Administrator's Guide

iPlanet Web Server, FastTrack Edition

Version 4.1

806-4641-01
March 2000

Contents

About This Guide

This guide describes how to configure and administer iPlanet™ Web Server. It is intended for information technology administrators in the corporate enterprise who want to extend client-server applications to a broader audience through the World Wide Web.

This preface includes the following sections:

- What's In This Guide?
- How This Guide Is Organized
- Conventions Used In This Guide
- Using the iPlanet Web Server Documentation
- Further Reading
- Contacting Technical Support

What's In This Guide?

This guide explains how to configure and administer the iPlanet FastTrack Server. After configuring your server, use this guide to help maintain your server.

After you install the server, this guide is available in HTML format in the server root at `manual/https/ag` in your server root directory.

How This Guide Is Organized

This guide is divided into five parts, plus various appendices, a glossary, and a comprehensive index. If you are new to iPlanet Web Server, begin with Part I, "Server Basics" for an overview of the iPlanet Web Server. If you are already familiar with iPlanet Web Server, skim the material in Part I, "Server Basics" before going on to Part II, "Using the Administration Server."

Once you are familiar with the fundamentals of using the Administration Server, you can refer to Part III, “Configuring and Monitoring,” which includes examples of how to configure and monitor your iPlanet Web Servers. Part IV, “Using Programs and Objects” provides information for using programs and configuration styles. Part V, “Managing Content and Access” provides information for managing your iPlanet Web Server content, and controlling access to your iPlanet Web Servers.

Finally, the appendices address specific reference topics that describe the various topics, including: HyperText Transfer Protocol (HTTP), server configuration files, ACL files, internationalization issues, server extensions, and the iPlanet Web Server user interface reference, which you may want to review. Note that the user interface appendix is available in the online version only.

Part I: Server Basics

This part provides an overview of the iPlanet Web Server. The following chapters are included:

- Chapter 1, “Introduction to iPlanet Web Server” provides an overview of iPlanet Web Server.
- Chapter 2, “Administering iPlanet Web Servers” describes how to manage your iPlanet Web Servers with the Administration Server.

Part II: Using the Administration Server

This part provides conceptual and procedural details using the Administration Server to administer your iPlanet Web Servers. The following chapters are included:

- Chapter 3, “Setting Administration Preferences” describes how to use the Administration Server Preferences and Global Settings forms to configure your iPlanet Web Servers.
- Chapter 4, “Managing Users and Groups” describes how to how to use the Administration Server Users and Groups forms to configure your iPlanet Web Servers.

- Chapter 5, “Working with Server Security” describes how to configure your iPlanet Web Server security. Note that before reading this chapter you should be familiar with the basic concepts of public-key cryptography and the SSL protocol. These concepts include encryption and decryption; keys; digital certificates and signatures; and SSL encryption, ciphers, and the major steps of the SSL handshake. For more information regarding these topics, see *Managing Servers with Netscape Console.*

Part III: Configuring and Monitoring

This part includes examples of how to use the Server Manager to configure and monitor your iPlanet Web Servers. The following chapters are included:

- Chapter 6, “Configuring Server Preferences” describes how to configure server preferences for your iPlanet Web Server.
- Chapter 7, “Understanding Log Files” describes how to monitor your iPlanet Web Server using the Hypertext Transfer Protocol (HTTP), by recording and viewing log files, or by using the performance monitoring tools provided with your operating system.
- Chapter 8, “Performance Configuration”Performance Configuration describes how to define your server workload and sizing your system to meet your performance needs. This chapter addresses miscellaneous configuration and Unix/Linux platform-specific issues, CGI-related performance tuning problems, and other common performance issues.

Part IV: Using Programs and Objects

This part provides information for using the Server Manager to programs and configuration styles. The following chapters are included:

- Chapter 9, “Extending Your Server With Programs” describes how to install Java applets, CGI programs, JavaScript applications, and other plug-ins onto your server.
- Chapter 10, “Working With Configuration Styles” describes how to use configuration styles with iPlanet Web Server.

Part V: Managing Content and Access

This part provides information for using the Server Manager to manage your iPlanet Web Server content, and control access to your iPlanet Web Servers. The following chapters are included:

- Chapter 11, “Managing Server Content” describes how you can configure and manage your server’s content.
- Chapter 12, “Controlling Access to Your Server” describes the methods you can use to determine who has access to what files or directories on your web site.

Appendixes

This section includes various appendixes for reference material that you may wish to review. This section includes the following appendixes:

- Appendix A, “HyperText Transfer Protocol provides a short introduction to a few HTTP basic concepts.
- Appendix B, “ACL File Syntax describes the access-control list (ACL) files and their syntax.
- Appendix C, “Internationalized iPlanet Web Server describes the internationalized version of the iPlanet Web Server.
- Appendix D, “Server Extensions for Microsoft FrontPage describes using server extensions on your iPlanet Web Server that provide support for Microsoft FrontPage.

In addition, a glossary is included to define frequently used terms that may be unfamiliar to iPlanet Web Server administrators.

Conventions Used In This Guide

The conventions used in this guide are as follows:

Italic

This typeface is used for book titles, emphasis, and any text that is a placeholder for text you need to replace for your system. For example, in a URL that contains a reference to your server’s port number, the URL might contain *portnumber* in italics. Replace the words in italics with the actual value for your server.

`Monospaced font`

This typeface is used for any text that you should type. It's also used for functions, examples, URLs, filenames, and directory paths.

bold

Bold style is used for new terminology and specific dialog box and drop down menu options. All new bold terms are also in the glossary.

Using the iPlanet Web Server Documentation

The following table lists the tasks and concepts that are described in the iPlanet Web Server printed manuals and online readme file. If you are trying to accomplish a specific task or learn more about a specific concept, refer to the appropriate manual.

Note that the printed manuals are also available as online files in PDF and HTML format.

Table 1 iPlanet Web Server Documentation

For information about	See the following
Late-breaking information about the software and the documentation.	http://www.iplanet.com/docs
Installing iPlanet Web Server and migrating your data to the new iPlanet Web Server.	*iPlanet Web Server Installation & Migration Guide*
Administering one or more iPlanet Web Servers using the Administrator Server to manage and configure your servers and to perform the following tasks: • Setting up server security. • Monitoring your servers using HTTP, via log files, or via the tools provided with your OS. • Defining your server workload and sizing your system to meet your performance needs. • Installing Java applets, CGI programs, JavaScript applications, and other plug-ins onto your server.	*Administrator's Guide*
The administration server and global information on topics such as encryption, access control, and performance monitoring.	*Managing Servers with Netscape Console*

Table 1 iPlanet Web Server Documentation *(Continued)*

For information about	See the following
Planning your directory service. How you can use the directory server to support simple usage that involves only a few hundred users and some key server applications, as well as how you can scale the directory server to support millions of users. You are also introduced to the basic directory service concepts and specific guidelines that you will need to deploy a production-grade directory service.	*Netscape Directory Server Deployment Manual*
An overview of the programming technologies and APIs you can use to extend and modify iPlanet Web Server, to dynamically generate content in response to client requests, and to modify the content of the server. Links are provided to the individual books that discuss each API. This book also contains information about API changes from Enterprise 3.x to iPlanet Web Server 4.x. Use this book as the starting place for developer-level information for iPlanet Web Server 4.x.	*Programmer's Guide to iPlanet Web Server*
How to enable and implement servlets and JavaServer Pages (JSP) in iPlanet Web Server.	*Programmer's Guide to Servlets in iPlanet Web Server*
How to use Netscape Server Application Programmer's Interface (NSAPI) to build plugins to extend and modify the iPlanet Web Server. The book also discusses the purpose and use of the configuration files `obj.conf`, `magnus.conf`, and `mime.types`, and provides a comprehensive list of the directives and functions that can be used in these configuration files. It also provides a reference of the NSAPI functions you can use to define new plugins.	*NSAPI Programmer's Guide for iPlanet Web Server*

Further Reading

The iPlanet Documentation site contains documentation for administrators, users, and developers, including:

- iPlanet Web Server *Release Notes*
- *JavaScript Reference*
- Netscape Internet Service Broker programmer's guides and reference guides for Java and C++
- *Web Publishing Client API Guide*

To access these documents, use the following URL:

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

Contacting Technical Support

For Technical Support assistance, please see the Technical Support Page for the iPlanet Web Server at:

```
http://www.iplanet.com/support/
```

Part 1

Server Basics

Chapter 1

Introduction to iPlanet Web Server

This chapter introduces iPlanet Web Server and discusses some of the fundamental server concepts. Read it to obtain an overview of how iPlanet Web Server works.

This chapter includes the following sections:

- iPlanet Web Server
- iPlanet Web Server Architecture
- How iPlanet Web Server is Configured
- Administration Server
- Server Manager
- Netscape Console
- Sending Error Information

iPlanet Web Server

iPlanet Web Server is an extremely powerful multi-process, multi-threaded, secure web server built on open standards that enables your business enterprise to seamlessly integrate with other internal and external systems. By providing high performance, reliability, scalability, and manageability, iPlanet Web Server solves the business-critical needs of your web site, regardless of the size of your enterprise.

This section includes the following topics:

- iPlanet Web Server Features
- Administering and Managing iPlanet Web Servers

iPlanet Web Server Features

iPlanet Web Server is primarily designed to provide access to your business HTML files. In addition, it offers the following features:

- **Security**—Users can establish encrypted and authenticated transactions between clients and the server through the Secure Sockets Layer (SSL) 3.0 protocol. In addition, iPlanet Web Server employs the following security-based standards: Public Key Cryptography Standard (PKCS) #11, which defines the interface used for communication between SSL and PKCS #11 modules; Federal Information Processing Standards (FIPS)-140; and special certificates that work with 56 bits.
- **Access control**—You can protect confidential files or directories by implementing access control (viewing, editing, and version control) by username, password, domain name, or IP address. This feature also represents another aspect of the NSAPI Content Management plug-in, which enables an end user (the owner of a document) to set access control on a document, rather than having to ask the administrator to accomplish the task.
- **High performance**—Delivers high performance for dynamic and secure content with features such as HTTP1.1, multi-threading, and support for SSL hardware accelerators.
- **Standards-based**—iPlanet Web Server includes support for a wide range of web software standards, including: JDK 1.2; Servlets 2.1; JavaServer Pages 1.1; HTTP 1.1; and various security-based standards, including PKCS #11, FORTEZZA, FIPS-140, and 128-bit step-up certificates.
- **Server-side Java Servlet and JavaServer Pages support**—enables development of server plugins, dynamic content, presentation logic, and JDBC database access.
- **Server-side JavaScript support**—enables development of scripting applications that access the database using native drivers.
- **Additional features**—Support for multiple processes and process monitors, failover, automatic recovery, and dynamic log rotation.

Administering and Managing iPlanet Web Servers

You can manage your iPlanet Web Server(s) via the following user interfaces:

- iPlanet Web Server Administration Server

- Server Manager
- Netscape Console

In previous releases, the FastTrack Server and other Netscape servers were administered by a single server, called the Administration Server. In the 4.x release, the "administration server" is now just an additional instance of the iPlanet Web Server, called **iPlanet Web Server Administration Server**, or **Administration Server**. You use the Administration Server to administer all of your iPlanet Web Server instances. For more information, see "Administration Server.".

NOTE You can also perform administrative tasks manually by editing the configuration files or by using command-line utilities.

For managing individual instances of iPlanet Web Server, you can use the Server Manager. For more information, see "Server Manager."

If you have other 4.x iPlanet Web Servers, you can manage them through the Netscape Console, a client-based Java application. For more information, see "Netscape Console" or *Managing Servers with Netscape Console.*

iPlanet Web Server Architecture

iPlanet Web Server incorporates a modular architecture that integrates seamlessly with all of the products in the Netscape/iPlanet family of servers. You can use the Netscape Console when you need to perform administrative functions across all of the Netscape/iPlanet servers. In addition, the iPlanet Web Server includes an administration server interface for coordinating administrative functions across all of your web servers. Note that this administrative interface is itself another instance of iPlanet Web Server.

iPlanet Web Server includes the following software modules:

- Content Engines
- Server Extensions
- Runtime Environments
- Application Services

These server modules are described in the following sections.

Content Engines

iPlanet Web Server content engines are designed for manipulating customer data. The following three content engines make up the Web Publishing layer of the iPlanet Web Server architecture: HTTP (Web Server), Content Management, and the Search (Verity).

The **HTTP engine** represents the core of the iPlanet Web Server. From a functional perspective, the rest of the iPlanet Web Server architecture resides on top of this engine for performance and integration functionality.

The **Content Management engine** enables you to manage your server's content. You create and store HTML pages, JavaServer Pages, and other files such as graphics, text, sound, or video on your server. When clients connect to your server, they can view your files provided they have access to them.

The **Search engine** enables iPlanet Web Server users to search the contents and attributes of documents on the server. As the server administrator, you can create a customized text search interface that works with various types of documents formats, such as HTML, Microsoft Word, Adobe PDF, and WordPerfect. iPlanet Web Server converts many types of non-HTML documents into HTML as it indexes them so that users can use your web browser to view the documents that are found for their search.

Server Extensions

The iPlanet Web Server extensions enable you to extend or replace the function of the server to better suit your business operations. The following server extensions are part of the core iPlanet Web Server architecture:

- Common Gateway Interface (CGI)
- Netscape Server Application Programming Interface (NSAPI)
- Java Servlets and JavaServer Pages
- SHTML & JavaScript

Common Gateway Interface (CGI) is a stand-alone application development interface that enables you to create programs that process your client requests dynamically.

Netscape Server Application Programming Interface (NSAPI) is used to implement the functions the server calls when processing a request (Server Application Functions) which provide the core and extended functionality of the iPlanet Web Server. It allows the server's processing of requests to be divided into small steps which may be arranged in a variety of ways for speed and flexible configuration.

Java Servlets and JavaServer Pages extensions enable all Java servlet and JavaServer page meta-functions, including instantiation, initialization, destruction, access from other components, and configuration management. Java servlets and JavaServer pages, are reusable Java applications that run on a web server rather than in a web browser.

Runtime Environments

In addition to the various server extensions, iPlanet Web Server includes a set of runtime environments which support the server extensions. These runtime environments include the following:

- CGI Processor
- NSAPI Engine
- Java Virtual Machine (JVM)
- JavaScript Virtual Machine

Application Services

Finally, the iPlanet Web Server architecture includes a set of application services for various application-specific functions. These application services include the following:

- LiveWire Database Service
- Security & Access Control
- Session Management Service
- File System Service
- Mail Service

How iPlanet Web Server is Configured

iPlanet Web Server is configured to enable you to turn on or off various features, determine how to respond to individual client requests, and write programs that run on and interact with the server's operation. The instructions (called directives) which identify these options are stored in **configuration files**. iPlanet Web Server reads the configuration files on startup and during client requests to map your choices with the desired server activity. For more information about these files, see "iPlanet Web Server Configuration Files."

The server includes a number configuration files which are stored in *server_root*/`config` when installed on your computer.

This section includes the following topics:

- iPlanet Web Server Component Options
- iPlanet Web Server Configuration Files
- Single-Server Configuration
- Multiple-Server Configuration

iPlanet Web Server Component Options

The following component options are available when you install iPlanet Web Server:

- iPlanet Web Server Core
- Java Runtime Environment
- Java and Servlets

iPlanet Web Server Configuration Files

iPlanet Web Server includes a variety of configuration files that enable you to set various global variables, and to customize how the server responds to specific events and client requests. You can modify the configuration files automatically using the Administrator Server or Server Manager user interface settings, or manually by editing the files directly. For more information, see Chapter 8, "Performance Configuration."

The main iPlanet Web Server configuration files are: `magnus.conf`, `obj.conf`, `mime.types`, and `admpw`. These configuration files are described in this section.

`magnus.conf`: the main iPlanet Web Server configuration file. This file contains global server configuration information (such as, port, security, and so on). This file sets the values for variables that configure the server during initialization. iPlanet Web Sever reads this file and executes the variable settings on startup. The server does not read this file again until it is restarted, so you must restart the server every time you make changes to this file. For more information, see "Viewing Server Settings," on page 132 in Chapter 6, "Configuring Server Preferences."

`obj.conf`: the server's object configuration file. This file contains additional initialization information, settings for server customization, and instructions that the server uses to process requests from clients (such as browsers). iPlanet Web Server reads this file every time it processes a client request. For more information, see "Viewing Server Settings," on page 132 in Chapter 6, "Configuring Server Preferences."

For more information about the actual file syntax and the specific directives used by the `obj.conf` and `magnus.conf` configuration files, see the *NSAPI Programmer's Guide for iPlanet Web Server.*

`mime.types`: the MIME (Multi-purpose Internet Mail Extension) type configuration file. This file maps file extensions to MIME types, to enable the server to determine the type of content being requested. For example, requests for resources with `.html` extensions indicate that the client is requesting an HTML file, while requests for resources with `.gif` extensions indicate that the client is requesting an image file in GIF format. For more information, see "Specifying a Default MIME Type," on page 213 in Chapter 11, "Managing Server Content." Note that you must restart the server every time you make changes to this file.

`admpw`: the username and password file for the Administrator Server superuser. For more information, see "Changing the Superuser Settings," on page 53 in Chapter 3, "Setting Administration Preferences."

Single-Server Configuration

If you have installed iPlanet Web Server on a single server, the installation process places all the files under the server root directory that you specified during installation.

All Platforms

For all platforms, the following directories are created under the server root directory:

- **alias** contains the key and certificate files for all Netscape/iPlanet servers (for example, https-adserv-*serverid-cert7.db* and secmod.db).
- **bin** contains the binary files for the server, such as the actual server, the Administration Server forms, and so on. In addition, this directory includes the https/install **folder that** contains files needed for migrating server settings and default configuration files needed for backward compatibility.
- **docs** is the server's default primary document directory, where your server's content files are usually kept. If you are migrating settings from an existing server, this directory doesn't appear until you finish the migration process.
- **extras** contains the log analyzer and log analysis tools.
  - The flexanlg directory contains a command-line log analyzer. This log analyzer analyzes files in flexlog format.
  - The log_anly directory contains the log analysis tool that runs through the Server Manager. This log analyzer analyzes files in common log format only.
- **httpacl** contains the files that store access control configuration information in the generated.*server-identifier*.acl and genwork.*server-identifier*.acl files. The file generated.*server-identifier*.acl contains changes you make using the Server Manager access control forms after saving your changes; genwork.*server-identifier*.acl contains your changes *before* you save your changes.
- **https-admserv** contains the directories for the Administration Server. This directory has the following subdirectories and files:
  - For Unix/Linux platforms, this directory contains shell scripts to start, stop, and restart the server and a script to rotate log files.
  - conf_bk contains backup copies of the server's configuration files.
  - config contains the server's configuration files: admpw, cron.conf, dsgw.conf, dsgwfilter.conf, dsgwlanguage.conf, dsgw-orgperson.conf, dsgwserarchprefs.conf, magnus.conf, magnus.conf.clfilter, mime.types, ns-cron.conf, obj.conf, obj.conf.clfilter, servers.lst. Working copies are kept here. For more information on magnus.conf and obj.conf, see the *NSAPI Programmer's Guide for iPlanet Web Server*.
  - logs contains any error or access log files.

- `startsvr.bat` is the script that starts the Server Manager. The Server Manager lets you configure all servers installed in the server root directory.
- `stopsvr.bat` is the script that stops the Server Manager.

- **`https-server_id.domain`** are the directories for each server you have installed on the machine. Each server directory has the following subdirectories and files:
  - `ClassCache` contains classes and Java files, generated as result of the compilation of JavaServer pages.
  - `conf_bk` contains backup copies of the server's configuration files.
  - `config` contains the Administration Server configuration files.
  - `logs` contains the Administration Server log files.
  - `search` contains the following directories: `admin` and `collections`
  - `SessionData` contains session database data from `MMapSessionManager`.
  - `startsvr.bat` is the script that starts the Server Manager. The Server Manager lets you configure all servers installed in the server root directory.
  - `stopsvr.bat` is the script that stops the Server Manager.
- **`manual`** contains the online manuals for the product.
- **`plugins`** contains directories for Java, search, and other plugins. This directory has the following subdirectories:
  - `content_mgr` contains directories for your server's content.
  - `htaccess` contains server plugin for `.htaccess` access control and `htconvert`, an `.nsconfig` to `.htaccess` converter.
  - `include` contains various include files.
  - `lib` contains shared libraries.
  - `nsacl` contains information for your server's access control lists.
  - `loadbal` contains the required files for the Resonate load-balancer integration plugin.
  - `nsapi` contains header files and example code for creating your own functions using NSAPI. For more information, see the iPlanet documentation web site at: `http://www.iplanet.com/docs`

  - `samples/js` contains the Application Manager and the samples for server-side JavaScript. Note that this is available only if JavaScript was installed.
  - `search` contains information for your server's search plugins.
  - `snmp` contains information for your server's SNMP plugins.
- **`setup`** contains the various iPlanet Web Server setup files.
- **`userdb`** contains user databases and related information.
- **`LICENSE.txt`** is the license file.
- **`README.txt`** is the readme file that contains a link to the iPlanet Web Server *Release Notes*.

Unix and Linux Platforms

In addition to the files and directories described in "All Platforms," the following files are created at the `server-root` directory for Unix and Linux platforms:

- **`startconsole`** launches a browser to the Administration Server page.

The following files are created under the **`server-root/https-admserv`** directory for Unix and Linux platforms:

  - `ClassCache` contains classes and Java files, generated as result of the compilation of JavaServer pages.
  - `conf_bk` contains backup copies of the server's configuration files.
  - `config` contains the Administration Server configuration files.
  - `logs` contains the Administration Server log files.
  - `SessionData` contains session database data from `MMapSessionManager`.
  - `restart` is the script that restarts the Server Manager.
  - `rotate`
  - `start` is the script that starts the Server Manager. The Server Manager lets you configure all servers installed in the server root directory.
  - `stop` is the script that stops the Server Manager.

Multiple-Server Configuration

You can also have multiple Web servers running on the same server—all of which can be configured from a single-server administration interface called Administration Server, or from the client-side application, Netscape Console. For more information about Netscape Console, see "Netscape Console."

For more information regarding how to use the Administration Server to configure multiple servers on your machine, see "Setting Encryption Preferences," on page 56 in Chapter 3, "Setting Administration Preferences."

Administration Server

The Administration Server is a web-based server that contains the Java and JavaScript forms you use to configure all of your iPlanet Web Servers.

After installing iPlanet Web Server, you use your browser to navigate to the Administration Server page and use its forms to configure your iPlanet Web Servers. When you submit the forms, the Administration Server modifies the configuration for the server you were administering.

The URL you use to navigate to the Administration Server page depends on the computer host name and the port number you choose for the Administration Server when you install iPlanet Web Server. For example, if you installed the Administration Server on port 1234, the URL would look like this:

```
http://myserver.mozilla.com:1234
```

Before you can get to any forms, the Administration Server prompts you to authenticate yourself. This means you need to type a user name and password. You set up the "superuser" user name and password when you install iPlanet Web Server on your computer. After installation, you can use distributed administration to give multiple people access to different forms in the Administration Server. For more information about distributed administration, see "Enabling Distributed Administration," on page 54 in Chapter 3, "Setting Administration Preferences."

The first page you see when you access the Administration Server, is called Servers. You use the buttons on this page to manage, add, remove, and migrate your iPlanet Web Servers. The Administration Server provides the following tabs for your administration-level tasks:

- Servers
- Preferences

- Global Settings
- Users and Groups
- Security
- Cluster Mgmt (Cluster Management)

NOTE You must enable cookies in your browser to run the CGI programs necessary for configuring your server.

For more information on using the Administration Server, including information regarding these administration-level tasks, see Chapter 2, "Administering iPlanet Web Servers."

Server Manager

The Server Manager is a web-based interface that contains the Java and JavaScript forms you use to configure individual instances of iPlanet Web Server.

This section includes the following topics:

- Accessing the Server Manager
- Using the Resource Picker
- Wildcards Used in the Resource Picker

Accessing the Server Manager

You can access the Server Manager for iPlanet Web Server by performing the following steps:

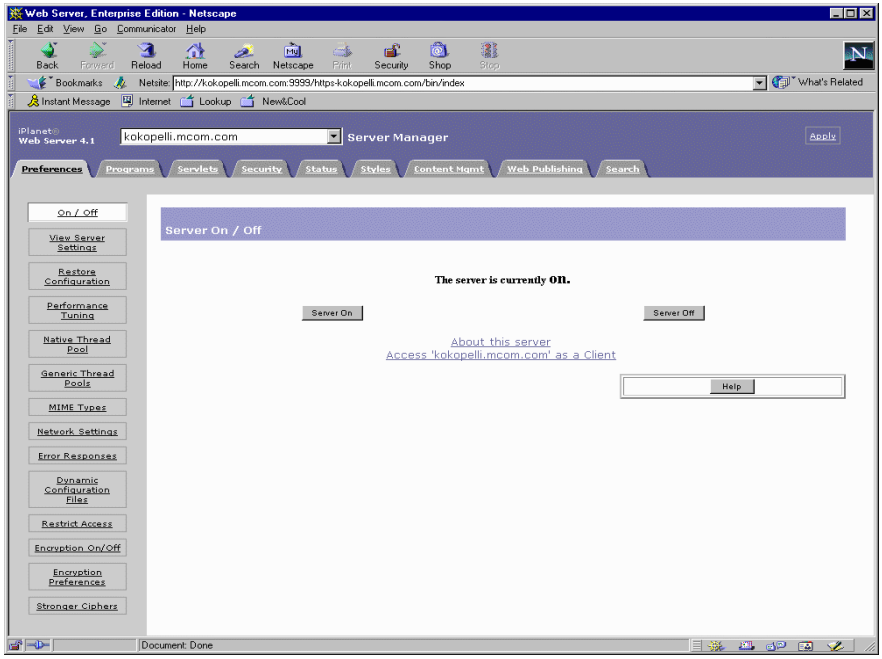
1. Install and start your iPlanet Web Server.

   The Administration Server displays the **Servers** page.

2. In the **Manage Servers** area, select the desired server and click **Manage**.

   iPlanet Web Server displays the Server Manager Preferences page, as shown in the following illustration:

Figure 1-1 The iPlanet Web Server Server Manager



NOTE Note that you must enable cookies in your browser to run the CGI programs necessary for configuring your server.

You use the links on the Preferences page to manage the following options:

- Turn iPlanet Web Server on / off
- Server settings
- Restore configuration
- Performance tuning actions
- Native thread pool
- Generic thread pool
- Global MIME types
- Network settings
- Error responses

- Dynamic configuration files
- Restrict access
- Encryption preferences
- Stronger ciphers

In addition, the Server Manager provides the following tabs for additional iPlanet Web Server managerial tasks:

- Programs
- Servlets
- Security
- Status
- Styles
- Content Mgmt
- Web Publishing
- Search

For more information, see “Server Manager”, in the online help.

Using the Resource Picker

Most of the Server Manager pages configure the entire iPlanet Web Server. Some pages can configure either the entire server or files or directories that the server maintains. These pages include the **Resource Picker**, shown in Figure 1-2, at the top. The Resource Picker lets you specify what resource to configure.

Figure 1-2 Resource Picker

Pick a resource from the drop-down list for configuration. Click Browse to browse your primary document directory; clicking Options allows you to choose other directories. Click Wildcard to configure files with a specific extension.

Wildcards Used in the Resource Picker

In many parts of the server configuration, you specify wildcard patterns to represent one or more items to configure. Please note that the wildcards for access control and text search may be different from those discussed in this section.

Wildcard patterns use special characters. If you want to use one of these characters without the special meaning, precede it with a backslash (\) character.

Table 1-1 Resource Picker wildcard patterns

Wildcard Pattern	Description
*	Match zero or more characters.
?	Match exactly one occurrence of any character.
|	An *or* expression. The substrings used with this operator can contain other special characters such as * or $. The substrings must be enclosed in parentheses, for example, (a|b|c), but the parentheses cannot be nested.
$	Match the end of the string. This is useful in *or* expressions.
[abc]	Match one occurrence of the characters a, b, or c. Within these expressions, the only character that needs to be treated as a special character is]; all others are not special.
[a-z]	Match one occurrence of a character between a and z.
[^az]	Match any character except a or z.
*~	This expression, followed by another expression, removes any pattern matching the second expression.
*.iplanet.com	Matches any string ending with the characters .iplanet.com.
quark|energy).iplanet.com	Matches either quark.iplanet.com or energy.iplanet.com.
198.93.9[23].???	Matches a numeric string starting with either 198.93.92 or 198.93.93 and ending with any 3 characters.
.	Matches any string with a period in it.

Table 1-1 Resource Picker wildcard patterns *(Continued)*

Wildcard Pattern	Description
`~iplanet-*`	Matches any string except those starting with `iplanet-`.
`*.iplanet.com~ quark.iplanet.com`	Matches any host from domain `iplanet.com` except for a single host `quark.iplanet.com`.
`*.iplanet.com~ (quark|energy|neutrino).iplanet.com`	Matches any host from domain `iplanet.com` except for hosts `quark.iplanet.com`, `energy.iplanet.com`, and `neutrino.iplanet.com`.
`*.com~*.iplanet.com`	Matches any host from domain `com` except for hosts from subdomain `iplanet.com`.

Netscape Console

Netscape Console is a Java application that provides server administrators with a graphical interface for managing all Netscape/iPlanet servers from one central location anywhere within your enterprise network. From any installed instance of Netscape Console, you can see and access all the Netscape/iPlanet servers on your enterprise's network to which you have been granted access rights. You can log in from any system connected to your network to manage a remote server or to make changes in a centralized directory.

NOTE For any given instance of Netscape Console, the limits of the network it can administer are defined by the set of resources whose configuration information is stored in the same configuration directory. That is the maximum set of hosts and servers that can appear in the Console window. For a given administrator using Netscape Console, the actual number of visible servers and hosts may be fewer, depending on the access permissions that administrator has.

For complete documentation on Netscape Console, see *Managing Servers with Netscape Console.*

Sending Error Information

iPlanet Web Server includes an error-handling mechanism called the **Quality Feedback Agent**. The Quality Feedback Agent enables you to automatically send error information (stack and register dump) to the Sun-Netscape Alliance if your iPlanet Web Server crashes.

By enabling the Quality Feedback Agent, you can assist the Sun-Netscape Alliance in determining the cause of errors that occur in the server. The Quality Feedback Agent only sends the Sun-Netscape Alliance information to help determine the cause of the error; it does not send documents or other sensitive information.

Details on Data Collected by the Quality Feedback Agent

The Quality Feedback Agent collects only the information needed to analyze and fix errors in the iPlanet Web Server. The following table summarizes all of the information collected by the agent and the reason why the Sun-Netscape Alliance collects this information.

Table 1-2 Data Collected by Quality Feedback Agent

Data Collected	OS-specific Data	Reason for Data Collection
Stack Trace	**Windows & Unix/Linux:** Stack Trace	Shows where iPlanet Web Server failed and what functions were called just before the failure.
PC (Program Counter)	**Windows & Unix/Linux:** PC	Can be used to see if the iPlanet Web Server was in a bad state when it failed.
Registers	**Windows:** Processor Registers **Unix/Linux:** No	Provides the state of the processor at the time of the failure.
Dynamic Libraries	**Windows:** Loaded dlls **Unix/Linux:** ELF32 Shared Objects	Shows any additional dlls that might have been running with or missing from the iPlanet Web Server when it failed.
Threads	**Windows:** Threads in Active Process **Unix/Linux:** No	Identifies potential race conditions with other applications or with different processes in the iPlanet Web Server.

Table 1-2 Data Collected by Quality Feedback Agent *(Continued)*

Data Collected	OS-specific Data	Reason for Data Collection
OS Version	**Windows:** Windows Version **Unix/Linux:** Unix Version	Provides the OS version. This information is necessary because the way the iPlanet Web Server interacts with different versions of an OS can cause different kinds of failures.
Processor Type	**Windows:** Processor Information **Unix/Linux:** Processor Information	Provides the processor version. This information is necessary because the iPlanet Web Server, like many software applications, can behave differently when it is running on different-speed processors.
Stack Data	**Windows & Unix/Linux:** Top 2048 bytes on the stack	Shows the value of variables passed into a function that was running at the time of failure.

Using the Quality Feedback Agent

The Quality Feedback Agent enables you to automatically send error information (stack and register dump) to the Sun-Netscape Alliance if your iPlanet Web Server crashes.

By enabling the Quality Feedback Agent, you can assist the Sun-Netscape Alliance in determining the cause of errors that occur in the server. The Quality Feedback Agent only sends the Sun-Netscape Alliance information to help determine the cause of the error; it does not send documents or other sensitive information.

NOTE If JVM is enabled, you can not use Quality Feedback Agent.

To enable the Quality Feedback Agent for your iPlanet Web Server, perform the following procedures:

1. If necessary, edit your `master.ini` file to allow the Quality Feedback Agent to send data through your firewall to the Sun-Netscape Alliance. For more information, see “Editing master.ini.”
2. Edit `magnus.conf` to enable the Quality Feedback Agent (plus any optional parameters) for your iPlanet Web server. For more information, see “Editing magnus.conf.”

Editing master.ini

If you are using automatic proxy configuration, and you want to use the Quality Feedback Agent to send incident reports to the Sun-Netscape Alliance, you need to edit the `master.ini` file to contain the appropriate proxy configuration information.

To enable the Quality Feedback Agent, perform the following steps:

1. If you are using an HTTP proxy, or both an HTTP and SOCKS proxy, open the file `master.ini` in the *`server_root`*`/bin/https/bin` directory.
2. Add the following three lines of code to your `master.ini` file, using your proxy host name, domain, and port:

```
UseUserHTTPProxyInfo=1
UserHTTPProxyHost="yourproxy.yourdomain.com"
UserHTTPProxyPort=xxxx
```

If you are using a SOCKS Proxy, add the following three lines of code to your `master.ini` file:

```
UseUserSOCKSInfo=1
UserSOCKSHost="yourproxy.yourdomain.com"
UserSOCKSPort=xxxx
```

Editing magnus.conf

To turn on the Quality Feedback Agent for your iPlanet Web server, add TalkBack on to your `magnus.conf` file. To disable it, either delete TalkBack, or specify TalkBack off.

In addition, there are two optional `magnus.conf` file variables for the Quality Feedback Agent:

- `TalkbackMaxIncidents`: If the server crashes more often than this number within a time interval, the Quality Feedback Agent will be turned off automatically. The default is 5.
- `TalkbackInterval`: The interval used by the parameter above, in seconds. The default is 86400 seconds (24 hours).

Note that both variables have no effect unless the Quality Feedback Agent is turned on. Once you restart the server, the counters are reset and the whole process starts over.

Administering iPlanet Web Servers

This chapter describes how to administer your iPlanet Web Servers with the iPlanet Web Server Administration Server. Using the Administration Server, you can manage servers, add and remove servers, and migrate servers from a previous release.

This chapter includes the following sections:

- Accessing the Administration Server
- Adding a Server: Running Multiple Servers
- Installing Multiple Instances of the Server
- Removing a Server
- Migrating a Server From a Previous Version

Accessing the Administration Server

This section describes how to access the Administration Server for Unix/Linux and Windows NT platforms.

Unix/Linux Platforms

To access the Administration Server in Unix or Linux platforms, go to the *server_root*/https-admserv/ directory (for example, /usr/netscape/server4/https-admserv/) and type ./start. This command starts the Administration Server using the port number you specified during installation.

Windows NT Platforms

The iPlanet Web Server installation program creates a program group with several icons for Windows NT platforms. The program group includes the following icons:

- Release Notes
- Start Administration Server
- Uninstall iPlanet Web Server 4.1

Note that the Administration Server runs as a services applet; thus, you can also use the Control Panel to start this service directly.

To access the Administration Server in Windows NT 4.0, perform the following steps:

1. Double-click the "Start Administration Server" icon, or type the following URL in your browser:

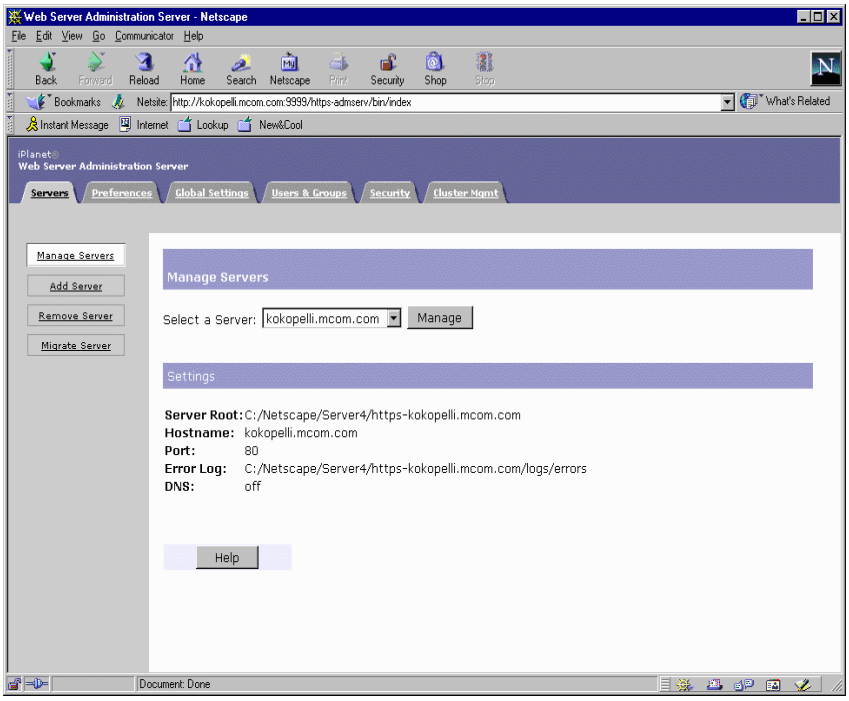
   `http://`*`hostname.domain-name:administration_port`*

   iPlanet Web Server then displays a window prompting you for a username and password.

