.com:8080/docs/usenglish/online_help/user_help_topics.html`
- `http://apps.sun.com:8080/docs/usenglish/online_help/user_help_index.html`

Applications

Generally, application links are targeted to new windows, so that the i-Planet Desktop page from which they are launched remains displayed.

- `http://apps.sun.com:8080/NetMail/netmail.html`:
  Starts NetMail from a small browser window (400 x 150 in the `delivered-userTemplate.html`)
- `http://apps.sun.com:8080/servlet/com.sun.webaccess.mail.Mail?realm=SunNet`:
  Starts NetMail Lite application
- `http://apps.sun.com:8080/servlet/com.sun.webaccess.calendar.Calendar?realm=SunNet`:
  Starts Calendar client application
- http://apps.sun.com:8080/servlet/SNDesktop?template=`http://apps.sun.com/apps/main/netsurf/netsurf.html`:
  Starts NetSurf. It is treated as a template file so that tag-swapping can be applied (starting URL to surf to is an administrable tag)
- `https://gw.sun.com/http://apps.sun.com:8080/servlet/SNDesktop?template=http://apps.sun.com:8080/apps/main/netlet/nf0.html`
  Starts Netlet in a small window, and provide link to NetFile. It runs through SNDesktopServlet to apply tag-swapping to the window's display. In the `delivered-userTemplate.html`, the spawned window is 420 x 220.

Note – This application *must* be started with the full i-Planet gateway URL prefix.

- `http://apps.sun.com:8080/cgi-bin/netfile/nf_htmlui.cgi`
  Starts the NetFile Lite application
- `http://apps.sun.com:8080/cgi-bin/skey/skeylogin.cgi`
  Creates the Generate S/Keys page

Custom Pages and Applications

For access from the Internet to intranet sites that do not require tag-swapping, use URLs of this form:

`https://gw.sun.com/http://`*`internal_machine`*`:`*`internal_port`*`/`*`url`*

Template File and Tag Swapping

When the i-Planet end user browses the i-Planet Desktop and the pages associated with these templates, an i-Planet application processes the template, substituting specific values (many specified through the Administration Console) for the place holders in the templates and sends the result to the user. This processing is required to allow you to customize the end-user interface easily through the Administration Console.

The processing and substitution are based on custom tags in the HTML template files. These are not HTML, but rather specialized extensions developed expressly for this application. The extension to HTML is provided by bracketed ([]) tags. Tags appear in-line like this: [`tagName`]. When a tag is found in any of the templates or other files processed by the i-Planet Desktop servlet, it is replaced with content retrieved from one of the following sources:

- User preferences
- System information
- i-Planet-provided services
- Configurable data that can be changed with the Administration Console
- Other configurable data
- Local files
- Content referenced by URLs.

These extensions function very much like server-side includes. Only when the file is served properly by the server, and in this case is processed through the Desktop servlet application, can you see the content accurately. If you try to view template files directly in your browser, they will appear to be broken, even if they are not.

Content Inserted from i-Planet End User's Preferences

The preferences that the i-Planet end user provides in the Edit Preferences page can be automatically substituted into a file with the tags listed in the following table. Tags marked with a (D) can be provided to new i-Planet end users as a default value through the Administration Console. The new i-Planet end user can change the default value through the Edit Preferences page of the i-Planet Desktop. TABLE A-1 contains tags for preferences that the i-Planet end user provides and a description of them.

TABLE A-1 Tag Names for User's Preferences

Tag Name	Content Inserted
firstName	User's first name
lastName	User's last name
userName	User's UNIX login name
mailPass	User's IMAP password
mailServer	User's IMAP server machine name (D)
SMTPmailServer	User's SMTP server (D)
calendarServer	User's Calendar server machine name (D)
serviceTimeout	Time-out for status check services (D)

System Information

TABLE A-2 contains the tag for the information that the system provides and a description of it.

TABLE A-2 Tag Names for System Information

Tag Name	Content Inserted
curDate	Current date and time of the machine running the i-Planet Application and web servers.

i-Planet-Provided Services

i-Planet contains services to check the status of the i-Planet end user's IMAP and calendar servers. They provide descriptive text of the machine's status. TABLE A-3 contains the tags for the services that i-Planet provides and a description of them.

TABLE A-3 Tag Names for i-Planet-Provided Services

Tag Name	Content Inserted
mailStat	Output of the "check for new mail" internal service
calendarStat	Output of the "check calendar server status" internal service

Administrator-Provided Values

The i-Planet end user cannot control the content inserted for these tags. They are provided to allow easy administrative control of the overall look of the templates. For these tags, a default value is provided by i-Planet; changing this value affects the appearance of all template files that contain the tag. The initial "A" in each tag name indicates that you can change it. Examining the template files shows the current use of these tags. TABLE A-4 contains the tags for the values that you provide and a description of them. If you examine the original HTML template files, you can see most of these tags in use.

TABLE A-4 Tag Names for Administrator-Provided Services

Tag Name	Description
AbgColor	Background color
AbannerImage	Image file in [installdir]/public_hmtl/content/common to place at the top of page
AprodName	Product/site name to place at the top of each page
AprodFont	Font to use for the product name
AprodSize	Font size of the product name
Acolor1-n	By defining values for the various colors. HTML items using those colors can be changed quickly.

Files

Files can be inserted into the output of a template. The file itself is passed through the tag-swapping mechanism, so files can contain any of the tags listed above. The initial "F" on the tag name indicates that the tag denotes a file. TABLE A-5 shows the format for tags that are used for files. Replace the *xyz* with the path and name referencing the file that you want to use.

TABLE A-5 Format for Tag Names for Files

Tag Name	Content Inserted
Fxyz	Contents of the file named xyz

URLs

The content of the URL is retrieved and inserted into the document after being passed through the swapper. The initial "U" denotes URL. TABLE A-6 contains the format for the tags that denote URLs and their description.

TABLE A-6 Format for Tag Names for URLs

Tag Name	Content Inserted
Uabc	contents of the URL named abc

Note – The URLs must be accessible by the server.

Other i-Planet Desktop Values Configured From the Administration Console

In addition to the tag values listed above, from the Administration Console you can configure the following i-Planet Desktop values shown in TABLE A-7 with their description.

TABLE A-7 Tag Names for i-Planet Desktop

Tag Name	Description
SMTP_host	The mailhost to use when sending the feedback form
Feedback_Address	When a user sends the feedback form via SMTP_host, send to this address.

Stopping and Restarting the Web Server

After you make your changes to the templates, you must restart the web server on the i-Planet server for the changes to take effect. See the procedure "To Stop and Restart the Web Server on the i-Planet Server" earlier in this Appendix.

APPENDIX **B**

Pluggable Authentication API

This appendix describes an abstract class used for writing pluggable authentication modules.

An Abstract Class Used for Writing Pluggable Authentication Modules

Caution – This API is classified Unstable. For an explanation of this classification, see the manpage attributes(5) in Solaris 2.6. The likelihood that this API will change is very high. Make a backup copy of any file that you are going to edit.

This is an abstract class that can be used to write pluggable authentication modules. Because it is an abstract class authentication, writers must subclass and override the abstract methods `init`, `validate`, and `getUserTokenId`.

How Authentication Works

The HTML for the authentication states is generated dynamically based on the parameters set in the configuration file for the authentication module developed. There must be a configuration file with the name of the class (no package name) and the extension `.properties`. This file must reside in `/etc/opt/SUNWstnr` on the i-Planet server when it is started.

The properties file is of the following form shown in CODE EXAMPLE B-1.

CODE EXAMPLE B-1 The Form for the Properties File

```
SCREEN
TIMEOUT 60
TEXT Sample Login Page
TOKEN Enter User Name:
PASSWORD Enter User Password:

SCREEN
TIMEOUT 30
TEXT Sample Login Page 2
TOKEN Enter Favorite Color
TOKEN Enter Secret Pin Number
PASSWORD Enter Challenge form
```

Each `SCREEN` entry corresponds to one authentication state or authentication HTML page. When an authentication session is invoked, one HTML page is sent for each state. In the previous sample `SCREENS`, the first state sends an HTML page asking the users to enter a token and a password. When the users submit the token and the password, the `validate()` method is called. Module writers get the tokens, validate them, and return them. The second page is then sent and the `validate()` routine is again called.

If the module writers throw a `LoginException`, an authentication failed page is sent to the user. If no exception is thrown, which implies successful completion, the users are redirected to their default page. The `TIMEOUT` parameter is used to ensure that the users respond in a timely manner. If the time between sending the page in response is greater than the `TIMEOUT`, a time-out page is sent.

Optional Pages

There are optional `HTML` and `IMAGE` parameters for each page. The `HTML` parameter allows the module writers to use their own HTML page for the authentication screens. The `IMAGE` parameter allows writers to display a background image on each page.

The `SetReplace` method allows module writers to substitute dynamic text for the token and password accompanying text descriptions.

When multiple pages are sent to the user, the tokens from a previous page may be retrieved by using the `getTokenForState` methods. Each page is referred to as a state. The underlying authentication module keeps the tokens from the previous states until the authentication is completed.

Using Your Authentication Module

For the i-Planet server to recognize your authentication module, you must add the full class name with package to the `/etc/opt/SUNWstnr/platform.conf` file after the `authenticators =` parameter. The `reverseproxy.policy` file on the i-Planet gateway must also be modified to allow requests to your authentication module. You will find this file on the i-Planet gateway in the directory `/opt/SUNWsnrp/policy/`. You must restart the reverse proxy server on the i-Planet gateway and the web server on the i-Planet server after you have modified these files.

Each authentication session creates a new instance of your authentication Java class. The reference to the class is released once the authentication session has either succeeded or failed.

Note – Any static data or reference to any static data in your authentication module must be thread safe.

For example, `.properties` and Java module files, see "Sample Files" section in this appendix or the `/`*`opt`*`/SUNWstnr/sample/auth/com/sun/login/sample` on the i-Planet server. `/opt` is the directory for the default installation. If you have customized your installation, you may have installed this file in another directory.

Constructors

`Login`

```
public Login () throws LoginException
```

If the `Login` constructor fails, `LoginException` should be thrown.

Methods

`init`

```
public abstract void init() throws LoginException
```

This method must be overridden. It is called each time an authentication session is started. If the initialization of the module fails, the `LoginException` should be thrown.

Overrides: init in class Authenicator

`validate`

```
public abstract void validate() throws LoginException
```

This method must be overridden. It is called once for each authentication page that is specified in the authentication modules properties file. The various `getToken` methods may be used to get the values for the user-entered tokens and passwords. `LoginException` should be thrown at some point during the `validate()` method if authentication has failed. The message in the exception is logged and users are sent an Authentication Failed page. If no exception is thrown, which implies successful completion, and all authentication pages have been sent, the user is authenticated. The abstract method `getUserTokenId()` is called to get the authenticated name of the user.

Overrides: `validate` in class Authenticator

`getUserTokenId`

```
public abstract String getUserTokenId()
```

This method must overridden. It is called once after the all authentication pages have been sent to the user.

Overrides: `getUserTokenId` in class Authenticator

getSessionId

```
public String getSessionId()
```

This method returns a unique key for this authentication session.

getCurrentState

```
public int getCurrentState()
```

This method returns the current state in the authentication process.

getNumberOfTokens

```
public int getNumberOfTokens()
```

This method returns the total number of tokens and passwords in the current authentication state.

getNumberOfTokensForState

```
public int getNumberOfTokensForState(int stateNumber)
```

This method returns the total number of tokens and passwords for the given authentication state. This method may be used to get token values from previous authentication states.

getToken

```
public String getToken(int index)
```

This method returns the user-entered value for the specified token in the current authentication state.

getToken

```
public String[] getToken()
```

This method returns the user-entered value for the first token in the current authentication state.

getAllTokens

```
public String[] getAllTokens()
```

This method returns all the user-entered tokens in the current authentication state.

getAllTokensForState

```
public String[] getAllTokensForState(int stateNumber)
```

Returns all the user-entered tokens in the specified authentication state.

getNumberOfStates

```
public int getNumberOfStates()
```

This method returns the number of authentication states for this authentication module.

setReplaceText()

```
public void setReplaceText(int token,
           String text)
```

The tokens and passwords have text descriptions for each authentication page. If your module needs to add to these descriptions, this can be done by inserting the keyword into the description. This method can then be used to substitute the specified text with generated dynamic text.

This method should be called for the next state, before returning from the validate `method()`.

setReplaceText

```
public void setReplaceText(int token,
               String text[])
```

Same as `setReplaceText()`, but allows replacement of multiple text strings.

logout

```
public void logout()
```

Not implemented. This method is a placeholder. It will be called when a user logs out.

Writing A Pluggable Authentication Module

This section is a task-oriented guide to writing a pluggable authentication module. It takes you through the steps for writing a pluggable authentication module. At the end of this section is a sample. You must first decide what your authentication mechanism is going to be and how many pages it will be and what inputs that the user will have to enter for each page.

Writing the Module

You must first write a stand-alone Java class that will call your specific authentication process, library, or the interface that it requires. In many cases, this will require the Java Native Interface (JNI) to have access to C or C++ library or system call.

You will most likely save time if you get it working in a stand-alone environment before you integrate it into i-Planet.

▼ To Write a Pluggable Authentication Module

1. **Write a stand-alone Java class that will call your specific authentication process, library, or the interface that it requires.**
2. **Test your module in a stand-alone environment.**

Integrating the Module

Assume you have a Java class called `com.companyx.auth.MyLogin` that takes two inputs on the command line from a user. One input is a `userId` and the second is a `password`. `MyLogin` then passes these two inputs to two routines called `myAuthenticateId(Id)` and `myAuthenticatePass(pass)`, which in turn calls the authentication-specific library and returns a success or fail with an error message if it fails.

After you have written your pluggable authentication module and tested it, you must integrate it into i-Planet. Use the following procedure to integrate your module into i-Planet.

▼ To Integrate Your Pluggable Authentication Module

1. **Modify your class to do the following:**

```
import com.sun.authd.*
extend com.sun.authd.Login
implement the validate(), init(), and getUserTokenId() methods
```

The validate method replaces your input gathering method. Each time the user submits an HTML page, the `validate()` method will be called. In the method, you call your authentication-specific routines. At any point in this method, if the authentication has failed, you must throw a `LoginException`. If desired, you can pass the reason for failure as an argument to the exception. This reason will be logged in the i-Planet authentication log.

`init()` should be used if your class has any specific initialization such as loading a JNI library. `init()` is called once for each instance of your class. Every authentication session creates a new instance of your class. Once a login session is completed the reference to the class is released.

`getUserTokenId()` is called once at the end of a successful authentication session by the i-Planet authentication server. This is the string the authenticated user will be known as in the i-Planet server. A login session is deemed successful when all pages in the `MyLogin.properties` file have been sent and your module has not thrown an exception.

2. **Create a** `MyLogin.properties` **file.**

   This file contains some simple directives which tell the i-Planet authentication daemon how to create the HTML pages for your login class dynamically. Since MyLogin requires two screens with one input each, the `MyLogin.properties` file will look like the following:

```
SCREEN
TEXT Welcome to my login pages
TIMEOUT 60
TOKEN Please enter your company ID

SCREEN
TIMEOUT 120
TEXT Welcome to my second page
PASSWORD Please enter your password
```

   This `.properties` file tells the i-Planet authentication daemon to send two successive pages to the user. After each submit, your `MyLogin` validate routine will be called with the inputs made available through public getXX methods of the Login class.

3. **Compile your java class.**

4. **Include /**`opt/SUNWjeev/classes/authd.jar` **and** `/opt/SUNWjeev/classes/acm.jar` **in your** `CLASSPATH.`

Note – If you use a package name to create the directories for the package, note the name that you used.