2. Type the administration username and password you specified during installation.

   iPlanet Web Server displays the Administration Server page, as shown in Figure 2-1:

Figure 2-1 The Administration Server Page



For more information, see “Administration Server,” in the online help.

NOTE You must enable cookies in your browser to run the CGI programs necessary for configuring your server.

You can also access the Administration Server from a remote location as long as you have access to client software such as Netscape Navigator. Since the Administrator Server is accessed through a browser, you can access it from any machine that can reach the server over the network. For more information, see “Netscape Console,” on page 38 in Chapter 1, “Introduction to iPlanet Web Server.”

Adding a Server: Running Multiple Servers

There are three ways you can have multiple web servers running on your system:

- Use hardware virtual servers
- Install multiple instances of the server

Hardware Virtual Servers

Hardware virtual servers allow you to map up to five IP addresses to multiple document roots. For example, if you have two IP addresses, you could map the first IP address to one document root and the second IP address to a second document root. While hardware virtual servers take fewer system resources than multiple instances of the server, they must share the same configuration information. For example, if one hardware virtual server has enabled security features, they all must have it enabled.

Configuring Multiple Hardware Virtual Servers on the Same IP Address with Different Ports

You can configure up to fivehardware virtual servers on the same IP address by assigning a unique port number for each hardware virtual server. Note that you can not use the Administration Server to accomplish this task, you must manually edit the `obj.conf` file.

For example, to configure four hardware virtual servers on the same IP address with port numbers 80-83, add the following lines to the `obj.conf` file:

```
NameTrans fn="document-root" dir="/vs1docroot" ip="a.b.c.d" port="80"
NameTrans fn="document-root" dir="/vs2docroot" ip="a.b.c.d" port="81"
NameTrans fn="document-root" dir="/vs3docroot" ip="a.b.c.d" port="82"
NameTrans fn="document-root" dir="/vs4docroot" ip="a.b.c.d" port="83"
```

For more information on hardware virtual servers, see “Setting Up Hardware Virtual Servers,” on page 214 in Chapter 11, “Managing Server Content.”

Multiple Server Instances

Multiple server instances enables you to define separate types of configuration information for each server. For example, one instance of the server could have security features enabled while another server could have them disabled. However, each instance of the server takes substantial resources of RAM, disk space, and swap space. For more information, see the following section, “Installing Multiple Instances of the Server.”

Installing Multiple Instances of the Server

You can use the Administration Server to configure multiple servers via the following options:

- Install multiple copies of the server on NT as separate instances, each with a different IP address.
- Configure up to fiveadditional hardware virtual servers, with one iPlanet Web Server which responds to the various virtual servers independently.
- Configure a set of servers that all use the same IP address, but different port numbers.

If you have installed iPlanet Web Server on multiple servers, the installation process places all the files under the server root directory that you specified during installation, as specified in "Single-Server Configuration," in Chapter 1, "Introduction to iPlanet Web Server." However, note that iPlanet Web Server also creates an additional `https-identifier` directory for each additional server you specify.

You can install another instance of the web server on your current computer. Your web server software license allows you to have as many web server instances as you want on one system. Each web server you have installed can run on any TCP/IP port on your system, but you cannot run two web servers on the same port at the same time unless they are configured to respond to different IP addresses. Contact your system's vendor for information on how to configure your system to respond to different IP addresses.

If your system is configured to listen to multiple IP addresses, for each server you install enter one of the IP addresses that your system is hosting.

If you installed your server before configuring your system to host multiple IP addresses, configure your system to respond to different IP addresses. Then you can either install hardware virtual servers or change the server's bind address using the Server Manager and install separate instances of the server for each IP address. For more information, see "Configuring Network Settings," on page 134 in Chapter 6, "Configuring Server Preferences."

To add another server instance, perform the following steps:

1. Access the Administration Server and choose the **Servers** tab.
2. Click the **Add Server** link.
3. Enter the desired information for the specified fields.

For more information, see "The Add Server Page," in the online help.

Removing a Server

You can remove a server from your system using the Administration Server. Be sure that you don't need the server anymore before you remove it, since this process cannot be undone.

NOTE Some NT servers have an uninstall program that you can use to remove a server and its associated administration server. For details, check with your product documentation.

To remove a server from your machine, perform the following steps:

1. Access the Administration Server and choose the **Servers** tab.
2. Click **Remove Server**.

The Administration Server subsequently deletes the server's configuration files, Server Manager forms, and the following directory (and any subdirectories):

server_root/<servertype>-<id>

For more information, see "The Remove Server Page," in the online help..

Migrating a Server From a Previous Version

You can migrate an iPlanet Web Server from 3.6 to 4.1. Your 3.6 server is preserved, and a new 4.1 server using the same settings is created.

You should stop running the 3.6 server before migrating settings. Make sure you have Netscape Navigator 3.0 or later installed on your computer before migrating settings.

For a complete description of how to migrate a server from a previous version to FastTrack Server 4.1, see the iPlanet Web Server *Installation and Migration Guide.*

For more information, see "The Migrate Server Page," in the online help.

Part 2

Using the Administration Server

Setting Administration Preferences

This document describes the administration forms available via the Preferences and Global Settings tabs in the Administration Server that you use to configure your iPlanet Web Servers. Note that you must enable cookies in your browser to run the CGI programs necessary for configuring your server.

This chapter includes the following sections:

- Shutting Down the Administration Server
- Changing Network Settings
- Changing the Superuser Settings
- Enabling Distributed Administration
- Configuring Secure Sockets Layer (SSL)
- Specifying Log File Options
- Configuring Directory Services
- Restricting Server Access

Shutting Down the Administration Server

Once the server is installed, it runs constantly, listening for and accepting HTTP requests. You can stop the server using one of the following methods:

- Access the Administration Server, choose the Servers tab, and perform the following steps:

  a. Select the **Manage Servers** option.

b. Select the server you want to shut down from the Select a Server drop-down list.

c. Click **Manage**. The iPlanet Web Server displays the Server Manager forms.

For more information about using the Server On/Off page, see "Starting and Stopping the Server," on page 125 in Chapter 6, "Configuring Server Preferences."

- Choose the **Preferences** tab, select the **Shut Down** option, and click **Shut down the administration server!** button. For more information, see "The Shutdown Page," in the online help.
- Use the Services window in the Control Panel (Windows NT).
- Use `stop`, which shuts down the server completely, interrupting service until it is restarted. If you set the `etc/inittab` file to automatically restart (using "`respawn`"), you must remove the line pertaining to the web server in `etc/inittab` before shutting down the server; otherwise, the server automatically restarts. (Unix/Linux platforms).

After you shut down the server, it may take a few seconds for the server to complete its shut-down process and for the status to change to "Off."

Changing Network Settings

Network settings affect the way the Administration Server works with your iPlanet Web Servers. You can change the system user account and password and port number for iPlanet Web Administration Server.

Changing the User Account and Password

To change the system user account, you must use the Server Manager forms. For more information, see "Configuring Network Settings," on page 134 in Chapter 6, "Configuring Server Preferences."

NT

You can also change the password that the server uses when the service starts. Make sure that the user account has a password and has both administrative and "log on as a service" permissions. You should change the permissions using the Windows NT User Manager program located in the Administrative Tools group for your desktop.

Changing the Port Number

You can also change the port number that the Administration Server listens to. The port number can be any number between 1 and 65535, but it is typically a random number greater than 1024. For security reasons, consider changing the port number regularly.

To change the Administration Server port number, perform the following steps:

1. Access the Administration Server and choose the **Preferences** tab.
2. Click the **Network Settings** link.
3. Make the desired changes and click OK.

Note that you must restart the server for the settings to take effect.

For more information, see “The Network Settings Page,”. in the online help.

Changing the Superuser Settings

You can configure superuser access for your Administration Server. These settings affect only the superuser account. That is, if your Administration Server uses distributed administration, you need to set up additional access controls for the administrators you allow.

CAUTION If you use Netscape Directory Server to manage users and groups, you need to update the superuser entry in the directory *before* you change the superuser username or password. If you don’t update the directory first, you won’t be able to access the Users & Groups forms in the Administration Server. To fix this, you’ll need to either access the Administration Server with an administrator account that does have access to the directory, or you’ll need to update the directory using the Netscape Directory Server’s Netscape Console or configuration files.

To change the superuser settings for the Administration Server, perform the following steps:

1. Access the Administration Server and choose the **Preferences** tab.
2. Click the **Superuser Access Control** link.
3. Make the desired changes and click OK.

For more information, see "The Superuser Access Control Page," in the online help.

NOTE You can change the Administration Server user from root to another user on the operating system to enable multiple users (belonging to the group) to edit/manage the configuration files. However, note that while on Unix/Linux platforms, the installer can give "rw" (read/write) permissions to a group for the configuration files, on Windows NT platforms, the user must belong to the "Administrators" group.

The superuser's username and password are kept in a file called *server_root*/admin-serv/config/admpw. If you forget the username, you can view this file to obtain the actual name; however, note that the password is encrypted and unreadable. The file has the format username:password.

CAUTION If you forget the password, you can edit the admpw file and simply delete the encrypted password. You can then go to the Server Manager forms and specify a new password. Because you can do this, it is very important that you keep the server computer in a secure place and restrict access to its file system. On Unix/Linux systems, consider changing the file ownership so that it's writable only by root or whatever system user runs the Administration Server daemon. On NT systems, restrict the file ownership to the user account Administration Server uses.

Enabling Distributed Administration

Distributed administration allows multiple administrators to change specific parts of the server. With distributed administration you have three levels of users:

- **superuser** is the user listed in the file *server_root*/admin-serv/config/admpw. This is the user name (and password) you specified during installation. This user has full access to all forms in the Administration Server, except the Users & Groups forms, which depend on the superuser having a valid account in an LDAP server such as Netscape Directory Server.

- **administrators** go directly to the Server Manager forms for a specific server, including the Administration Server. The forms they see depend on the access control rules set up for them (usually done by the superuser). Administrators can perform limited administrative tasks and can make changes that affect other users, such as adding users or changing access control.
- **end users** can view read-only data stored in the database. Additionally, end users may be granted access permissions to change only specific data.

For an in-depth discussion of access control for iPlanet Web Server, see "What Is Access Control?," on page 221 in Chapter 12, "Controlling Access to Your Server."

NOTE Before you can enable distributed administration, you must install a Directory Server. For more information, see *Netscape Directory Server Administrator's Guide.*

To enable distributed administration, perform the following steps:

1. Verify that you have installed a Directory Server.
2. Access the Administration Server.
3. One you've installed a Directory Server, you may also need to create an administration group, if you have not previously done so.

   To create a group, perform the following steps:

   a. Choose the **Users & Groups** tab.

   b. Click the **New Group** link.

   c. Create an "administrators" group in the LDAP directory and add the names of the users you want to have permission to configure the Administration Server, or any of the servers installed in its server root. All users in the "administrators" group have full access to the Administration Server, but you can use access control to limit the servers and forms they will be allowed to configure.

CAUTION Once you create an access-control list, the distributed administration group is added to that list. If you change the name of the "administrators" group, you must manually edit the access-control list to change the group it references.

4. Choose the **Preferences** tab.
5. Click the **Distributed Admin** link.
6. Make the desired changes and click OK.

For more information, see "The Distributed Administration Page," in the online help.

Configuring Secure Sockets Layer (SSL)

Using the Administration Server, you can activate the iPlanet Web Server encryption feature. For more information regarding iPlanet Web Server encryption features, see "About iPlanet Web Server Security," on page 86 in Chapter 5, "Working with Server Security."

Note that prior to activating SSL for your iPlanet Web Server you need to set up some preliminary requirements, such as creating a trust database, and requesting and installing an encryption certificate. For more information, see "Configuring iPlanet Web Server for SSL," on page 91 in Chapter 5, "Working with Server Security."

Activating SSL

To activate SSL for your Administration Server, perform the following steps:

1. Access the Administration Server and choose the **Preferences** tab.
2. Click the **Encryption On/Off** link.
3. Make the desired changes and click OK.

For more information, see "The Encryption On / Off Page," in the online help.

Setting Encryption Preferences

The Administration Server enables you to set the following SSL encryption preferences:

- Specify whether to require client certificates.
- Set the SSL 2.0 ciphers.
- Set the SSL 3.0 ciphers.

Your server can perform encryption with a number of different encryption functions, called ***ciphers***. Some ciphers are more resistant to cracking than others. During an SSL connection, the client and the server agree to use the strongest cipher they can both use for communication. For more information regarding ciphers, see *Managing Servers with Netscape Console.*

To set these encryption preferences, perform the following steps:

1. Access the Administration Server and choose the **Preferences** tab.
2. Click the **Encryption Prefs** link.
3. Check the SSL versions you want your server to communicate with. The latest and most secure version is SSL version 3, but a few older clients use only SSL version 2. You will probably want to enable your server to use both versions.
4. Check the ciphers you want your server to use. The ciphers are listed for each version of SSL. Some ciphers are more secure, or *stronger*, than others. Generally speaking, the more bits a cipher uses during encryption, the harder it is to decrypt the data. Ciphers are described after this list.
5. Click OK. Make sure you restart your server.

When a client initiates an SSL connection with a server, the client lets the server know what ciphers it prefers to use to encrypt information. In any two-way encryption process, both parties must use the same ciphers. Since there are a number of ciphers available, you should consider enabling all ciphers.

You can choose ciphers from both the SSL 2 and SSL 3 protocols. Unless you have a compelling reason why you don't want to use a specific cipher, you should check them all.

For more information, see "The Encryption Preferences Page," in the online help.

Setting Stronger Ciphers

You can set stronger ciphers via the **Stronger Ciphers** option on the Server Manager **Preferences** tab. The Stronger Ciphers option presents a 56-bit secret keysize restriction or no restriction. You can specify a filename to be served when the restriction is not met. If no filename is specified, iPlanet Web Server returns a "Forbidden" status.

If you select a restriction that is not consistent with the current cipher settings under Security Preferences, iPlanet Web Server displays a popup dialog that warns that you need to enable ciphers with larger secret keysizes.

The implementation of the keysize restriction is now based on an NSAPI `PathCheck` directive, rather than Service `fn=key-toosmall`. This directive is:

```
PathCheck fn="ssl-check" [secret-keysize=<nbits>]
[bong-file=<filename>]
```

where <nbits> is the minimum number of bits required in the secret key, and <filename> is the name of a file (not a URI) to be served if the restriction is not met.

This function returns REQ_NOACTION if SSL is not enabled, or if the secret-keysize parameter is not specified. If the secret keysize for the current session is less than the specified secret-keysize, the function returns REQ_ABORTED with a status of PROTOCOL_FORBIDDEN if bong-file is not specified, or else REQ_PROCEED, and the "path" variable is set to the bong-file <filename>. Also, when a keysize restriction is not met, the SSL session cache entry for the current session is invalidated, so that a full SSL handshake will occur the next time the same client connects to the server.

NOTE The Stronger Ciphers form removes any Service fn=key-toosmall directives that it finds in an object when it adds a PathCheck fn=ssl-check.

For more information, see "The Enforce Strong Security Requirements Page," in the online help.

Specifying Log File Options

Log files can help you monitor your server's activity. You can use these logs to monitor your server and troubleshoot problems.

To configure logging options for the Administration Server, perform the following steps:

1. Access the Administration Server and choose the **Preferences** tab.
2. Click the **Logging Options** link.
3. Make the desired changes and click OK.

For more information, see "The Logging Options Page," in the online help.

This section also includes topics that describe how to configure the iPlanet Web Server Log File options to perform the following tasks:

- Viewing the Access Log File

- Viewing the Error Log File
- Archiving Log Files

Viewing the Access Log File

The `access` log, located in `admin/logs` in the server root directory, records information about requests to the server and the responses from the server.You can specify the server log format—what is included in the `access` log file—to be the Common Logfile Format, a commonly supported format that provides a fixed amount of information about the server, or you can create a custom log file format that better suits your server requirements.

To view the access log file, perform the following steps:

1. Access the Administration Server and choose the **Preferences** tab.
2. Click the **View Access Log** link and click OK.

For more information, see "The View Error Log Page," in the online help.

Viewing the Error Log File

The `error` log file, located in `admin/logs` in the server root directory, lists all the errors the server has encountered since the log file was created. It also contains informational messages about the server, such as when the server was started and who tried unsuccessfully to log in to the server.

To view the error log file, perform the following steps:

1. Access the Administration Server and choose the **Preferences** tab.
2. Click the **View Error Log** link and click OK.

You can also view the server's active and archived log files from the Server Manager. For more information regarding these log files, see "The View Access Log Page," in the online help.

Archiving Log Files

You can set up your log files to be automatically archived. At a certain time, or after a specified interval, iPlanet Web Server rotates your access logs. iPlanet Web Server saves the old log files and stamps the saved file with a name that includes the date and time they were saved.

For example, you can set up your files to rotate every hour, and iPlanet Web Server saves and names the file "`access.199907152400`," where "name | year | month | day | 24-hour time" is concatenated together into a single character string. The exact format of the access log archive file varies depending upon which type of log rotation you set up.

iPlanet Web Server offers the two types of log rotation for archiving files:

- **Internal-daemon log rotation**—this type of log rotation happens within the HTTP daemon, so the server doesn't need to restart.
- **Cron-based log rotation**—this type of log rotation is based on the time stored in the `cron.conf` file. For more information about cron controls, see "Using Cron Controls (Unix/Linux)," on page 60.

Access log rotation is initialized at server startup. If rotation is turned on, iPlanet Web Server creates a time-stamped access log file and rotation starts at server startup.

Once the rotation starts, iPlanet Web Server creates a new time stamped access log file when there is a request that needs to be logged to the access log file and it occurs after the previously-scheduled "next rotate time."

For more information about archiving log files, see "Archiving Log Files," on page 153 in Chapter 7, "Understanding Log Files."

Using Cron Controls (Unix/Linux)

You can configure several features of your iPlanet Web Server to operate automatically and set to begin at specific times. The Netscape cron daemon checks the computer clock and then spawns processes at certain times. (These settings are stored in the `ns-cron.conf` file.)

This cron daemon controls scheduled tasks for your iPlanet Web Server and can be activated and deactivated from the Administration Server. The tasks performed by the cron process depends on the various servers. (Note that on NT platforms, the scheduling occurs within the individual servers.)

Some of the tasks that can be controlled by cron daemons include scheduling collection maintenance and archiving log files. You need to restart cron control whenever you change the settings for scheduled tasks.

To restart, start, or stop cron control, perform the following steps:

1. Access the Administration Server and choose the **Global Settings** tab.
2. Click the **Cron Control** link.
3. Click Restart, Start, or Stop to change the cron controls.

Note that any time you add a task to cron, you need to restart the daemon.

Configuring Directory Services

You can manage all your user information from a single source via an open-systems server protocol called the **Lightweight Directory Access Protocol (LDAP)**. You can also configure the server to allow your users to retrieve directory information from multiple, easily accessible network locations.

To configure the directory services preferences, perform the following steps:

1. Access the Administration Server and choose the **Global Settings** tab.
2. Click the **Configure Directory Service** link.
3. Make the desired changes and click OK.

For more information, see “The Configure Directory Service Page,” in the online help.

Restricting Server Access

You can control access to the entire server or to parts of the server (that is, directories, files, file types). When the server evaluates an incoming request, it determines access based on a hierarchy of rules called **access-control entries (ACEs)**, and then it uses the matching entries to determine if the request is allowed or denied. Each ACE specifies whether or not the server should continue to the next ACE in the hierarchy. The collection of ACEs is called an **access-control list (ACL)**.When a request comes in to the server, the server looks in `obj.conf` for a reference to an ACL, which is then used to determine access. By default, the server has one ACL file that contains multiple ACLs.

You can set access control globally for all servers through the Administration Server or for a resource within a specific server instance through the Server Manager. For more information about setting access control for a resource, see “Restricting Access to Your Web Site,” on page 230 in Chapter 12, “Controlling Access to Your Server.”

NOTE You must turn on distributed administration before you can restrict server access.

To restrict access to your iPlanet Web Servers, perform the following steps:

1. Access the Administration Server and choose the **Global Settings** tab.
2. Click the **Restrict Access** link.
3. Select the desired server and click **Edit ACL**.

   The Administration Server displays the access control rules for the server you specified.

Make the desired access control changes and click OK.“

Chapter 4

Managing Users and Groups

This chapter describes how to use the forms in the Administration Server Users and Groups tab.

This chapter includes the following sections:

- About Users and Groups
- Creating Users
- Managing Users
- Creating Groups
- For more information, see “The New Group Page,” in the online help.Managing Groups
- Creating Organizational Units
- Managing Organizational Units
- Managing a Preferred Language List

About Users and Groups

The Administration Server provides you access to your application data about user accounts, group lists, access privileges, organization units, and other user/group-specific information. You can use the Administration Server to create, locate, and manage records for users and groups within your iPlanet Web Servers.

iPlanet Web Server 4.x does not support local LDAP. In order to add users and groups, you must have a directory server installed, such as Netscape Directory Server. If you need to create, locate, or manage records for users and groups on any other servers within your network, you should use Netscape Console with your Directory Server. For more information, see *Managing Servers with Netscape Console*.

Warning (NT)
You cannot install Netscape Directory Server 4.0 and iPlanet Web Server 4.x on the same Windows NT machine because of system library conflicts. Install Directory Server on a separate machine and use the Administration Server's Global Settings tab to configure iPlanet Web Server to use that Directory Server.

The Users and Groups tab of the Administration Server enables you to create or modify users, groups, and organizational units. Each user and group in your enterprise is represented by a **Distinguished Name (DN)** attribute. A DN attribute is a text string that contains identifying information for an associated user, group, or object. You use DNs whenever you make changes to a user or group directory entry. For more information regarding distinguished name syntax and frequently used attributes, see *Managing Servers with Netscape Console.*

Note that if you do not currently have a directory, or if you want to add a new subtree to an existing directory, you can use the Directory Server's Administration Server LDIF import function. This function accepts a file containing LDIF and attempts to build a directory or a new subtree from the LDIF entries. You can also export your current directory to LDIF using the Directory Server's LDIF export function. This function creates an LDIF-formatted file that represents your directory. For more information, see your Directory Server documentation.

Creating Users

Use the Users and Groups tab of the Administration Server to create or modify user entries. A user entry contains information about an individual person or object in the database.

This section includes the following topics:

- Guidelines for Creating User Entries
- How to Create a New User Entry
- Directory Server User Entries

Guidelines for Creating User Entries

Consider the following guidelines when using the administrator forms to create new user entries:

- If you enter a given name (or first name) and a surname, then the form automatically fills in the user's full name and user ID for you. The user ID is generated as the first initial of the user's first name followed by the user's last name. For example, if the user's name is Billie Holiday, then the user ID is automatically set to *bholiday*. You can replace this user ID with an ID of your own choosing if you wish.
- The user ID must be unique. The Administration Server ensures that the user ID is unique by searching the entire directory from the search base (base DN) down to see if the user ID is in use. Be aware, however, that if you use the Directory Server `ldapmodify` command line utility (if available) to create a user, that it does not ensure unique user IDs. If duplicate user IDs exist in your directory, the affected users will not be able to authenticate to the directory.
- Note that the base DN specifies the distinguished name where directory lookups will occur by default, and where all iPlanet Web Administration Server's entries are placed in your directory tree. A "DN" is the string representation for the name of an entry in a directory server.
- Note that at a minimum, you must specify the following user information when creating a new user entry:
  - surname or last name
  - full name
  - user ID
- If any organizational units have been defined for your directory, you can specify where you want the new user to be placed using the Add New User To list. The default location is your directory's base DN (or root point).

NOTE The user edit text fields for international information differs between the Administration Server and Netscape Console. In Netscape Console, in addition to the untagged `cn` fields, there is a preferred language `cn` field which doesn't exist in the Administration Server.

How to Create a New User Entry

To create a user entry, read the guidelines outlined in "Guidelines for Creating User Entries," on page 64,.and then perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.

2. Click the **New User** link and add the associated information to the displayed page.

For more information, see "The New User Page," in the online help. For information on editing users, see "Managing Users," on page 67.

Directory Server User Entries

The following user entry notes may be of interest to the directory administrator:

- User entries use the `inetOrgPerson`, `organizationalPerson`, and `person` object classes.
- By default, the distinguished name for users is of the form:

  ```
  cn=full name, ou=organization, ...,o=base organization, c=country
  ```

  For example, if a user entry for Billie Holiday is created within the organizational unit Marketing, and the directory's base DN is o=Ace Industry, c=US, then the person's DN is:

  ```
  cn=Billie Holiday, ou=Marketing, o=Ace Industry, c=US
  ```

  However, note that you can change this format to a uid-based distinguished name.
- The values on the user form fields are stored as the following LDAP attributes (note that any stored information other than 'user' and 'group' requires a full Directory Server license):

Table 4-1 LDAP Attributes

User Field	Corresponding LDAP Attribute
Given Name	`givenName`
Surname	`sn`
Full Name	`cn`
User ID	`uid`
Password	`userPassword`
Email Address	`mail`

The following fields are also available when editing the user entry:

Table 4-2 User Entry LDAP Attributes

User Field	Corresponding LDAP Attribute
Title	`title`
Telephone	`telephoneNumber`

- Sometimes a user's name can be more accurately represented in characters of a language other than the default language. You can select a preferred language for users so that their names will display in the characters of the that language, even when the default language is English. For more information regarding setting a user's preferred language, see "The Manage Users Page," in the online help.

Managing Users

You edit user attributes from the Administration Server Manage Users form. From this form you can find, change, rename, and delete user entries; manage user licenses; and potentially change product-specific information.

Some, but not all, Netscape/iPlanet servers add additional forms to this area that allow you to manage product-specific information. For example, if a messaging server is installed under your Administration Server, then an additional form is added that allows you to edit messaging server-specific information. See the server documentation for details on these additional management capabilities.

This section includes the following topics:

- Finding User Information
- Editing User Information
- Managing a User's Password
- Managing User Licenses
- Renaming Users
- Removing Users

Finding User Information

Before you can edit a user entry, you must display the associated information. To find the specific user information, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Users** link.
3. In the **Find User** field, enter some descriptive value for the entry that you want to edit. You can enter any of the following in the search field:
   - A name. Enter a full name or a partial name. All entries that equally match the search string will be returned. If no such entries are found, all entries that contain the search string will be found. If no such entries are found, any entries that sounds like the search string are found.
   - A user ID.
   - A telephone number. If you enter only a partial number, any entries that have telephone numbers ending in the search number will be returned.
   - An email address. Any search string containing an at (@) symbol is assumed to be an email address. If an exact match cannot be found, then a search is performed to find all email addresses that begin with the search string.
   - An asterisk (*) to see all of the entries currently in your directory. You can achieve the same effect by simply leaving the field blank.
   - Any LDAP search filter. Any string that contains an equal sign (=) is considered a search filter.

   As an alternative, use the pull down menus in the Find all users whose field to narrow the results of your search.
4. In the **Look within** field, select the organizational unit under which you want to search for entries. The default is the directory's root point (or top most entry).
5. In the **Format** field, choose either On-Screen or Printer.
6. Click **Find**. All the users in the selected organizational unit are displayed.
7. In the resulting table, click the name of the entry that you want to edit.
8. The user edit form is displayed. Change the displayed fields as desired and click Save Changes. The changes are made immediately.

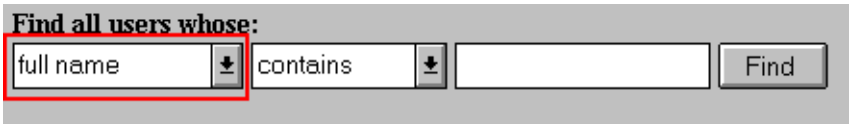
Building Custom Search Queries

The Find all users whose field allows you to build a custom search filter. Use this field to narrow down the search results returned by a “Find user” search.

The Find all users whose field provides the following search criteria:

- The left-most pull-down list allows you to specify the attribute on which the search will be based, as shown in the following illustration:

Figure 4-1 Search Attribute



  For a complete list of the available search attribute options, see “Search Attribute Options.”

- In the center pull-down list, select the type of search you want to perform, as shown in the following illustration:

Figure 4-2 Search Type

  For a complete list of the available search type options, see “Search Type Options.”

- In the right-most text field, enter your search string:

Figure 4-3 Search String

To display all of the users entries contained in the Look Within directory, enter either an asterisk (*) or simply leave this text field blank.

Search Attribute Options

The available search attribute options are described in the following table:

Table 4-3 Search Attribute Options

Option Name	Description
full name	Search each entry's full name for a match.
last name	Search each entry's last name, or surname for a match.
user id	Search each entry's user id for a match.
phone number	Search each entry's phone number for a match.
email address	Search each entry's email address for a match.
unit name	Search each entry's name for a match.
description	Search each organizational unit entry's description for a match.

Search Type Options

The available search type options are described in the following table:

Table 4-4 Search Type Options

Option Name	Description
`contains`	Causes a substring search to be performed. Entries with attribute values containing the specified search string are returned. For example, if you know an user's name probably contains the word "Dylan," use this option with the search string "Dylan" to find the user's entry.

Table 4-4 Search Type Options

Option Name	Description
`is`	Causes an exact match to be found. That is, this option specifies an equality search. Use this option when you know the exact value of an user's attribute. For example, if you know the exact spelling of the user's name, use this option.
`isn't`	Returns all the entries whose attribute value does not exactly match the search string. That is, if you want to find all the users in the directory whose name is not "John Smith," use this option. Be aware, however, that use of this option can cause an extremely large number of entries to be returned to you.
`sounds like`	Causes an approximate, or phonetic, search to be performed. Use this option if you know an attribute's value, but you are unsure of the spelling. For example, if you are not sure if a user's name is spelled "Sarret," "Sarette," or "Sarett," use this option.
`starts with`	Causes a substring search to be performed. Returns all the entries whose attribute value starts with the specified search string. For example, if you know a user's name starts with "Miles," but you do not know the rest of the name, use this option.
`ends with`	Causes a substring search to be performed. Returns all the entries whose attribute value ends with the specified search string. For example, if you know a user's name ends with "Dimaggio," but you do not know the rest of the name, use this option.

Editing User Information

To change a user's entry, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Display the user entry as described in "Finding User Information," on page 68.
3. Edit the field corresponding to the attribute that you wish to change.

For more information, see "The Edit Users Page," in the online help.

NOTE It is possible that you will want to change an attribute value that is not displayed by the edit user form. In this situation, use the Directory Server `ldapmodify` command line utility, if available.

In addition, note that you can change the user's first, last, and full name field from this form, but to fully rename the entry (including the entry's distinguished name), you need to use the Rename User form. For more information on how to rename an entry, see "Renaming Users," on page 73.

Managing a User's Password

The password you set for user entries is used by the various servers for user authentication.

To change or create a user's password, perform the following steps:

1. Access the Administration Server and choose **Users & Groups** tab.
2. Display the user entry as described in "Finding User Information," on page 68.
3. Make the desired changes and click OK.

For more information, see "The Manage Users Page," in the online help.

NOTE You can change the Administration Server user from root to another user on the operating system to enable multiple users (belonging to the group) to edit/manage the configuration files. However, note that while on Unix/Linux platforms, the installer can give "rw" permissions to a group for the configuration files, on Windows NT platforms, the user must belong to the "Administrators" group.

You can also disable the user's password by clicking the Disable Password button. Doing this prevents the user from logging into a server without deleting the user's directory entry. You can allow access for the user again by using the Password Management Form to enter a new password.

Managing User Licenses

Administration Server enables you to track which iPlanet server products your users are licensed to use.

To manage the licenses available to the user, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.

2. Display the user entry as described in “Finding User Information,” on page 68.
3. Click the **Licenses** link at the top of the User Edit form.
4. Make the desired changes and click OK.

For more information, see “The Manage Users Page,” in the online help.

Renaming Users

The rename feature changes only the user’s name; all other fields are left intact. In addition, the user’s old name is still preserved so searches against the old name will still find the new entry.

When you rename a user entry, you can only change the user’s name; you cannot use the rename feature to move the entry from one organizational unit to another. For example, suppose you have organizational units for Marketing and Accounting and an entry named “Billie Holiday” under the Marketing organizational unit. You can rename the entry from `Billie Holiday` to `Doc Holiday`, but you cannot rename the entry such that `Billie Holiday` under the Marketing organizational unit becomes `Billie Holiday` under the Accounting organizational unit.

To rename a user entry, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Display the user entry as described in “Finding User Information,” on page 68.

   Note that if you are using common name-based DNs, specify the user’s full name. If you are using uid-based distinguished names, enter the new uid value that you want to use for the entry.
3. Click the **Rename User** button.
4. Change the Given Name, Surname, Full Name, or UID fields as is appropriate to match the new distinguished name for the entry.
5. You can specify that the Administration Server no longer retains the old full name or uid values when you rename the entry by setting the `keepOldValueWhenRenaming` parameter to false. You can find this parameter in the following file:

   `server_root``/admin-serv/config/dsgw-orgperson.conf`

For more information, see “The Manage Users Page,” in the online help.

Removing Users

To delete a user entry, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Display the user entry as described in “Finding User Information,” on page 68.
3. Click **Delete User**.

For more information, see “The Manage Users Page,” in the online help.

Creating Groups

A group is an object that describes a set of objects in an LDAP database. An iPlanet Web Server group consists of users who share a common attribute. **Static groups** enumerate their member objects explicitly. A static group is a CN and contains `uniqueMembers` and/or `memberURLs` and/or `memberCertDescriptions`. For static groups, the members do not share a common attribute except for the `CN=<Groupname>` attribute.

For static groups, members can share a common attribute from a certificate if you use the `memberCertDescription`. Note that these will only work if the ACL uses the SSL method.

Once you create a new group, you can add users, or members, to it.

This section includes the following topics for creating groups:

- Static Groups

Static Groups

The Administration Server enables you to create a static group by specifying the same group attribute in the DNs of any number of users. A static group doesn’t change unless you add a user to it or delete a user from it.

Guidelines for Creating Static Groups

Consider the following guidelines when using the Administration Server forms to create new static groups:

- Static groups can contain other static groups.
- You can optionally also add a description for the new group.

- If any organizational units have been defined for your directory, you can specify where you want the new group to be placed using the Add New Group To list. The default location is your directory’s root point, or top-most entry.
- When you are finished entering the desired information, click Create Group to add the group and immediately return to the New Group form. Alternatively, click Create and Edit Group to add the group and then proceed to the Edit Group form for the group you have just added. For information on editing groups, see “Editing Group Attributes,” on page 77.

To Create a Static Group

To create a static group entry, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **New Group** link.
3. Enter the required information and click OK.

For more information, see “The New Group Page,” in the online help.

Managing Groups

The Administration Server enables you to edit groups and manage group memberships from the Manage Group form. This section describes the following topics:

- Finding Group Entries
- Editing Group Attributes
- Adding Group Members
- Adding Groups to the Group Members List
- Removing Entries from the Group Members List
- Managing Owners
- Managing See Alsos
- Removing Groups
- Renaming Groups

Finding Group Entries

Before you can edit a group entry, you must display the entry.

To find a group entry, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Groups** link.
3. Enter the name of the group that you want to find in the **Find Group** field. You can enter any of the following values in the search field:
   - A name. Enter a full name or a partial name. All entries that equally match the search string are returned. If no such entries are found, all entries that contain the search string will be found. If no such entries are found, any entries that sounds like the search string are found.
   - An asterisk (*) to see all of the groups currently residing in your directory. You can achieve the same effect by simply leaving the field blank.
   - Any LDAP search filter. Any string that contains an equal sign (=) is considered to be a search filter.

   As an alternative, use the pull down menus in **Find all groups whose** to narrow the results of your search.
4. In the **Look within** field, select the organizational unit under which you want to search for entries. The default is the directory’s root point, or top-most entry.
5. In the **Format** field, choose either On-Screen or Printer.
6. Click **Find**. All the groups matching your search criteria are displayed.
7. In the resulting table, click the name of the entry that you want to edit.