---

5. **Copy your class file to** `/opt/SUNWjeev/classes`**.**

Note – If you use a jar file, you will need to edit the `/opt/SUNWjeev/bin/iplsrv` script and add your jar file to the web server's `CLASSPATH`. You can also just add it to your root CLASSPATH. The `iplanet_srv` script will pick it up.

If you have JNI library, you must copy it into `/opt/SUNWjeev/lib/sparc`, or you will need to modify the `LD_LIBRARY_PATH` of `iplsrv` script.

6. **Copy your** `MyLogin.properties` **file to** `/etc/opt/SUNWstnr`**.**
7. **Add your full package.class name to the authenticators property in the** `platform.conf` **file.**

```
authenticators=com.sun.login.unix.Unix com.companyx.auth.MyLogin
```

8. **Add the lines to the** `/opt/SUNWsnrp/policy/reverseproxy.policy` **file on the i-Planet gateway.**

`http://host:port/login/MyLogin`

`https://host/login/MyLogin`

Be sure to add both http and https.

9. **Restart the web server on the i-Planet server.**
10. **Restart the reverse proxy server on the i-Planet gateway.**
11. **Test your login.**

The java file for `MyLogin` Module

CODE EXAMPLE B-2 contains a sample Java file for `MyLogin` Module.

CODE EXAMPLE B-2 Sample Java File for `MyLogin` Module

```
package com.companyx.auth;

import com.sun.authd.*;

public class MyLogin extends Login {

    private String userTokenId;

    public MyLogin() throws LoginException{}

    public void init() throws LoginException {}

    public void validate() throws LoginException {

        String token = getToken();
        if (getCurrentState() == 1) {
            int ret = myAuthenticateId(token);
            if (ret == 0) {
                throw new LoginException("Invalid UserId: " + userTokenId);
            }
        }
        else {
            int ret = myAuthenticatePassword(token);
            if (ret == 0) {
                throw new LoginException("Invalid Password: " + userTokenId);
            }
            userTokenId = token;
        }


    }

    public String getUserTokenId() {
        return userTokenId;
    }

    public int myAuthenticateId(
        String userId
    )
    {
        return 1;
    }
```

```
    public int myAuthenticatePassword(
        String userId
    )
    {
        return 1;
    }

}
```

There is also a sample in `/opt/SUNWstnr/sample/auth/com/sun/login` that uses most of the methods in the Login class. There is also a javadoc in `/opt/SUNWstnr/docs/javadocs/com/sun/authd` for the Login class.

Sample Files

Each authentication module must have a corresponding *`module`*`.properties` file.The following sample files show the form and content of the `.properties` file and samples of the code.

Examples

There are two examples of `.properties` and Java code files.

Sample `.properties` File 1

CODE EXAMPLE B-3 is a sample `.properties` file.

CODE EXAMPLE B-3 Sample `MySampleLogin.properties` File

```
SCREEN
TEXT This is a sample login page
TOKEN First Name
TOKEN Last Name
TOKEN Favorite Car
PASSWORD Favorite Car’s password

SCREEN
TIMEOUT 200
TEXT   The all password page
PASSWORD password 1
PASSWORD password 2
PASSWORD password 3
PASSWORD password 4

SCREEN
TEXT 3rd page
TOKEN Enter anything
TOKEN This will be your userID
```

Sample Java Module 1

CODE EXAMPLE B-4 is the sample code for `MySampleLogin.java`.

CODE EXAMPLE B-4 Sample Java Module—`MySampleLogin.java`

```
package com.sun.login.sample;

import java.util.*;
import com.sun.authd.*;

public class MySampleLogin extends Login {

    private String userTokenId;

    public MySampleLogin() throws LoginException{
        System.out.println("MySampleLogin()");
    }

    public void init() throws LoginException {
        System.out.println("MySampleLogin initialization");
    }

    public void validate() throws LoginException {
        System.out.println("SampleLoginModule validate()");
       // get the current login page

       int login_page = getCurrentState();

       // print out all the tokens and passwords the user entered

       String[]tokens = getAllTokens();
       for (int i = 0; i < tokens.length; i++) {
            System.out.println(i + "->" + " " + tokens[i]);
       }

       if (login_page == 2) {
            userTokenId = new String(getToken(1));
       }

    }
    public String getUserTokenId() {
        return new String(userTokenId);
    }
    public String getDescription() {
       return "My Sample Login Module";
    }
}
```

Sample `.properties` File 2

You can also find the following sample file `SampleLoginModule.properties` in `/`*`opt`*`/SUNWstnr/sample/auth/com/sun/login/sample`, where `/opt` is the directory in which it is installed by default.

CODE EXAMPLE B-5 Sample `.properties` File—`SampleLoginModule.properties`

```
SCREEN
TEXT This is a sample login page
TOKEN First Name
TOKEN Last Name
SCREEN
TIMEOUT 30

TEXT   You made it to page 2
PASSWORD Enter any password
SCREEN

TIMEOUT 60
TEXT You made it past the first page
TOKEN Enter <REPLACE>'s favorite car
PASSWORD Enter <REPLACE>'s favorite color

SCREEN
TEXT 4th page
PASSWORD who cares
TOKEN anything here
```

Sample Java Module 2

You can also find the following sample in a file named `SampleLoginModule.java` in `/`*`opt`*`/SUNWstnr/sample/auth/com/sun/login/sample`, where `/opt` is the directory in which it is installed by default.

CODE EXAMPLE B-6 Sample Java Module—`SampleLoginModule.java`

```
package com.sun.login.sample;

import java.util.*;
import com.sun.authd.*;

public class SampleLoginModule extends Login {

    private String userTokenId;
    private String firstName;
    private String lastName;

    public SampleLoginModule() throws LoginException{
        System.out.println("SampleLoginModule()");
    }

    public void init() throws LoginException {
        System.out.println("SampleLoginModule initialization");
    }

    public void validate() throws LoginException {

        int currentState = getCurrentState();
        if (currentState == 1) {
            firstName = getToken(1);
            lastName = getToken(2);
            if (firstName.equals("") || lastName.equals("")) {
                throw new LoginException("Sample failed names must not be\
empty");
        }
        return;
    }
    else if (currentState == 2) {
        String pass = getToken(1);
        System.out.println("Replace Text first: " + firstName + " last: "\
+ lastName);
        setReplaceText(1, firstName);
        setReplaceText(2, lastName);
        return;
        }
    else if (currentState == 3) {
        String[] tokens = getAllTokens();
        for (int i=0; i<getNumberOfTokens(); i++) {
            System.out.println("Token-> " + tokens[i]);
```

```
        }
        return;
    }
    else if (currentState == 4) {
        String[] tokens = getAllTokensForState(1);
        for (int i=0; i<getNumberOfTokensForState(1); i++) {
            System.out.println("Token-> " + tokens[i]);
        }
    }

        userTokenId = firstName;
     }

    public String getUserTokenId() {
        return userTokenId;
     }

}
```

APPENDIX **C**

Third-Party Software

This appendix describes how to install and configure supported third-party software:

- pcANYWHERE
- GO-Joe
- Microsoft Exchange
- NetCon
- Samba
- Other software for controlling PCs remotely

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.

An evaluation version of pcANYWHERE 32 version 8.0 client software is included in the i-Planet 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 – You must purchase a copy of pcANYWHERE for each desktop that you want to control remotely.

Installing the Trial Version Included With i-Planet

i-Planet application includes a 30-day trial version of pcANYWHERE on the i-Planet CD-ROM labelled "Contains 3rd Party Software Only." Follow the procedure below to install the trial version of pcANYWHERE.

▼ To Install the 30-Day Trial Version of pcANYWHERE

1. **Insert the i-Planet CD-ROM "Contains 3rd Party Software Only" in the CD-ROM drive of the computer to be controlled remotely.**

2. **Use Windows Explorer to copy the file** `pca_802.zip` **from the CD-ROM to a temp directory on the local hard drive (c:\windows\temp or c:\temp).**

3. **Use an unzip program (like WinZip) to decompress the file** `pca_802.zip`**.**

Note – Be sure to choose to preserve the directory structure.

You see seven new subdirectories or folders (`pcadisk1` through `pcadisk7)` under the temp directory.

4. **Use Windows Explorer to browse to the** `pcadisk1` **subdirectory, then double-click** `setup.exe`**.**

The installation begins with the dialog box shown in FIGURE C-1.

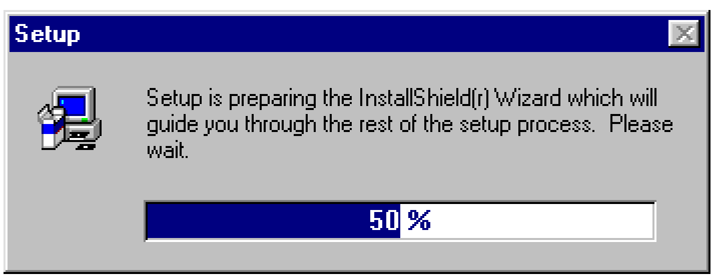

FIGURE C-1 Setup Wizard

5. **Read the introductory information on the first screen of the Setup Wizard shown in** FIGURE C-2 **and click Next.**

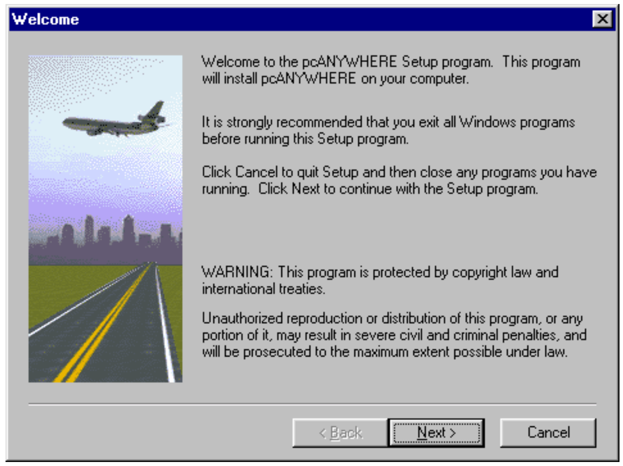

FIGURE C-2 First Screen of the pcANYWHERE Setup Wizard

6. **Fill in your name and the company name in the next dialog box shown in** FIGURE C-3 **and click Next.**

FIGURE C-3 Identification Screen of the Setup Wizard

7. **Read the license agreement shown in** FIGURE C-4 **and click Yes to accept it and continue.**

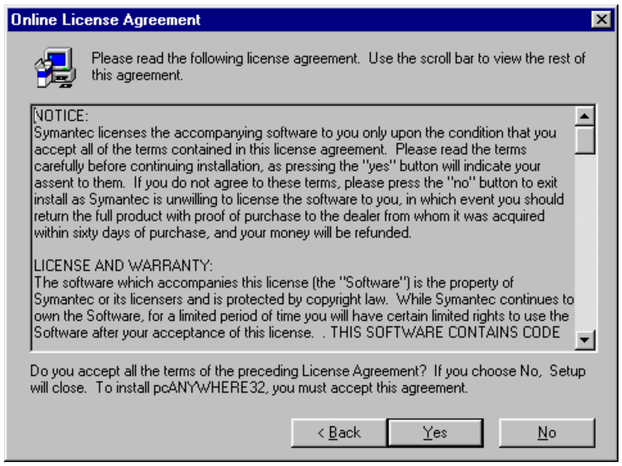

FIGURE C-4 pcANYWHERE License Agreement

8. **Confirm the location in which to install pcANYWHERE (or click Browse to choose a new location) shown in** FIGURE C-5 **and click Next to continue.**

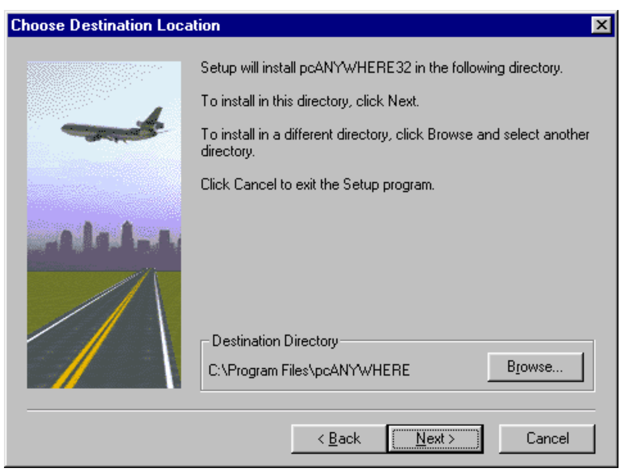

FIGURE C-5 Choose the pcANYWHERE Installation Folder

9. **pcANYWHERE, as shown in** FIGURE C-6**, informs you of the setup processes and where it is being installed. Click Next to continue.**

FIGURE C-6 pcANYWHERE Installation Information

10. **Tell the Setup Wizard where to find the next folder of files, as shown in** FIGURE C-7**.**

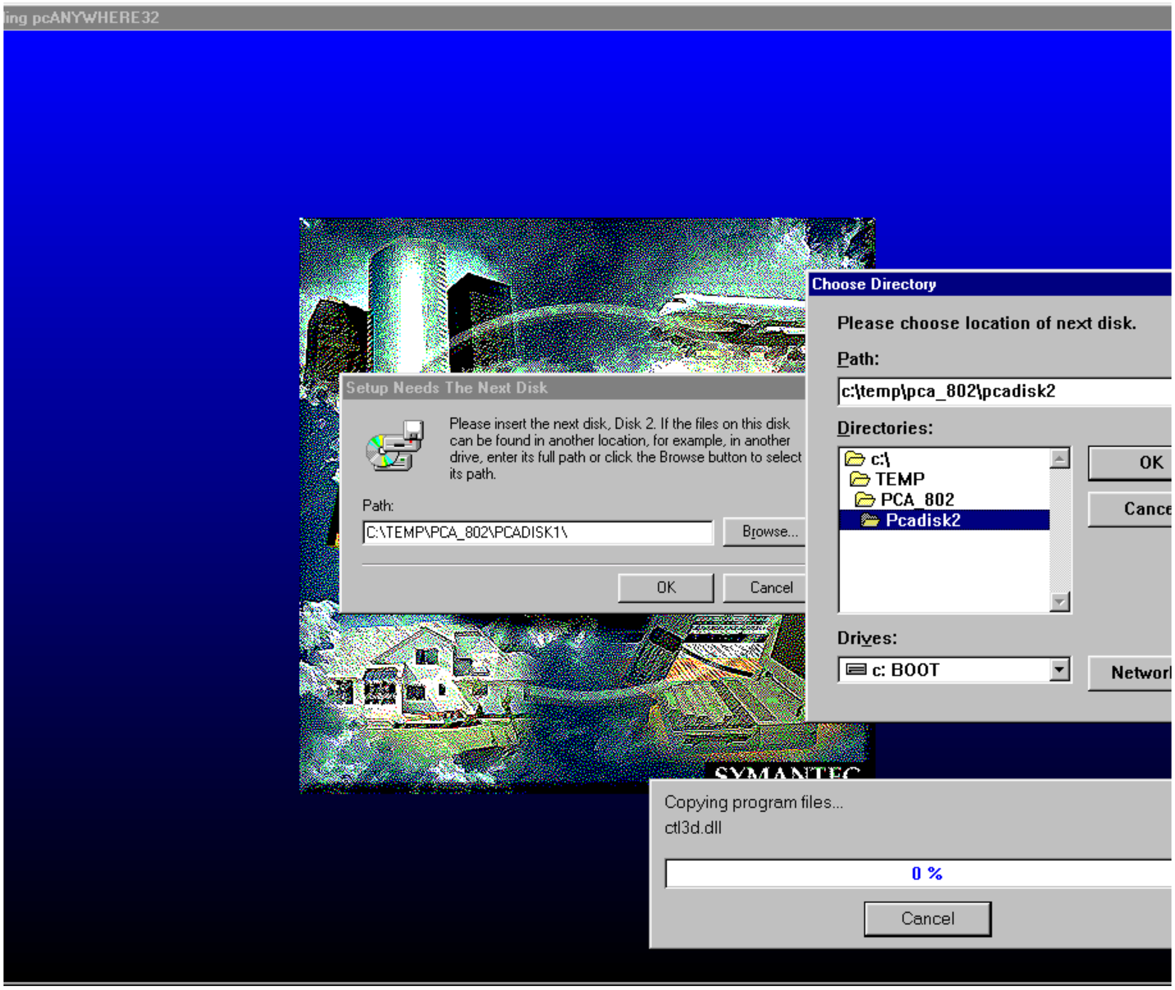

FIGURE C-7 Setup Wizard Asks the Location of Each Folder of Program Files

a. **Click Browse to select a new path and click OK to close the dialog boxes.**

   The progress dialog box shows the percentage of the software being copied.