The “Find all groups whose” Field

The Find all groups whose field allows you to build a custom search filter. Use this field to narrow down the search results that are otherwise returned by Find groups. For more information regarding how to build a custom search filter, see “Building Custom Search Queries,” on page 69.

To display all of the group entries contained in the **Look Within** directory, enter either an asterisk (*) or simply leave this text field blank.

Editing Group Attributes

To edit a group entry, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Groups** link.
3. Locate the group you want to edit, and type the desired changes.

   For more information regarding how to find specific entries, refer to the concepts outlined in “Finding Group Entries,” on page 76.

NOTE You can change the Administration Server user from root to another user on the operating system to enable multiple users (belonging to the group) to edit/manage the configuration files. However, note that while on Unix/Linux platforms, the installer can give “rw” permissions to a group for the configuration files, on Windows NT platforms, the user must belong to the “Administrators” group.

For more information about editing group attributes, see “The Manage Groups Page,” in the online help.

NOTE It is possible that you will want to change an attribute value that is not displayed by the group edit form. In this situation, use the Directory Server `ldapmodify` command line utility, if available.

Adding Group Members

To add members to a group, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Groups** link.
3. Locate the group you want to manage as described in “Finding Group Entries,” on page 76, and click the **Edit** button under Group Members.

   iPlanet Web Server displays a new form that enables you to search for entries. If you want to add user entries to the list, make sure Users is shown in the **Find** pull-down menu. If you want to add group entries to the group, make sure Group is shown.

4. In the right-most text field, enter a search string. Enter any of the following options:
   - A name. Enter a full name or a partial name. All entries whose name matches the search string is returned. If no such entries are found, all entries that contain the search string are found. If no such entries are found, any entries that sounds like the search string are found.
   - A user ID if you are searching for user entries.
   - A telephone number. If you enter only a partial number, any entries that have telephone numbers ending in the search number are returned.
   - An email address. any search string containing an at (@) symbol is assumed to be an email address. If an exact match cannot be found, then a search is performed to find all email addresses that begin with the search string.
   - Enter either an asterisk (*) or simply leave this text field blank to see all of the entries or groups currently residing in your directory.
   - Any LDAP search filter. Any string that contains an equal sign (=) is considered to be a search filter.
5. Click **Find and Add** to find all the matching entries and add them to the group.

   If the search returns any entries that you do not want add to the group, click the box in the Remove from list? column. You can also construct a search filter to match the entries you want removed and then click **Find and Remove**.
6. When the list of group members is complete, click **Save Changes**. The currently displayed entries are now members of the group.

For more information about adding groups members, see “The Edit Members Page,” in the online help.

Adding Groups to the Group Members List

You can add groups (instead of individual members) to the group’s members list. Doing so causes any users belonging to the included group to become a member of the receiving group. For example, if Neil Armstrong is a member of the Engineering Managers group, and you make the Engineering Managers group a member of the Engineering Personnel group, then Neil Armstrong is also a member of the Engineering Personnel group.

To add a group to the members list of another group, add the group as if it were a user entry. For more information, see “Adding Group Members,” on page 77.

Removing Entries from the Group Members List

To delete an entry from the group members list, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Groups** link, locate the group you want to manage as described in “Finding Group Entries,” on page 76, and click the **Edit** button under Group Members.
3. For each member that you want to remove from the list, click the corresponding box under the Remove from list? column.

   Alternatively, you can construct a filter to find the entries you want to remove and click the **Find and Remove** button. For more information on creating a search filter, see “Adding Group Members,” on page 77.
4. Click **Save Changes**. The entry(s) are deleted from the group members list.

Managing Owners

You manage a group’s owners list the same way as you manage the group members list. The following table identifies which section to read for more information:

Table 4-5 Additional Information

Task You Want to Complete	Read Section
Add owners to the group	“Adding Group Members,” on page 77.
Add groups to the owners list	“Adding Groups to the Group Members List,” on page 78.
Remove entries from the owners list	“Removing Entries from the Group Members List,” on page 79.

Managing See Alsos

“See alsos” are references to other directory entries that may be relevant to the current group. They allow users to easily find entries for people and other groups that are related to the current group.

You manage see alsos the same way as you manage the group members list. The following table shows you which section to read for more information:

Table 4-6 Additional Information

Task You Want to Complete	Read Section
Add users to see alsos	“Adding Group Members,” on page 77.
Add groups to see alsos	“Adding Groups to the Group Members List,” on page 78.
Remove entries from see alsos	“Removing Entries from the Group Members List,” on page 79.

Removing Groups

To delete a group, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Groups** link, locate the group you want to manage as described in “Finding Group Entries,” on page 76, and click **Delete Group**.

NOTE The Administration Server does not remove the individual members of the group(s) you remove; only the group entry is removed.

Renaming Groups

To rename a group, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Groups** link and locate the group you want to manage as described in “Finding Group Entries,” on page 76.
3. Click the **Rename Group** button and type the new group name in the resulting dialog box.

When you rename a group entry, you only change the group’s name; you cannot use the Rename Group feature to move the entry from one organizational unit to another. For example, a business might have the following organizations:

- organizational units for Marketing and Product Management
- a group named Online Sales under the Marketing organizational unit

In this example, you can rename the group from Online Sales to Internet Investments, but you cannot rename the entry such that Online Sales under the Marketing organizational unit becomes Online Sales under the Product Management organizational unit.

Creating Organizational Units

An organizational unit can include a number of groups, and it usually represents a division, department, or other discrete business group. A DN can exist in more than one organizational unit.

To create an organizational unit, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **New Organizational Unit** link and enter the required information.

For more information, see "The New Organizational Unit Page," in the online help.

The following notes may be of interest to the directory administrator:

- New organizational units are created using the `organizationalUnit` object class.
- The distinguished name for new organizational units is of the form:

  ```
  ou=new organization, ou=parent organization, ...,o=base
  organization, c=country
  ```

For example, if you create a new organization called Accounting within the organizational unit West Coast, and your Base DN is o=Ace Industry, c=US, then the new organization unit's DN is:

```
ou=Accounting, ou=West Coast, o=Ace Industry, c=US
```

Managing Organizational Units

You edit and manage organizational units from the Organizational Unit Edit form. This section describes the following tasks:

- Finding Organizational Units

- Editing Organizational Unit Attributes
- Renaming Organizational Units
- Deleting Organizational Units

Finding Organizational Units

To find organizational units, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Organizational Units** link.
3. Type the name of the unit you want to find in the Find organizational unit field. You can enter any of the following in the search field:
    - A name. Enter a full name or a partial name. All entries that equally match the search string will be returned. If no such entries are found, all entries that contain the search string will be found. If no such entries are found, any entries that sounds like the search string are found.
    - An asterisk (*) to see all of the groups currently residing in your directory. You can achieve this same result by simply leaving the field blank.
    - Any LDAP search filter. Any string that contains an equal sign (=) is considered to be a search filter.

    As an alternative, use the pull down menus in the Find all units whose field to narrow the results of your search.
4. In the **Look within** field, select the organizational unit under which you want to search for entries. The default is the root point of the directory.
5. In the **Format** field, choose either On-Screen or Printer.
6. Click **Find**. All the organizational units matching your search criteria are displayed.
7. In the resulting table, click the name of the organizational unit that you want to find.

The “Find all units whose” Field

The Find all units whose field allows you to build a custom search filter. Use this field to narrow down the search results that are otherwise returned by Find organizational unit. For more information regarding how to build a custom search filter, see “Building Custom Search Queries,” on page 69.

To display all of the group entries contained in the Look Within directory, enter either an asterisk (*) or simply leave this text field blank.

Editing Organizational Unit Attributes

To change a organizational unit entry, access the Administration Server and perform the following steps:

1. Locate the organizational unit you want to edit as described in “Finding Organizational Units,” on page 82.
2. The organizational unit edit form is displayed. Change the displayed fields as desired and click **Save Changes**. The changes are made immediately.

Note
It is possible that you will want to change an attribute value that is not displayed by the organizational unit edit form. In this situation, use the Directory Server `ldapmodify` command line utility, if available.

Renaming Organizational Units

To rename an organizational unit entry, access the Administration Server and perform the following steps:

1. Make sure no other entries exist in the directory under the organizational unit that you want to rename.
2. Locate the organizational unit you want to edit as described in “Finding Organizational Units,” on page 82.
3. Click the **Rename** button.
4. Enter the new organizational unit name in the resulting dialog box.

NOTE	When you rename an organizational unit entry, you can only change the organizational unit’s name; you cannot use the rename feature to move the entry from one organizational unit to another. For more information, see “Renaming Organizational Units,” on page 83.

Deleting Organizational Units

To delete an organizational unit entry, access the Administration Server and perform the following steps:

1. Make sure no other entries exist in the directory under the organizational unit that you want to rename.
2. Locate the organizational unit you want to delete as described in “Finding Organizational Units,” on page 82.
3. Click the **Delete** button.
4. Click OK in the resulting confirmation box. The organizational unit is immediately deleted.

Managing a Preferred Language List

iPlanet Web Server enables you to display and maintain the list of preferred languages.

To manage the preferred language list, perform the following steps:

1. Access the Administration Server and choose the **Users & Groups** tab.
2. Click the **Manage Preferred Language List** link.
3. In the Display Language Selection List field, click Yes or No to specify whether iPlanet Web Server displays the Language Selection List.
4. In the **Languages in the Selection List** field, click the **Add to List** checkbox to add each language you want specified as part of the Preferred Language List.
5. Click the default value for the language you want to specify as the default language in the Preferred Language List.
6. Click **Save Changes**.

Chapter 5

Working with Server Security

This chapter describes how to activate the Secure Sockets Layer (SSL) protocol and other features designed to safeguard your data, deny intruders access, and designate who has access to the server. iPlanet Web Server incorporates the security architecture of all Netscape/iPlanet servers: it's built on industry standards and public protocols for maximum interoperability and consistency.

Before reading this chapter you should be familiar with the basic concepts of public-key cryptography. These concepts include encryption and decryption; public and private keys; digital certificates; and the SSL protocol. For more information, see *Managing Servers with Netscape Console.*

This chapter includes the following sections:

- About iPlanet Web Server Security
- Creating a New Server Instance
- Creating a Certificate Trust Database
- Requesting a Certificate
- Installing and Managing Certificates and Certificate Lists
- Using Secure Sockets Layer (SSL)
- Using Client Certificates
- Changing the Trust Database/Key Pair File Password
- Migrating Enterprise Server 3.x Certificates
- Additional Server Security Considerations

About iPlanet Web Server Security

iPlanet Web Server security is based on a number of interrelated and inter-dependent components, all of which work together to ensure that only authorized individuals can gain access to the server, that passwords or identities are not compromised, and that user identities can be trusted.

This section provides an overview for the following iPlanet Web Server security components:

- Encryption
- Certificates
- Configuring iPlanet Web Server for SSL

Encryption

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a **cipher**, is a mathematical function used for encryption or decryption. iPlanet Web Server 4.1 includes support for various ciphers.types of ciphers.

The encryption process alone isn't enough to secure your server's confidential information. Once the information has been encrypted, and possibly transmitted to another server, a number called a **key** must be used with the encrypting cipher to produce the actual encrypted result, or to decrypt previously encrypted information. The encryption process uses two keys to achieve this result: a public key and a private key. The public key is published as part of a certificate; only the associated private key is safeguarded. (For more information about keys and certificates, see *Managing Servers with Netscape Console*.) Consequently, information encrypted with a public key can be decrypted only with the associated private key.

SSL Protocol

All Netscape / iPlanet 4.x servers support the **SSL protocol** for encrypted communication and PKCS#11 APIs for communication with software or hardware modules that perform cryptographic operations. You need to configure the Administration Server for SSL if you want to enable encryption and other cryptographic operations.

The SSL protocol supports the use of a variety of ciphers, for use in operations such as authenticating the server and client to each other, transmitting certificates, and establishing session keys. Clients and servers may support different cipher suites, or sets of ciphers, depending on factors such as the version of SSL they support, company policies regarding acceptable encryption strength, and government restrictions on export of SSL-enabled software. Among its other functions, the SSL handshake protocol determines how the server and client negotiate which cipher suites they will use to authenticate each other, to transmit certificates, and to establish session keys.

For more information regarding how to enable SSL for iPlanet Web Server, see "Configuring Secure Sockets Layer (SSL)," on page 56 in Chapter 3, "Setting Administration Preferences."

FORTEZZA Encryption

FORTEZZA is an encryption system used by U.S. government agencies to manage sensitive but unclassified information. Use the Administration Server to configure your server to work with FORTEZZA. For information on installing the FORTEZZA hardware, see the documentation that came with your card reader.

FORTEZZA encryption support allows the web server to perform the following encryption tasks:

- use FORTEZZA ciphers for SSL connections
- use FORTEZZA card readers to store certificates and keys
- import and use FORTEZZA Compromised Key Lists (CKLs) and Certificate Revocation Lists (CRLs)
- serve files pre-encrypted with FORTEZZA ciphers

NOTE iPlanet Web Server, FastTrack Edition 4.1 includes FORTEZZA support for Windows NT, Solaris, and HPUX platforms.

The FORTEZZA cipher standard is a hardware smartcard standard for secure storage of private keys. The FORTEZZA operations are supported through an external PKCS#11 library. The library is added to the web server security modules database. The library handles all interfaces with external hardware (card readers) and all encryption functions. To iPlanet Web Server, FastTrack Edition, FORTEZZA support looks almost identical to any other PKCS#11 library.

Once added the security modules database (`secmod.db`), the server treats the FORTEZZA modules as any other PKCS#11 module. The FORTEZZA module is flagged as the default provider of SSL services for FORTEZZA ciphers. Then, any FORTEZZA request handled by the server is handed off to the library (via calls to NSS libraries; nothing in the actual web server code actually invokes functions in the FORTEZZA library).

The run time layer, then, is just the server and the library (no different from any PKCS#11 module).

The pre-encrypted file support runs as a web server plugin. A request for a file with a given extension (`.enc`) is routed to the plugin which invokes a function in the NSS library to send the encrypted file as a stream back to the client (no actual calls to the FORTEZZA library need to be made). The client then decrypts the data on the other side (presuming the client has a certificate with the public key corresponding to the private key that encrypted the file).

The whole configuration is managed through the Administration Server (or corresponding entries in the `magnus.conf` or `obj.conf` configuration files). The user interface enables users to select which certificate to use at run time, to collect multiple passwords (so that the server can log in to the FORTEZZA card as well as the default key database), and to allow the user to add Compromised Key Lists (CKLs) / Certificate Revocation Lists (CRLs).

When a CKL is added or updated, the certificate database is updated to make compromised keys known to the server. The NSS library validates FORTEZZA client requests against the compromised keys for each request to make sure that the client key is not a key known to be compromised.

The FORTEZZA module interoperates with the following standards and modules:

- FORTEZZA encryption standards. The FORTEZZA module allows the web server to use FORTEZZA encryption, authentication, and key validation.
- Secure Sockets Layer (SSL). FORTEZZA connections use SSL, version 3.
- The NSS libraries. Currently using NSS 2.72. The web server calls NSS functions which in turn, call the FORTEZZA library.
- The PKCS#11 web server infrastructure. FORTEZZA modules are added and configured using existing methods for managing PKCS#11 modules.
- NSAPI. The FORTEZZA module uses an NSAPI plugin to handle pre-encrypted files.
- `Modutil`: a utility for updating `secmod.db`, for adding and deleting PKCS#11 modules.

For more information regarding FORTEZZA encryption, see *Managing Servers with Netscape Console.*

FIPS-140 Compliance

You can configure iPlanet Web Server to be Federal Information Processing Standards (FIPS)-140 compliant. To make your server FIPS-140 compliant, you need to turn on the following two ciphers in your encryption preferences:

- (FIPS) DES with 56 bit encryption and SHA-1 message authentication
- (FIPS) Triple DES with 168 bit encryption and SHA-1 message authentication

You can set encryption preferences in the Administration Server by clicking the Preferences tab and the Encryption Preferences link. You can also set the encryption preferences for an instance of the iPlanet Web Server in the Server Manager by clicking the Preferences tab and the Encryption Preferences link. For more information, see "The Encryption Preferences Page," in the online help.

Certificates

Over the Internet and many extranets and intranets, identification can take place with the aid of a ***certificate***. A certificate consists of digital data that specifies the name of an individual, company, or other entity and certifies that a public key, which is also included in the certificate, belongs to that entity.

A certificate is issued and digitally signed by a ***Certificate Authority***, or ***CA***. A CA can be a company that sells certificates over the Internet, or it can be a department responsible for issuing certificates for your company's intranet or extranet. You decide which CAs you trust enough to serve as verifiers of other people's identities.

In addition to a public key and the name of the entity identified by the certificate, a certificate also includes additional information, such as an expiration date, the name of the CA that issued the certificate, and the "digital signature" of the issuing CA. For more information regarding the content and format of a certificate, see *Managing Servers with Netscape Console.*

Client and Server Authentication

Authentication is the process of confirming an identity. In the context of network interactions, authentication involves the confident identification of one party by another party. Certificates are one way of supporting authentication. **Client authentication** refers to the confident identification of a client by a server (that is,

identification of the person assumed to be using the client software). **Server authentication** refers to the confident identification of a server by a client (that is, identification of the organization assumed to be responsible for the server at a particular network address).

Both clients and servers can have certificates. Also, clients can have multiple certificates, much like a person might have several different pieces of identification. For example, if you participate in newsgroup discussions with a Netscape Collabra Server called news.mozilla.com, you might find it possesses a certificate issued from a company named CertSafe, assuring you that this site is the one true news.mozilla.com. If you trust CertSafe's judgment, then you can trust that news.mozilla.com is the site it claims to be.

Conversely, you might be in charge of a company's internal Human Resources server. You could use your server's access-control features in conjunction with client authentication to allow *only* Human Resources employees access to certain directories. For more information on access control, see "What Is Access Control?," in Chapter 12, "Controlling Access to Your Server."

How iPlanet Web Server Uses Certificates to Authenticate Users

Netscape/iPlanet servers support using client certificates to authenticate a user. There are two basic ways the server can use a client certificate:

- The server matches the CA in the client certificate with a trusted CA listed in the Administration Server. This simply ensures that the client has a valid certificate from a CA the server trusts. (If the client is Netscape Navigator or Netscape Communicator and the certificate is expired, the client warns the user before sending the out-of-date certificate. Most Netscape/iPlanet servers will log an error, reject the certificate, and return a message to the client.)
- The server additionally gathers information from the client certificate and matches it with a user entry in an LDAP directory. This ensures that the client has a valid certificate and an entry in the LDAP directory. It can also ensure that the client certificate matches the one in the LDAP directory.

NOTE A Netscape/iPlanet server must have SSL turned on to use client certificates, and the Administration Server must trust the CA that issued the certificate to the client. For information on trusting CAs, see "Managing Certificates," on page 98.

You can configure the web server so that it refuses any client that doesn't have a client certificate from a trusted CA. This differs from access control in that all requests must be through SSL connections and they must be from clients who have certificates from trusted CAs. For details on configuring trusted CAs, see *Managing Servers with Netscape Console.*

Configuring iPlanet Web Server for SSL

This section explains how to get client certificate authentication working with iPlanet Web Server. When you have finished following the procedures outlined in this chapter, you will have a web server that requires a user to present a valid client SSL certificate in order to access restricted areas on the server. The certificate that the user presents must match the certificate that was published to the LDAP directory when it was issued.

This chapter focuses on setting up, installing, and managing the security components necessary to secure your iPlanet Web Server. To activate the SSL protocol for your iPlanet Web Server, you need to perform the various procedures described in the following sections:

- Creating a New Server Instance
- Creating a Certificate Trust Database
- Requesting a Certificate
- Installing and Managing Certificates and Certificate Lists
- Using Secure Sockets Layer (SSL)

Creating a New Server Instance

To use SSL with iPlanet Web Server, you must either have an existing instance of iPlanet Web Server 4.x that you want to be an SSL server or create a new instance to be an SSL server. If you have an existing instance of iPlanet Web Server that you want to simply convert to be an SSL server, you can skip this section. Otherwise, follow the steps described in this section to create a new instance of iPlanet Web Server, and then perform the remaining procedures outlined in this chapter to configure the new instance for SSL and client authentication.

To add another server instance, perform the following steps:

1. Access the Administration Server and choose the **Servers** tab.

2. Click the **Add Server** link.
3. Enter the desired information for the specified fields.
4. Click the radio button that corresponds to how you want the server to resolve IP addresses.
5. Click OK.

For more information, see "The Add Server Page," in the online help.

Creating a Certificate Trust Database

A certificate database is a key-pair and certificate database installed on the local host. When you use an internal token, the certificate database is the database into which you install the key and certificate. In iPlanet Web Server 4.x, each server instance (including the Administration Server) has its own certificate/key pair which is referred to as a **trust database**.

A **key-pair** file contains both the public and private keys used for SSL encryption. You use the key-pair file when you request and install a certificate. The key-pair file is stored encrypted in the following directory:

server_root/alias/<serverid-hostname>-key3.db.

When you create the key, you specify a password that you later use when you request the certificate and when you start a server that is using encrypted communications.

To create the certificate trust database, perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Type the password in Database Password.
3. Re-type the password in Password (again).
4. Click OK.

If no database exists, iPlanet Web Server creates the proper key and certificate database files and stores them in the `alias/` directory (otherwise, iPlanet Web Server displays an error message).

For more information, see "The Create a Trust Database Page," in the online help.

Requesting a Certificate

After you generate a trust database, you must create a PKCS #10 certificate request and submit it to a Certificate Authority to obtain your server SSL certificate. To enable SSL for a particular server instance, you must obtain a server SSL certificate for the server, then configure the server to require client authentication and optionally to check users' client certificates against certificate information that a CA has published to the LDAP directory.

If your company has its own internal CA for issuing certificates, you should request your certificate from them. If you plan to purchase your certificate from a commercial CA, choose a CA and ask for the specific format of the information they require. (For more information on what some CAs require, see "Required CA Information.")

NOTE Not everyone who requests a certificate from a commercial CA is given one. Many CAs require you to prove your identity before issuing you a certificate. Also, it can take anywhere from a day to two months or more to approve a certificate. You are responsible for promptly providing all the necessary information to the CA.

To request a certificate, make sure you know what information your CA requires, and then perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Click the **Request Certificate** link.
3. In the form that iPlanet Web Server displays, specify if this is a new certificate or a certificate renewal. Many certificates expire after a set period of time, such as six months or a year. Some CAs will automatically send you a renewal.
4. Perform the following steps to specify how you want to submit the request for the certificate:
    a. If the CA expects to receive the request in an email message, check CA Email and enter the email address of the CA. For a list of CAs, click List of available certificate authorities.
    b. If you are requesting the certificate from an internal CA that is using Netscape Certificate Server, click **CA URL** and enter the URL for the Certificate Server. This URL should point to the certificate server's program that handles certificate requests. A sample URL might be: `https://CA.mozilla.com:444/cms`.

5. From the drop-down list, select the cryptographic module for the key-pair file you want to use when requesting the certificate.

   For information about installing additional cryptographic modules, see "Adding a PKCS#11Module," on page 103, or see "The Install a New PKCS#11 Module Page," in the online help.

6. Type the password for your key-pair file. This is the same password you specified when you created the trust database in "Creating a Certificate Trust Database." The server uses the password to get your private key and encrypt a message to the CA. The server then sends both your *public key* and the encrypted message to the CA. The CA uses the public key to decrypt your message.

7. Type your identification information. The format of this information varies by CA. For a general description of these fields, see "Required CA Information." Note that most of this information usually isn't required for a certificate renewal.

8. Double-check your work to ensure accuracy. The more accurate the information, the faster your certificate is likely to be approved.

9. Click OK once you've checked that the information is correct. If your request is going to a certificate server, you'll be prompted to verify the form information before the request is submitted. You should re-read the information and then click OK to submit the request to the certificate server.

For more information, see "The Request a Server Certificate Page," in the online help.

The server generates a certificate request that contains your information. The request has a digital signature created with your private key. The CA uses a digital signature to verify that the request wasn't tampered with during routing from your server machine to the CA. In the rare event that the request is tampered with, the CA will usually contact you by phone.

If you chose to email the request, the server composes an email message containing the request and sends the message to the CA. Typically, the certificate is sent to you via email. If instead you specified a URL to a certificate server, your server uses the URL to submit the request to the Certificate Server. You might get a response via email or other means depending on the CA.

If the CA agrees to issue you a certificate, the CA will notify you. (In most cases, the CA will send your certificate via email. If your organization is using a certificate server, you may be able to search for the certificate by using the certificate server's forms.)

Once you receive the certificate, you can install it. In the meantime, you can still use your server without SSL.

Required CA Information

Whether you are requesting a server certificate from a commercial CA or an internal CA, you need to provide the following information:

- **Common Name** must be the fully qualified hostname used in DNS lookups (for example, *www.iplanet.com*). This is the hostname in the URL that a browser uses to connect to your site. It's important that these two names are the same, otherwise a client is notified that the certificate name doesn't match the site name, which will make people doubt the authenticity of your certificate. However, some CAs might require different information, so it's important to contact them. Note that you can not use wildcards in a common name.
- **Email Address** is your business email address. This is used for correspondence between you and the CA.
- **Organization** is the official, legal name of your company, educational institution, partnership, and so on. Most CAs require that you verify this information with legal documents (such as a copy of a business license).
- **Organizational Unit** is an optional field that describes an organization within your company. This can also be used to note a less formal company name (without the *Inc.*, *Corp.*, and so on).
- **Locality** is an optional field that usually describes the city, principality, or country for the organization.
- **State or Province** is usually required, but can be optional for some CAs. Note that most CAs won't accept abbreviations, but check with them to be sure.
- **Country** is a required, two-character abbreviation of your country name (in ISO format). The country code for the United States is US.

All this information is combined as a series of attribute-value pairs called the distinguished name (DN), which uniquely identifies the subject of the certificate.

If you are purchasing your certificate from a commercial CA, you must contact the CA to find out what additional information they require before they issue a certificate. Most CAs require that you prove your identity. For example, they want to verify your company name and who is authorized by the company to administer the server, and they might ask whether you have the legal right to use the information you provide.

Some commercial CAs offer certificates that indicate a greater level of detail and veracity to vendors or individuals who provide greater proof of their identity. For example, you might be able to purchase a certificate stating that the CA has not only verified that you are the rightful administrator of the www.mozilla.com computer, but that you really are a company that has been in business for ten years and have no outstanding customer litigation against you. Generally, these certificates cost more than standard ones.

Installing and Managing Certificates and Certificate Lists

This section includes the following topics:

- Installing Certificates
- Managing Certificates
- Managing Certificate Lists

Installing Certificates

There are three types of certificates that you can install:

- Your own server's certificate to present to clients.
- A CA's own certificate for use in a certificate chain.

Each of these certificates is installed through the process described here.

When you receive a certificate from the CA, it will be encrypted with your public key so that only you can decrypt it. The server will use the key-pair file password you specify to decrypt the certificate when you install it. You can either save the email somewhere accessible to the server, or copy the text of the email and be ready to paste the text into the Install Certificate form, as described here.

A **certificate chain** is a hierarchical series of certificates signed by successive certificate authorities. A CA certificate identifies a certificate authority (CA) and is used to sign certificates issued by that authority. A CA certificate can in turn be signed by the CA certificate of a parent CA and so on up to a root CA.

NOTE CAs' certificates for use in a certificate chain are installed using the same process as installing your own certificate. If your CA doesn't automatically send you their certificate, you should request it. However, many CAs include their certificate in the same email that contains your certificate. In this case, your server installs both certificates at the same time when you install your certificate. For more information on certificate chaining, see "Appendix D Introduction to Public-Key Cryptography," in *Managing Servers with Netscape Console.*

To install a certificate and associate it with an alias, perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Click the **Install Certificate** link.
3. Check the type of certificate you are installing:
   - **This Server** is for a single certificate associated only with your server.
   - **Server Certificate Chain** is for a CA's certificate to include in a certificate chain.
   - **Trusted Certificate Authority (CA)** is for a certificate of a CA that you want to accept as a trusted CA for client authentication.
4. If the certificate is for a chain, name the certificate. iPlanet Web Server displays this name in the Manage Certificates list. The name should be descriptive and can include spaces. For example, "United States Postal Service CA" is the name of the CA, and "VeriSign Class 2 Primary CA" describes both the CA and the type of certificate. If the certificate is for "this server," the Administration Server uses the name Server-Cert.
5. Either type the full pathname to the saved email or paste the email text in the field called **Message text (with headers)**. If you copy and paste the text, be sure to include the headers "Begin Certificate" and "End Certificate"—including the beginning and ending hyphens. Make sure you check the corresponding radio button for either the file or the text.
6. Click **OK**.
7. Click **Add**.

   The certificate is stored in the server's certificate database. The filename will be `<alias>-cert.db`. For example:

`https-<serverid>-<hostname>-cert7.db`

For more information, see “The Install a Server Certificate Page,” in the online help.

If you have just installed your own certificate, you can now activate SSL for your server. To activate SSL, see “Activating SSL,” on page 101.

Managing Certificates

You can view, delete, or edit the trust settings of all the certificates installed on your server. This includes your own certificate and certificates from CAs.

To manage this list of certificates, perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Click the **Manage Certificates** link.

   iPlanet Web Server displays the Manage Server Certificates page.
3. Select a certificate file alias, and then click OK.

   All of the installed certificates associated with the alias appear with their type and expiration date. The link text is the name given to the certificate when it was installed. The Administration Server comes with several default certificates, which are listed above the certificates you installed. all certificates are stored in the directory *server_root*`/alias`.
4. To view more information about a certificate, click the link for the certificate. A window appears, containing information about that certificate. Figure 5-1 shows a sample.

Figure 5-1 Certificate information includes the owner and who issued it.

5. To trust the CA, click **Trust**. If the CA is already trusted, you can click **Do Not Trust**. By default, all CAs are not trusted.

   To delete the certificate, click the **Delete Certificate** button.

   To close the window, click the **Quit** button.

For more information, see "The Manage Server Certificates Page (Administration Server)," in the online help.

Note that trust settings refer specifically to whether a certificate is trusted as a signer of client certificates (the user does not, for example, have to trust a CA after the CA issues a server certificate).

Managing Certificate Lists

The purpose of certificate revocation lists (CRLs) and compromised key lists (CKLs) is to make known any certificates and keys that either client or server users should no longer trust. If data in a certificate changes (for example, a user changes offices or leaves the organization) before the certificate expires, the certificate is revoked and its data appears in a CRL. If a key is tampered with or otherwise compromised, the key and its data appear in a CKL. Both CRLs and CKLs are produced and periodically updated by a CA.

This section includes the following topics:

- Obtaining a CRL or CKL
- Adding a CRL or CKL to the Trust Database
- Managing CRLs

Obtaining a CRL or CKL

To obtain a CRL or CKL from a Certificate Authority (CA), perform the following steps:

1. Use a browser to go to the CA's web site. Contact your CA administrator for the exact URL to use.
2. Follow the CA's instructions for downloading the CRL or CKL to a local directory.

Once you've saved the CRL file or CKL file to a local directory, you can add information from it to the Trust Database.

Adding a CRL or CKL to the Trust Database

To add CRL or CKL to the trust database, perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Click the **Install CRL/CKLs** link.

   iPlanet Web Server displays the Install a Certificate Revocation List page.
3. Click the **File contains** radio button for either **Certificate Revocation List** or **Compromised Key List**.
4. In **The CRL/CKL is in this file** field, type the full path name to the associated file.
5. Click OK. If the list already exists in the database, the list you specify here will replace the existing list.

Managing CRLs

To manage CRLs, perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Click the **Manage CRLs** link.

   iPlanet Web Server displays the Manage Certificate Revocation Lists page. All installed CRLs are listed along with their expiration dates.

3. Click on the desired CRL for more information and options.
4. Click a CRL to select it.
5. To add the CRL to the trust database, click **Add**.

To delete CRL from the trust database, click **View**. In the Certificate window, click **Delete**.

Using Secure Sockets Layer (SSL)

After you have generated a key-pair file and installed your certificate, you can activate SSL for your Administration Server or any other iPlanet Web Server.

This section includes the following topics:

- Activating SSL
- Specifying Ciphers
- Setting Security (SSL) Preferences
- Adding a PKCS#11Module
- Using SSL Configuration File Directives

Activating SSL

To activate SSL for iPlanet Web Server, perform the steps described in “Activating SSL,” on page 56 in Chapter 3, “Setting Administration Preferences.”

URLs to an SSL-enabled iPlanet Web Administration Server are constructed using `https` instead of simply `http`. URLs that point to documents on an SSL-enabled server have this format:

```
https://<servername.[domain.[dom]]:[port#]>
```

For example, `https://admin.mozilla.com:443`. If you use the default secure http port number (443), you don’t have to use the port number in the URL.

Specifying Ciphers

A *cipher* is an algorithm used in encryption. Some ciphers are more secure, or *stronger*, than others. Generally speaking, the more bits a cipher uses during encryption, the harder it is to decrypt the data.

When initiating an SSL connection with a server, a client lets the server know what ciphers it prefers for encrypting information. In any two-way encryption process, both parties must use the same ciphers. Because a number of ciphers are available, your server needs to be able to use the most popular ones.

You can choose ciphers from the SSL 2 protocol, as well as from SSL 3. Improvements were made to the protocol after version 2 that improve security and performance; you should not use SSL 2 unless you have a real need to service clients that are not capable of using SSL 3. Client certificates are not guaranteed to work with SSL 2 ciphers. To specify which ciphers your server can use, check them in the list. Unless you have a compelling reason not to use a specific cipher, you should check them all.

Another reason for not enabling all ciphers is to prevent SSL connections with less than optimal encryption.

CAUTION You might not want to click the "No Encryption, only MD5 message authentication" checkbox. If no other ciphers are available on the client side, the server will use this, and no encryption will occur.

For more information regarding specific ciphers, see *Managing Servers with Netscape Console.*

Setting Security (SSL) Preferences

You can set preferences for using SSL encryption on any server. To set the SSL preferences for iPlanet Web Server, perform the steps described in "Setting Encryption Preferences," on page 56 in Chapter 3, "Setting Administration Preferences."

Adding a PKCS#11Module

iPlanet Web Server supports Public Key Cryptography Standard (PKCS) #11, which defines the interface used for communication between SSL and PKCS#11 modules. The PKCS#11 modules are used for standards-based connectivity to SSL hardware accelerators. You can import PKCS#11 modules in the form of `.jar` files or object files.

Guidelines for Installing a PKCS#11 Module

Even though you install an external PKCS#11 module, you still must create a Trust Database using the Internal (software) module. The PKCS#11 and SSL code relies on the default certificate and key databases.

If you do not create a Trust Database (using the Security tab "Create Database" link), one will be created for you when you request or install a certificate for an external PKCS#11 module. However, when a module is created for you, it has no password and cannot be accessed. This means that your external module will continue to work, but that you will not be able to create and install server certificates using the internal PKCS#11 module in the future.

For reference: If you allow a default database to be created without a password and later discover you want to use the internal PKCS#11 module, you can simply delete the existing database files:

`$SERVER_ROOT/alias/https-$SERVERID-$HOSTNAME-key3.db`

`$SERVER_ROOT/alias/https-$SERVERID-$HOSTNAME-cert7.db`

For example, for the server named *secure.example.com* installed in

`/usr/local/netscape`

the files would be:

`/usr/local/netscape/alias/https-secure.example.com-secure-key3.db`

`/usr/local/netscape/alias/https-secure.example.com-secure-cert7.db`

After deleting the existing databases, you can re-create them using the Security tab **Create Database** link.

If you install a certificate for your server into an external PKCS#11 module (for example, a hardware accelerator), the server will not be able to start using that certificate until you manually edit `magnus.conf`.

The server always tries to start with the certificate named “Server-Cert.” However, certificates in external PKCS#11 modules include one of the module’s token names in their identifier. For example, a sever certificate installed on an external smartcard reader called “smartcard0” would be named “smartcard0:Server-Cert.”

To tell the server to start with that server certificate instead, you must edit `magnus.conf` and add the following line anywhere in the file:

```
CERTDefaultNickname $TOKENNAME:Server-Cert
```

To find out what value to use for `$TOKENNAME`, go to the server’s Security tab and select the Manage Certificates link. When you log in to the external module where Server-Cert is stored, its certificates are displayed in the list in the `$TOKENNAME:$NICKNAME` form.

To Import a PKCS#11 Module

To import a PKCS#11 module, perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Click the **Add PKCS#11 Module** link.
3. Type the path for the .jar file in **Path to Jar File**.
4. Click OK.

For information on using PKCS#11, see “The Install a New PKCS#11 Module Page,” in the online help.

Adding a FORTEZZA PKCS#11 Module

The library is the only integration per se done on the server side. The server gets use of the library for “free”, as it appears like any other PKCS#11 library to the server. The user may be required to do further integration offline to ensure that the FORTEZZA library integrates with drivers for the FORTEZZA card reader.

Once the library is installed, the you need to acquire FORTEZZA credentials (a card with certificates) offline.

NOTE The library must be installed with `-ciphers FORTEZZA` so that the NSS library recognizes it as the default service provider for FORTEZZA encryption.

The iPlanet Web Server is used to enable FORTEZZA ciphers, select a certificate from a FORTEZZA card for the server to use, and install a Compromised Key List (CKL). A CKL is the current list of revoked key material. The CKL needs to be loaded into the certificate database on both the client and the 4.x servers in order to use the FORTEZZA ciphers.

It is possible to run a server that uses a FORTEZZA certificate and an RSA certificate. There is no explicit integration required. The user will be able to select more than one certificate to be used as the server certificate. At connection time, the NSS libraries will handle selecting the appropriate certificate for the client connection during the SSL handshake.

If pre-encrypted file support is to be used, `obj.conf` needs to be modified to load the plugin.

NOTE If you have the FORTEZZA ciphers enabled on both your client and the server, the common cipher suite of communication should be FORTEZZA. This can be checked using the Page Info on your client. Otherwise, there should not be any difference in the behavior of the server.

For more information regarding FORTEZZA encryption, see *Managing Servers with Netscape Console.*

Using SSL Configuration File Directives

Installing an SSL-enabled server creates directive entries in the `magnus.conf` file (the server's main configuration file). These directives are briefly described in the following sections.

Security

The `Security` tells the server whether encryption (Secure Sockets Layer version 2 or version 3 or both) is enabled or disabled.

Syntax

`Security` *value*

value specifies if SSL is on or off. Set the value parameter to `on` to enable SSL; and to `off` to disable SSL.

If Security is set to on, and both SSL2 and SSL3 are enabled, then the server tries SSL3 encryption first. If that fails, the server tries SSL2 encryption. By default, security is off.

SSL2

The SSL2 directive tells the server whether Secure Sockets Layer, version 2 encryption is enabled or disabled. The Security directive dominates the SSL2 directive; if SSL2 encryption is enabled but the Security directive is set to off, then it is as though SSL2 were disabled.

Syntax

SSL2 *value*

value specifies whether SSL version 2 is enabled or disabled. Set the value parameter to on to enable SSL 2 and to off to disable SSL 2. By default, security is off.

SSL3

The SSL3 directive tells the server whether Secure Sockets Layer, version 3 security is enabled or disabled. The Security directive dominates the SSL3 directive; if SSL3 security is enabled but the Security directive is set to off, then it is as though SSL3 were disabled.

Syntax

SSL3 *value*

value specifies whether SSL version 3 is enabled or disabled. Set the value parameter to on to enable SSL 3, and to off to disable SSL 3. By default, security is off.

Ciphers

The Ciphers directive specifies the ciphers enabled for your server.

Syntax

```
Ciphers +rc4,+rc4export,+rc2,+rc2export,+des,+desede3
```

A + means the cipher is active, and a - means the cipher is inactive. Any cipher with export as part of its name is not stronger than 40 bits.

SSL3Ciphers

The SSL3Ciphers directive specifies which SSL 3 ciphers are enabled for your server.

Syntax

```
SSL3Ciphers
+fortezza,+fortezza_null_md5,+rsa_rc4_128_md5,+rsa_3des_sha,+rsa_de
s_sha,+rsa_rc4_40_md5,+rsa_rc2_40_md5,rsa_null_md5,+rsa_des_56_sha,
+rsa_rc4_56_sha
```

`A +` means the cipher is active, and `a -` means the cipher is inactive. Any cipher with `40` as part of its name is 40 bits.

SSL3SessionTimeout

The SSL3SessionTimeout directive controls SSL3 session caching.

Syntax

`SSL3SessionTimeout` seconds

`seconds` is the number of seconds until a cached SSL3 session becomes invalid. The default value is 86400 (24 hours). If the `SSL3SessionTimeout` directive is specified, the value of seconds is silently constrained to be between 5 and 86400 seconds.

SSLCacheEntries

Specifies the number of SSL sessions that can be cached.

SSLClientAuth

The `SSLClientAuth` directive specifies whether a client must have a certificate in order to communicate with the server. You don't need to turn on this directive to use client authentication with access control.

Syntax

`SSLClientAuth` *value*

value specifies if certificates are always required. Set the value parameter to `on` to require certificates, and to `off` to specify that certificates are not required.

SSLSessionTimeout

The SSLSessionTimeout directive controls SSL2 session caching.

Syntax

`SSLSessionTimeout` *seconds*

`seconds` is the number of seconds until a cached SSL2 session becomes invalid. The default value is 100. If the `SSLSessionTimeout` directive is specified, the value of seconds is silently constrained to be between 5 and 100 seconds.

Using Client Certificates

If you have enabled the Administration Server Preferences “Require client certificates” option, the server asks the client to send its certificate before the server will grant the request. The server doesn’t care who the user is as long as that user has a valid certificate from a trusted CA. However, you can combine client certificates with access control so that in addition to being from a trusted CA, the user associated with the certificate must match the access-control rules. For more information, see “Access Control Files,” on page 227 in Chapter 12, “Controlling Access to Your Server.” In addition, you can process information from client certificates. For more information, see the *NSAPI Programmer’s Guide for iPlanet Web Server*.

Mapping Client Certificates to LDAP

This section describes the process iPlanet Web Server uses to map a client certificate to an entry in an LDAP directory.

When the server gets a request from a client, it asks for the client’s certificate before proceeding. Netscape clients, such as Netscape Navigator and Netscape Communicator, send the client certificate to the server (with or without prompting the end user, depending on the browser’s security configuration). (Note that you also need to set up the required ACLs; for more information, see “ACL File Syntax,” in Appendix , “ACL File Syntax,” on page 259).

The server then takes the CA listed in the certificate and tries to match it to a trusted CA listed in the Administration Server. If there isn’t a match, some servers end the connection and some perform a different operation based on the failed match. iPlanet Web Server ends the connection. If there is a match, the server continues processing the request.

After the server checks that the certificate’s CA is trusted, the server performs the following steps to map the certificate to an LDAP entry:

1. Maps the subject (user’s) DN from the user’s cert to a branch point in the LDAP directory.
2. Searches the LDAP directory for an entry that matches the information about the subject (end-user) of the client certificate.
3. Optionally verifies the client certificate with one in the LDAP entry that corresponds to the DN.

The server uses a certificate mapping file called `certmap.conf` to determine how to do the LDAP search. The mapping file tells the server what values to take from the client certificate (such as the end-user's name, email address, and so on). The server uses these values to search for a user entry in the LDAP directory, but first the server needs to determine where in the LDAP directory it needs to start its search. The certificate mapping file also tells the server where to start.

Once the server knows where to start its search and what it needs to search for (step 1), it performs the search in the LDAP directory (step 2). If it finds no matching entry or more than one matching entry, and the mapping is *not* set to verify the certificate, the search fails. For a complete list of the expected search result behavior, see the following Table 5-2 table. Note that you can specify the expected behavior in the ACL; for example, you can specify that iPlanet Web Server accepts only you if the certificate match fails. For more information regarding how to set the ACL preferences, see "Access Control Files," on page 227 in Chapter 12, "Controlling Access to Your Server."

Table 5-1 LDAP Search Results

LDAP Search Result	Certificate Verification ON	Certificate Verification OFF
No entry found	Authorization fails	Authorization fails
Exactly one entry found		Authorization succeeds
More than one entry found		Authorization fails

After the server finds a matching entry and certificate in the LDAP directory, it can use that information to process the transaction. For example, some servers use certificate-to-LDAP mapping to determine access to a server.

The following section describes the `certmap.conf` file. You need to edit this file to fit the entries in your LDAP directory and to match the certificates you expect your users to have.

Using the certmap.conf File

The certificate mapping file determines how a server should look up a user entry in the LDAP directory. You edit this file and add entries to match the organization of your LDAP directory and to list the certificates you want your users to have. Specifically, the mapping file defines the following information:

- where in the LDAP tree the server should begin its search
- what certificate attributes the server should use as search criteria when searching for the entry in the LDAP directory
- whether or not the server goes through an additional verification process

The certificate mapping file is located in the following location:

```
server_root/userdb/certmap.conf
```

The file contains one or more named mappings, each applying to a different CA. A mapping has the following syntax:

```
certmap <name> <issuerDN>

<name>:<property> [<value>]
```

The first line specifies a name for the entry and the attributes that form the distinguished name found in the CA certificate. The name is arbitrary; you can define it to be whatever you want. However, `issuerDN` must *exactly* match the issuer DN of the CA who issued the client certificate. For example, the following two `issuerDN` lines differ only in the spaces separating the attributes, but the server treats these two entries as different:

```
certmap moz1 ou=Mozilla Certificate Authority,o=Netscape,c=US
certmap moz2 ou=Mozilla Certificate Authority, o=Netscape, c=US
```

The second and subsequent lines in the named mapping match properties with values. The `certmap.conf` file has six default properties (you can use the certificate API to customize your own properties):

- `DNComps` is a list of comma-separated attributes used to determine where in the LDAP directory the server should start searching for entries that match the user's information (that is, the owner of the client certificate). The server gathers values for these attributes from the client certificate and uses the values to form an LDAP DN, which then determines where the server starts its search in the LDAP directory. For example, if you set `DNComps` to use the `o` and `c` attributes of the DN, the server starts the search from the `o=<org>, c=<country>` entry in the LDAP directory, where `<org>` and `<country>` are replaced with values from the DN in the certificate.

Note the following situations:

- If there isn't a `DNComps` entry in the mapping, the server uses either the `CmapLdapAttr` setting or the entire subject DN in the client certificate (that is, the end-user's information).
- If the `DNComps` entry is present but has no value, the server searches the entire LDAP tree for entries matching the filter.

- `FilterComps` is a list of comma-separated attributes used to create a filter by gathering information from the user's DN in the client certificate. The server uses the values for these attributes to form the search criteria used to match entries in the LDAP directory. If the server finds one or more entries in the LDAP directory that match the user's information gathered from the certificate, the search is successful and the server optionally performs a verification.

  For example, if `FilterComps` is set to use the email and userid attributes (`FilterComps=e,uid`), the server searches the directory for an entry whose values for email and uid match the end user's information gathered from the client certificate. Email addresses and userids are good filters because they are usually unique entries in the directory. The filter needs to be specific enough to match one and only one entry in the LDAP database.

  For a list of the x509v3 certificate attributes, see the following table:

Table 5-2 Attributes for x509v3 Certificates

Attribute	Description
`c`	Country
`o`	Organization
`cn`	Common name
`l`	Location
`st`	State
`ou`	Organizational unit
`uid`	Unix/Linux userid
`e|mail`	Email address

Note that the attribute names for the filters need to be attribute names from the certificate, not from the LDAP directory. For example, some certificates have an `e` attribute for the user's email address; whereas LDAP calls that attribute `mail`.

- `verifycert` tells the server whether it should compare the client's certificate with the certificate found in the LDAP directory. It takes two values: on, and off. You should only use this property if your LDAP directory contains certificates. This feature is useful to ensure your end-users have a valid, unrevoked certificate.
- `CmapLdapAttr` is a name for the attribute in the LDAP directory that contains subject DNs from all certificates belonging to the user. The default for this property is `certSubjectDN`. This attribute isn't a standard LDAP attribute, so to use this property, you have to extend the LDAP schema. For more information, see *Managing Servers with Netscape Console*.

  If this property exists in the `certmap.conf` file, the server searches the entire LDAP directory for an entry whose attribute (named with this property) matches the subject's full DN (taken from the certificate). If the search doesn't find any entries, the server retries the search using the `DNComps` and `FilterComps` mappings.

  This approach to matching a certificate to an LDAP entry is useful when it's difficult to match entries using `DNComps` and `FilterComps`.
- `Library` is a property whose value is a pathname to a shared library or DLL. You only need to use this property if you create your own properties using the certificate API. For more information, see the *NSAPI Programmer's Guide for iPlanet Web*.
- `InitFn` is a property whose value is the name of an init function from a custom library. You only need to use this property if you create your own properties using the certificate API.

For more information on these properties, refer to the examples described in "Example Mappings," on page 113

Creating Custom Properties

You can use the client certificate API to create your own properties. For information on programming and using the client certificate API, see *NSAPI Programmer's Guide for iPlanet Web Server*.

Once you have a custom mapping, you reference the mapping as follows:

```
<name>:library <path_to_shared_library>
<name>:InitFn <name_of_init_function>
```

For example:

```
certmap default1 o=Netscape Communications, c=US
default1:library /usr/netscape/enterprise/userdb/plugin.so
default1:InitFn plugin_init_fn
default1:DNComps  ou o c
default1:FilterComps l
default1:verifycert on
```

Example Mappings

The `certmap.conf` file should have at least one entry. The following examples illustrate the different ways you can use the `certmap.conf` file.

Example #1

This example represents a `certmap.conf` file with only one "default" mapping:

```
certmap default default
default:DNComps ou, o, c
default:FilterComps e, uid
default:verifycert on
```

Using this example, the server starts its search at the LDAP branch point containing the entry `ou=<orgunit>, o=<org>, c=<country>` where the text in <> is replaced with the values from the subject's DN in the client certificate.

The server then uses the values for email address and userid from the certificate to search for a match in the LDAP directory. When it finds an entry, the server verifies the certificate by comparing the one the client sent to the one stored in the directory.

Example #2

The following example file has two mappings: a default one and another for the US Postal Service:

```
certmap default default
default:DNComps
default:FilterComps e, uid

certmap usps ou=United States Postal Service, o=usps, c=US
usps:DNComps ou,o,c
usps:FilterComps e
usps:verifycert on
```

When the server gets a certificate from anyone other than the US Postal Service, it uses the default mapping, which starts at the top of the LDAP tree and searches for an entry matching the client's email and userid. If the certificate is from the US Postal Service, the server starts its search at the LDAP branch containing the organizational unit and searches for matching email addresses. Also note that if the certificate is from the USPS, the server verifies the certificate; other certificates are not verified.

CAUTION The issuer DN (that is, the CA's information) in the certificate must be identical to the issuer DN listed in the first line of the mapping. In the previous example, a certificate from an issuer DN that is `o=United States Postal Service,c=US` won't match because there isn't a space between the o and the c attributes.

Example #3

The following example uses the `CmapLdapAttr` property to search the LDAP database for an attribute called `certSubjectDN` whose value exactly matches the entire subject DN taken from the client certificate.

```
certmap myco ou=My Company Inc, o=myco, c=US
myco:CmapLdapAttr certSubjectDN
myco:DNComps  o, c
myco:FilterComps mail, uid
myco:verifycert on
```

If the client certificate subject is:

```
uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

the server first searches for entries that contain the following information:

```
certSubjectDN=uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

If one or more matching entries are found, the server proceeds to verify the entries. If no matching entries are found, the server will use `DNComps` and `FilterComps` to search for matching entries. In this example, the server would search for `uid=Walt Whitman` in all entries under `o=LeavesOfGrass Inc, c=US`.

NOTE This example assumes the LDAP directory contains entries with the attribute `certSubjectDN`.

Changing the Trust Database/Key Pair File Password

It's a good practice to change your trust database / key pair file password periodically. If your Administration Server is SSL enabled, this password is required when starting the server. Changing your password periodically adds an extra level of server protection.

For a list of guidelines to consider when changing a password, see "Guidelines for Creating Hard-to-Crack Passwords," on page 117

To change your trust database / key pair file) password, perform the following steps:

1. Access the Administration Server and choose the **Security** tab.
2. Click the **Change Password** link.
3. Type the required information and click OK.

For more information, see "The Change the Key Pair File Password Page," in the online help.

Migrating Enterprise Server 3.x Certificates

If you need to migrate certificates from an Enterprise Server 3.6 to iPlanet Web Server 4.x make sure that the 4.x iPlanet Web Administration Server user has read and write permissions on the old 3.6 database files. The files are `<alias>-cert.db` and `<alias>-key.db`, located in the `<3.6_server_root>/alias` directory.

Keys and certificates are migrated as part of the migration process only if your server has security enabled. You can also migrate keys and certificates by themselves using the Security tabs in the Administration Server page and the Server Manager page.

In Enterprise Server 3.6, a certificate / key pair was referred to by an alias which could be used by multiple server instances. The administration server managed all the aliases and their constituent certificates. In iPlanet Web Server 4.x, each server instance (including the Administration Server) has its own certificate / key pair which is referred to as a trust database instead of an alias. You manage the trust database and its constituent certificates, including the server certificate and all the included Certificate Authorities, from the Server Manager's Security tab. The

certificate and key database files are now named after the server instance that uses them. If multiple 3.6 server instances use the same alias, when you migrate each instance the certificate/key pair are migrated and named for the new server instance.

The migration not only migrates the server certificate, it migrates the whole trust database associated with the server instance. All the Certificate Authorities (CAs) in your 3.6 database are migrated to the 4.x database. If they duplicate the 4.x CAs, you use the 3.6 CA until it expires, then the 4.x CA. Do not attempt to delete duplicate CAs.

Additional Server Security Considerations

There are other security risks besides someone trying to break your encryption. Networks face risks from external and internal hackers, using a variety of tactics to gain access to your server and the information on it.

So in addition to enabling SSL on your server, you should take extra security precautions. For example, put the server machine into a secure room, and don't allow untrusted individuals to upload programs to your server.

The following sections describe the most important things you can do to make your server more secure:

- Limit Physical Access
- Limit Administration Access
- Choose Good Passwords
- Secure Your Key-Pair File
- Limit Other Applications on the Server
- Prevent Clients from Caching SSL Files
- Limit Ports
- Know Your Server's Limits
- Consider Additional Measures for Unprotected Servers

Limit Physical Access

This simple security measure is often forgotten. Keep the server machine in a locked room that only authorized people can enter. This prevents anyone from hacking the server machine itself.

Also, protect your machine's administrative (root) password, if you have one.

Limit Administration Access

If you use remote configuration, be sure to use access control to allow administration from only a few users and computers. If you want your Administration Server to provide end-user access to the LDAP server or local directory information, consider maintaining two Administration Servers and using cluster management so that the SSL-enabled Administration Server acts as the master server and the other Administration Server is available for end-users' access. For more information regarding clusters, see "About Clusters," on page 131 in Chapter 6, "Managing Server Clusters

You should also turn on encryption for the Administration Server. If you don't use an SSL connection for administration, then you should be cautious when performing remote server administration over an unsecure network. Anyone could intercept your administrative password and reconfigure your servers.

Choose Good Passwords

You use a number of passwords with your server—the administrative password, the private key password, database passwords, and so on. Your administrative password is the most important password of all, since anyone with that password can configure any and all servers on your computer. Most important after that is your private key password. If someone gets your private key and your private key password, they can create a fake server that appears to be yours, or intercept and change communications to and from your server.

A good password is one you'll remember but others won't guess. For example, you could remember *MCi12!mo* as "My Child is 12 months old!" A bad password is your child's name or birthdate.

Guidelines for Creating Hard-to-Crack Passwords

There are some simple guidelines that will help you create a stronger password.

It is not necessary to incorporate all of the following rules in one password, but the more of the rules you use, the better your chances of making your password hard to crack:

- Passwords should be 6-14 characters long.
- Mac passwords cannot be longer than 8 characters.
- Do not use the “illegal” characters: *, ", or spaces.
- Do not use dictionary words (any language).
- Do not make common letter substitutions (like replacing 3’s for E’s and 1’s for L’s) within dictionary words.
- Include characters from as many of these classes as possible:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols

Secure Your Key-Pair File

Make sure your key-pair file is protected. The Administration Server stores key-pair files in the directory *server_root*/`alias`. Consider making the files and directory readable only to Netscape/iPlanet servers installed on your computer. It’s also important to know if the file is stored on backup tapes or is otherwise available for someone to intercept. If so, you must protect your backups as completely as your server.

Limit Other Applications on the Server

Carefully consider all applications that run on the same machine as the server. It’s possible to circumvent your server’s security by exploiting holes in other programs running on your server. Disable all unnecessary programs and services. For example, the Unix `sendmail` daemon is difficult to configure securely and it can be programmed to run other possibly detrimental programs on the server machine.

Unix/Linux

Carefully choose the processes started from `inittab` and `rc` scripts. Don't run `telnet` or `rlogin` from the server machine. You also shouldn't have `rdist` on the server machine (this can distribute files but it can also be used to update files on the server machine).

Windows NT

Carefully consider which drives and directories you share with other machines. Also, consider which users have accounts or Guest privileges.

Similarly, be careful about what programs you put on your server or allow other people to install on your server. Other people's programs might have security holes. Worst of all, someone might upload a malicious program designed specifically to subvert your security. Always examine programs carefully before you allow them on your server.

Prevent Clients from Caching SSL Files

You can prevent pre-encrypted files from being cached by a client by adding the following line inside the `<HEAD>` section of a file in HTML:

```
<meta http-equiv="pragma" content="no-cache">
```

Limit Ports

Disable any ports not used on the machine. Use routers or firewall configurations to prevent incoming connections to anything other than the absolute minimum set of ports. This means that the only way to get a shell on the machine is to physically use the server's machine, which should be in a restricted area already.

Know Your Server's Limits

The server offers secure connections between the server and the client. It can't control the security of information once the client has it, nor can it control access to the server machine itself and its directories and files.

Being aware of these limitations helps you know what situations to avoid. For example, you might acquire credit card numbers over an SSL connection, but are those numbers stored in a secure file on the server machine? What happens to those numbers after the SSL connection is terminated? You should be responsible for securing any information clients send to you through SSL.

Consider Additional Measures for Unprotected Servers

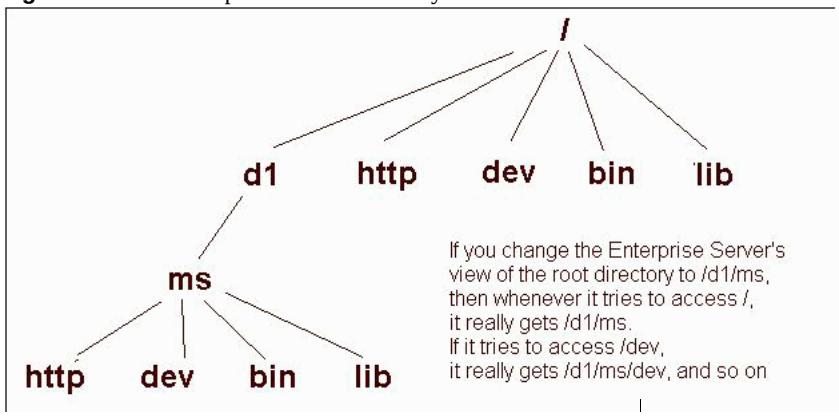
If you want to have both protected and unprotected servers, you should operate the unprotected server on a different machine from the protected one. If your resources are limited and you must run an unprotected server on the same machine as your protected server, do the following.

- Assign proper port numbers. Make sure that the protected server and the unprotected server are assigned different port numbers. The registered default port numbers are 443 for the protected server and 80 for the unprotected one.
- For Unix/Linux, enable the `chroot` feature for the document root directory. The unprotected server should have references to its document root redirected using `chroot`.

The purpose of `chroot` is to allow you to create a second root directory to limit the server to specific directories. You'd use this feature to safeguard an unprotected server. For example, you could say that the root directory is `/d1/ms`. Then any time the web server tries to access the root directory, it really gets `/d1/ms`. If it tries to access `/dev`, it gets `/d1/ms/dev` and so on. This allows you to run the web server on your Unix/Linux system, without giving it access to all the files under the actual root directory.

However, if you use `chroot`, you need to set up the full directory structure that iPlanet Web Server needs, under the alternative root directory, as shown in the following illustration:

Figure 5-2 Example Chroot Directory Structure



For more information regarding how to implement `chroot` in the `magnus.conf` file, see the *NSAPI Programmer's Guide for iPlanet Web Server*.

Part 3

Configuring and Monitoring

Chapter 6

Configuring Server Preferences

This chapter describes how to configure server preferences for your iPlanet Web Server.

This chapter contains the following sections:

- Starting and Stopping the Server
- Viewing Server Settings
- Adding and Using Thread Pools
- Configuring Network Settings
- Customizing Error Responses
- Working with Dynamic Configuration Files
- Restricting Symbolic Links (Unix/Linux)
- Using the Watchdog (uxwdog) Process (Unix/Linux)

Starting and Stopping the Server

Once the server is installed, it runs constantly, listening for and accepting HTTP requests. The status of the server appears in the Server On/Off page. You can start and stop the server using one of the following methods:

- Click the Server On or Server Off in the Server On/Off page.
- Use the Services window in the Control Panel (Windows NT).
- Use `start`. If you want to use this script with `init`, you must include the start command `http:2:respawn:`*`server_root/type-identifier/`*`start -start -i` in `/etc/inittab`. (Unix/Linux)

- Use `stop`, which shuts down the server completely, interrupting service until it is restarted. If you set the `etc/inittab` file to automatically restart (using "`respawn`"), you must remove the line pertaining to the web server in `etc/inittab` before shutting down the server; otherwise, the server automatically restarts. (Unix/Linux)

After you shut down the server, it may take a few seconds for the server to complete its shut-down process and for the status to change to "Off."

If your machine crashes or is taken offline, the server stops and any requests it was servicing may be lost.

Setting the Termination Timeout

When the server is off, it stops accepting new connections. Then it waits for all outstanding connections to complete. The time the server waits before timing out is configurable in the `magnus.conf` file. By default it is set to 3 seconds. To change the value, add the following line to `magnus.conf`:

```
TerminateTimeout seconds
```

where *seconds* represents the number of seconds the server will wait before timing out.

The advantages to configuring this value is that the server will wait longer for connections to complete. However, because servers often have connections open from nonresponsive clients, increasing the termination timeout may increase the time it takes for the server to shut down.

Restarting the Server (Unix/Linux)

You can restart the server using one of the following methods:

- Automatically restart it from the `inittab` file.

  Note that if you are using a version of Unix/Linux not derived from System V (such as SunOS 4.1.3), you will not be able to use the `inittab` file.

- Automatically restart it with daemons in `/etc/rc2.d` when the machine reboots.
- Restart it manually.

Because the installation scripts cannot edit the `/etc/rc.local` or `/etc/inittab` files, you must edit those files with a text editor. If you do not know how to edit these files, consult your system administrator or system documentation.

Normally, you cannot start an SSL-enabled server with either of these files because the server requires a password before starting. Although you can start an SSL-enabled server automatically if you keep the password in plain text in a file, this is *not* recommended.

CAUTION Leaving the SSL-enabled server's password in plain text in the server's start script is a large security risk. Anyone who can access the file has access to the SSL-enabled server's password. Consider the security risks before keeping the SSL-enabled server's password in plain text.

The server's start script, key pair file, and the key password should be owned by root (or, if a non-root user installed the server, that user account), with only the owner having read and write access to them.

If security risks are not a concern for you, follow these steps to start your SSL-enabled server automatically:

1. Using a text editor, open the start file, which is located in *server_root/http-server-id.*
2. In the 10th line counting from the top of the script, insert the following:

   ```
   echo "your_SSL-enabled_server_password"|
   ```

   For example, the edited line might look like this:

   ```
   echo "MBi12!mo"|./$PRODUCT_BIN -d $PRODUCT_SUBDIR/config $@
   ```

Restarting With Inittab (Unix/Linux)

To restart the server using `inittab`, put the following text on one line in the `/etc/inittab` file:

```
http:2:respawn:server_root/type-identifier/start -start -i
```

Replace *server_root* with the directory where you installed the server, and replace *type-identifier* with the server's directory.

The `-i` option prevents the server from putting itself in a background process.

You must remove this line before you stop the server.

Restarting With the System RC Scripts (Unix/Linux)

If you use `/etc/rc.local`, or your system's equivalent, place the following line in `/etc/rc.local`:

```
server_root/type-identifier/start
```

Replace *server_root* with the directory where you installed the server.

Restarting the Server Manually (Unix/Linux)

To restart the server from the command line, log in as root if the server runs on ports with numbers lower than 1024; otherwise, log in as root or with the server's user account. At the command-line prompt, type the following line and press Enter:

```
server_root/type-identifier/start
```

Replace *server_root* with the directory where you installed the server.

You can use the optional parameters `-p` and `-i` at the end of the line:

The `-p` option starts the server on a specific port number. This overrides the setting in `magnus.conf`.

The `-i` option runs the server in `inittab` mode, so that if the server process is ever killed or crashed, `inittab` will restart the server for you. This option also prevents the server from putting itself in a background process.

NOTE If the server is already running, the `start` command will fail. You must stop the server first, then use the `start` command. Also, if the server startup fails, you should kill the process before trying to restart it.

Stopping the Server Manually (Unix/Linux)

If you used the `etc/inittab` file to restart the server you must remove the line starting the server from `/etc/inittab` and type `kill -1 1` before you try to stop the server. Otherwise, the server restarts automatically after it is stopped.

To stop the server manually, log in as `root` or use the server's user account (if that is how you started the server), and then type the following at the command line:

```
server_root/type-identifier/stop
```

Restarting the Server (Windows NT)

You can restart the server by:

- Using the Services Control Panel to restart any server.
- Using the Services Control Panel to configure the operating system to restart the server or the administration server each time the machine is restarted.

For Windows NT 3.51, perform the following steps:

1. In the Main group, double-click the **Control Panel** icon.
2. Double-click the **Services** icon.
3. Scroll through the list of services and select the service for your server.
4. Check **Automatic** to have your computer start the server each time the computer starts or reboots.
5. Click OK.

For Windows NT 4.0, perform the following steps:

1. From the Start menu, choose **Settings**, and then **Control Panel**.
2. Double-click the **Services** icon.
3. Scroll through the list of services and select the service for your server.
4. Check **Automatic** to have your computer start the server each time the computer starts or reboots.
5. Click OK.

NOTE You can also use the Services dialog box to change the account the server uses. For more information about changing the account the server uses, see “Changing the Server’s User Account (Windows NT)” on page 135.

Normally, you can’t start an SSL-enabled server automatically because you have to enter its password. There is a way to have an SSL-enabled server start without having to enter a password if you keep the password in plain text in a text file. This practice is *not* recommended.

CAUTION Leaving your SSL-enabled server's password in a text file on your system is a large security risk. In essence, you are trading security for convenience. Anyone who can access the file has access to your SSL-enabled server's password. Consider whether you can afford the security risks before keeping your SSL- enabled server's password in plain text on your system.

If the security risk is not a concern for you, follow these steps to start your SSL-enabled server automatically:

1. Using a text editor, such as Notepad, create a new text file called `password.txt` in *`server_root`*`\https-`*`server_id`*`\config`. For a default web server installation, `password.txt` would be stored in the `C:\Netscape\server4\https-`*`server_id`*`\config` directory.
2. Type your private-key password in the first line, making sure not to put carriage returns or linefeeds after the password. The file must contain only the password.

   When you start your SSL-enabled server, it first tries to read the password in `password.txt`. If the file does not exist, you will be prompted for the password. If `password.txt` exists but the password is incorrect, the server will add an entry to the error log and exit.

CAUTION If you have an NTFS file system, you should protect the directory that contains `password.txt` by restricting its access, even if you do not use the file. The directory should have read / write permissions for the administration server user and the web server user. Protecting the directory prevents others from creating a false `password.txt` file.

On FAT file systems, you cannot protect directories or files by restricting access to them.

Using the Automatic Restart Utility (Windows NT)

The server is automatically restarted by a server-monitoring utility if the server crashes. On systems that have debugging tools installed, a dialog box with debugging information appears if the server crashes. To help debug server plug-in API programs (for example, NSAPI programs), you can disable the auto-start feature by setting a very high timeout value. You can also turn off the debugging dialog boxes by using the Registry Editor.

Changing the Time Interval (Windows NT)

To change the time interval that elapses between startup and the time the server can automatically restart, perform the following steps:

1. Start the Registry Editor.
2. Select your server's key (in the left side of the Registry Editor window, located in `HKEY_LOCAL_MACHINE\SOFTWARE\Netscape\`).
3. Choose **Add Value** from the Edit menu. The Add Key dialog box appears.
4. In **Value Name**, type `MortalityTimeSecs`.
5. Select REG_DWORD from the **Data Type** pull-down list.
6. Click OK. The DWORD Editor dialog box appears.
7. Type the time interval (in seconds) that will elapse between startup and the time the server can restart automatically.

   The interval can be in binary, decimal, or hexadecimal format.
8. Click the numerical format for the value you entered in the previous step (binary, decimal, or hexadecimal).
9. Click OK.

   The `MortalityTimeSecs` value appears in hexadecimal format at the right side of the Registry Editor window.

Turning Off the Debugging Dialog Box (Windows NT)

If you've installed an application (such as a compiler) that has modified the system debugging settings and the server crashes, you might see a system-generated application error dialog box. The server will not restart until you click OK.

To turn off the debugging dialog box that appears if the server crashes, perform the following steps:

1. Start the Registry Editor.

2. Select the **AeDebug** key, located in the left side of the Registry window in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`.
3. Double-click the Auto value in the right side of the window.

   The String Editor dialog box appears.
4. Change the string value to 1.

Viewing Server Settings

You can see if your server is running and view your server's technical and content settings. The technical settings come from `magnus.conf`, and the content settings come from `obj.conf`. These files are located in the server root, in the directory `https-`*server_id* `\config`. For more information about the `magnus.conf` and `obj.conf` files, see the *NSAPI Programmer's Guide for iPlanet Web Server*.

To view your server settings, see the View Server Settings page in the Server Manager.

The content settings displayed in the View Server Settings page depend on how you've configured your server. Common server content settings include the server's document directory, its index filenames, name and location of its access log, and default MIME type.

Adding and Using Thread Pools

Use thread pools to allocate a certain number of threads to a specific service. For example, you can set up a thread pool specifically for Server-Side JavaScript applications. As part of adding the Server-Side JavaScript thread pool, you specify the maximum number of threads you want to allocate to Server-Side JavaScript applications, and they cannot take up more than their allocated number of threads.

Another use for thread pools is for running thread-unsafe plugins. By defining a pool with the maximum number of threads set to 1, only one request is allowed into the specified service function.

When you add a thread pool, the information you specify includes the minimum and maximum number of threads, the stack size, and the queue size.

The Native Thread Pool and Generic Thread Pools (Windows NT)

On Windows NT, you can use two types of thread pools: the native thread pool (`NativePool`) and additional generic thread pools.

The native thread pool is defined by default for backwards compatibility with Netscape Enterprise Server 3.6. To edit the native thread pool, see the Native Thread Pool page in the Server Manager.

You can create as many generic thread pools as you want, for as many purposes as you want. To create generic thread pools, see the Generic Thread Pools page in the Server Manager.

Thread Pools (Unix/Linux)

Since threads on Unix/Linux are always OS-scheduled (as opposed to user-scheduled) Unix/Linux users do not need to use the `NativePool`, and do not have a Server Manager page for editing its settings. However, Unix/Linux users can still create thread pools. To create thread pools, see the Thread Pools page in the Server Manager.

Editing Thread Pools

Once you have added a thread pool, you cannot change the values of the thread pool settings (minimum threads, maximum threads and so on) through the Server Manager. Instead you must edit the thread pool settings in `obj.conf`.

A thread pool appears in `obj.conf` as follows:

```
Init fn="thread-pool-init" name=name_of_the_pool MaxThreads=n
MinThreads=n QueueSize=n StackSize=n
```

Use the following parameters to change the pool: `MinThreads`, `MaxThreads`, `QueueSize`, and `StackSize`.

Windows NT users can always edit the settings for the native pool using the Server Manager.

Using Thread Pools

After you've set up a thread pool, use it by designating it as the thread pool for a specific service.

To configure a thread pool, go to the Administration Server **Preferences** tab and select **Thread Pool**.

You can also designate a thread pool by using the `pool` parameter of the `load-modules` function in `obj.conf`.

```
pool="name_of_pool"
```

In addition, you can use the `pool` parameter on any NSAPI function so that only that NSAPI function runs on the pool you specify.

Configuring Network Settings

You can change the following network settings on your server: server user, server name, server port, bind to address, and MTA host.

Changing the Server's Location (Unix/Linux)

For various reasons, you might move the server from one directory to another. If you move the server, you must change the location the server references—it needs to know where the binary files are. After changing the location, you must shut down the server and copy the server files and subdirectories to a new location.

To change the server's location edit the Server Location field in the Network Settings page in the Administration Server.

Changing the Server's User Account (Unix/Linux)

The server user specifies a Unix/Linux user account that the server uses. All the server's processes run as this user.

You do not need to specify a server user if you chose a port number greater than 1024 and are not running as the `root` user (in this case, you do not need to be logged on as `root` to start the server). If you do not specify a user account here, the server runs with the user account you start it with. Make sure that when you start the server, you use the correct user account.

NOTE If you do not know how to create a new user on your system, contact your system administrator or consult your system documentation.

Even if you start the server as root, you should not run the server as root all the time. You want the server to have restricted access to your system resources and run as a non-privileged user. The user name you enter as the server user should already exist as a normal Unix/Linux user account. After the server starts, it runs as this user.