b. **You must repeat Steps 11 and 11a for each of the remaining folders (Pcadisk3 through Pcadisk7).**

11. **Read each of the four additional screens that appear from the Setup Wizard and click Next to continue.**

12. Choose No when asked if you want to view the Readme file shown in FIGURE C-8**.**

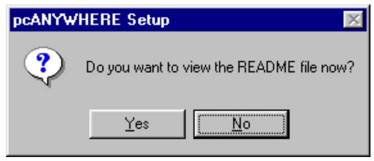

FIGURE C-8 Setup Wizard's Offer of the Readme file

13. At the end of the installation process, you are prompted to restart your computer, as shown in FIGURE C-9**.**

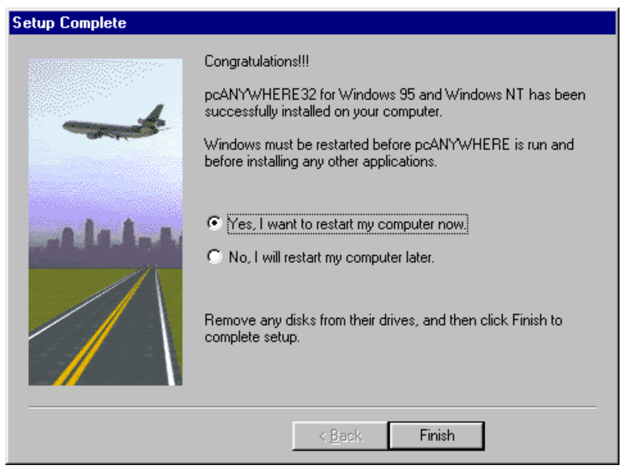

FIGURE C-9 pcANYWHERE Setup Completion Window

You can restart you computer immediately or later, but you cannot continue with the pcANYWHERE configuration until you have restarted your computer.

Configuring the Trial Version Included With i-Planet

Follow the procedure below to configure the trial version of pcANYWHERE.

▼ To Configure pcANYWHERE

1. **After restarting your computer, choose Start | Programs | pcANYWHERE32 | pcANYWHERE.**

   pcANYWHERE starts.

2. **Click I Agree button to accept the evaluation license agreement shown in** FIGURE C-10 **to proceed to use pcANYWHERE.**

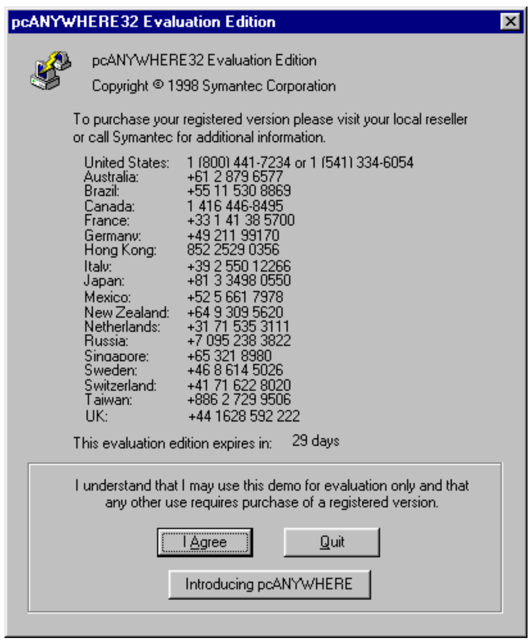

FIGURE C-10 pcANYWHERE Evaluation Agreement

3. **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 i-Planet product.

4. **Choose Quick Start | Add Be a Host PC Item shown in** FIGURE C-11.

   The Quick Start wizard walks you through the configuration steps.

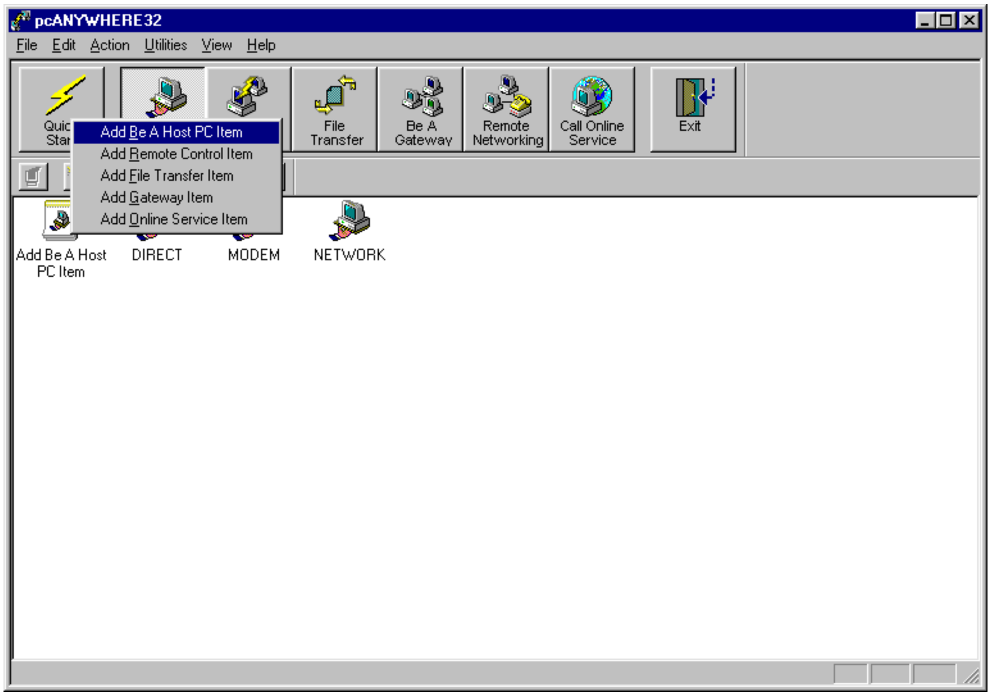

FIGURE C-11 Quick Start with Add Be a Host PC Item

5. **Provide a name (for example, i-Planet) for the connection as shown in** FIGURE C-12 **and click Next.**

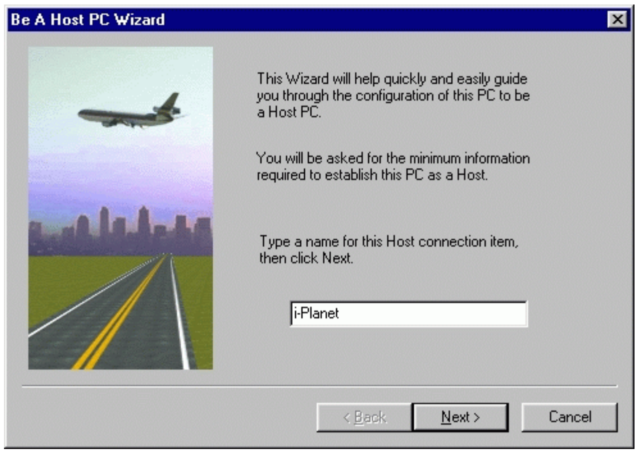

FIGURE C-12 Provide a Name for the Connection

6. **Select TCP/IP for the connection device shown in** FIGURE C-13 **and click Next.**

FIGURE C-13 Specify TCP/IP for the Connection Device

You *must* select TCP/IP from the dropdown list to use pcANYWHERE with i-Planet.