If you want to avoid creating a new user account, you can choose the user `nobody` or an account used by another HTTP server running on the same host. On some systems, however, the user `nobody` can own files but not run programs.

To change the server's user account, edit the Server User field in the Network Settings page in the Administration Server.

Changing the Server's User Account (Windows NT)

By using a specific user account (other than `LocalSystem`), you can restrict or enable system features for the server. For example, you can use a user account that can mount files from another machine.

To change the web server user account after installation, perform the following steps:

1. Create a user with the Windows NT Users Manager. The user must have "Log in as a service" rights.
2. Stop the server.
3. From the Windows Control Panel, choose **Services**.
4. Select the iPlanet Web Server service.

5. In the Service pop-up, in the **Log on As** section, click the **This Account** radio button.
6. Type the user account you want the web server to use.
7. Type the password for that account; type it again for confirmation.
8. Click OK.
9. Restart the server using the Services program or the Server Administration page.

Changing the Server Name

The server name is the full hostname of your server machine. When clients access your server, they use this name. The format for the server name is *machinename.yourdomain.domain*. For example, if your full domain name is `iplanet.com`, you could install a server with the name `www.iplanet.com`.

If your system administrator has set up a DNS alias for your server, use that alias on the Network Settings page in the Administration Server. If you do not have a DNS alias for your server, use the machine's name combined with your domain name to construct the full hostname.

To change the server name, edit the Server Name field in The Network Settings Page in the Administration Server.

Changing the Server Port Number

The Server Port Number specifies the TCP port that the server listens to. The port number you choose can affect your users—if you use a nonstandard port, then anyone accessing your server must specify a server name and port number in the URL. For example, if you use port 8090, the user would specify something like this URL:

```
http://www.iplanet.com:8090
```

Port numbers for the most commonly used network-accessible services are maintained in the file `/etc/services` (on Unix/Linux) or `\WINNT\System32\drivers\etc\services` (on Windows NT).

Although the port number can be any port from 1 to 65535, the standard insecure web server port number is 80, and the standard secure web server port number is 443.

For Unix/Linux, if you are not running as the `root` user when you install or start the server, you must use a port number higher than 1024.

To change the server port number, edit the Server Port field in the Network Settings page in the Administration Server.

Changing the Server Binding Address

At times you'll want the server machine to answer to two URLs. For example, you might want to answer both `http://www.iplanet.com/` and `http://www.mozilla.com/` from one machine.

If you have already set up your system to listen to multiple IP addresses and want to use this feature, use the Bind To Address field in the Network Settings window to tell the server which IP address is associated with this hostname.

To change the server binding address, edit the Bind To Address field in the Network Settings page in the Administration Server.

Changing the Server's MTA Host

You can change the server's MTA (Message Transfer Agent) host. You must enter a valid MTA host if you want to use the agent email function.

To change the MTA Host, edit the MTA host field in the Network Settings page in the Administration Server.

Customizing Error Responses

You can specify a custom error response that sends a detailed message to clients when they encounter errors from your server. You can specify a file to send or a CGI program to run.

You might want to change the way the server behaves when it gets an error for a specific directory. Instead of sending back the default file, you might want to send a custom error response instead. For example, if a client tries repeatedly to connect to a part of your server protected by access control, you might return an error file with information on how to get an account.

Before you can enable a custom error response, you must create the HTML file to send or the CGI program to run in response to an error. After you do this, enable the response in the Network Settings page in the Administration Server.

Working with Dynamic Configuration Files

Server content is seldom managed entirely by one person. You may need to allow end users to access a subset of configuration options so that they can configure what they need to, without giving them access to the iPlanet Web Server. The subset of configuration options are stored in dynamic configuration files. Two types of dynamic configuration files are supported by iPlanet Web Server: `.htaccess` and `.nsconfig`. You can enable `.nsconfig` files in iPlanet Web Server; you have to manually enable `.htaccess` files.

NOTE There is no support for LDAP or the 3.0 Netscape user databases in the dynamic configuration files. You should not use dynamic configuration files if you use LDAP. You must use NCSA-style user databases to use `.htaccess` files. You must use either NCSA-style user databases or Enterprise 2.x DBM- format user databases with `.nsconfig` files. For more information on user databases, see *Managing Servers with Netscape Console.*

If you already use `.nsconfig` files, you might want to continue using them. However, iPlanet Web Server also includes a utility for converting your `.nsconfig` files to `.htaccess` files.

Using .htaccess Files

The files that support `.htaccess` are in the directory *`server_root`*`/plugins/htaccess`. These files include a plug-in that enables you to use `.htaccess` files and a script for converting `.nsconfig` files to `.htaccess` files.

Activating .htaccess checking

To use `.htaccess` files, you must first modify the server's `obj.conf` file to load, initialize, and activate the plug-in. At the top of the `obj.conf` file, after the other `Init` directives, add the following lines:

For Unix/Linux:

```
Init fn="load-modules" funcs="htaccess-init,htaccess-find"\
shlib="server_root/plugins/htaccess/htaccess.so"
Init fn="htaccess-init"
```

For Windows NT:

```
Init fn="load-modules" funcs="htaccess-init,htaccess-find" \
shlib="server_root/plugins/htaccess/bin/htaccess.dll"
Init fn="htaccess-init"
```

These lines load and initialize the module when the server is started. *server_root* is the path to your server root.

To activate `.htaccess` file processing for all directories managed by the server, add the `PathCheck` directive:

```
PathCheck fn="htaccess-find"
```

to the default server object, which is delimited by:

```
<Object name="default"
...
</Object
```

Generally, the directive to activate `.htaccess` processing should be the last `PathCheck` directive in the object.

To activate `.htaccess` file processing for particular server directories, place the `PathCheck` directive in the corresponding object definition in `obj.conf`.

If you want to name your `.htaccess` files something other than `.htaccess`, you must specify the filename in the `PathCheck` directive using the following format:

```
PathCheck fn="htaccess-find" filename="filename"
```

Replace *filename* with the filename you are using.

After editing the configuration file, stop and start your server. Apply your configuration file changes in the iPlanet Web Server by clicking the Apply button. Subsequent accesses to the server will be subject to `.htaccess` access control in the specified directories.

To restrict write access to `.htaccess` files, create a configuration style for them, and apply access control to that configuration style. For more information, see Chapter 10, “Working With Configuration Styles.” and Chapter 12, “Controlling Access to Your Server.”

Converting Existing .nsconfig Files to .htaccess Files

The iPlanet Web Server includes a script for converting your existing `.nsconfig` files to `.htaccess` files. To convert your files, at the command prompt, enter the path to Perl on your system, the path to the script, and the path to your `obj.conf` file. For example you might type the following (it should all be on one line when you type it):

```
server_root\install\perl server_root/plugins/htaccess/htconvert
server_root/https-server_name/config/obj.conf
```

The script converts all `.nsconfig` files to `.htaccess` files, but does not delete the `.nsconfig` files.

Supported .htaccess Directives

The following `.htaccess` directives are supported in this release:

- `AuthName`
- `AuthType` (The only `AuthType` supported is `Basic`.)
- `Limit`
  - order
  - deny
  - allow
  - `require`
- `AuthGroupFile`
- `AuthUserFile` (This has different formats depending on your usage. See below.)

There is an option, called `groups-with-users`, that facilitates handling large numbers of users in groups. That is, if you have many users in a group, you can follow these steps:

1. Revise the format of the user file format to list all the groups a user belongs to:

   ```
   username:password:group1,group2,group3,...groupn
   ```

2. Revise the `AuthGroupFile` directive to point to the same file as the `AuthUserFile`.

Or, alternatively, you can perform these steps:

1. Remove the `AuthGroupFile` directive entirely.

2. And add this option to the `'Init fn=htaccess-init'` line in the `obj.conf` file:

   ```
   groups-with-users="yes"
   ```

Example of an .htaccess File

The following example shows an `.htaccess` file:

```
<Limit> GET POST
order deny,allow
deny from all
allow from all
</Limit>
<Limit> PUT DELETE
order deny,allow
deny from all
</Limit>
AuthName mxyzptlk.kawaii.com
AuthUserFile /server_root/mxyz-docs/service.pwd
AuthGroupFile /server_root/mxyz-docs/service.grp
```

Using .nsconfig Files

With `.nsconfig` files, you can allow end users to apply access control or customize error messages without allowing them to use CGI or parsed HTML. The format and capability of these dynamic configuration files is described in “Writing .nsconfig Files” on page 143.

When a request is made for a resource in which dynamic configuration is enabled, the server must search for the configuration files within one or more directories of that resource. This search can be an expensive operation in terms of performance, so the server lets you configure how much flexibility you need, weighing it against the efficiency cost.

You can provide a base directory to the server, in which case the server starts its search for configuration files from the filesystem directory. Alternatively, you can provide no base directory, in which case the server attempts to infer the base directory from the URL. That is, if the requested URL is to a file in the document root, the server starts searching from the document root.

You also specify the name of the configuration file to search for within the base directory.

If you centralize all of your configuration information for the subdirectories of the base directory in the base directory's configuration file, the server is more efficient because it doesn't have to search for configuration files in the subdirectories.

However, you may sometimes want the server to search the subdirectories. If you do, the server searches for `.nsconfig` files starting from the top level directory and searching downward until reaching the directory in which the referenced resource resides. The server processes `.nsconfig` files in the order it encounters them. If a top level file restricts a user's access, the server does not give the user access, even though a lower level file might allow access.

The server processes all restrictions based on IP address and DNS entry (`RestrictAccess` directive) as it finds them in a file. If the server finds a file that denies a user access because of IP address or DNS entry, it stops processing files. The server collects restrictions based on user name (`RequireAuth` directive) and processes them at the end, unless the request has already been denied because of IP address or DNS entry.

For example, if you selected the base directory inferred from URL translation, selected `.nsconfig` for your filename, and chose to search subdirectories, the following search would occur.

When a user requests the filesystem path `C:\Netscape\server4\docs\icons\gfx\logo.gif`, instead of searching for `C:\Netscape\server4\docs\.nsconfig` the server would search all of the subdirectories:

```
C:\Netscape\server4\docs\.nsconfig
C:\Netscape\server4\docs\gfx\.nsconfig
C:\Netscape\server4\docs\gfx\icons\.nsconfig
```

You can also enter a wildcard pattern of file types you want to disable in directories where dynamic configuration is enabled. To disable CGI programs and parsed HTML, for example, use * (`cgi|parsed-html`).

To configure `.nsconfig` files, perform the following steps:

1. From the Server Manager, choose **Server Preferences**.
2. Click the **Dynamic Configuration Files** link.
3. Choose a resource from the Resource Picker.
4. Choose whether to base the directory from the URL or from a specified directory.
5. Type the filename.
6. Choose whether to search only the base directory.

7. Type the disabled types.
8. Click OK.
9. Click Save and Apply.

Writing .nsconfig Files

The `.nsconfig` files consist of sets of directives that control the server. These directives are surrounded by `Files` directives that tell the server which files in the configuration file's directory the directives apply to. For example:

```
<Files PATTERN1
... directives ...
</Files
<Files PATTERN2
... directives ...
</Files
```

PATTERN1 and *PATTERN2* are wildcard patterns that tell the server which filesystem paths to apply the directives to. For example, * would apply the directive to all filesystem pathnames. Any pattern given is first prefixed with the directory containing the configuration file to ensure that the directives are applied only to subdirectories. There can be as many sets of `Files` directives in the `.nsconfig` file as you need.

The file can contain blank lines. Lines beginning with # are treated as comments. Note that lines are limited to a maximum of 1024 characters.

For Windows NT, all paths must use the forward slash (/) instead of the backwards slash (\), otherwise you receive a server "path not found" error.

Each directive can take a variable number of parameters, all of which must be lowercase. The `Files` directives include:

- `AddType exp=`*SHEXP* `type=`*mime-type* `enc=`*http-encoding* `AddType` assigns the give type or encoding to the paths represented by the wildcard pattern *SHEXP*. One or both of `type` and `encoding` can appear, but only one expression can be used. You cannot apply two MIME types or encodings to the same pattern of the files.
- `ErrorFile reason=`*error-string* `code=`*error-code* `path=`*html-file* `ErrorFile` causes the HTML file described by the URL suffix *path* to be sent in place of the server's default error message. The file is substituted when an error described by one or both of `reason` and `code` occurs. `path` is a valid URL to the local server but without the `http://`*server* prefix. The error codes are the standard HTTP error codes:
  - 401 Unauthorized

- 403 Forbidden
- 404 Not found
- 500 Server error

- `RequireAuth dbm=`*`dbmfile`* `userfile=`*`database_name`* `realm=`*`string`* `userpat=`*`PATTERN`*
  `RequireAuth` lets you ask the user for a username and a password when accessing the directory. `dbm` is a user database. Note that `dbm` can only be used on a 2.x Enterprise user database. `userfile` is an NCSA-style user database filename. The file consists of lines in the format *user:encrypted_password*. `realm` is a unique string to tell your users which password they should use. `userpat` determines which users from the given `dbm` or `userfile` are allowed access. `userpat` is a wildcard pattern or list of user names. For example, you can use the syntax `userpat="user1"` or `userpat="(user1|user2)"` for specifying a user or a list of users.

- `RestrictAccess method=HTTP-method type=allow|deny ip=addrpattern dns=hostpattern return-code=403|404`
  `RestrictAccess` applies access control to the directory and restricts certain users. `method` is an optional parameter specifying a wildcard pattern of HTTP methods to protect (no method specified means all of them). `type` determines whether the IP address wildcard pattern or hostname wildcard pattern is allowed or denied access. If the only `RestrictAccess` directives in a `Files` set are of type `allow`, then all hosts not specified by the patterns are denied. `ip` must be typed in lowercase for the directive to work. More than one `RestrictAccess` can appear in the file. The order in which these lines appear is important; later `RestrictAccess` lines override earlier ones.

Example of an .nsconfig File

The following example shows an `.nsconfig` file:

```
<Files *
ErrorFile reason="Unauthorized" code="401" path="/errors/unauthorized.html"
ErrorFile reason="Forbidden" code="403" path="/errors/forbidden.html"
ErrorFile reason="Not Found" code="404" path="/errors/notfound.html"
ErrorFile reason="Server Error" code="500" path="/errors/server-error.html"
RestrictAccess method="(GET|HEAD|POST)" type="allow" ip="*"
RestrictAccess method="(GET|HEAD|POST)" type="deny" ip="198.95.251.30" return-code="404"
</Files
<Files *.gif
AddType exp=*.gif type=application/octet-stream
</Files
<Files *.txt
RequireAuth dbm="server_root/authdb/default" realm=Text userpat="user*"
</Files
```

Restricting Symbolic Links (Unix/Linux)

You can limit the use of the filesystem links in your server. Filesystem links are references to files stored in other directories or filesystems. The reference makes the remote file as accessible as if it were in the current directory. There are two types of filesystem links:

- **Hard links**—A hard link is really two filenames that point to the same set of data blocks; the original file and the link are identical. For this reason, hard links cannot be on different filesystems.
- **Symbolic (soft) links**—A symbolic link consists of two files, an original file that contains the data, and another that points to the original file. Symbolic links are more flexible than hard links. Symbolic links can be used across different filesystems and can be linked to directories.

For more information about hard and symbolic links, see your Unix/Linux system documentation.

Filesystem links are an easy way to create pointers to documents outside of the primary document directory and anyone can create these links. For this reason you might be concerned that people might create pointers to sensitive files (for example, confidential documents or system password files).

To restrict symbolic links, use the Limit Symbolic Link page in the Server Manager.

Using the Watchdog (uxwdog) Process (Unix/Linux)

The `uxwdog` process is the name of the web server watchdog process, introduced in Enterprise Server 3.01. Prior to Enterprise Server 3.01, the server would fork a copy of itself at startup, and the parent server process would serve as the watchdog for the child. In Enterprise 2.x, a server restart operation would cause the parent server process (`ns-httpd`) to terminate the child `ns-httpd` process, and then recreate it. This result had the advantage that the parent process could maintain the key file password for a secure server, so that restarting the server would not require the server administrator to reenter the password.

However, with the addition of a number of subsystems to the server in Enterprise Server 3.0, it was felt that the server should be completely stopped and started for a restart operation, as the most expedient way to be sure that all subsystems were properly initialized. This had several immediate drawbacks. First, it became

necessary to reenter the key file password for a secure server during a restart. This was particularly a problem for a secure server with automatic log rotation enabled, since log rotation relies on a server restart operation. Finally, every server configuration change required the server to be completely stopped and started.

The basic idea of uxwdog is to have a lightweight process that keeps around just enough state information to be able to start a new server process during a restart operation, without human intervention. This state consists mainly of any passwords or PINs required to start a secure server, and open file descriptors for sockets on which the server will listen. The socket file descriptors had to be kept around because some of them might be for privileged TCP ports, port 80 for example, which would require a process running as root to bind them. When this is the case, the Administration Server generally runs as root, and starts uxwdog as root, or else an administrator who is running as root executes the server `start` script. Once uxwdog binds the server listen port(s), it changes its `uid` to the server `uid`, often "nobody," and then starts the server process as that `uid`.

One consequence of this behavior is that the NSAPI Init directives always run under the server `uid`, unlike in Enterprise 3.0 and earlier, where it was possible to have them run as root. This has created some problems in upgrade situations, when a plugin Init function was creating a file during the Init. The file would be owned by root in the older server version, and when installing the plugin in Enterprise 3.01 and later, it would be necessary to change the ownership or protection on the migrated file.

In order to determine on which ports the server listens, uxwdog must read `magnus.conf` and `obj.conf`. It does this each time the server is restarted, and verifies that the port numbers have not been changed. If they have, a restart operation is not possible, uxwdog will exit, and the server will have to be manually started. This is also true if security is turned on, the server `uid` is changed, or the `PidLog` filename is changed.

The `restart` and `stop` scripts send `SIGHUP` and `SIGTERM`, respectively, to uxwdog. In both cases, uxwdog sends `SIGTERM` to the `ns-httpd` process to shut down the server. For a restart operation, uxwdog then creates a new server process, passing it the file descriptors of the listen ports, and any passwords or PINs it has saved.

The default behavior of the server watchdog process automatically restarts the server if the server process should terminate unexpectedly. You can revert to the previous default behavior, which was for the watchdog process to exit if the server terminates unexpectedly. To revert to the original default behavior, set the environment variable, `UXWDOG_NO_AUTOSTART`, at the beginning of the server start script as follows:

(following the "`#!/bin/sh`" line):

```
UXWDOG_NO_AUTOSTART=1; export UXWDOG_NO_AUTOSTART
```

You also now have the option to have the watchdog restart the server if the server process calls `exit()` with a non-zero argument value. This feature is disabled by default, but can be enabled by setting the `UXWDOG_RESTART_ON_EXIT` environment variable in the server start script as follows:

```
UXWDOG_RESTART_ON_EXIT=1; export UXWDOG_RESTART_ON_EXIT
```

Between Enterprise Server 3.01 and Enterprise Server 3.5.1, the Administration Server CGIs for Enterprise Server were changed to actually restart, rather than start and stop the server, when configuration changes are applied. As part of this change, these CGIs will create a file, `wdnotify`, in the server's logs directory, which will contain a TCP port number on which the CGI listens for status from the watchdog. During a start or restart operation, `uxwdog` checks for the existence of this file, and if it finds it, connects to that port, and reads the name of a file to which `stderr` is to be redirected during the operation. uxwdog opens that file, redirects `stderr` to it, and performs the operation. If the operation is successful, `uxwdog` writes a single byte value of zero back to the CGI. Otherwise it writes a non-zero status byte, typically a value of one. Finally `uxwdog` closes the connection to the CGI, and redirects `stderr` to `/dev/console`.

There may be some cases where `wdnotify` does not get deleted when it should, which may cause `uxwdog` to exit instead of starting or restarting the server. This can be corrected by manually removing the `wdnotify` file from the `logs` directory.

Chapter 7

Understanding Log Files

You can monitor your server's activity using several different methods. You can view the server's status in real time by using the Hypertext Transfer Protocol (HTTP). This chapter discusses how to monitor your server by recording and viewing log files or by using the performance monitoring tools provided with your operating system.

This chapter contains the following sections:

- About Log Files
- Viewing an Access Log File
- Monitoring the Server Using HTTP
- Archiving Log Files
- Setting Log Preferences
- Flushing the Log Buffer
- Running the Log Analyzer
- Viewing Events (Windows NT)

About Log Files

Server log files record your server's activity. You can use these logs to monitor your server and to help you when troubleshooting. The error log file, located in `https-`*`servername`*`/logs/errors` in the server root directory, lists all the errors the server has encountered. The access log, located in `https-`*`servername`*`/logs/access` in the server root directory, records information

about requests to the server and the responses from the server. You can configure the information recorded in the iPlanet Web Server access log file. You use the log analyzer to generate server statistics. You can back up server error and access log files by archiving them.

Viewing an Access Log File

You can view the server's active and archived access log files.

To view the Administration Server's access log from the Administration Server, choose the Preferences tab, and then choose the **View Access Log** page.

To view an access log from the Server Manager, choose the Status tab, and then choose the **View Access Log** page.

The following is an example of an access log in the Common Logfile Format (you specify the format in the Log Preferences window; see "Setting Log Preferences" on page 155 for more information):

```
wiley.a.com - - [16/Feb/1999:21:18:26 -0800] "GET / HTTP/1.0" 200 751
wiley.a.com - - [17/Feb/1999:1:04:38 -0800] "GET /docs/grafx/icon.gif HTTP/1.0" 204 342
wiley.a.com - - [20/Feb/1999:4:36:53 -0800] "GET /help HTTP/1.0" 401 571
arrow.a.com - john [29/Mar/1999:4:36:53 -0800] "GET /help HTTP/1.0" 401 571
```

Table 7-1 describes the last line of this sample access log.

Table 7-1 The fields in the last line of the sample access log file

Access Log Field	Example
Hostname or IP address of client	arrow.a.com. (In this case, the hostname is shown because the web server's setting for DNS lookups is enabled; if DNS lookups were disabled, the client's IP address would appear.
RFC 931 information	- (RFC 931 identity not implemented)
Username	john (username entered by the client for authentication)
Date / time of request	29 / Mar / 1999:4:36:53 -0800
Request	GET / help
Protocol	HTTP / 1.0

Table 7-1 The fields in the last line of the sample access log file *(Continued)*

Access Log Field	Example
Status code	401
Bytes transferred	571

The following is an example of an access log using the flexible logging format (you specify the format in the Log Preferences page; see "Setting Log Preferences" on page 155 for more information):

```
wiley.a.com - - [25/Mar/1999:12:55:26 -0800] "GET /index.htm HTTP/1.0" "GET"
"/?-" "HTTP/   1.0" 304 0 - Mozilla/2.0 (WinNT; I)
wiley.a.com - - [25/Mar/1999:12:55:26 -0800] "GET / HTTP/1.0" "GET" "/?-"
"HTTP/1.0" 304 0    - Mozilla/2.0 (WinNT; I)
wiley.a.com - - [25/Mar/1999:12:55:26 -0800] "GET / HTTP/1.0" "GET" "/?-"
"HTTP/1.0" 304 0    - Mozilla/2.0 (X11; I; IRIX 5.3 IP22)
```

Viewing the Error Log File

The error log file contains errors the server has encountered since the log file was created; it also contains informational messages about the server, such as when the server was started. Unsuccessful user authentication is also recorded in the error log. Use the error log to find broken URL paths or missing files.

To view the Administration Server's error log file, from the Administration Server, choose the Preferences tab, and choose the **View Error Log** page.

To view a server's error log file, from the Server Manager, choose the Status tab, and choose the **View Error Log** page.

The following is an example of an error log for Unix/Linux:

```
[13/Feb/1999:16:56:51] info: successful server startup
[20/Mar/1999 19:08:52] warning: for host wiley.a.com trying to GET
/report.html,     append-trailer reports: error opening
/usr/netscape/server4/docs/report.html (No such file or directory)
```

The following is an example of an error log for Windows NT:

```
[13/Feb/1996:16:56:51] info: successful server startup
[20/Mar/1996 19:08:52] warning: for host wiley.a.com trying to GET
/report.html,     append-trailer reports: error opening
C:/Netscape/Server4/docs/report.html     (ERROR_FILE_NOT_FOUND)
```

In these examples, the first line is an informational message—the server started up successfully. The second log entry shows that the client `wiley.a.com` requested the file `report.html`, but the file wasn't in the primary document directory on the server.

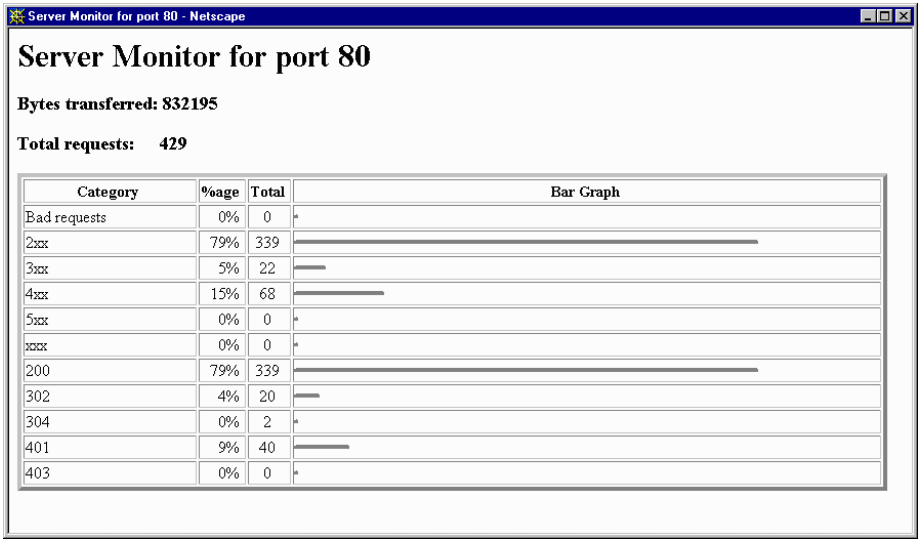
Monitoring the Server Using HTTP

You can monitor your server's usage with the interactive server monitor. You can see how many requests your server is handling and how well it is handling these requests. If the interactive server monitor reports that the server is handling a great number of requests, you may need to adjust the server configuration or the system's network kernel to accommodate the requests. The interactive server monitor is shown in Figure 7-1.

For a description of the various server statistics for which the interactive server monitor reports the totals, see the Monitor Current Activity page in the online help.

To monitor your server, use launch the monitoring program from the Monitor Current Activity page.

Figure 7-1 The Interactive Server Monitor



Archiving Log Files

You can set up your log files to be automatically archived. At a certain time, or after a specified interval, your logs will be rotated. iPlanet Web Server saves the old log files and stamps the saved file with a name that includes the date and time they were saved. For example, you can set up your access log files to rotate every hour, and iPlanet Web Server saves and names the file "`access.199907152400`," where name of the log file, year, month, day, and 24-hour time is concatenated together into a single character string. The exact format of the access log archive file varies depending upon which type of log rotation you set up.

iPlanet Web Server offers the two types of log rotation for archiving files: Internal-daemon log rotation and Cron-based log rotation.

Internal-daemon Log Rotation

This type of log rotation happens within the HTTP daemon, and can only be configured at startup time. Internal daemon log rotation allows the server to rotate logs internally without requiring a server restart. Logs rotated using this method are saved in the following format:

```
access.<4 digit year><2 digit month><2 digit day><4 digit 24-hour time>
```

You can specify the time used as a basis to rotate log files and start a new log file. For example, if the rotation start time is 12:00 a.m., and the rotation interval is 1440 minutes (one day), a new log file will be created immediately upon save regardless of the present time and collect information until the rotation start time. The log file will rotate every day at 12:00 a.m., and the access log will be stamped at 12:00 a.m. and saved as `access.199907152400`. Likewise, if you set the interval at 240 minutes (4 hours), the 4 hour intervals begin at 12:00 a.m. such that the access log files will contain information gathered from 12:00 a.m. to 4:00 a.m., from 4:00 a.m. to 8:00 a.m., and so forth.

If access log rotation is enabled, log file rotation starts at server startup. The first access log file to be rotated gathers information from the current time until the next rotation time. Using the previous example, if you set your start time at 12:00 a.m. and your rotation interval at 240 minutes, and the current time is 6:00 a.m., the first log file to be rotated will contain the information gathered from 6:00 a.m. to 8:00 a.m, and the next log file will contain information from 8:00 a.m. to 12:00 p.m. (noon), and so forth.

Cron-based Log Rotation

This type of log rotation is based on the time stored in the `cron.conf` file in the *`server_root`*`/https-admserv/config/` directory. This method allows you to archive log files immediately or have the server archive log files at a specific time on specific days. The server's cron configuration options are stored in `ns-cron.conf` in the *`server_root`*`/https-admserv/config/` directory. Logs rotated using the cron based method are saved as the original filename followed by the date and time the file was rotated. For example, `access` might become `access.24Apr-0430PM` when it is rotates at 4:30 p.m. For more information about cron controls, see "Using Cron Controls (Unix/Linux)" on page 60.

Log rotation is initialized at server startup. If rotation is turned on, iPlanet Web Server creates a time-stamped access log file and rotation starts at server startup.

Once the rotation starts, iPlanet Web Server creates a new time stamped log file when there is a request that needs to be logged to the access log file and it occurs after the prior-scheduled "next rotate time".

NOTE You should archive the server logs before running the log analyzer.

To archive log files and to specify whether to use the Internal daemon method or the cron based method, use the Archive Log Files page in the Server Manager.

Setting Log Preferences

During installation, an access log file named `access` was created for the server. You can customize access logging for any resource by specifying whether to log accesses, what format to use for logging, and whether the server should spend time looking up the domain names of clients when they access a resource.

Server access logs can be in Common Logfile Format or flexible log formator your own customizable format. The Common Logfile Format is a commonly supported format that provides a fixed amount of information about the server. The flexible log format allows you to choose (from iPlanet Web Server) what to log. A customizable format uses parameter blocks that you specify to control what gets logged. For a list of customizable format parameters, see the *NSAPI Programmer's Guide for iPlanet Web Server.*

Once an access log for a resource has been created, you cannot change its format unless you archive it or create a new access log file for the resource.

You can specify logging preferences using The Log Preferences Page in the Server Manager, or you can manually configure the following directives in the `obj.conf` file. In `obj.conf`, the server calls the function `flex-init` to initializes the flexible logging system and the function `flex-log` to record request-specific data in a flexible log format. To log requests using the common log file format, the server calls `init-clf` to initialize the Common Log subsystem which is used if `obj.conf`, and `common-log` to record request-specific data in the common log format (used by most HTTP servers).

For more information on the NSAPI logging functions, including valid directives and parameters, see the *NSAPI Programmer's Guide for iPlanet Web Server.*

Easy Cookie Logging

In previous versions of iPlanet Web Server, if you want to log the value of a specific cookie, you had to write a plugin API that extracted the cookie's value out of the "`Cookie`" header sent by the client, insert this value as a new variable to the request's `pblock`, and log that new variable.

iPlanet Web Server has an easy way to log a specific cookie using the flexlog facility. Add "`Req->headers.cookie.`*`cookie_name`*" to the line that initializes the `felxlog` subsystem in the configuration file `obj.conf`. This logs the value of the cookie variable *`cookie_name`* if the cookie variable is present in the request's headers, and logs "-" if it is not present.

Relaxed Logging

There is an unpleasant side effect to logging a variable other than the following standard variables: `Status`, `Content-Length`, `Client-Host`, `Full-Request`, `Method`, `Protocol`, `Query-String`, `URI`, `Referer`, `User-Agent`, `Authorization`, and `Auth-User`. Because other variables cannot be provided by the static file accelerator cache, the accelerator cache will not be used at all. Therefore performance numbers will decrease significantly for requests that would typically benefit from the accelerator, such as static files and images.

iPlanet Web Server eases the requirements of the log subsystem. Adding "`relaxed.`*`logname`*`=`*`true`*" to the "`flex-init`" line in `obj.conf` allows you to log variables outside of the standard set and still use the accelerator cache. If the accelerator is used, unavailable variables are logged as "`-`". The server does not use the accelerator for dynamic content such as CGI scrips or SHTML pages, so all the variables are always logged correctly for these requests.

Flushing the Log Buffer

You can flush the log buffer instantaneously or at a schedule other than the default time by setting buffer-flush in the `logbufInit` function in `obj.conf`. The value should be in milliseconds and greater that 0. For example:

```
int logbuf_init(pblock *args) {
    char err[MAGNUS_ERROR_LEN];
    char *t;

    logbuf_size = 0;
    logbuf_flush = DEFAULT_LOGBUF_FLUSH;
    if((t = pblock_findval("buffer-size", args)) ) {
    logbuf_size = atoi(t);
    if(logbuf_size < 0) {
        util_snprintf(err, MAGNUS_ERROR_LEN, "buffer size of %d is invalid",
logbuf_size);
        pblock_nvinsert("error", err, args);
        return REQ_ABORTED;
    }
    if(logbuf_size < (REQ_MAX_LINE * 2))
        logbuf_size = REQ_MAX_LINE * 2;
    }
    if( (t = ("buffer-flush", args)) ) {
        logbuf_flush = atoi(t) * 1000;
        if(logbuf_flush < 0) {
            util_snprintf(err, MAGNUS_ERROR_LEN,"flush rate of %d seconds is
invalid", logbuf_flush);
            pblock_nvinsert("error", err, args);
            return REQ_ABORTED;
        }
    }
    }
    return REQ_PROCEED;
}
```

Running the Log Analyzer

The *server-install*/extras/log_anly directory contains the log analysis tool that runs through the Server Manager. This log analyzer analyzes files in common log format only. The HTML document in the log_anly directory that explains the tool's parameters. The *server-install*/extras/flex_anlg directory contains the command-line log analyzer for the flexible log file format. However, Server Manager defaults to using the flexible log file reporting tool, regardless of whether you've selected common or flexible log file format.

Use the log analyzer to generate statistics about your server, such as a summary of activity, most commonly accessed URLs, times during the day when the server is accessed most frequently, and so on. You can run the log analyzer from iPlanet Web Server or the command line.

NOTE Before running the log analyzer, you should archive the server logs. For more information about archiving server logs, see "Archiving Log Files" on page 153.

The following section contains instructions for running the log analyzer from the command line. To run the log analyzer from the Server Manager, see the Generate Report page in the online help.

To analyze access log files from the command line, run the tool, `flexanlg`, which is in the directory *`server-install`*`/extras/flex_anlg`.

To run `flexanlg`, type the following command and options at the command prompt:

```
flexanlg [ -P ] [-n name] [-x] [-r] [-p order] [-i file]* [ -m metafile ]*
[ o file][ c opts] [-t opts] [-l opts]
```

The following describes the syntax. (You can get this information online by typing Using Performance Monitor (Windows NT)

```
flexanlg -h.):
-P: proxy log format                                    Default: no
-n servername: The name of the server
-x : Output in HTML                                     Default: no
-r : Resolve IP addresses to hostnames                  Default: no
-p [c,t,l]: Output order (counts, time stats, lists)  Default: ctl
-i filename: Input log file(s)                          Default: none
-o filename: Output log file                            Default: stdout
-m filename: Meta file(s)                               Default: none
-c [h,n,r,f,e,u,o,k,c,z]: Count these item(s) -       Default: hnreuokc
    h: total hits
    n: 304 Not Modified status codes (Use Local Copy)
    r: 302 Found status codes (Redirects)
    f: 404 Not Found status codes (Document Not Found)
    e: 500 Server Error status codes (Misconfiguration)
    u: total unique URL's
    o: total unique hosts
    k: total kilobytes transferred
    c: total kilobytes saved by caches
    z: Do not count any items.
-t [sx,mx,hx, xx,z]: Find general stats - Default:s5m5h24x10
    s(number): Find top (number) seconds of log
    m(number): Find top (number) minutes of log
    h(number): Find top (number) hours of log
    u(number): Find top (number) users of log
    a(number): Find top (number) user agents of log
    r(number): Find top (number) referers of log
    x(number): Find top (number) for miscellaneous keywords
    z: Do not find any general stats.
-l [cx,hx]: Make a list of - Default: c+3h5
    c(x,+x): Most commonly accessed URLs
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    h(x,+x): Hosts (or IP addresses) most often accessing your server
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    z: Do not make any lists
```

You can also monitor your server by using the Windows NT Performance Monitor, which graphically shows information about your computer's performance. Use Performance Monitor to see performance data about iPlanet Web Server.

To monitor iPlanet Web Server performance using Performance Monitor:

1. From the Start menu, select Programs and then Administrative Tools. Choose Performance Monitor in the Administrative Tools program group.
2. Choose **Add to Chart** from the Edit menu.

   The Add to Chart window appears.
3. If the iPlanet Web Server you want to monitor is on a remote system, type its name in the **Computer** field.
4. Choose Netscape Server from the **Object** pull-down menu.
5. Choose the instance you want to monitor.