7. **Click the Finish shown in** FIGURE C-14 **to complete the pcANYWHERE Wizard.**

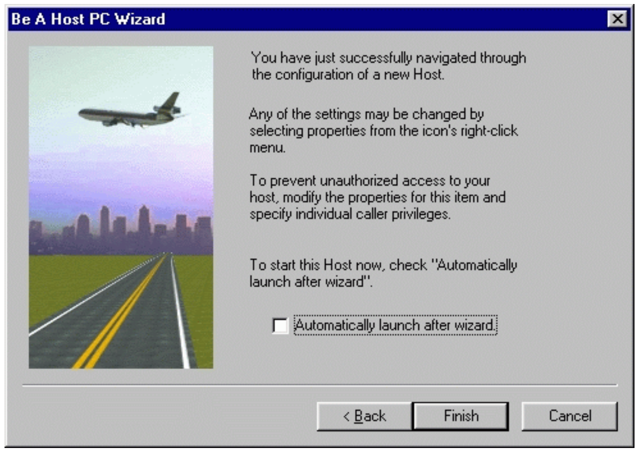

FIGURE C-14 Last Screen of the Quick Start Wizard

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 i-Planet.

8. **Right-click the i-Planet icon and choose Properties from the pop-up menu.**

Caution – Do *not* double-click the **i-Planet** icon.

The i-Planet Properties window appears as shown in FIGURE C-15.

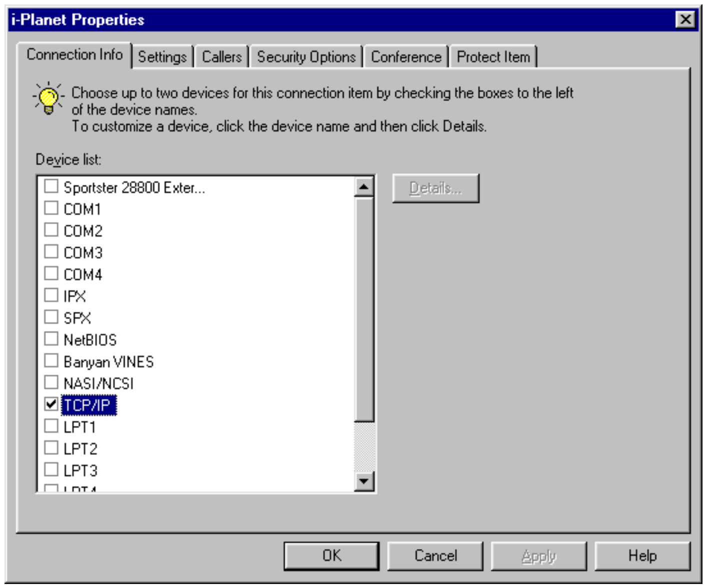

FIGURE C-15 i-Planet Properties Window

9. **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.

10. **Click the Settings tab at the top of the i-Planet Properties window to move to the next set of options.**

11. **Configure the Settings shown in** FIGURE C-16 **according to** TABLE C-1**.**

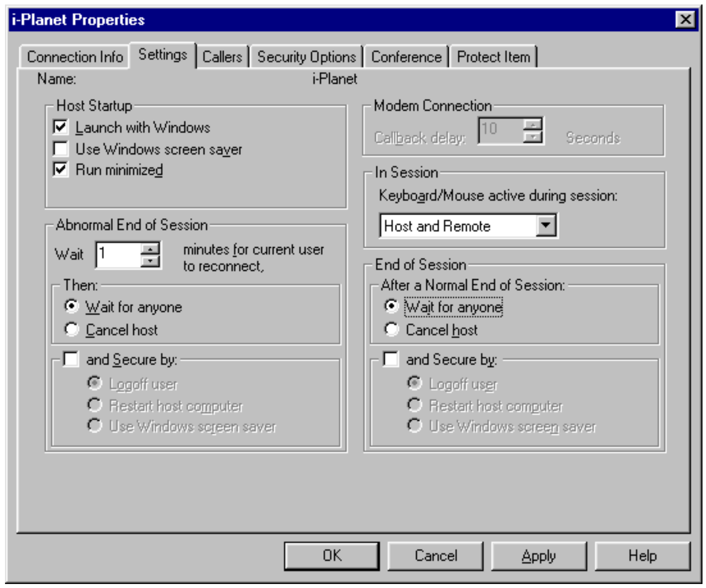

FIGURE C-16 Specify the Settings for Your Connection.

TABLE C-1 Required Choices for **i-Planet** 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

12. **Click the Callers tab at the top of the i-Planet Properties window shown in** FIGURE C-16 **to move to the next tab.**

13. **Choose Specify individual caller privileges.**

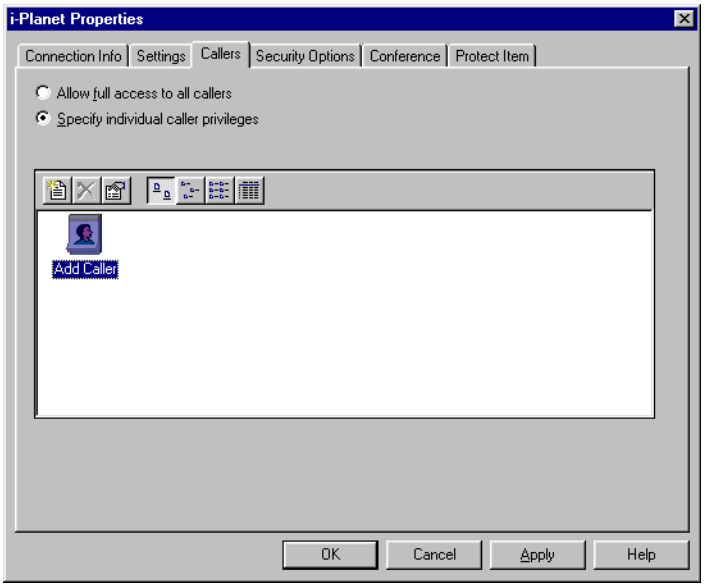

FIGURE C-17 Callers Tab for Individual Caller Privileges.

14. **Double-click the Add Caller icon to start the Add Caller Wizard.**

15. **Type the caller's name shown in** FIGURE C-18**.**

This is typically your user name for your system. It identifies you when you connect from the Internet.

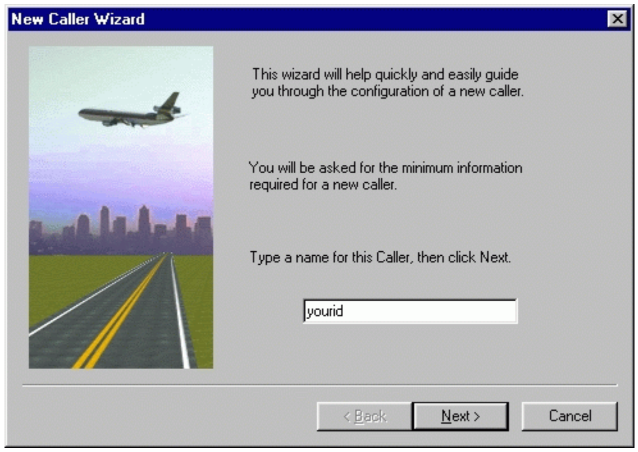

FIGURE C-18 Specify the Name for the Caller.

16. **Click Next.**

17. **Specify the caller's login name shown** FIGURE C-19**.**

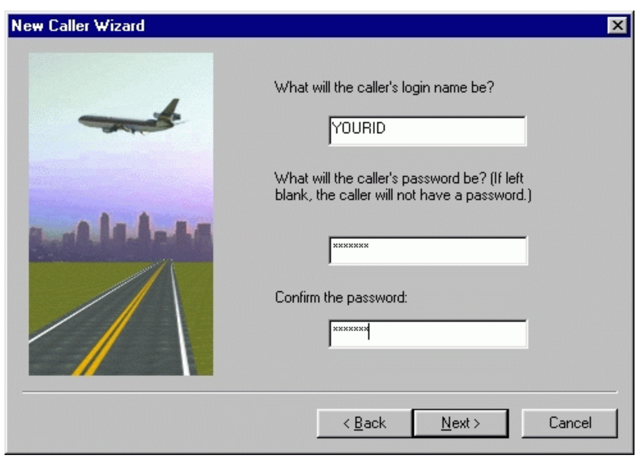

FIGURE C-19 Specify the Login name and Password.