   If you have multiple servers installed, you can choose multiple instances.
6. Choose the counters you want to see in your chart.

   The following counters are available:

   - Server Conn/sec—Rate of incoming connections per second.
   - Server Throughput (Kb/sec)—Rate of outgoing data from the server.
   - Server Total Bytes—Total bytes sent by the server.
   - Server Total Errors—Number of errors requests handled by the server.
   - Server Total Requests—Total requests handled by the server.
   - Status: 403 Forbidden—Number of "Forbidden" requests.
   - Status: 200 level—Number of 200-level status requests handled by the server.
   - Status: 200 OK—Number of "OK" requests.
   - Status: 300 level—Number of 300-level status requests handled by the server.
   - Status: 302 Moved Temporarily—Number of "Moved Temporarily" requests.
   - Status: 304 Not Modified—Number of "Not modified" requests.
   - Status: 400 level—Number of 400-level status requests handled by the server.
   - Status: 401 Unauthorized—Number of "Unauthorized" requests.
   - Status: 500 level—Number of 500-level status requests handled by the server.

To see the counter definition online, click **Explain**.

7. Click **Add**.
8. To monitor other computers or objects, repeat steps 1 through 7 for each item you want to monitor.
9. Click **Done**.

   The Performance Monitor displays a chart with your selected items. A legend at the bottom of the page displays your choices.

For more information about Performance Monitor, see the documentation for your operating system.

Viewing Events (Windows NT)

In addition to logging errors to the server error log (see “Viewing the Error Log File” on page 151), iPlanet Web Server logs severe system errors to the Event Viewer. The Event Viewer lets you monitor events on your system. Use the Event Viewer to see errors resulting from fundamental configuration problems, which can occur before the error log can be opened.

To use the Event Viewer:

1. From the Start menu, select Programs and then Administrative Tools. Choose Event Viewer in the Administrative Tools program group.
2. Choose **Application** from the **Log** menu.

   The Application log appears in the Event Viewer. Errors from iPlanet Web Server has a source label of `https-`*`serverid`* or `WebServer4.1`.
3. Choose **Find** from the View menu to search for one of these labels in the log. Choose **Refresh** from the View menu to see updated log entries.

For more information about Event Viewer, consult your system documentation.

Chapter 8

Performance Configuration

Because the iPlanet Web Server, FastTrack Edition is not intended to run under load, there are limits on the performance tuning options. Though this section describes some of the parameters that affect performance, you can do very little tuning with this server. For best results, use iPlanet Web Server, Enterprise Edition.

This chapter includes the following section:

- Server Tuning Limits

Server Tuning Limits

Performance for iPlanet Web Server, FastTrack Edition has the following limits on its performance. If you attempt to set the value for one of these parameters higher than the maximums listed here, the value is set to the limit listed below.

Non-SSL Servers

- Maximum of 16 KeepAlive sessions.
- Maximum of 16 threads.
- Maximum of 4 minimum threads (the minimum limit is a goal for how many threads the server attempts to keep in the `WaitingThreads` state).
- Maximum of 64 files in the file cache.

SSL Servers

- Maximum of 5 KeepAlive sessions.

- Maximum of 6 threads.
- Maximum of 2 minimum threads (the minimum limit is a goal for how many threads the server attempts to keep in the `WaitingThreads` state).
- Maximum of 64 files in the file cache.

Part 4

Using Programs and Objects

Chapter 9

Extending Your Server With Programs

This chapter discusses how to install programs on the iPlanet Web Server that dynamically generate HTML pages in response to requests from clients. These programs are known as *server-side applications*. (*Client-side applications*, which are downloaded to the client, run on the client machine.)

This chapter includes the following sections:

- Overview of Server-Side Programs
- Java Servlets and JavaServer Pages (JSP)
- Installing CGI Programs
- Installing Windows NT CGI Programs
- Installing Shell CGI Programs for Windows NT
- Using the Query Handler
- Server-Side JavaScript Programs
- Enabling WAI Services

Overview of Server-Side Programs

Java servlets, JavaScript applications, and CGI programs have different strengths and uses. The following list illustrates the differences between these server-side programs:

- Java servlets are written in Java, which is a full-featured programing language for creating network applications.

- **CGI (*Common Gateway Interface*)** programs can be written in C, Perl, or other programming languages. All CGI programs have a standard way of passing information between clients and servers.

CAUTION Note that you must enable cookies in your browser to run CGI programs.

- JavaScript applications are written in JavaScript, an object-based scripting language. JavaScript is easier to learn than languages such as Java and C and it lends itself to rapid application development.

NOTE iPlanet Web Server 4.1 does not support server-side Java applets.

Types of Server-Side Applications That Run on the Server

The iPlanet Web Server can run the following types of server-side applications to dynamically generate content:

- Java servlets
- CGI programs
- JavaScript applications

The iPlanet Web Server can also run programs that extend or modify the behavior of the server itself. These programs, known as plug-ins, are written using the Netscape Server Application Programming Interface (NSAPI). For information about writing and installing plug-in programs, see the *NSAPI Programmer's Guide for iPlanet Web Server*.

How Server-Side Applications Are Installed on the Server

Each type of program is installed onto the server differently. The following list summarizes the procedures:

- For Java servlets, you can configure your server to recognize all files in certain directories as servlets, or you can set up virtual pathnames for servlets, or both. For more information, see “What the Server Needs to Run Servlets and JSPs.”
- For CGI programs, you can configure your server to recognize all files with certain filename extensions, or all files in specified directories as CGI programs, or both. For more information, see “Installing CGI Programs,” “Installing Windows NT CGI Programs,” and “Installing Shell CGI Programs for Windows NT.”
- For JavaScript applications, you must check in each application individually through the Application Manager, which you can access from iPlanet Web Server. For more information, see “Installing Server-Side JavaScript Applications.”

These installation procedures are described in the following sections.

Java Servlets and JavaServer Pages (JSP)

This section discusses how to install and use Java Servlets and JavaServer Pages on iPlanet Web Server.

This section describes the following topics:

- Overview of Servlets and JavaServer Pages
- What the Server Needs to Run Servlets and JSPs
- Enabling Servlets and JSP
- Making JSPs Available to Clients
- Making Servlets Available to Clients
- Specifying Servlet Directories
- Configuring Global Attributes
- Configuring Servlet Attributes
- Configuring Servlet Virtual Path Translations
- Configuring JRE/JDK Paths
- Configuring JVM Attributes
- Deleting Version Files

Overview of Servlets and JavaServer Pages

iPlanet Web Server supports Java servlets and JavaServer Pages (JSP).

Java servlets are server-side Java programs that can be used to extend the functionality of a web server in much the same way as CGI programs do. Servlets can be thought of as applets that run on the server side without an interface. Servlets are invoked through URL invocation. iPlanet Web Server includes support for JavaSoft's Servlet API at the level of the Java Servlet Development Kit (JSDK) 2.2.1PR.

To develop servlets, use Sun Microsystems' Java Servlet API. For information about using the Java Servlet API, see the documentation provided by Sun Microsystems at:

```
http://www.javasoft.com/products/servlet/2.2/javadoc/index.html
```

For information about developing servlets for use with iPlanet Web Server, see *Programmer's Guide to Servlets in iPlanet Web Server*.

A JavaServer Page (JSP) is a page, much like an HTML page, that can be viewed in a web browser. However, as well as containing HTML tags, it can include a set of JSP tags that extend the ability of the web page designer to incorporate dynamic content in a page. These tags provide functionality such as displaying property values and using simple conditionals. iPlanet Web Server supports JavaServer Pages (JSP) to the level of JSP API 1.0 compliance.

For information about creating JavaServer Pages, see Sun Microsystem's JavaServer Pages web page at:

```
http://www.javasoft.com/products/jsp/index.html
```

What the Server Needs to Run Servlets and JSPs

iPlanet Web Server includes the Java Runtime Environment (JRE) but not the Java Development Kit (JDK). The server can run servlets using the JRE, but it needs the JDK to run JSP. If you want to run JSP, you must tell iPlanet Web Server to use a custom JDK.

iPlanet Web Server 4.1 requires you to use official versions of JDK, with different platforms requiring different versions, as summarized in Table 9-1.

Table 9-1 Supported JavaSoft JDK Versions by Platform

Platform	JRE/JDK Version
Solaris Sparc	1.2.2_01
Windows NT	1.2.2_01
HPUX	1.2.2_02
AIX	1.2.1
Compaq	1.2.2-3
Linux	1.2.2RC4
IRIX	1.2.1

Check the *iPlanet Web Server Installation and Migration Guide* and the latest *Release Notes* for updates on required JDK versions.

JDK 1.2 (and other JDK versions) are available from Sun Microsystems at:

```
http://www.javasoft.com/products/jdk/1.2/
```

You can specify the path to the JDK in either of the following ways:

- You can specify the path during the server installation process.

  When you install iPlanet Web Server, one of the dialog boxes in the installation process asks if you want to use a custom Java Development Kit (JDK), and if so, you can specify the path to it.

- You can specify it after the server is installed.

  To specify the path to the JDK, switch to the Web Server Administration Server, select the **Global Settings** tab, and use the **Configure JRE/JDK Paths** page. You can also change the path to the JDK in this page.

Whether you specify the path to the JDK during installation or later, the path is the folder in which you installed the JDK.

Enabling Servlets and JSP

Before iPlanet Web Server can run servlets, the servlet engine must be enabled. Before the server can serve JSP, the servlet engine must be enabled and JSP must be enabled. (The server cannot serve JSP if servlets are not enabled.)

To enable and disable servlets and JSP in iPlanet Web Server, use the Enable / Disable Servlets / JSP page in the Servlets tab in the Server Manager. This page lets you enable or disable servlets and also enable or disable JSP. If servlets are disabled, you cannot enable JSP.

If servlets are enabled, JSP can be enabled or disabled. However, if you disable servlets, JSP is automatically also disabled. In this case, if you enable servlets later, you must re-enable JSP also if desired.

You can also define a thread pool to be used for servlets. For any server subsystem you can specify which thread pool the servlet's going to run on. For more information about thread pools, see "Adding and Using Thread Pools," on page 132 in , "Configuring Server Preferences."

Making JSPs Available to Clients

You can install JSP files simply by putting them in any directory in or under the document root—you do not need to do anything special to install JSP files—so long as the following conditions are true:

- iPlanet Web Server has been instructed to use the JDK.
- Both servlets and JSP are enabled in the server.

Making Servlets Available to Clients

For servlets, you have a choice of two ways to make a servlet accessible to clients:

- Put the servlet class file in a directory that has been registered with iPlanet Web Server as a servlet directory. For more information, see "Specifying Servlet Directories."
- Define a servlet virtual path translation for the servlet. In this case, the servlet class can be located anywhere in the file system or even reside on a remote machine. For more information, see "Configuring Servlet Virtual Path Translations," on page 175.

You can choose both these options. You can specify a servlet directory and define servlet virtual path translations for servlets outside the servlet directory.

Specifying Servlet Directories

One of the ways to make a servlet accessible to clients is to put it into a directory that has been registered with iPlanet Web Server as a servlet directory. Servlets in registered servlet directories are dynamically loaded when needed. The server monitors the servlet files and automatically reloads them on the fly as they change.

For example, if the `SimpleServlet.class` servlet is in the `servlet` subdirectory of the server's document root directory, you can invoke the servlet by pointing the web browser to:

```
http://your_server/servlet/SimpleServlet
```

You can register any number of servlet directories for iPlanet Web Server. Initially, the web server has a single servlet directory per server instance, which is *server_id*`/docs/servlet/`.

iPlanet Web Server expects all files in a registered servlet directory to be servlets. Any files, including applets, in that directory that have the `.class` extension will be treated as servlets. iPlanet Web Server does not correctly serve other files, such as HTML files or JSPs, that reside in that directory.

The server can have multiple servlet directories, all of which must reside below the primary document directory in the directory hierarchy. You can map servlet directories to virtual directories if desired. For example, you could specify that `http://my_domain.com/products/` invokes servlets in the directory *server_id*`/docs/servlet/january/products/servlets/`.

To register servlet directories and to specify their URL prefixes (virtual or not), use the Servlet Directory page in the Servlets tab of the Server Manager. Set the following fields:

URL Prefix. The prefix for accessing the directory. For example, if you want the logical URL `http://`*servername*`/plans` to translate to the directory `d:/netscape/server4/docs/plans` then enter `plans` in the URL Prefix field.

Servlet Directory. The absolute pathname to the directory to be registered as a servlet directory, for example, `d:/netscape/server4/docs/plans`. iPlanet Web Server treats all files in the directory as servlets.

NOTE By default, URLs that are redirected are always escaped. To prevent this, add `escape="no"`. For example:

```
NameTrans fn="redirect" from="/foobar"
url-prefix="index.html" escape="no"
```

Configuring Global Attributes

You can set some global attributes for servlets, including:

- Servlets to run when the server starts up.
- The Session Manager to be used by servlets.
- The Session Manager Args (arguments) to be used by servlets.
- The amount of time the server waits before reloading servlets if they have changed.

To set the global attributes, use the "Configure Global Servlet Attributes" page in the Servlets tab of the Server Manager. Set the following fields:

Startup Servlets. In this field, enter the name of servlets to be loaded when the web server starts up. You do not need to include the `.class` extension.

Session Manager. If you have a session manager class, enter its value here.

Session Manager Args. If you want to specify session manager arguments, enter the values here. Separate multiple *name=value* parameters with a comma. Input must be in the format *name=value, name2=value2*, and so on. For more information, see Appendix A, "Session Managers," in *Programmer's Guide to Servlets for iPlanet Web Server*.

Reload Interval. This is the interval in seconds the server waits before reloading servlets and JavaServer Pages if they have changed. Specify an integer value here between 0 and 600 inclusive. The default value is 5 seconds.

Configuring Servlet Attributes

If you want to specify input parameters, class paths, or virtual translations for a servlet, you need to individually configure the servlet. Do this in the Configure Servlet Attributes page of the Servlets tag in the Server Manager.

NOTE	When you configure a servlet through the Configure Servlet Attributes page, the servlet is automatically added to the `servlets.properties` file in iPlanet Web Server's `config` directory.

In this page, you can specify the following fields:

Choose Servlet. Specifies the servlet to edit. If no virtual paths have previously been set up, the list is empty. Upon choosing the servlet from this drop-down list, the servlet's information is displayed in the page. (Ignore this field if you are adding a new virtual path entry).

Servlet Name. Specifies an identifier for the servlet. This identifier is used internally by iPlanet Web Server; it is not used in the URL for accessing the servlet. This identifier can be the same name or a different name than the servlet class name.

Servlet Code (class name). Specifies the name of the servlet's main class file. The `.class` extension is optional. Do not specify any directories in this field.

Servlet Classpath. This is the absolute pathname or URL to the directory or zip/jar file containing the servlet. The classpath can point anywhere in the file system. The servlet classpath may contain a directory, a `.jar` or `.zip` file, or a URL to a directory.(You cannot specify a URL as a classpath for a zip or jar file.) If the servlet classpath is not a registered servlet directory, you must additionally provide a servlet virtual path translation for it (as discussed in "Configuring Servlet Virtual Path Translations" on page 175) to make the servlet accessible to clients.

iPlanet Web Server supports the specification of multiple directories, jars, zips, and URLs in the servlet classpath.

Servlet Args. If the servlet takes additional parameters, enter them here. Separate multiple *name=value* parameters with a comma. Input must be in the format *name=value*, *name2=value2*`...`. For example, `arg1=45`, `arg2=online`, `arg3="quick shopping"`.

Configuring Servlet Virtual Path Translations

One way to make servlets available to clients is to put them in registered servlet directories. Another way is to define servlet virtual path translations for individual servlets. For example, you could specify that the URL:

```
http://my_domain.com/plans/plan1
```

invokes the servlet defined in

server_id`/docs/servlets/plans/releaseA/planP2Version1A.class`

You can set up servlet virtual path translations for servlets that reside anywhere, on a local or remote file system, or in or out of a registered servlet directory.

Before setting up a servlet virtual path translation, the servlet must have been configured in the Configure Servlet Attributes page of the Servlets tab in the Server Manager, as discussed in "Configuring Servlet Attributes."

To specify a servlet virtual translation path, use the Configure Servlet Virtual Path Translation page in the Servlets tab in the Server Manager. This page has the following fields:

Choose Virtual Path Entry. Specifies a virtual path to modify. If no virtual paths have previously been set up, the list is empty. Upon choosing the virtual path from this drop-down list, the information for the virtual path is displayed in the page. Ignore this field if you are adding a new virtual path entry.

Virtual Path. If you are adding a new path, enter it here. (It's OK to overwrite existing virtual path names.) If you are modifying a path, select the appropriate path from the Choose Virtual Path Entry list to make the path name show up in this field.

The value to enter here is the URL for the virtual path without the `http://`*servername* part. For example, if you want the virtual path to be `http://`**servername**`/virtual/tracker`, enter `/virtual/tracker`.

Servlet Name. Specifies an identifier for the servlet, as entered in the Configure Servlet Attributes page. It's OK if the servlet identifier has not been specified already, but it must be specified before the virtual path will work.

Configuring JRE/JDK Paths

When you install iPlanet Web Server, you can choose to install the Java Runtime Environment (JRE) or you can specify a path to the Java Development Kit (JDK).

The server can run servlets using the JRE, but it needs the JDK to run JSP. The JDK is not bundled with iPlanet Web Server, but you can download it for free from Sun Microsystems at:

```
http://www.javasoft.com/products/jdk/1.2/
```

Regardless of whether you choose to install the JRE or specify a path to the JDK during installation, you can tell the iPlanet Web Server to switch to using either the JRE or JDK at any time. Switch to the Web Server Administration Server, select the **Global Settings** tab, and use the **Configure JRE/JDK Paths** page. You can also change the path to the JDK in this page.

Supply values for the following fields if you select the JDK radio button:

JDK Path. Enter the path for the JDK. This is the directory where you installed the JDK.

JDK Runtime Libpath. Enter the runtime library path for the JDK.

JDK Runtime Classpath. The class path includes the paths to the directories and jar files needed to run the servlet engine, the servlet examples, and any other paths needed by servlets that you add. Values are separated by semicolons. You can add new values to the existing class path, but don't delete the existing value since it includes paths that are essential for servlet operation.

Supply values for the following fields if you select the JRE radio button:

JRE Path. Enter the path for the JRE. This is the directory where you installed the JRE.

JRE Runtime Libpath. Enter the runtime library path for the JRE.

NOTE	If you are not sure of the JDK runtime libpath, the JDK runtime classpath, or the JRE runtime libpath, leave these fields blank to tell the server to use default paths.

Configuring JVM Attributes

You can configure attributes for the Java Virtual Machine (JVM) in the Configure JVM page of the Servlets tab in the Server Manager.

For more information on these options, see *Programmer's Guide to iPlanet Web Server*.

Deleting Version Files

The server uses two directories to cache information for JavaServer Pages (JSP) and servlets:

- `ClassCache`

  When the server serves a JSP page, it creates a `.java` and a `.class` file associated with the JSP and stores them in the JSP class cache, in a directory structure under the `ClassCache` directory.

- `SessionData`

  If the server uses the `MMappedSessionManager` session manager, it stores persistent session information in the `SessionData` directory.

Each cache has a `version` file containing a version number that the server uses to determine the structure of the directories and files in the caches. You can clean out the caches by simply deleting the version file.

When the server starts up, if it does not find the version files, it deletes the directory structure for the corresponding caches and re-creates the version files. Next time the server serves a JSP page, it recreates the JSP class cache. The next time the server serves a JSP page or servlet while using `MMappedSessionManager` session manager, it recreates the session data cache.

If a future upgrade of the server uses a different format for the caches, the server will check the number in the version file and clean up the caches if the version number is not correct.

The Delete Version Files page allows you to delete the files that contain the version number for the JavaServer Pages class cache and the session data cache. This page has the following fields:

Delete the SessionData Version File . Deletes the version file for the session data. When you apply this change, the version file is deleted immediately. The next time the server starts up, it deletes the session data cache and recreates the version file. The next time the server serves a JSP page or servlet while using the `MMappedSessionManager` session manager, it recreates the session data cache.

Delete the ClassCache Version File . Deletes the class cache version file for JSP pages. When you apply this change, the version file is deleted immediately. The next time the server starts up, it deletes the JSP class cache and recreates the version file. The next time the server serves a JSP page, it recreates the class cache.

Installing CGI Programs

This section discusses how to install CGI programs. It has the following sub-sections:

- Overview of CGI
- Specifying a CGI Directory
- Specifying CGI as a File Type
- Downloading Executable Files

In addition, the following sections discuss how to install Windows NT-specific CGI programs:

- Installing Windows NT CGI Programs
- Installing Shell CGI Programs for Windows NT

Overview of CGI

Common Gateway Interface (CGI) programs can be defined with any number of programming languages. On a Unix/Linux machine, you're likely to find CGI programs written as Bourne shell or Perl scripts.

NOTE Under Unix/Linux, there are extra `CGIStub` processes running that the server uses to aid in CGI execution. These processes are created only during the first access to a CGI. Their number varies depending upon the CGI load on the server. Do not kill these CGIStub processes. They disappear when the server is stopped.

On a Windows NT computer, you might find CGI programs written in C++ or batch files. For Windows NT, CGI programs written in a Windows-based programming language such as Visual Basic use a different mechanism to operate with the server. They are called Windows NT CGI programs. See "Installing Windows NT CGI Programs" on page 183 for information about Windows NT CGI.

NOTE In order to run the command-line utilities, you need to manually set the `Path` variable to include *server_root*`/bin/https/bin`.

Regardless of the programming language, all CGI programs accept and return data in the same manner. For information about writing CGI programs, see the following sources of information:

- *Programmer's Guide for iPlanet Web Server*
- *The Common Gateway Interface* at:

  `http://hoohoo.ncsa.uiuc.edu/cgi/overview.html`
- Articles about CGI available on the online documentation web site at:

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

There are two ways to store CGI programs on your server machine:

- Specify a directory that contains only CGI programs. All files are run as programs regardless of the file extensions.
- Specify that CGI programs are all a certain file type. That is, they all use the file extensions `.cgi`, `.exe`, or `.bat`. The programs can be located in any directory in or under the document root directory.

You can enable both options at the same time if desired.

There are benefits to either implementation. If you want to allow only a specific set of users to add CGI programs, keep the CGI programs in specified directories and restrict access to those directories. If you want to allow anyone who can add HTML files to be able to add CGI programs, use the file type alternative. Users can keep their CGI files in the same directories as their HTML files.

If you choose the directory option, your server attempts to interpret any file in that directory as a CGI program. By the same token, if you choose the file type option, your server attempts to process any files with the file extensions `.cgi`, `.exe`, or `.bat` as CGI programs. If a file has one of these extensions but is not a CGI program, an error occurs when a user attempts to access it.

CAUTION Note that you must enable cookies in your browser to run CGI programs.

NOTE By default, the file extensions for CGI programs are `.cgi`, `.exe` and `.bat`. However, you can change which extensions indicate CGI programs by modifying the MIME types file. You can do this by choosing the Server Preferences tab and clicking the MIME Types link.

Specifying a CGI Directory

To specify a CGI-only directory, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **CGI Directory** link.

   The CGI Directory window appears.

3. In the URL Prefix field, type the URL prefix to use for this directory. That is, the text you type appears as the directory for the CGI programs in URLs.

   For example, if you type `cgi-bin` as the URL prefix, then all URLs to these CGI programs have the following structure:

   `http://`*`yourserver`*`.`*`domain`*`.com/cgi-bin/`*`program-name`*

NOTE The URL prefix you specify can be different from the real CGI directory you specify in the next step.

4. In the **CGI Directory** text field, type the location of the directory as an absolute path. Note that this directory doesn't have to be under your document root. This is the reason that you need to specify a URL prefix in the previous step.
5. Click OK.
6. Save and apply your changes.

To remove an existing CGI directory, click that directory's Remove button in the CGI Directory form. To change the URL prefix or CGI directory of an existing directory, click that directory's Edit button.

Copy your CGI programs into the directories you've specified. Remember that any files in those directories will be processed as a CGI file so don't put HTML files in your CGI directory.

Configuring a Unique CGI Directory for Each Software Virtual Server

You can manually configure a unique CGI directory for each software virtual server by manually editing the `obj.conf` file:

```
<Object name="default">
    .
    .
    .
<Client urlhost="www.yourvirtualserver.chm">
 NameTrans fn="pfx2dir" from="/cgi-bin"
 dir="/dir/for/virtual/server/cgi-bin/" name="cgi"
 ...
 </Client>
```

Note that you can not use the Administration Server to accomplish this task.

Specifying CGI as a File Type

To specify CGI programs as a file type, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **CGI File Type** link.

   The CGI as a File Type window appears.
3. From the Resource Picker, choose the resource you want this change to apply to.
4. Click the **Yes** radio button under Activate CGI as a File Type.
5. Click OK.
6. Save and apply your changes.

The CGI files must have the file extensions `.bat`, `.exe`, or `.cgi`. Any non-CGI files with those extensions are processed by your server as CGI files, causing errors.

Downloading Executable Files

If you're using `.exe` as a CGI file type, you cannot download `.exe` files as executables.

One solution to this problem is to compress the executable files that you want users to be able to download, so that the extension is not `.exe`. This solution has the added benefit of making the download time shorter.

Another possible solution is to remove `.exe` as a file extension from the `magnus-internal/cgi` type and add it instead to the `application/octet-stream` type (the MIME type for normal downloadable files). You can do this through the Server Manager, by choosing the Server Preferences tab and clicking the MIME Types link. However, the disadvantage to this method is that after making this change you cannot use `.exe` files as CGI programs.

Another solution is to edit your server's `obj.conf` file to set up a download directory, where any file in the directory is downloaded automatically. The rest of the server won't be affected. For directions on setting up this directory, see the technical note at:

```
http://help.netscape.com/kb/server/960513-130.html
```

Installing Windows NT CGI Programs

This section discusses how to install Windows NT CGI Programs. The following topics are included in this section:

- Overview of Windows NT CGI Programs
- Specifying a Windows NT CGI Directory
- Specifying Windows NT CGI as a File Type

Overview of Windows NT CGI Programs

Windows NT CGI programs are handled much as other CGI programs. You specify a directory that contains only Windows NT CGI programs, or you specify that all Windows NT CGI programs have the same file extension. Note that like other CGI programs, you can use both methods at the same time if you want to. For example, you can create a directory for all your Windows NT CGI programs, and specify a Windows NT CGI file extension.

Although Windows NT CGI programs behave like regular CGI programs, your server processes the actual programs slightly differently. Therefore, you need to specify different directories for Windows NT CGI programs. If you enable the Windows NT CGI file type, it uses the file extension `.wcg`.

iPlanet Web Servers support the Windows NT CGI 1.3a informal specification, with the following differences:

- The following keywords have been added to the [CGI] section to support security methods:
  - **HTTPS**: its value is on or off, depending on whether the transaction is conducted through SSL.
  - **HTTPS Keysize**: when HTTPS is on, this value reports the number of bits in the session key used for encryption.
  - **HTTPS Secret Keysize**: when HTTPS is on, this value reports the number of bits used to generate the server's private key.
- The keyword Document Root in the [CGI] section might not refer to the expected document root because the server does not have a single document root. The directory returned in this variable is the root directory for the Windows NT CGI program.
- The keyword Server Admin in the [CGI] section is not supported.

- The keyword Authentication Realm in the [CGI] section is not supported.
- Forms sent with multi-part/form-data encoding are not supported.

Specifying a Windows NT CGI Directory

To specify a Windows NT CGI-only directory:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **Win CGI Directory** link.

   The WinCGI Directory window appears.
3. In the **URL Prefix** text field, enter the URL prefix you want to use for this directory.

   That is, the text you type appears as the directory for the Windows NT CGI programs in URLs. For example, if you type `wcgi-programs` as the URL prefix, then all URLs to these Windows NT CGI programs have the following structure:

   http://*yourserver.domain*.com/wcgi-programs/program-name

NOTE The URL prefix you specify can be different from the real Windows NT CGI directory you specify in Step 5.

4. Choose whether you want to enable script tracing.

   Click the Yes or No radio button under “Enable Script Tracing?”.

   CGI parameters are passed from the server to Windows NT CGI programs through files, which the server normally deletes after the Windows NT CGI program finishes execution. If you enable script tracing, these files are retained in a `/temp` directory or wherever the environment variables TMP and TEMP are pointing. Also, any window that the Windows NT CGI program brings up is shown when script tracing is enabled.
5. In the **WinCGI Directory** field, enter the location of the directory as an absolute path.

   Note that this directory doesn’t have to be under your document root. This is the reason that you need to specify a URL prefix in Step 3.
6. Click OK.

7. Save and apply your changes.

To remove an existing Windows NT CGI directory, click that directory's Remove button in the Windows NT CGI Directory form. To change the URL prefix or Windows NT CGI directory of an existing directory, click that directory's Edit button.

Copy your Windows NT CGI programs into the directories you've specified. Remember that any file in those directories is processed as a Windows NT CGI file.

Specifying Windows NT CGI as a File Type

To specify a file extension for Windows NT CGI files, perform the following steps:

1. From the Server Manager, choose the **Server Preferences** tab.
2. Click the **MIME Types** link.

   The Global MIME Types window appears. For more information on the Global MIME Types, see the "Specifying a Default MIME Type," on page 213 in , "Managing Server Content."
3. Add a new MIME type with the following settings:
   - Type: `type`
   - Content type: `magnus-internal/wincgi`.
   - File Suffix: Enter the file suffixes that you want the server to associate with Windows NT CGI. If you activated CGI, WinCGI, and shell CGI file types, you must specify a different suffix for each type of CGI. For example, you can't use the suffix `.exe` for both a CGI program and a shell CGI program. If you need to, you can edit the other MIME type fields on the page so that the suffixes are unique.
4. Click the **New Type** button.
5. Save and apply your changes.

Installing Shell CGI Programs for Windows NT

This section discusses how to install Shell CGI Programs for Windows NT. The following topics are included in this section:

- Overview of Shell CGI Programs for Windows NT

- Specifying a Shell CGI Directory (Windows NT)
- Specifying Shell CGI as a File Type (Windows NT)

Overview of Shell CGI Programs for Windows NT

Shell CGI is a server configuration that lets you run CGI applications using the file associations set in Windows NT.

For example, if the server gets a request for a shell CGI file called `hello.pl`, the server uses the Windows NT file associations to run the file using the program associated with the `.pl` extension. If the `.pl` extension is associated with the program `C:\bin\perl.exe`, the server attempts to execute the `hello.pl` file as follows:

```
c:\bin\perl.exe hello.pl
```

The easiest way to configure shell CGI is to create a directory in your server's document root that contains only shell CGI files. However, you can also configure the server to associate specific file extensions with shell CGI by editing MIME types from the iPlanet Web Server.

NOTE For information on setting Windows NT file extensions, see your Windows NT documentation.

Specifying a Shell CGI Directory (Windows NT)

To create a directory for your shell CGI files, perform the following steps:

1. Create the shell directory on your computer. This directory doesn't have to be a subdirectory of your document root directory.
2. From the Server Manager, choose the **Programs** tab.
3. Click the **Shell CGI Directory** link.

   The Shell CGI window appears.
4. In the **URL Prefix** field, enter the URL prefix you want to associate with your shell CGI directory.

For example, suppose you store all shell CGI files in a directory called `C:/docs/programs/cgi/shell-cgi`, but you want users to see the directory as `http://www.`*yourserver*`.com/shell/`. In this case, you would type `shell` as the URL prefix.

5. In the **Shell CGI Directory** field, enter the absolute path to the directory you created.

CAUTION The server must have read and execute permissions to this directory. For Windows NT, the user account the server runs as (for example, `LocalSystem`) must have rights to read and execute programs in the shell CGI directory.

6. Make sure that any files in the shell CGI directory also have file associations set in Windows NT. The server returns an error if it attempts to run a file that has no file-extension association.

Specifying Shell CGI as a File Type (Windows NT)

You can use the iPlanet Web Server's MIME Types window to associate a file extension with the shell CGI feature. This is different from creating an association in Windows NT.

To associate a file extension with the shell CGI feature in the server, for example, you can create an association for files with the `.pl` extension. When the server gets a request for a file with that extension, the server knows to treat the file as a shell CGI file by calling the executable associated in Windows NT with that file extension.

To associate a file extension as a shell CGI file, perform the following steps:

1. Create the shell directory on your computer. This directory doesn't have to be a subdirectory of your document root directory.
2. From the Server Manager, choose **Server Preferences**.
3. Click the **MIME Types** link.

   The Global MIME Types window appears. For more information on the Global MIME Types, see the "Specifying a Default MIME Type," on page 213 in Chapter 11, "Managing Server Content."

4. Add a new MIME type with these settings:
   - Type: `type`
   - Content type: `magnus-internal/shellcgi`.
   - File Suffix: Enter the file suffixes that you want the server to associate with shell CGI. If you activated CGI, WinCGI, and shell CGI file types, you must specify a different suffix for each type of CGI. For example, you can't use the suffix `.exe` for both a CGI program and a shell CGI program. If you need to, you can edit the other MIME type fields on the page so that the suffixes are unique.
5. Click the **New Type** button.
6. Save and apply your changes.

Using the Query Handler

NOTE The use of Query Handlers is outdated. Although iPlanet Web Server and Netscape Navigator clients still support it, it is rarely used. It is much more common for people to use forms in their HTML pages to submit queries.

You can specify a default query handler CGI program. A query handler processes text sent to it via the ISINDEX tag in an HTML file.

ISINDEX is similar to a form text field in that it creates a text field in the HTML page that can accept typed input. Unlike the information in a form text field, however, the information in the ISINDEX box is immediately submitted when the user presses Return. When you specify your default query handler, you tell your server to which program to direct the input. For an in-depth discussion of the ISINDEX tag, see an HTML reference manual.

To set a query handler, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **Query Handler** link.

   The Query Handler window appears.
3. Use the Resource Picker to select the resource you want to set a default query handler for.

If you choose a directory, the query handler you specify runs only when the server receives a URL for that directory or any file in that directory.

4. In the **Default Query Handler** field, enter the full path for the CGI program you want to use as the default for the resource you chose.
5. Click OK.
6. Save and apply your changes.

Server-Side JavaScript Programs

To allow iPlanet Web Server to run Server-Side JavaScript programs, you need to enable Server-Side JavaScript, which you can do in the Activate Server Side JavaScript page in the Programs tab of the Server Manager.

To install and manage Server-Side JavaScript programs on the server, use the JavaScript Application Manager.

The following topics are included in this section:

- Activating Server-Side JavaScript
- Running the Application Manager
- Securing the Application Manager
- Installing Server-Side JavaScript Applications
- Application URLs
- Controlling Access to a Server-Side JavaScript Application
- Modifying Installation Parameters
- Removing a Server-Side JavaScript Application
- Starting, Stopping, and Restarting a Server-Side JavaScript Application
- Running a Server-Side JavaScript Application
- Configuring Default Settings

For more information about writing JavaScript applications, see *Writing Server-Side JavaScript Applications* at:

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

Activating Server-Side JavaScript

To enable Server-Side JavaScript on iPlanet Web Server, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **Server Side Javascript** link.

   The Activate Server Side Javascript window appears.
3. Under **Activate the Server Side Javascript application environment**, click the **Yes** radio button.
4. If you want to require the administration server username and password before allowing access to the Application Manager, select the second Yes radio button.

   For more information on securing the application manager, see “Securing the Application Manager” on page 192.
5. Click OK.
6. Save and apply your changes.

Running the Application Manager

For applications written in Server-Side JavaScript, you can perform many administrative tasks with the Server-Side JavaScript Application Manager. Using the Application Manager, you can do the following:

- Install a new JavaScript application. You must add an application before users can run it.
- Modify any of the attributes of an installed application (for example, its default home page, path to the `.web` file, and type of client-object maintenance).
- Stop, start, and restart an installed application.
- Run and debug an active application.
- Remove an installed application.

To run the Application Manager, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **Server Side Javascript** link.

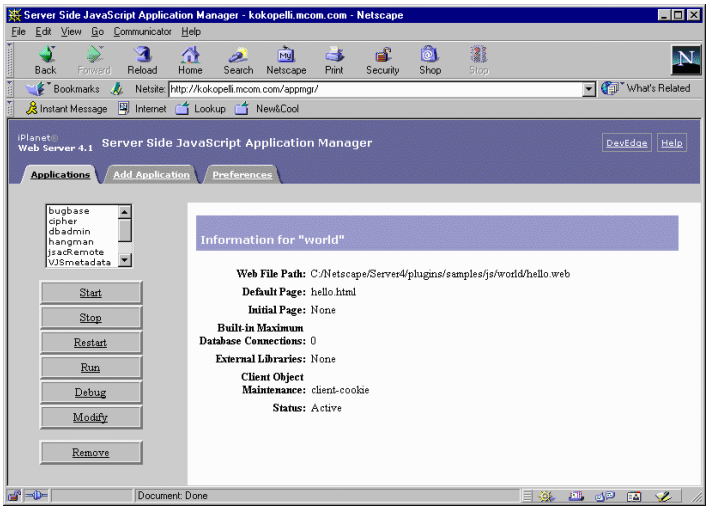
The Activate Server Side Javascript window appears.

3. Click the link to the Application Manager.
4. Click OK.

   You can also run the Application Manager by loading the following URL in Navigator: `http://`*server*`.`*domain*`/appmgr`.

   iPlanet Web Server displays the following page:

Figure 9-1 The Application Manager



The Application Manager displays all applications currently installed on the server in a scrolling list in the left frame.

5. Select an application by clicking its name in the scrolling list.

   For the selected application, the right frame displays the following information:

   - The application name at the top of the frame.
   - The path of the application `.web` file on the server. (The `.web` file is the compiled JavaScript application.)
   - The default and initial pages for the application.
   - The number of built-in database connections allowed.

- The external libraries used by the application (if any).
- The client object maintenance technique.
- The status of the application: active or stopped. Users can run only active applications. Stopped applications are not accessible.

6. Click the task buttons in the left frame to perform the indicated action on the selected application.

   For example, to modify the installation parameters of the selected application, click Modify.

7. Click the **Add Application** tab at the top to add a new JavaScript application.
8. Click the **Preferences** tab at the top to configure the default settings to use when adding a new application.

Securing the Application Manager

The Application Manager runs on iPlanet Web Server. It is installed into the `js/appmgr` directory. It can be accessed with the URL:

`http://`*`server`*`.`*`domain`*`:port/appmgr`.

Consequently, you may want to restrict access to the Application Manager URL and the application URI so that only you and any other trusted administrators can access them. If you don't restrict access to the Application Manager, anyone can add, remove, modify, start, and stop applications on your server.

If you want to require the administration server username and password for access to the Application Manager, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the Server Side Javascript link.

   The Activate Server Side Javascript window appears.

3. Under "Require administration server password for Server Side Javascript Application Manager" click the Yes radio button.
4. Click OK.
5. Save and apply your changes.

If your server does not use the Secure Sockets Layer (SSL), the username and password for the Application Manager are transmitted unencrypted over the network. Any intruder who intercepts this data may be able to access the Application Manager. If you use the same password for your administration server, the intruder can also control your server. For security reasons, do not use the Application Manager from outside your firewall unless you are using SSL.

Installing Server-Side JavaScript Applications

You can install up to 120 JavaScript applications on one server.

You must install (add) an application with the Application Manager before you can run it.

To install a new application, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **Server Side Javascript** link.

   The Activate Server Side Javascript window appears.
3. Click the link to the Application Manager.
4. Click the **Add Application** tab at the top of the page.

   The Add Application window appears.
5. In the **Name** field, type the name of the JavaScript application.

   This name defines the application URL. For example, the name of the Hello World application is "world," and its application URL is:

   `http://`*`server.domain:port`*`/world`

   This is a required field, and the name you type must be different from all other application names on the server. The name must include only alphanumeric characters and cannot include spaces. For more information on application URLs, see "Application URLs," on page 195.
6. In the **Web File Path** field, type the absolute path to the `.web` file for the application.

   This is a required field.
7. In the **Default Page** field, note what file to send to a client who does not indicate a specific page for the application.

This page is analogous to `index.html` for a standard URL. This is a required field.

8. In the **Initial Page** field, specify a page to run when the application is first started.

   This page only runs once during the life of the application and is used to initialize values and establish database connections. This is an optional field.

   In the **Built-in Maximum Database Connections** field, specify the maximum number of database connections that this application can have at one time if you are using the built-in database object. (This is provided for backward compatibility with applications that use database objects; for new applications that use a `dbpool`, ignore this field. See Chapter 8, "Connecting to a Database," in the *iPlanet Web Server Server-Side JavaScript Guide* for how to set this parameter for a `dbpool`.)

9. In the **External Libraries** field, specify the absolute paths of any libraries to be used with the application.

   This is an optional field. Libraries installed for one application can be used by all applications on the server.

10. In the **Client Object Maintenance** field, specify the mode for maintaining the client object. For additional information on client objects, refer to *Writing Server-Side JavaScript Applications* at:

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

    The choices for the client object maintenance technique are:

    - **client-cookie**—Specifies that the JavaScript runtime engine on the server should use the Netscape cookie protocol to transfer the properties of the client object and their values to the client. It creates one cookie per client property. The properties are sent to the client once, in the response header of the generated HTML page.
    - **client-url**—Specifies that the runtime engine on the server should transmit the properties of the client object and their values to the client by appending them to each URL in the generated HTML page. Consequently, the properties and their values are sent as many times as there are links on the generated HTML page, resulting in the largest increase in network traffic of all of the maintenance techniques.

- **server-ip**—Specifies that the server should index the data structure based on the application and the client's IP address. This technique is the fastest, because it does not require sending any information to the client. Since the index is based on both the application and the IP address, this technique creates a separate index for every application/client pair running on the server.
- **server-cookie**—Specifies that the server should use a long unique name, generated by the runtime engine, to index the data structure on the server. The runtime engine uses the Netscape cookie protocol to store the generated name as a cookie on the client. It does not store the property names and values as cookies. For this reason, this technique creates a single cookie, whereas the client-cookie technique creates a separate cookie for each property of the client object.
- **server-url**—Specifies that the server should use a long unique name, generated by the runtime engine, to index the data structure on the server. In this case, rather than making that generated name be a cookie on the client, the server appends the name to each URL in the generated HTML page. Consequently, the name is sent as many times as there are links on the generated HTML page. (Property names and values are not appended to URLs, just the generated name.)

11. After you have entered all the required information, click OK to install the application, Reset to clear all the fields, or Cancel to cancel the operation.

NOTE Don't give any JavaScript applications the same names as any subdirectories of your primary document directory. If you do, the server will no longer correctly process requests for resources in the directory. For example, if you have a directory *server_root*`/docs/bug`, and a JavaScript application named `bug`, all requests for any files in the bug directory (or any of its subdirectories) will attempt to launch the JavaScript application `bug`. The JavaScript application URI takes precedence.

Application URLs

When you install a Server-Side JavaScript application, you must enter a name for it. This name determines the ***application URL***, the URL that clients use to access a JavaScript application. Application URLs are of the form

`http://`*server.domain:port*`/`*appName*`/page.html`

where *server* is the name of the HTTP server, *domain* is the Internet domain (including any subdomains), *port* is the port number of the HTTP server, *appName* is the application name you enter when you install it, and *page* is the name of a page in the application, such as the default page name.

You can also access the application with the URL

```
http://server.domain:port/appName/
```

since the server knows the default page to open.

For example, if your server is named `myserver` and your domain name is `mozilla.com`, the application name is `world`, and the default page is `hello.html`, you can access the application with either of the following URLs:

```
http://myserver.mozilla.com/world/hello.html
```

or

```
http://myserver.mozilla.com/world/
```

When a client requests an application URL, the server runs the Server-Side JavaScript code inside the default page then sends the resultant HTML page to the client.

Important

Before you install an application, make sure the application name you choose does not usurp an existing URL on your server. All client requests for URLs that match the application URL are routed to the directory specified for the `.web` file, circumventing the server's normal document root.

Using the previous example, any requests for URLs that begin with `http://myserver.mozilla.com/world` will look for documents in the `js/samples/world` directory and not in your server's normal document root.

Controlling Access to a Server-Side JavaScript Application

When you install an application, you may want to restrict its use to only certain users. You can do this by applying a configuration style to the application. For more information, see Chapter 10, "Working With Configuration Styles." For more information on restricting access to part of your server, see Chapter 12, "Controlling Access to Your Server."

Modifying Installation Parameters

To modify an application's installation parameters, open the Application Manager as described in the section "Running the Application Manager," on page 190. Then select the application name in the left frame of the Application Manager and click Modify.

You can change any of the parameters defined when you installed the application except the application name. To change the name of an application, you must remove the application and then reinstall it.

If you modify the parameters of a stopped application, the Application Manager automatically starts it. When you modify parameters of an active application, Application Manager automatically stops and restarts it.

Removing a Server-Side JavaScript Application

To remove the selected application, open the Application Manager as described in "Running the Application Manager," on page 190, then click Remove. This action removes the application from the Application Manager but does not delete files from the server. At this point, clients can no longer access the application.

If you delete an application and you subsequently want to run it, you must install it again.

Starting, Stopping, and Restarting a Server-Side JavaScript Application

To start an installed application that is stopped, open the Application Manager as described in "Running the Application Manager," on page 190, and then click Start. If the application starts successfully, clients can invoke the application.

To stop an active application, click Stop. The application's status changes to "stopped," and clients can no longer invoke the application. You must stop an application if you want to move the `.web` file or update an application from a development server to a deployment server.

To restart a running application, click Restart. Before any changes take effect, you must restart an application after you compile it.

You can also start, stop, and restart an application by entering a special URL of the form:

`http://server.domain:port/appmgr/control.html?name=`*`appName`*`&cmd=`*`action`*

where *appName* is the application name and *action* is either `stop`, `start`, or `restart`.

Running a Server-Side JavaScript Application

There are two ways to run an installed application:

- Open the Application Manager as described in “Running the Application Manager,” on page 190, then select the application name in the Application Manager, and click Run. A new Navigator window accesses the application.
- Enter the application URL in Navigator.

If you attempt to run a stopped application (one that is not active), then the Application Manager tries to start it first.

Configuring Default Settings

To configure default settings for new applications, open the Application Manager as described in “Running the Application Manager,” on page 190, and then click the Preferences tab. When you install a new application, the default installation parameters are used for the initial settings.

You can specify the following default settings:

- Installation parameters: `.web` file path, default page, initial page, maximum number of built-in database connections, external libraries, and client object maintenance technique. You can specify a default directory path for your development area and native executables libraries.
- Whether you are prompted to confirm your action when you remove, start, stop, or restart an application.
- When debugging an application, whether the application trace appears in the same window as the application but in another frame, or in a window separate from the application.

Enabling WAI Services

NOTE Web Application Interface (WAI) is provided in iPlanet Web Server 4.x, but is not guaranteed to be supported in future releases. We recommend that you do not develop new WAI applications.

WAI services are a kind of plug-in that uses the **Common Object Request Broker Architecture (CORBA)**. WAI applications can be written in C, C++, or Java, and they interact with iPlanet Web Server over Internet Inter-ORB Protocol (IIOP). A WAI application runs within its own process. WAI applications need an object request broker (ORB) to work.

iPlanet Web Server 4.x does not ship with an object request broker (ORB). Before using WAI applications, you must install Visibroker 3.3+ from Inprise. You can get Visibroker3.3+ from the Inprise web site at:

```
http://www.inprise.com/products/
```

After installing Visibroker 3.3+, you will need to install WAI on your iPlanet Web Server. You can do this by running through the installation process, and choosing to install only WAI.

After you have installed WAI, the next step is to enable it on your server. Enabling WAI services essentially turns on Internet Inter-ORB Protocol (IIOP) support in the server.

To enable WAI services on your server, perform the following steps:

1. From the Server Manager, choose the **Programs** tab.
2. Click the **WAI Handler** link.

   The WAI Administration window appears.
3. To enable WAI services, click the **Yes** radio button.
4. Save and apply your changes.

For more information about WAI, see *Writing Web Applications with WAI* at:

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

Working With Configuration Styles

Configuration styles are an easy way to apply a set of options to specific files or directories that your server maintains. For example, you can create a configuration style that sets up access logging. When you apply that configuration style to the files and directories that you want to log, you don't have to individually configure access logging for all the files and directories.

This chapter includes the following sections:

- Creating a Configuration Style
- Removing a Configuration Style
- Editing a Configuration Style
- Assigning a Configuration Style
- Listing Configuration Style Assignments

Creating a Configuration Style

To create a configuration style, perform the following steps:

1. Access the Administration Server and click the **Servers** tab.
2. In the Manage Servers area, select the desired server and click **Manage**.

   iPlanet Web Server displays the Server Manager Preferences page, as shown in Figure 1-1. on page 35 of Chapter 1, "Introduction to iPlanet Web Server."
3. Choose the **Styles** tab.
4. Click the **New Style** link.
5. Type the name you want to give the configuration style. Click OK.

iPlanet Web Server displays the Edit a Style page.

6. From the drop-down list, choose a configuration style to edit and click **Edit this Style**.
7. From the list of links available, click the category you want to configure for your style.

   You can configure the information listed in Table 10-1.
8. Fill out the form that appears, and click OK.
9. Repeat step 4 and step 5 to make any other configuration changes to the configuration style. Click OK.
10. Click **Save and Apply** to confirm your changes to the configuration style.

When you choose a style to edit, your Resource Picker lists configuration styles instead of other resources. After you have finished editing a style, click OK and Save and Apply. The Resource Picker exits the styles mode. You can also choose to exit the styles mode by choosing Exit styles mode from the Resource Picker.

Table 10-1 Configuration Style Categories

Category	Description
CGI file type	Allows you to activate CGI as a file type. For more information about CGIs, see “Installing CGI Programs,” on page 178 in Chapter 9, “Extending Your Server With Programs.”
Character Set	Allows you to change the character set for a resource. For more information about character sets, see “To use the Server Manager for the hardware virtual servers that are uses with ISPs, see the section “Setting Up Hardware Virtual Servers for ISPs” on page 215.Changing the Character Set,” on page 218 in Chapter 11, “Managing Server Content.”
Default Query Handler	Allows you to set a default query handler for a server resource. For more information about query handling, see “Using the Query Handler,” on page 188 in Chapter 9, “Extending Your Server With Programs.”
Document Footer	Allows you to add a document footer to a server resource.
Dynamic Configuration	Allows you to give people a subset of configuration options without giving them access to the Server Manager. For more information about dynamic configuration, see “Working with Dynamic Configuration Files,” on page 138 in Chapter 6, “Configuring Server Preferences.”

Table 10-1 Configuration Style Categories *(Continued)*

Category	Description
Error Responses	Allows you to customize the error responses that clients see when they encounter an error from your server. For more information about error responses, see "Customizing Error Responses," on page 137 in Chapter 6, "Configuring Server Preferences."
Log preferences	Allows you to set preferences for access logs. For more information about log preferences, see "Setting Log Preferences," on page 155 in Chapter 7, "Understanding Log Files."
Restrict Access	Allows you to restrict access to the entire server or parts of it. For more information about access control, see Chapter 12, "Controlling Access to Your Server."
Server Parsed HTML	Allows you to specify whether the server parses files before they are sent to the client.
Symbolic links (Unix/Linux)	Allows you to limit the use of file system links in your server. For more information about symbolic links, see "Restricting Symbolic Links (Unix/Linux)," on page 145 in Chapter 6, "Configuring Server Preferences."

For more information, see "The Create a New Style Page," in the online help.

Removing a Configuration Style

Before removing a configuration style, remove assignments that had the configuration style applied to them.If you do not do this before removing the configuration style, you must manually edit your `obj.conf` file, searching for the configuration style in the file and replacing it with `None`. If you don't do this search and replace, anyone who accesses the files or directories that had the deleted configuration style applied will get a server misconfiguration error message.

To remove a configuration style, perform the following steps:

1. Access the Server Manager and choose the **Styles** tab.
2. Click **List Assignments** link.
3. Select **Edit Style Assignment** you want to remove.

4. Click **Remove this Assignment**.
5. Click the **Remove Style** link.
6. Select the configuration style you want to remove and click OK.

For more information, see "The Remove a Style Page," in the online help.

Editing a Configuration Style

To edit a configuration style, perform the following steps:

1. Access the Server Manager and choose the **Styles** tab.
2. Click the **Edit Style** link.
3. Select the configuration style you want to edit and click the **Edit this style** button.
4. From the list of links available, click the category you want to configure for your style.

   For more information on these categories, see the section "Creating a Configuration Style" on page 201.
5. Fill out the form that appears, and then click OK.
6. Repeat Step 4 and Step 5 to make any other changes to the configuration style. Click OK.
7. Click **Save and Apply** to confirm your changes to the configuration style.

When you choose a style to edit, your Resource Picker lists configuration styles instead of other resources. After you have finished editing a style, click OK and Save and Apply. The Resource Picker exits the styles mode. You can also choose to exit the styles mode by choosing Exit styles mode from the Resource Picker.

For more information, see "The Edit a Style Page," in the online help.

Assigning a Configuration Style

Once you've created a configuration style, you can assign it to files or directories in your server. You can specify either individual files and directories or wildcard patterns (such as `*.gif`).

To assign a configuration style, perform the following steps:

1. Access the Server Manager and choose the **Styles** tab.
2. Click the **Assign Style** link.
3. Enter the prefix of the URL to which you are applying this configuration style.

   If you choose a directory inside the document root, only enter the path after the document root. If you enter `/*` after the directory, you apply the configuration style to all of the directory's contents.
4. Select the configuration style you want to apply. To remove any configuration style previously applied to the resource, apply the None configuration style. Click OK.

For more information, see "The Apply a Configuration Style Page," in the online help.

Listing Configuration Style Assignments

After you have created configuration styles and applied them to files or directories, you can get a list of the configuration styles and where you applied them.

To list the configuration style assignments, perform the following steps:

1. Access the Server Manager and choose the **Styles** tab.
2. Click the **List Assignments** link.

   iPlanet Web Server displays the List Assignments page, showing the configuration styles you applied to server resources.
3. To edit a configuration style assignment, click the Edit link next to the configuration style name.

For more information, see "The View, Edit, or Remove Style Assignments Page," in the online help.

Chapter 11

Managing Server Content

You can use the Server Manager to help manage your server's content. You create HTML pages and other files such as graphics, text, sound, or video, and then you store those files on your server. When clients connect to your server, they can view your files provided they have access to them. This chapter describes how you can configure and manage your server's content.

This chapter contains the following sections:

- Changing the Primary Document Directory
- Setting Additional Document Directories
- Customizing User Public Information Directories (Unix/Linux)
- Enabling Remote File Manipulation
- Configuring Document Preferences
- Setting Up Hardware Virtual Servers
- Setting Up Hardware Virtual Servers for ISPs
- To use the Server Manager for the hardware virtual servers that are uses with ISPs, see the section "Setting Up Hardware Virtual Servers for ISPs" on page 215.Changing the Character Set

Changing the Primary Document Directory

The primary document directory or document root is the central directory where you store all the files you want to make available to remote clients. You specified a primary document directory when you installed the iPlanet Web Server software. This section describes how to change the primary document directory from what you specified in the installation process.

The primary document directory provides an easy way to restrict access to the files on your server. It also makes it easy to move your documents to a new directory (perhaps on a different disk) without changing any of your URLs because the paths specified in the URLs are relative to the primary document directory.

For example, if your document directory is `C:\Netscape\server4\docs`, a request such as `http://www.mozilla.com/products/info.html` tells the server to look for the file in `C:\Netscape\Server4\docs\products\info.html`. If you change the document root (that is, you move all the files and subdirectories), you only have to change the document root that the server uses, instead of mapping all URLs to the new directory or somehow telling clients to look in the new directory.

To set your server's primary document directory, use the Primary Document Directory page in the Server Manager. For more information, see the online help.

NOTE Each server instance should have its own primary document directory. If server instances share primary document directories, users could simultaneously modify a document without knowing it.

Setting Additional Document Directories

Most of the time, you keep all of your documents in the primary document directory. Sometimes, though, you may want to serve documents from a directory outside of your document root. You can do this by setting additional document directories. By serving from a document directory outside of your document root, you can let someone manage a group of documents without giving them access to your primary document root.

To add an additional document directory you first need to choose the URL prefix to map. Clients send this URL to the server when they want documents. Next, you specify the directory to map those URLs to. Finally, you might want to use an existing configuration style to specify how this directory should be configured.

To add additional document directories, use the Additional Document Directories page in the Server Manager.

By default, the server has several additional document directories. They have the following prefixes:

- `/help`
- `/search-ui`

- /webpub-ui
- /publisher

You should restrict access to these directories so that users cannot write to them. A sample ACL for the /publisher directory would be:

```
deny (all) anyone;
allow (rxli) all;
allow (wd) privileged_user;
```

Customizing User Public Information Directories (Unix/Linux)

Sometimes users want to maintain their own web pages. You can configure public information directories that let all the users on your server create home pages and other documents without your intervention.

Another way to do this is to create a URL mapping to a central directory that all of your users can modify.

With this system, clients can access your server with a certain URL that the server recognizes as a public information directory. For example, suppose you choose the prefix ~ and the directory public_html. If a request comes in for http://www.iplanet.com/~jdoe/aboutjane.html, the server recognizes that ~jdoe refers to a users' public information directory. It looks up jdoe in the system's user database and finds Jane's home directory. The server then looks at ~/jdoe/public_html/aboutjane.html.

To configure your server to use public directories, you need to choose a user URL prefix. The usual prefix is ~ because the tilde character is the standard Unix/Linux prefix for accessing a user's home directory. Next, you need to choose the subdirectory in the user's home directory where the server looks for HTML files. A typical directory is public_html.

The server needs to know where to look for a file that lists users on your system. The server uses this file to determine valid usernames and to find their home directories. If you use the system password file for this purpose, the server uses standard library calls to look up users. Alternatively, you can create another user file to look up users. You can specify that user file with an absolute path.

Each line in the file should have this structure (the elements in the /etc/passwd file that aren't needed are indicated with *):

```
username:*:*:groupid:*:homedir:*
```

Restricting Content Publication

In some situations a system administrator may want to restrict what user accounts are able to publish content via User Document Directories. This can easily be accomplished by adding a trailing slash to the user's home directory path in the `/etc/passwd file`:

```
jdoe::1234:1234:John Doe:/home/jdoe:/bin/sh
```

becomes:

```
jdoe::1234:1234:John Doe:/home/jdoe/:/bin/sh
```

When this modification is made, iPlanet Web Server will not serve pages from this user's directory. The browser requesting the URI receives a "404 File Not Found" error and a 404 error will be logged to the web server access log. No error will be logged to the errors log.

If, at a later time, the system administrator decides to allow this user to publish content the trailing slash should be removed from the `/etc/passwd` entry followed by restarting the web server.

Loading the Entire Password File on Startup

You also have the option of loading the entire password file on startup. If you choose this option, the server loads the password file into memory when it starts, making user lookups much faster. If you have a very large password file, however, this option can use too much memory.

Using Configuration Styles

Finally, you can apply a configuration style for the server to control access to directories from public information directories. This prevents users from creating symbolic links to information you do not want made public.

To set up user directories, use the User Document Directories page in the Server Manager.

Enabling Remote File Manipulation

When you enable remote file manipulation, clients are able to upload files, delete files, create directories, remove directories, list the contents of a directory, and rename files on your server. The file `obj.conf` in the directory *`server_root`*`/https-`*`serve-id`*`/config` contains the commands that are activated when you enable remote file manipulation. By activating these commands, you allow remote browsers to change your server's documents. You should use access control to restrict write access to these resources to prevent unauthorized tampering.

Unix/Linux: You must have the correct permissions for your files or this function will not work; that is, the document root user must be the same as the server user.

To enable remote file manipulation, use the File Manipulation page in the Server Manager.

Configuring Document Preferences

You use the Document Preferences page to set document preferences. This section discusses these topics:

- Entering an Index Filename
- Selecting Directory Indexing
- Specifying a Server Home Page
- Specifying a Default MIME Type
- Parsing the Accept Language Header

Entering an Index Filename

If a document name is not specified in the URL the server automatically displays the index file. The default index files are `index.html` and `home.html`. If more than one index file is specified, the server looks in the order in which the names appear in this field until one is found. For example, if your index filenames are `index.html` and `home.html`, the server looks for `index.html` and if it doesn't find it looks for `home.html`.

To enter an index filename, edit the Index Filenames field in the Document Preferences page of the Server Manager.

Selecting Directory Indexing

In your document directory, you'll probably have several subdirectories. For example, you might create a directory called `products`, another called `people`, and so on. It's often helpful to let clients access an overview (or index) of these directories.

The server indexes directories by searching the directory for an index file called `index.html` or `home.html`, which is a file you create and maintain as an overview of the directory's contents. (Note that these defaults are configurable for the whole server, so your server's files may vary. For more information, see the previous section, "Entering an Index Filename" on page 211). You can specify any file as an index file for a directory by naming it one of these default names, which means you can also use a CGI program as an index if CGI is activated.

If an index file isn't found, the server generates an index file that lists all the files in the document root.

To select directory indexing, use the Document Preferences page in the Server Manager.

CAUTION If your server is outside the firewall, turn off directory indexing to ensure that your directory structure and, filenames are not accessible.

Specifying a Server Home Page

When users first access your server, they usually use an URL such as `http://www.mozilla.com/`. When the server receives a request for this document, it returns a document called a *home page.* Usually, this file has general information about your server and links to other documents.

By default, the server finds the index file specified in the Index Filename field in the Document Preferences page and uses that for the home page. However, you can also specify a file to use as the home page in the Document Preferences page of the Server Manager. For more information, see the online help.

Specifying a Default MIME Type

When a document is sent to a client, the server includes a section that identifies the document's type, so the client can present the document in the right way. However, sometimes the server can't determine the proper type for the document because the document's extension is not defined for the server. In those cases, a default value is sent. For information about maintaining your server's MIME types, see the Global MIME Types page in the online help.

The default is usually text/plain, but you should set it to the type of file most commonly stored on your server. Some common MIME types include the following:

- `text/plain`
- `text/richtext`
- `image/jpeg`
- `application/x-tar`
- `application/x-gzip`
- `text/html`
- `image/tiff`
- `image/gif`
- `application/postscript`
- `audio/basic`

To specify a default MIME type, use the Document Preferences page of the Server Manager. For more information, see the online help

Parsing the Accept Language Header

When clients contact a server using HTTP 1.1, they can send header information describing the languages they accept. You can configure your server to parse this language information.

For example, if you store documents in Japanese and English, you could choose to parse the accept language header. When clients that have Japanese as the accept language header contact the server, they receive the Japanese version of the page. When clients that have English as the accept language header contact the server, they receive the English version.

If you do not support multiple languages, you should not parse the accept language header.

For more information on using the accept language header, see the section "Using the Accept Language Header" on page 269.

To parse the accept language header, use the Document Preferences page in the Server Manager.

Setting Up Hardware Virtual Servers

A hardware virtual server is a way to have your server respond to multiple IP addresses without installing multiple servers. With hardware virtual servers you map multiple IP addresses to multiple document roots. For example, if you have two IP addresses, you could map the first IP address to one document root and the second IP address to a second document root. iPlanet Web Server can respond to up to 256 IP addresses.

NOTE If you are using more than 100 hardware virtual servers, you should use the method described in the section “Setting Up Hardware Virtual Servers for ISPs” on page 215 for setting up hardware virtual servers.

Hardware virtual servers share the same server configuration information. For example, if you turn on encryption for one hardware virtual server, any other hardware virtual servers you create would also have encryption turned on.

If you need servers that respond to different IP addresses and require that they have separate configuration information, install separate instances of the server with specific IP addresses. Alternatively, you can also configure multiple hardware virtual servers on the same IP address by assigning different port numbers for each hardware virtual server. For more information, see “Adding a Server: Running Multiple Servers” on page 45.

Unix/Linux. Before you set up hardware virtual servers, make sure you specified a specific bind-to-address for your server in the Network Settings page (from the iPlanet Web Server, choose Server Preferences and then click Network Settings). If you left the Bind To Address field blank, you may experience errors when using hardware virtual servers. If you are an ISP using hardware virtual servers, the bind-to-address should be your main IP address.

You can set up hardware virtual servers through the Hardware Virtual Servers page in the Server Manager. For more information, see the online help.

Setting Up Hardware Virtual Servers for ISPs

ISPs that need to support more than 256 IP addresses or that want the server to use less memory can use the ISP-version of the hardware virtual server function. As with default hardware virtual servers (discussed in the previous section), ISP-version hardware virtual servers allow you to configure your server to respond to multiple IP addresses without installing multiple servers, but you can configure your server to support an arbitrary number of IP addresses.

ISP-version hardware virtual servers share the same server configuration information. For example, if you turn on encryption for one hardware virtual server, any other hardware virtual servers you create would also have encryption turned on. If you need servers that respond to different IP addresses and require that they have separate configuration information, install separate instances of the server with specific IP addresses. For more information, see “Changing Network Settings” on page 52.

For HP servers, the number of virtual servers must work well with the `max_thread_proc` entry in the HP-UX kernel and `RqThrottle`. Since threads are never “released,” but moved to another pool, the number of threads used can get quite high when using hardware virtual servers in the object model.

NOTE If you set up this hardware virtual server function, make sure that the B**ind to Address** field in the Network Settings page is blank (choose **Server Preferences** and click **Network Settings**).

This section includes the following topics:

- To Set Up Hardware Virtual Servers For an ISP
- To Edit a Server Instance
- To Remove a Server Instance
- Migrating Hardware Virtual Server Configuration Files

To Set Up Hardware Virtual Servers For an ISP

To set up hardware virtual servers for an ISP, perform the following steps:

1. Uncomment the line for setting up hardware virtual servers for an ISP in the `index.1st` file in *`server_root`*`/bin/https/httpadmin/html` directory.

The default `index.lst` file comments out the line for the ISP-version hardware virtual server. You must uncomment the line containing "`Option:perl/virtual, Hardware Virtual Servers`" and comment out the line containing "`Option:multiple, Hardware Virtual Servers`".

2. From the Server Manager, choose the **Content Management** tab.

   Click **Content Management** even if it's already selected to make sure the file name change is picked up by the server.

3. Click **Hardware Virtual Servers**.

   The Hardware Virtual Servers page appears.

4. Enter the server's IP address in the IP field.

5. Enter the primary document directory in the Doc Root field, and click OK.

   You must type in the absolute path, such as C:`/Netscape/server4/docs`.

6. Click **Apply** in the top right portion of the Server Manager to apply your changes.

To Edit a Server Instance

To edit a server instance, perform the following steps:

1. Click **Edit** on the line for the server instance you want to edit.
2. On the Hardware Virtual Servers page, enter the new IP address and document root, and click OK.
3. Click **Apply** in the top right portion of the Server Manager to apply your changes.

To Remove a Server Instance

To remove a server instance, perform the following steps:

1. Click **Remove** on the line for the server instance you want to remove.
2. Click OK in the confirmation dialog box.
3. Click **Apply** in the top right portion of the Server Manager to apply your changes.

The ISP-hardware virtual servers are listed in the `virtual.conf` configuration file. This file lists the IP addresses you entered through the Server Manager and the document root to which they apply.

You can return to using the default hardware virtual server function, by performing the following steps:

1. From the Server Manager, choose **Content Management** tab.
2. Click **Hardware Virtual Servers**.

   The Hardware Virtual Servers Page appears.
3. Click **No** to deactivate the ISP-version hardware virtual server function, then click OK.
4. Click **Save and Apply**.

Migrating Hardware Virtual Server Configuration Files

If you run multiple IP addresses using the `obj.conf` file, you may have restrictions using virtual servers. For better reliability, you can migrate from the `obj.conf` file to the `virtual.conf` file by running the following script:

```
server_root/bin/https/httpadmin/bin/vserverupgrd -r server_root
-p administration_port -i https-server-id
```

When you do this, the executable removes all the `NameTrans` directives, for individual hardware virtual servers, from the obj.conf file that corresponds to the `config` directory *`server_root`*`/http-`*`server-id`*, and replaces them with corresponding directives in a virtual.conf file, located in the same directory. It also references the virtual.conf file from the `magnus.conf`. file in the *`server_root`*`/https-`*`server-id/`*`config/` directory, and removes addresses that are found in the `magnus.conf` file.

To use the Server Manager for the hardware virtual servers that are uses with ISPs, see the section “Setting Up Hardware Virtual Servers for ISPs” on page 215.

Changing the Character Set

The character set of a document is determined in part by the language it is written in. You can override a client’s default character set setting for a document, a set of documents, or a directory by selecting a resource and entering a character set for that resource.

Netscape Navigator can use the MIME type `charset` parameter in HTTP to change its character set. If the server includes this parameter in its response, Netscape Navigator changes its character set accordingly. Examples are:

- `Content-Type: text/html;charset=iso-8859-1`
- `Content-Type: text/html;charset=iso-2022-jp`

The following `charset` names recognized by Netscape Navigator are specified in RFC 1700 (except for the names that begin with `x-`):

- `us-ascii`
- `iso-8859-1`
- `iso-2022-jp`
- `x-sjis`
- `x-euc-jp`
- `x-mac-roman`

Additionally, the following aliases are recognized for `us-ascii`:

- `ansi_x3.4-1968`
- `iso-ir-6`
- `ansi_x3.4-1986`
- `iso_646.irv:1991`
- `ascii`
- `iso646-us`
- `us`
- `ibm367`
- `cp367`

The following aliases are recognized for `iso_8859-1`:

- `latin1`
- `iso_8859-1`

- `iso_8859-1:1987`
- *iso-ir-100*
- `ibm819`
- `cp819`

To change the character set, use the International Characters page in the Server Manager.

To use the Server Manager for the hardware virtual servers that are uses with ISPs, see the section “Setting Up Hardware Virtual Servers for ISPs” on page 215.Changing the Character Set

Chapter 12

Controlling Access to Your Server

This chapter discusses the various methods you can use to control access to the Administration Server and to the files or directories on your web site. For example, for the Administration Server, you can specify who has full control of all the servers installed on a machine and who has partial control of one or more servers. Before you can use access control on the Administration Server, you must enable distributed administration from the Distributed Administration page and set up an administration group in your LDAP database. This chapter assumes you have already configured distributed administration and have defined users and groups in your LDAP database.

You should also ensure the security of the web server as discussed in Chapter 5, “Working with Server Security.”

This chapter contains the following sections:

- What Is Access Control?
- How Access Control Works
- Restricting Access to Your Web Site
- Access Control Examples

What Is Access Control?

Access control allows you determine who can access iPlanet Web Administration Server and which servers and tabs (also called programs) they can access as well as who can access the files or directories on your web site.

You can control access to the entire server or to parts of the server such as specific tabs or pages in the Administration Server or the files or directories on your web site. When the server evaluates an incoming request, it determines access based on a hierarchy of rules called **access control entries** (ACEs), and then it uses the matching entries to determine if the request is allowed or denied. Each ACE specifies whether or not the server should continue to the next ACE in the hierarchy. The collection of ACEs is called an **access control list** (ACL).When a request comes in to the server, the server looks in `obj.conf` for a reference to an ACL, which is then used to determine access. By default, the server has one ACL file that contains multiple ACLs.

You can use two methods for controlling access:

- **User-Group.** This method requires users to enter a username and password before accessing the server. The server compares the information in a client certificate or the client certificate itself with a directory server entry. This methods requires the use of a directory server. If you choose to use client certificates, you should increase the value of the `AcceptTimeout` directive in `magnus.conf`.
- **Host-IP.** This method requires the user to access the web server from a specific computer, where the web server recognizes the computer by either its hostname or its IP address. This methods does not require a directory server.

This section includes the following topics:

- Setting ACL User Cache Time
- User-Group Authentication
- Host-IP Authentication
- Access Control Files

Setting ACL User Cache Time

To control the amount of time that ACL user cache is valid, use the `ACLCacheLifetime` directive in the `magnus.conf` file. Each time an entry in the cache is referenced, its age is calculated and checked against `ACLCacheLifetime`. The entry is not used if its age is greater than or equal to the `ACLCacheLifetime`. The default value is 120 seconds. If this value is set to 0, the cache is turned off. If you use a large number for this value, you may need to restart iPlanet Web Server when you make changes to the LDAP entries. For example, if this value is set to 120 seconds, iPlanet Web Server might be out of sync with the LDAP server for as long as two minutes. If your LDAP is not likely to change often, use a large number.

The maximum number of entries that can be held in the cache is configurable as of iPlanet Web Server 4.0, using the `magnus.conf` parameter, `ACLUserCacheSize`. The default value for this parameter is 200, which is the fixed size of the cache in ES 3.x. New entries are added to the head of a list, and entries at the end of this list are recycled to make new entries when the cache reaches its maximum size.

The maximum number of group memberships that can be cached per user entry is configurable as of ES 4.x, using the `magnus.conf` parameter, `ACLGroupCacheSize`. The default value for this parameter is 4, although in ES 3.x it has a fixed value of 1. Unfortunately non-membership of a user in a group is not cached, and will result in several Directory Server operations for each such check on every request.

User-Group Authentication

User-Group authentication requires users to *authenticate* themselves before getting access to the Administration Server or the files or directories on your web site. Authentication means that users verify their identity either by entering a username and password or by using a client certificate installed in their network browser, such as Netscape Communicator. The first method of getting the username and password is the basic method, which can be done with or without encryption. The latter method of using client certificates is the SSL method, which must be done with encryption on. For information on using SSL, see Chapter 5, “Working with Server Security.”