This is the same name or user ID that you typed in the screen shown in FIGURE C-18.

18. **Type the password that you want to use, then confirm the password by typing it again in the next field shown in** FIGURE C-19**, and click Next when you have finished.**

19. **Click Finish to complete the New Caller Wizard as shown in** FIGURE C-20**.**

FIGURE C-20 Last Screen of the New Caller Wizard.

20. **Click the Security Options tab at the top of i-Planet Properties window.**

21. Configure the Security Options shown in FIGURE C-21 **according to** TABLE C-2**.**

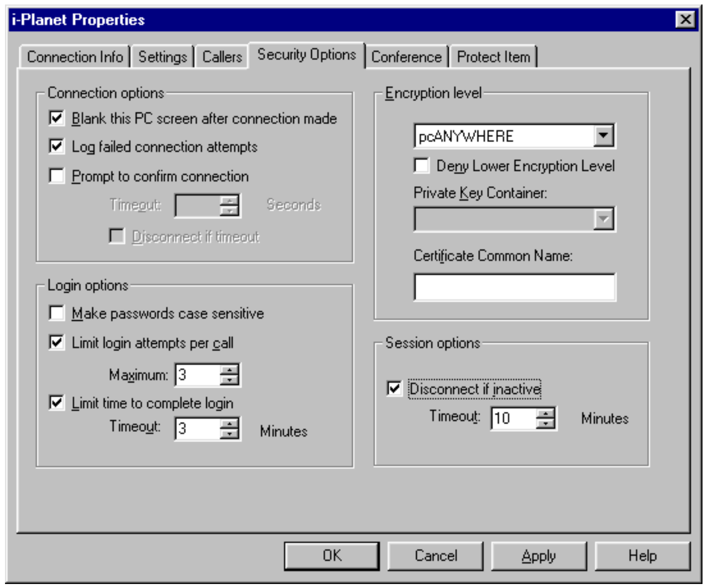

FIGURE C-21 Specify the Security Options for the Connection.

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* enter a value for the Disconnect if Inactive n Minutes option. You can, however, enter whatever value you want. A good value for this option is typically 5 to 10 minutes. There is a trade-off between entering a value that is too large or too small. If you specify a large value and are unexpectedly disconnected from the Internet, you will not be able to 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.

22. **Click OK.**

23. **Double-click the new i-Planet 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 will delay logging in because the PC has to send all the image data from it over the network.

Enabling pcANYWHERE Connections in i-Planet

In the Administration Console, you must enable pcANYWHERE in the Predefined Netlet Applications section of the Netlet frame and in the Remote Control Connections of the NetFile frame of the Administration Console so that the end users can use it.

▼ To Enable pcANYWHERE

1. **Start the Administration Console.**

2. **Click the Netlet link under Applications in the navigation frame.**

3. **Click the box beside pcANYWHERE to enable pcANYWHERE connections.**

4. **Click the Enter button at the bottom of the page.**

5. **Click the NetFile link under Applications in the navigation frame.**

6. **Click the box after Allow Remote Control Connections to show the check mark that means that Remote Control connections are enabled in the NetFile Configuration frame.**

7. **Click the Enter button at the bottom of the NetFile Configuration frame.**

8. **Open a terminal window on the i-Planet server.**

9. **As root, stop and restart the i-Planet server so that the changes will take effect.**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

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.

Note – You must purchase a copy of GO-Joe for each desktop that you want to control remotely.

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/`

Licenses

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.

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 i-Planet CD-ROM on the machines that they want to control. This package is on the i-Planet CD-ROM, "**Contains 3rd Party Software Packages Only**."

Note – If you are using the Solaris 2.5.1 Operating Environment, you must install the Common Desktop Environment (CDE) package from Sun Microsystems, Inc., before you install GO-Joe. This package is on a separate Solaris 2.5.1 CD-ROM.

▼ To Add the Package `SUNWgjvxs`

1. **Mount** the i-Planet CD-ROM, "**Contains 3rd Party Software Packages Only," on the machine that you want to control remotely.**
2. **As root, 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.

Note – If you are using GO-Joe with Internet Explorer 4.71 or 4.72, pressing the **Enter** key after you have typed the username and password during login will cause Internet Explorer to hang.

Enabling GO-Joe in the Administration Console

In the Administration Console, you must enable GO-Joe (Remote X-Window) in the Administration Console in the Netlet Administration and the NetFile Configuration pages so that your end users can use it.

▼ To Enable Go-Joe

1. **Start the Administration Console**
2. **Click the Netlet link under Applications in the navigation frame.**
3. **Click the box after GO-Joe (Remote X-Window) in the Netlet Configuration page to show the check mark denoting that GO-Joe is enabled.**
4. **Click the Enter button at the bottom of the Netlet Administration page.**
5. **Click the NetFile link under Applications in the navigation frame.**
6. **Click the box after Allow X-Window Connections in the NetFile Configuration page to show the check mark denoting that X-Window Connections are enabled.**
7. **Click Enter at the bottom of the NetFile Configuration page.**
8. **Open a terminal window on the i-Planet server.**
9. **As root on the i-Planet server, type the following to stop and restart the web server so that the changes will take effect.**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

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.

▼ Using 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.

Microsoft Exchange Server

You can use Microsoft Exchange Server software with i-Planet, Release 2.0.

Note – The information in this section applies to Microsoft Exchange Server, Versions 4.0 and 5.0.

Configuring Microsoft Exchange Directory Service, Information Store Service, and System Attendant Service to use predefined TCP/IP port numbers is helpful when configuring Internet firewalls or routers.

For the complete, official version, go to Microsoft's Web site `http://www.microsoft.com` and retrieve document Q148732.

Configuring Microsoft Exchange Software

Some Internet firewalls do not accept the TCP/IP port numbers that Microsoft Exchange Server uses for Remote Procedure Call (RPC) communication, in which case, add port 135 to your firewall. You must then configure Microsoft Exchange to use the ports that your firewall will permit.

Caution – Use Registry Editor at your own risk. The following procedures involve editing your Registry. Before you modify your Registry, back up the Registry files. Using Registry Editor incorrectly can cause serious problems that can require you to reinstall Microsoft Windows NT. It may not be possible to solve problems arising from using Registry Editor incorrectly.

After you configure your Microsoft Exchange Server, you must create Netlet rules (Section "Netlet" in Chapter 2, "Administration Console") for the Location Service on port 135 and the three remaining services: Information Store, Directory, and System Attendant. You must restart your computer for these changes to take effect. The Netlet rules for the three remaining services must map to the ports that you chose when you configured Microsoft Exchange. You create the rules for these four services in the Netlet page of the Administration Console.

▼ To Configure the RPC Port for Microsoft Exchange Directory Service

1. **From the Microsoft Windows NT program, start Registry Editor by running the command:**

   `Regedt32.exe`

2. **Under the** `HKEY_LOCAL_MACHINE` **subtree, go to the subkey**
   `SYSTEM\Current controlSet\Services\MSEXchangeDS\Parameters`

3. **Add the following registry value as the DWORD value, which must be in decimal, that specifies the port to be used:**

   `TCP/IP port`

   The RADIX should be set to decimal when you enter the value.

4. **Quit Registry Editor.**

▼ To Configure the RPC Port for Microsoft Exchange Information Store Service

1. **From the Microsoft Windows NT program, start Registry Editor by running the command:**

   `Regedt32.exe`

2. **Under the** `HKEY_LOCAL_MACHINE` **subtree, go to the subkey**
   `SYSTEM\Current controlSet\Services\MSEXchangeIS\Parameters`

3. **Add the following registry value as the DWORD value, which must be in decimal, that specifies the port to be used:**

   `TCP/IP port`

   The RADIX should be set to decimal when you enter that value.

4. **Quit Registry Editor.**

▼ To Configure the RPC Port for Microsoft Exchange System Attendant Service

To administer an Exchange server across a firewall, you must configure the Microsoft Exchange Server to use a specific port on the computer that is running Microsoft Exchange Server. Clients always connect to port 135, the endpoint mapper, and then ask what port they should use for the Directory and Information Store Services.

1. **From the Microsoft Windows NT program, start Registry Editor by running the command:**

   `Regedt32.exe`

2. **Under the** `HKEY_LOCAL_MACHINE` **subtree, go to the subkey** `SYSTEM\Current controlSet\Services\MSEXchangeSA\Parameters`

3. **Add the following registry value as the DWORD value, which must be in decimal, that specifies the port to be used:**

   `TCP/IP port`

   The RADIX should be set to decimal when you enter that value.

4. **Quit Registry Editor.**

Caution – Assign ports with numbers 2000 or above.

You only need to change the Registry on the computer running Microsoft Exchange Server. Clients always connect to port 135, the RPC endpoint mapper, and then ask what port they should use for the Directory and Information Store Server.

Microsoft Exchange Implementation Note

You must configure your site's name server so Internet-based requests for the Exchange servers you make available to the Internet users resolve to 127.0.0.1. For example, suppose that `cluster.mycompany.com` is an Exchange server behind your firewall with the IP address 154.23.45.1. You would create a name server record for your ISP (not for internal users) that maps `cluster.mycompany.com` to 127.0.0.1.

If you cannot do this, users must add an entry to the hosts file for the Exchange server pointing to 127.0.0.1. In Window 95, this file is `c:\windows\hosts`.

Information on Microsoft Exchange Services

For the guidelines and more information about the effects of assigning static ports of Exchange services, see the following article in the Microsoft Knowledge Base:

- Article-ID: Q180795
  Title: *XADM: Intrasite Directory Replication Fails with Error 1720*

For more information about Exchange services for Internet firewalls, see the following article in the Microsoft Knowledge Base:

- Article-ID: Q155831
  Title: *XCLN: How to Force Static Mapping of Sockets*

NetCon

i-Planet, Release 2.0, does not ship with software that will allow end users access to NetWare machines from the NetFile application. If you want your end users to have access to NetWare machines, you must buy the NetWare connectivity product called NetCon 7.0 from the NetCon Corporation in Crystal River, Florida.

Note – NetCon 7.0 only supports Solaris 2.5.1. and 2.6.

Installing NetCon

You must first purchase the NetCon 7.0 software from the NetCon Corporation. Install NetCon 7.0 on the i-Planet server according to the instructions from the NetCon Corporation.

Modifying the `netcon.rc` File

If you have more than 1,000 end users, you must modify the `netcon.rc` file on the i-Planet server. If you do not modify this file, NetCon will be unable to come up.

▼ To Modify the `netcon.rc` File

1. **Modify the file** `/usr/bin/local/bin/netcon.pc` **on the i-Planet server so that the line** `/usr/local/bin/netserv -c -a…` **includes the option** `-b 9000`**.**

   The line will now look something like this:

   `/usr/local/bin/netserv -b 9000 -c -a…`

2. **Reboot the i-Planet server.**

   If you have "several thousands of end users," the NetCon service will require some time to come up.

3. **Type the following to verify that the NetCon service is up:**

   ```
   % ps -ef | grep netserv | grep -v grep | wc -l
   ```

   If the return value is not `1`, the NetCon service is up. Otherwise you must wait until it is up.

Adding a Default User Map

This is a one-time set up. You do this from the NetCon Web Administration menu.

▼ To Add a Default User Map

1. **Start a browser.**
2. **Type the following URL in the Location field to connect to NetCon web server:**

   ```
   http://NetCon_install_host_name:port_number
   ```

3. **Log in to the GUI that comes up using** `netcon` **as the default user name and** `netcon` **as the default password.**
4. **From the NetCon Main Menu, choose the User Administration option.**
5. **From the User Administration menu, choose Map Network User to UNIX.**
6. **From the Login to NetCon/NetWare File Server menu, type any valid user name and password (**`root` **is preferred).**

7. **Click Login to add the default user map.**

   You will see a list of NetWare servers that are known to the machine.

Allowing Access to NetWare Machines from the i-Planet Administration Console

You must enable access to NetWare machines on the NetFile Configuration page of the Administration Console.

▼ To Allow Access to NetWare Machines from the i-Planet Administration Console

1. **As root on the i-Planet server, mount the i-Planet CD-ROM, "Contains 3rd Party Software Packages Only."**
2. **Change to the directory on the CD-ROM:**

```
# cd /cdrom/cdrom0
```

3. **Type the following to run the `enable_netcon` script:**

```
# enable_netcon
```

4. **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.

5. As root on the i-Planet server, type the following to **stop and restart the web server so that the changes will take effect.**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

Verifying NetCon Installation

You can verify that NetCon has been correctly installed and is working by going to the Administration Console.

1. **Connect to the Administration Console and log in.**
2. **Go to the NetFile Configuration page.**

   You should see that the statement "Allow access to NetWare systems" and the check box are visible.The check box should be checked to show that access to NetWare is enabled.

Samba

Samba is an open source software suite that provides seamless file and print services to SMB/CIGs clients. If you want to allow end users access to Microsoft Windows networks, you must install Samba on the i-Planet platform server. For more information about Samba, see the URL:

`http://us1.samba.org/samba/about.html`

▼ To install Samba software

1. **Mount** the i-Planet CD-ROM, "**Contains 3rd Party Software Packages Only.**"
2. **As root on the i-Planet platform server, change to the directory on the CD-ROM:**

```
# cd /cdrom/cdrom0
```

3. **Run the** `install_3ps` **script.**

   `# install_3ps`

   This adds the package `SUNWsrsmb` to the i-Planet platform server.

4. **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.

5. As root on the i-Planet server, type the following to **stop and restart the web server so that the changes will take effect.**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

Installing Other Remote Control Software for Machines Running Microsoft Windows

The i-Planet software comes with support for CarbonCopy, LapLink, RapidRemote, ReachOut, and RemotelyPossible, all of which are software from several third parties for remotely controlling PCs running under Microsoft Windows.

You must buy the software that you want your end users to use in controlling their machines running under Microsoft Windows.

The following procedure for installing these products is generic in nature and similar to the procedure for installing the pcANYWHERE software. They run slightly differently from **i-Planet's** NetFile and Netlet applications than does pcANYWHERE.

▼ To Install the Software

1. **Install the server software on the machines that your end users want to control.**
2. **Install the client software on the machine that the end users will be using to connect to the i-Planet NetFile application.**

Note – The client must alway have the target or destination machine specified as `localhost` when going through NetFile and Netlet.

3. **Click the check box behind the individual software item (**CarbonCopy, LapLink, RapidRemote, ReachOut, and RemotelyPossible) **in the Netlet Administration page of the Administration Console to enable it.**
4. **Click Enter at the bottom of the Netlet Administration page to save your changes.**
5. **Click the check box for remote control on the NetFile Configuration page of the Administration Console to enable it.**
6. **Click Enter at the bottom of the NetFile Configuration page to save your changes.**
7. **As root on the i-Planet server, stop and restart the web server so that the changes will take effect.**

```
# /opt/SUNWjeev/bin/iplanet_serv stop
# /opt/SUNWjeev/bin/iplanet_serv start
```

8. **When the end users are running the NetFile application from the i-Planet Desktop, they must:**

   a. **Select the system to be controlled remotely.**

      This is the system on which the software was installed in Step 1.

   b. **Start their own client software with the target host localhost.**

      This is the system on which the software was installed in Step 2.

Note – For all these third-party products, the end user must start the client.

Index

A

B

C

D

E

G

H

I

J

L

M

N

O

P

R

S

T

U

W