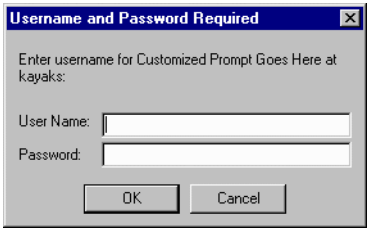
Username and Password Authentication

To require users to enter a username and password to get access to the web server or your web site, you must store the list of users and groups in an LDAP database such as the Netscape Directory Server. The directory server can be running on the same machine as the web server, or you can use a directory server installed on a remote machine.

When users attempt to access a resource that has User-Group authentication in the Administration Server or on your web site, the web browser displays a dialog box asking the user to enter a username and password. The server receives this information encrypted or unencrypted, depending on whether encryption is turned on for your server.

After entering the username and password, the user either sees the Server Administration page if logging in to iPlanet Web Administration Server, the file or directory listing requested if logging in to a web site, or a message denying access if the username or password was invalid. You can customize the access denied message that unauthorized users see through the Access Denied Response page. Figure 12-1 shows the authentication dialog box. This dialog box displays a customized login prompt message.

Figure 12-1 Users see this dialog box when authenticating themselves to the server.



NOTE If your server does not use SSL encryption, the username and password that the end user types are sent in unencrypted text across the network. Someone could intercept the network packets and read the username and password being sent to the Administration Server. For this reason, User-Group authentication is most effective when combined with SSL encryption or Host-IP authentication, or both.

The server maintains two connections to the directory server. One of these is used to authenticate users, by doing an LDAP bind as the specified user. The other is permanently bound as the `binddn` specified in the Configure Directory Service page, and is used for locating user entries and checking group memberships. Only one HTTP request thread can access the directory server at a time, which means that a global lock controls access to both LDAP connections. This can be a potential performance bottleneck, especially when combined with the fixed size of the ACL user / group cache.

Client Certificate Authentication

You can confirm users' identities with security certificates before giving the users access to your web site. You can do this in two ways:

- The server can use the information in the certificate as proof of identity.

- The server can verify the certificate itself if certificates are published in an LDAP directory.

When a server with client authentication enabled receives a request, the server performs the following actions:

1. When the browser sends the certificate, the server checks if the certificate is from a trusted CA. If not, the server ends the transaction, and the authorization fails.
2. If the certificate is from a trusted CA, the server maps the certificate to a user's entry using the `certmap.conf` file. See "Using the certmap.conf File" on page 110 for more information on setting up the certificate mapping file.
3. If the certificate maps correctly, then the web server checks the ACL rule specified for that user. Therefore, even though the certificate maps correctly, if the ACL denies the user access, the rule can deny the request.

The web server looks up the entry in an LDAP directory, so the access appears seamless to the end user.

Requiring client authentication for controlling access to specific resources is different than requiring client authentication for all connections to the server. To require client authentication with access control, choose the SSL authentication methods you want to use from the Encryption Preferences page (in the Preferences tab, click Encryption Preferences). To require client authentication for the entire server, select "Require Client Certificates (regardless of access control)" in the Encryption Preferences page.

NOTE Only the SSL authentication method requires modification to the `certmap.conf` file. Allowing client authentication for all connections to the server does not.

In order for a client to successfully gain access to a SSL authenticated resource requiring client certificates, the client must install a certificate on their browser which is from a certificate authority trusted by the web server. It may be necessary to have the same client certificate published in a directory server if the web server's `certmap.conf` file is configured to compare the entire certificate between the client's certificate in the browser and the client certificate in the directory server entry. However, the `certmap.conf` file can be configured so that it only compares selected information from the certificate to the entry in the directory server. For example, you can configure the `certmap.conf` file so that the server only compares

a user ID and an email address in the browser certificate with the directory server entry. In such a case, it would not be necessary to publish the entire client certificate to the directory server since only the user ID and email address must match to gain access.

Host-IP Authentication

You can limit access to the Administration Server or the files or directories on your web site by making them available only to clients using specific computers. You specify hostnames or IP addresses for the computers that you want to allow or deny. You can use wildcard patterns to specify multiple computers or entire networks. End user access to a file or directory using Host-IP authentication appears seamless. Users can access the files and directories immediately without entering a username or password. If the machine does not have access, the user will see a message denying access. For information on customizing this message, see “Responding When Access is Denied” on page 241.

NOTE It is possible for more than one person to have access to a particular system. For this reason, Host-IP authentication is more effective when combined with User-Group authentication. If both methods of authentication are used, the end user will have to enter a username and password on a particular computer before getting access.

IP authentication does not require DNS to be configured on your server. If you want to use hostname authentication, however, you must have DNS running in your network and your server must be configured to use it. You can enable DNS on your server through the Performance Tuning page in the Preferences tab.

Enabling DNS degrades the performance of iPlanet Web Server since the server is forced to do DNS look-ups. To reduce the effects of DNS look-ups on your server’s performance, resolve IP addresses only for access control and CGI instead of resolving the IP address for every request. To do this, add the line “`iponly=1`” to the line that begins: `AddLog fn="flex-log" name="access"` in your `obj.conf` file. The resulting line is as follows:

```
AddLog fn="flex-log" name="access" iponly=1
```

Access Control Files

When you use access control on the Administration Server or the files or directories on your web site, the settings are stored in a file with the extension `.acl`. Access control files are stored in the directory *server_install*`/httpacl` where *server_install* is the location where the server is installed. For example, if you installed the server in `/usr/netscape/server4`, the ACL files for both the Administration Server and each server instance configured on your server would be located in `/usr/netscape/server4/httpacl/`.

The main ACL file name is `generated-https-`*server-id*`.acl`; the temporary working file is called `genwork-https-`*server-id*`.acl`. If you use iPlanet Web Server to restrict access, you'll have these two files. However, if you want more complex restrictions, you can create multiple files and reference them from the `magnus.conf` file. There are also a few features available only by editing the files such as restricting access to the server based on the time of day or day of the week.

Also, you can manually create and edit `.acl` files to customize access control. For example, if you want to use an Oracle or Informix database of users instead of an LDAP database, you need to use the access control API to program a hook into the server's access control structure. This API is written in the C programming language. For more information on the API, see the iPlanet documentation site at `http://www.iplanet.com/docs`.

For more information on access control files and their syntax, see "ACL File Syntax" on page 259.

How Access Control Works

When the server gets a request for a page, the server uses the rules in the ACL file to determine if it should grant access or not. The rules can reference the hostname or IP address of the computer sending the request. The rules can also reference users and groups stored in the LDAP directory.

For example, the following ACL file contains the two default entries for the Administration Server (`admin-serv`) plus an additional entry that allows users in the "admin-reduced" group to access the Preferences tab in the Administration Server.

```
version 3.0;
# The following "es-internal" rules protect files such
# as icons and images related to iPlanet Web Server.
# These "es-internal" rules should not be modified.
  acl "es-internal";
  allow (read, list, execute,info) user = "anyone";
  deny (write, delete) user = "anyone";
# The following "default" rules apply to the entire document
# directory of iPlanet Web Server. In this example, the rules
# are set up so that "all" users in the directory server are
# allowed to read, execute, list, and get information.
# The "all" users are not allowed to write to or delete any files.
# All clients that accesses the document directory of the web
# server will be required to submit a username and password
# since this example is using the "basic" method of
# authentication. A client must be in the directory server
# to gain access to this default directory since "anyone"
# not in the directory server is denied, and "all" in the
# directory server are allowed.
  acl "default";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");
  allow (read,execute,list,info)
  (user = "all");
# The following rules deny access to the directory "web"
# to everyone not in the directory server and deny everyone
# in the directory server who is not in GroupB.
# Only the users in GroupB are allowed read, execute, list,
# and info permissions. GroupA can not gain access to the
# directory "web" even though (in the ACL rule below) they
# can access the directory “my_stuff”. Furthermore, members
# of GroupB can not write or delete files.
  acl "path=/export/user/990628.1/docs/my_stuff/web/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");

  allow (read,execute,list,info)
  (group = "GroupB");

# The following rule denies everyone not in the directory
# server and denies everyone in the directory server except
# user with the ID of "SpecificMemberOfGroupB". The ACL rule
# in this setting also has a requirement that the user
# connect from a specific IP address. The IP address setting
# in the rule is optional; it has been added to for extra
# security. Also, this ACl rule has a Customized prompt
```

```
# of "Presentation Owner". This Customized prompt appears
# in the username and password dialog box in the client's
# browser.

  acl
"path=/export/user/990628.1/docs/my_stuff/web/presentation.html"
;
  authenticate (user,group) {
     database = "default";
     method = "basic";
     prompt = "Presentation Owner";
  };
  deny (all)
  (user = "anyone" or group = "my_group");
  allow (all)
  (user = "SpecificMemberOfGroupB") and
  (ip = "208.12.54.76");

# The following ACL rule denies everyone not in the directory
# server and everyone in the directory server except for
# GroupA and GroupB access to the directory "my_stuff"
  acl "path=/export/user/990628.1/docs/my_stuff/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");
  allow (read,execute,list,info)
  (group = "GroupA,GroupB");
```

If someone requests the URL: `http://`*`server_name`*`/my_stuff/web/presentation.html`, the server would first check access control for the entire server. If the ACL for the entire server was set to continue, the server checks to see if there is an ACL for the file type (`*.html`). Then, it checks for an ACL for the directory, `my_stuff`. If one exists, it checks the ACE and then moves on to the next directory. The server continues traversing the path either until it reaches an ACL that says not to continue or until it reaches the final ACL for the requested URL (in this case, the file `presentation.html`).

To set up access control for this example using the Server Manager, you could create an ACL for the file only or for each resource leading to the file. That is, one for the entire server, one for the `my_stuff` directory, one for the `my_stuff/web` directory, and one for the file.

Restricting Access to Your Web Site

This section takes you through the process of restricting access to the files or directories on your web site. The sections following this one describe in detail each option available when using access control. Keep in mind that most access control rules use only a subset of the available options.

You can set access control through two iPlanet Web Server mechanisms, both offer flexibility in the scope of your desired settings:

- Administration Server
- Server Manager

NOTE You can set access control globally for all servers through the Administration Server or for a resource within a specific server instance through the Server Manager. This section describes how to use the Server Manager to set up access control within a specific server instance. For more information regarding how to use the Administration Server to set access control globally, see "Restricting Server Access," on page 61 in Chapter 3, "Setting Administration Preferences."

There is also a section of examples you can review in the section "Access Control Examples" on page 242Access Control Examples.

To create an access control rule:

1. From the Server Manager, choose the **Preferences** tab.
2. Click the **Restrict Access** link.

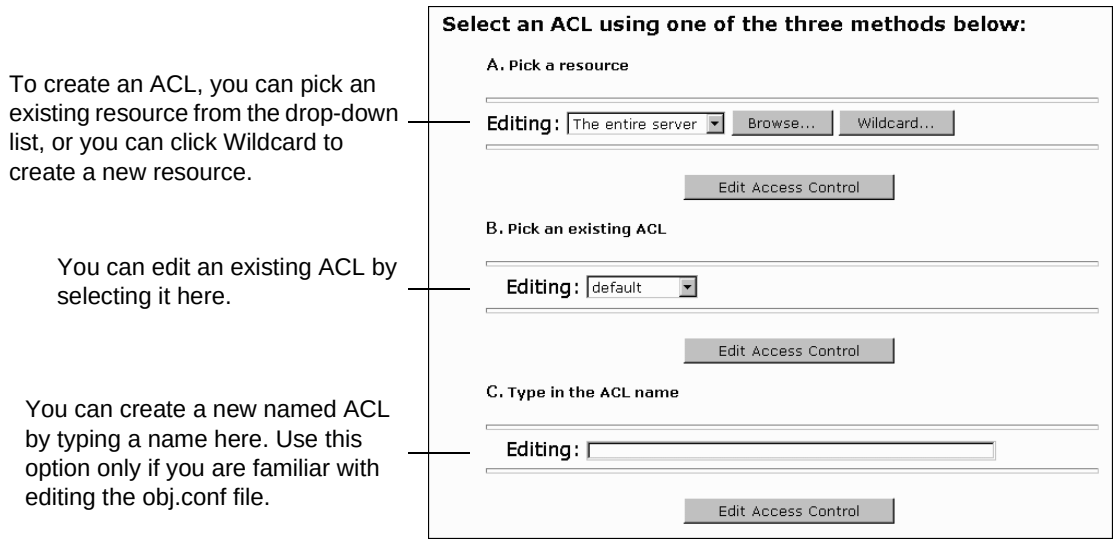
   The Access Control List Management Page appears. There are three parts to this page:

   - **Pick a resource** allows you to specify a wildcard pattern for files or directories to restrict access to (such as `*.html`), or you can choose a directory or a filename to restrict. You can also browse for a file or directory by using the Browse button.
   - **Pick an existing ACL** lists all the ACLs you have enabled. Even if an ACL exists, if you have not enabled it, it will not appear in this list.

Do not delete all the ACL rules from the ACL files. At least one ACL file is required to start the server, and the ACL file must have at least one ACL rule. If you delete all the ACL rules in the ACL files, and try to restart the server, you will see a syntax error.

- **Type in the ACL name** allows you to create named ACLs. Use this option only if you're familiar with ACL files and the `obj.conf` configuration file—you'll need to manually edit `obj.conf` if you want to apply named ACLs to resources.

Figure 12-2 The Restrict Access page has three sections.



3. Specify the part of the server (the resource) that you want to control in the **Pick a resource** section.

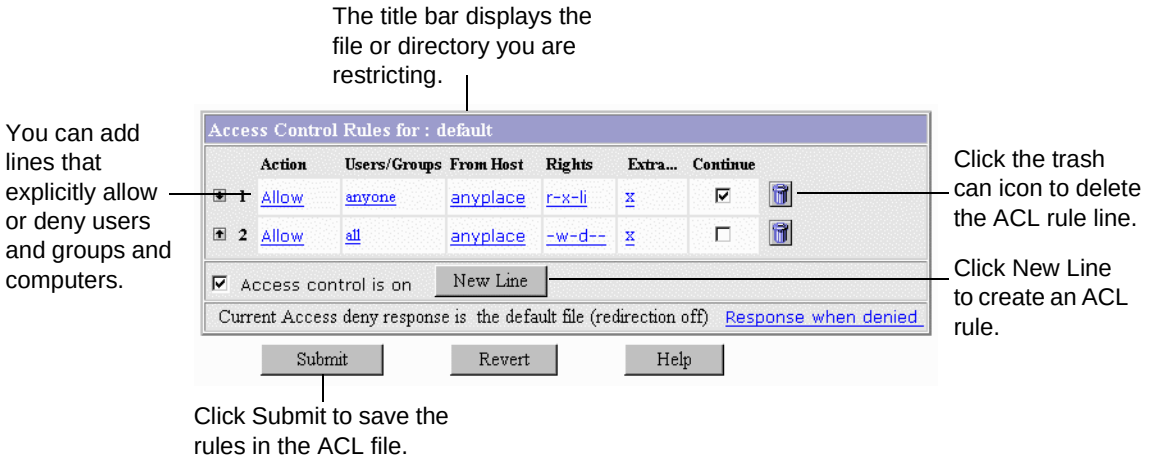
   For example, you can select Entire Server to set up access control for the entire server. The drop-down list contains an entry for each ACL resource defined in the server root.

   For some common examples of resources you might use for access control, see Table 12-1.

4. Click **Edit Access Control**.

The page divides into two frames that you use to set the access control rules. If the resource you chose already has access control, the rules will appear in the top frame. The ACL for iPlanet Web Administration Server, begins with two non-editable deny statements by default. The following figure briefly describes the page elements.

Figure 12-3 The ACL page contains links that, when clicked, display additional information in the bottom frame
(not shown).



5. Click **New Line**.

   This adds a default ACL rule to the bottom row of the table. You can use the up and down arrows in the left column to move the rule.

6. Select the action you want to apply to the rule by clicking **Deny**.

   You can specify whether to deny or allow access to the users, groups, or hosts specified in the following steps in the bottom frame. Select the option you want, and then click **Update**.

7. Specify User-Group authentication by clicking "**anyone"** listed under the Users / Groups column.

   The bottom frame allows you to configure User-Group authentication. By default, there is no authentication, meaning anyone can access the server resource. Select the options you want, and then click **Update**.

8. Specify the computers you want to include in the rule by clicking **anyplace**.

You can enter wildcard patterns of host names or IP addresses to allow or deny in the bottom frame. Select the options you want, and then click **Update**.

9. Specify the access rights you want to include in the rule by clicking **all**. Select the access rights in the bottom frame, and then click **Update**.

10. Specify the programs you want to restrict. Programs are the forms in the Server Manager for the server you selected. For example, you can restrict access to all forms for configuring the administration server by checking the "All Programs" radio button. If you want to restrict access to one or two sets of forms, choose the categories in the drop-down list. If you want to restrict access to one form in a category, type the name of the form in the "Program Items" field. For example, to restrict access to the access control form, type `distacl` in the Program Items field. For more information, see "Access to Programs" on page 238.

    Click **Update** to add the programs options to the rules for the line you're editing.

11. If you are familiar with ACL files, you can enter a customized ACL entry by clicking **X** under the Extra column.

    This area is useful if you use the access control API to customize ACLs.

12. Select **Continue** if you want the access control rule to continue in a chain.

    This means the next line is evaluated before the server determines if the user is allowed access. When creating multiple lines in an access control entry, it's best to work from the most general restrictions to the most specific ones.

13. Repeat steps 5 through 11 for each rule you need.

    If you want the user to be redirected to another URL if their request is denied, check **Response when denied**. Click the link to specify the URL for redirection.

14. Click **Submit** to store the new access control rules in the ACL file.

    If you click **Revert**, the server removes any changes you made to the rules from the time you first opened the two-frame page. Be cautious when using **Revert** because you can't restore your edits. In most cases, it's probably better to delete the rule lines individually.

Table 12-1 LDAP Attributes

Resource wildcard	What it means
default	A named ACL created during installation that restricts write access so only users in the LDAP directory can publish documents.
Entire Server	One set of rules determines the access to your entire web site, including any virtual servers you have running. To restrict access to a virtual server, specify the path of its document root.
`*.html`	Controls access to all files with the `.html` extension
`*.cgi`	Controls access to all files with the `.cgi` extension
`/usr/netscape/server4/docs/cgi-bin/*`	Controls access to all files and directories in the `cgi-bin` directory. You must specify an absolute path. On NT, the path must include the drive letter.
`uri="/sales"`	Controls access to the `sales` directory in the document root. To specify URIs, create a named ACL.

The following sections describe the options that appear in the bottom frame of the access control page.

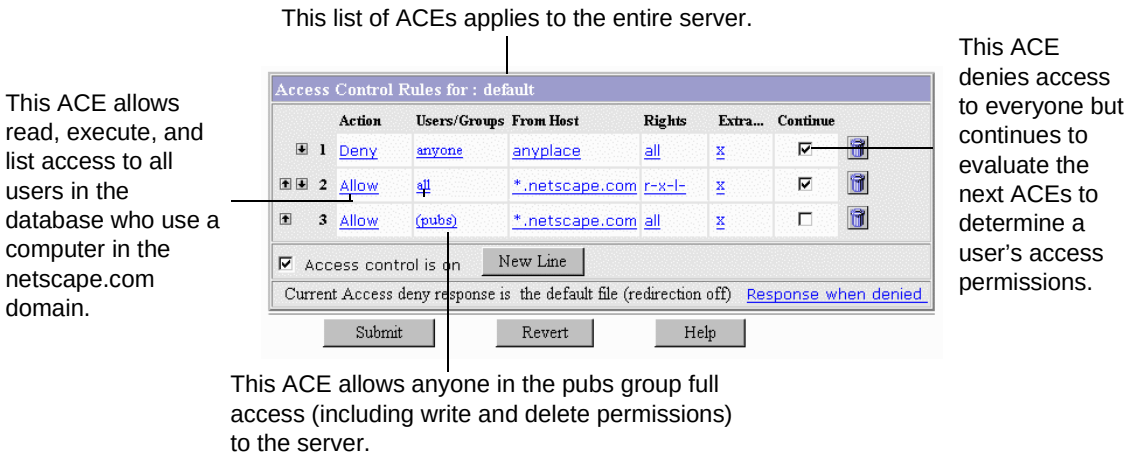
Setting Access Control Actions

You can specify the action the server takes when a request matches the access control rule.

- **Allow** means the users or systems can access the requested resource.
- **Deny** means the users or systems cannot access the resource.

The server goes through the list of ACEs to determine the access permissions. For example, the first ACE is usually to deny everyone. If the first ACE is set to "continue," the server checks the second ACE in the list. (If continue is *not* checked, everyone would be denied access to the resource.) If the second entry matches, then the next ACE is used. The server continues down the list until it reaches either an ACE that doesn't match or that matches but is set to not continue. The last ACE that matches is used to determine if access is allowed or denied. For example, in Figure 12-4 any user in the database can view a file (read access), but they must be in the "pubs" group if they want to publish a file to the server.

Figure 12-4 You can combine Deny and Allow statements in an ACL.



Specifying Users and Groups

You can restrict access to the Administration Server or your web site based on the user who requests a resource. With user and group authentication, users are prompted to enter a username and password before they can access the resource specified in the access control rule.

iPlanet Web Server uses a list of users, who might be sorted into groups, to determine access rights for the user requesting a resource. You must define an administrators group (the group you set up for distributed administration) for access control in the Administration Server. The list of users (and the groups they are included in) are stored in an LDAP server, such as Netscape Directory Server. You should make sure the database contains users and groups (including the administrators group) before you set access control.

You can allow or deny access to everyone in the database, or you can allow or deny specific people by using wildcard patterns or lists of users or groups.

To configure access control with users and groups, follow the general directions for restricting access. When you click the **Users/Groups** field, a additional options appear in the bottom frame. The following list describes the options in the bottom frame.

- **Anyone (No Authentication)** is the default and means anyone can access the resource without having to enter a username or password. However, the user might be denied access based on other settings, such as host name or IP address. For the Administration Server, this means that anyone in the administrators group that you specified with distributed administration can access the pages.
- **All in the authentication database** matches any user who has an entry in the database. To use this option, you must also check "**Authenticated people only**." For the Administration Server, the users you specify must also be in the "administrators" group you specified for distributed administration.
- **Only the following people** lets you specify certain users and groups to match. You can list the users and groups of users individually by separating the entries with commas. Or, you can enter a wildcard pattern. To use this option, you must also check "**Authenticated people only**."
  - **Group** matches all users in the groups you specify. For the Administration Server, the users in the groups you specify must also be in the "administrators" group you specified for distributed administration.
  - **User** matches the individual users you specify.
- **Prompt for authentication** lets you specify message text that appears in the authentication dialog box. You can use this text to describe what the user needs to enter. Depending on the operating system, the user will see about the first 40 characters of the prompt. Netscape Navigator and Netscape Communicator cache the username and password and associate them with the prompt text. This means that if the user accesses areas (files and directories) of the server that have the same prompt, the user won't have to retype usernames and passwords. Conversely, if you want to force users to reauthenticate for various areas, you simply need to change the prompt for the ACL on that resource.
- **Authentication Methods** specifies the method the server uses when getting authentication information from the client.
  - **Default** uses the default method you specify in the `obj.conf` file, or "Basic" if there is no setting in `obj.conf`. If you check Default, the ACL rule doesn't specify a method in the ACL file. Default is the best choice because you can easily change the methods for all ACLs by editing one line in the `obj.conf` file.
  - **Basic** uses the HTTP method to get authentication information from the client. The username and password are only encrypted if encryption is turned on for the server.

  - **SSL** uses the client certificate to authenticate the user. If you use this method, SSL must be turned on for the server. If you have encryption on, you can combine Basic and SSL methods.
  - **Other** uses a custom method you create using the access control API.

- **Authentication Database** lets you select a database that the server uses to authenticate users. The default setting means the server looks for users and groups in an LDAP directory. However, you can configure individual ACLs to use different databases. You can specify different databases and LDAP directories in the file *server_root*`/userdb/dbswitch.conf`. Then, you can choose the database you want to use in the ACL by selecting it in the drop-down list. If you use the access control API to use a custom database (for example, to use an Oracle or Informix database), you can type the name of the database in the "Other" field in the User/Group window.

Specifying Host Names and IP Addresses

You can restrict access to the Administration Server or your web site based on which computer the request comes from. You specify this restriction by using wildcard patterns that match the computers' host names or IP addresses. For example, to allow or deny all computers in a specific domain, you would enter a wildcard pattern that matches all hosts from that domain, such as `*.iplanet.com`. You can set different hostnames and IP addresses that the superuser must use when accessing the Administration Server.

To specify users from hostnames or IP addresses, follow the directions for restricting access in "Restricting Access to Your Web Site" on page 230. When you click the From Host field (the link called **anyplace**), additional options appear in the bottom frame. Check the **Only from** option and then type either a wildcard pattern or a comma-separated list of hostnames and IP addresses. Restricting by hostname is more flexible than by IP address—if a user's IP address changes, you won't have to update this list. Restricting by IP address, however, is more reliable—if a DNS lookup fails for a connected client, hostname restriction cannot be used.

The hostname and IP addresses should be specified with a wildcard pattern or a comma-separated list. The wildcard notations you can use are specialized; you can only use the `*`. Also, for the IP address, the `*` must replace an entire byte in the address. That is, `198.95.251.*` is acceptable, but `198.95.251.3*` is not. When the `*` appears in an IP address, it must be the right-most character. For example, `198.*` is acceptable, but not `198.*.251.30`.

For hostnames, the * must also replace an entire component of the name. That is, `*.iplanet.com` is acceptable, but `*sers.iplanet.com` is not. When the * appears in a hostname, it must be the left-most character. For example, `*.iplanet.com` is acceptable, but `users.*.com` is not.

Setting Access Rights

You can set access rights to files and directories on your web site. That is, in addition to allowing or denying all access rights, you can specify a rule that allows or denies partial access rights. For example, you can give people read-only access rights to your files, so they can view the information but not change the files.

When you create an access control rule, the default access rights are set to all access rights. To change access rights, click the **Rights** link in the top frame, and then choose the access rights you want to set for a particular rule. The following list describes each access right you can check.

- **Read** access lets a user view a file. This access right includes the HTTP methods GET, HEAD, POST, and INDEX.
- **Write** access lets a user change or delete a file. Write access right includes the HTTP methods PUT, DELETE, MKDIR, RMDIR, and MOVE. To delete a file, a user must have both write and delete privileges.
- **Execute** access applies to server-side applications, such as CGI programs, Java applets, and agents.
- **Delete** access means a user who also has write privileges can delete a file or directory.
- **List** access means the user can get directory information. That is, they can get a list of the files in that directory.
- **Info** access means the user can get headers (`http_head` method).

Access to Programs

You can select areas of the administration server that administrators can access. You can choose groups of tabs that appear in the Server Manager , or you can choose specific pages that appear as links in the left frame of the Server Manager (such as “New User” in the User & Groups tab).

To control access to a program in a server, perform the following steps:

1. From the Administration Server, choose the **Global Settings** tab
2. Choose **Restrict Access**.
3. From the drop-down list, choose the server whose administration access you want to restrict. The administration server is labeled "`https-admserv`." Other servers are labeled with their type and their server id (for example, `https-mozilla`).

   When you select a server to restrict, you are restricting who can view the Server Manager pages and which pages they can use to configure that server. For example, you might allow some administrators to configure the Users & Groups section of the administration server and not allow them access to the Global Settings.
4. Click **Edit ACL**. The web server displays the two-frame access control pages.
5. Each ACL begins with two deny lines (the default setting), one that restricts access to only those users in the "administrators" group set for distributed administration, and another that restricts access to all users. If you want to change either of these lines, you need to manually edit the ACL file. Click **New Line** to add a rule to the ACL. Each rule you create allows access to the server. By specifically allowing access for users, you reduce the risk that you'll allow access to users you don't want.
6. Choose the users, groups, hosts, and IP addresses you want to apply to this access control rule.
7. By default, administrators have access to all programs for a server. Click the **All** link under **Programs** in the top frame. The bottom frame displays a page that lists the programs for the server type you selected.
8. Select **Only the following**, and then select the Program Groups you want to apply to the rule. You can choose multiple groups by pressing the Control key and then clicking the groups you want.

   The Program Groups listed use the same name as the buttons in the top frame of the Server Manager for the server type you selected. For example, in the administration server, there are tabs labeled Preferences, Global Settings, and so on. When an administrator accesses the administration server, the server uses their username, host, and IP to determine what pages they'll see. If they have access to only one or two pages, they will only see those pages.

9. You can control access to a specific page within a tab. Type the name of the page in the **Program Items** field. To determine the name of a page, place your pointer over the link in the left frame of the Administration Server and then view the text in the status bar on the bottom of your browser. The last word after the last %2b is the name for that page.

   For example, suppose you have one person who administers a Netscape Directory Server and you want that person to have access only to the "Configure Directory Service" page. In this case, you would set up a rule that applies to them (host, IP, and so on), and then you would enter `dsconfig` in the Program Items field.

10. Click Update and then Submit to save the access control rule.

Writing Customized Expressions

You can enter custom expressions for an ACL. You can use this feature if you are familiar with the syntax and structure of ACL files. There are a few features available only by editing the ACL file or creating custom expressions. For example, you can restrict access to your server depending on the time of day, day of the week, or both.

The following customized expression shows how you could restrict access by time of day and day of the week. This example assumes you have two groups in your LDAP directory: the "regular" group gets access Monday through Friday, 8:00am to 5:00pm. The "critical" group gets access all the time.

```
allow (read)
{
    (group=regular and dayofweek="mon,tue,wed,thu,fri");
    (group=regular and (timeofday>=0800 and timeofday<=1700));
    (group=critical)
}
```

For more information on valid syntax and ACL files, see "ACL File Syntax" on page 259 and "Referencing ACL Files in obj.conf" on page 265.

Selecting “Access control on”

When you uncheck the option labeled “Access control on,” you’ll get a prompt asking if you want to erase records in the ACL. When you click OK, the server deletes the ACL entry for that resource from the ACL file.

If you want to deactivate an ACL, you can comment out the ACL lines in the file `generated-https-server-id.acl` by putting # signs at the beginning of each line.

From the Administration Server, you could create and turn on access control for a specific server instance and leave it off (which is the default) for other servers. For example, you could deny all access to the Server Manager pages from the Administration Server. With distributed administration on and access control off by default for any other servers, administrators could still access and configure the other servers, but they cannot configure the Administration Server.

NOTE This access control is in addition to the user being in the administrators group set for distributed administration. The the Administration Server first checks that a user (other than superuser) is in the administrators group, and then it evaluates the access control rules.

Responding When Access is Denied

You can choose the response a user sees when denied access. You can vary the message for each access control object. By default, the user is sent a message that says the file was not found (the HTTP error code 404 Not Found is also sent).

To change what message is sent for a particular ACL, perform the following steps:

1. In the ACL page, click the **Response when denied** link.
2. In the lower frame, check the **Respond with the following file** radio button.
3. In the text field, type a URL or URI to a text or HTML file in your server’s document root that you want to send to users when they are denied access. The server must have read access to this file, so you should consider putting the file in the document root.

   Make sure the file does not contain references to other files or images because they will not be sent.
4. Click **Update**.

Make sure any users who get the response file have access to that file. If you have access control on the response file and the user is denied access to both the original resource and the response file, the server will send the default denied response.

5. Make sure you submit the access control rule by clicking **Submit** in the top frame.

Access Control Examples

This section describes some common examples for restricting access to a web server and its contents. Some of these examples assume you set up the "default" ACL to deny anyone access to the server. You can also add a "deny all" line as the first rule to each of these examples, as done in the example for the entire server (see "Restricting Access to the Entire Server" on page 242).

This section includes the following topics:

- Restricting Access to the Entire Server
- Restricting Access to a Directory (Path)
- Restricting Access to a URI (Path)
- Restricting Access to a File Type
- Restricting Access Based on Time of Day

Restricting Access to the Entire Server

This example allows access to users in a group called "employees" who access the server from computers in a subdomain. There are no access control rules for other resources on the server. You might use this example if you have a server for a department and you only want users to access the server from computers in a specific subdomain of your network.

To restrict access to the entire server, perform the following steps:

1. In iPlanet Web Server, choose **Server Preferences**.
2. Click the **Restrict Access** link.

   The web server displays the Access Control List Management page.

3. In the section called **Pick a Resource**, select “The entire server” from the Editing drop-down list and then click **Edit Access Control**.

   The two-frame page appears.

4. Click **New Line**.

   The default rule appears, which denies all access to the server. Typically, you should deny all access to your server, and then allow specific access to users, groups, and computers; however, you might change this if you want to deny access only to a small group of users or groups. Click New Line again to create a second rule.

5. Click the **Deny** link in the second rule. In the bottom frame that appears, check **Allow**, and then click **Update**.

6. Click the “**anyone”** link in the second rule. In the bottom frame, type the group you want to have access to the server.

   For this example, type `employees` in the Group field. Note that the two options called “**Authenticated people only”** and “**Only the following people”** are checked automatically. Click **Update**.

7. Click the “**anyplace”** link in the second rule. In the bottom frame, type a wildcard pattern for the host names of the computers you want to allow.

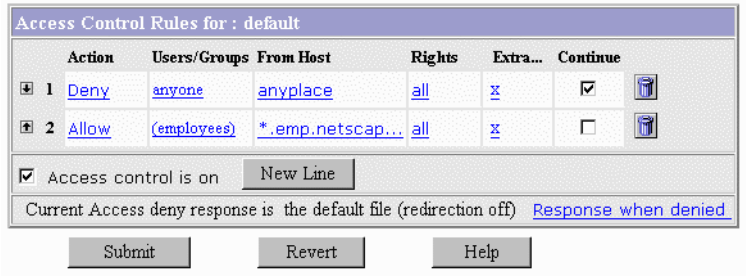
   For example, type `*.emp.mozilla.com` in the Host Names field. Click **Update**.

8. Unselect **Continue** in the top frame, and then click **Submit**.

   The frame should look like the one in Figure 12-5.

9. Submit your changes.

Figure 12-5 Restricting access to the entire server



Be sure to restart the server for the changes to take affect. The following text is the ACL file for this example.

```
# File automatically written
#
# You may edit this file by hand
#
version 3.0;
acl "default";
authenticate (user,group) {
  prompt = “Web Server”
}
deny (all)
  user = "anyone";
allow absolute (all)
  (group = "employees") and
  (dns = "*.emp.netscape.com");
```

Restricting Access to a Directory (Path)

This example lets users in a group called “executives” have read access to a directory and its subdirectories and files on the server. The user called “ceo” has full permissions to the directory.

You might use this example if you have a directory on your server that one person owns (that is, they publish to this directory) and you want one group of users to read the files. For example, you might have a project owner who publishes status information for the project team to review.

To restrict access to a directory on the server, perform the following steps:

1. In the Server Manager, choose **Server Preferences**.
2. Click the **Restrict Access** link.

   The web server displays the Access Control List Management page.
3. In the section called **Pick a Resource**, click the **Browse** button.

   In the page that appears, click the link for the directory you want to restrict. The directories listed in this page are in the servers document root. Once you click a link, the **Editing** drop-down list displays the absolute path to the directory.

NOTE If you want to view all files in your server root, click **Options** and check the box labeled **List files as well as directories** and then click OK.

4. Click **Edit Access Control**.

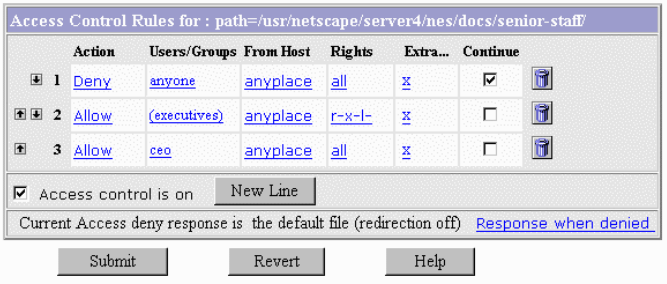
   The two-frame pages appear.
5. Click **New Line** twice to create two rules.

   Don't edit the default values for the first rule—they deny all access to the directory. You'll edit the second rule to allow read access to the "executives" group.
6. Click **Deny** in the second rule. In the bottom frame that appears, check Allow, and then click **Update**.
7. Click **anyone** in the second rule. In the bottom frame, type the group you want to have access to the server. For this example, type `executives` in the Group field. Click **Update**.
8. Click **all** in the top frame. Uncheck the **Write and Delete** access rights.

   This means the users in the executives group can't add or remove files, but they can view them and run any applications in the directories. Click **Update**.
9. Click **New Line** to create a rule for the "ceo" user. Check **Allow** for the third rule.
10. Click **anyone**. In the bottom frame, type `ceo` in the User field. Click **Update**.
11. Uncheck **Continue** for both the second and the third rules.

This means that the server ignores any ACLs for directories or files under the directory you specified in Step 3. The frame should look like the one in Figure 12-6.

Figure 12-6 Restricting access to a path in the server



12. Click **Submit** and save and apply your changes.

The entry in the `generated.https-`*serverid*`.acl` file for this example looks like this:

```
acl "path=/usr/netscape/server4/nes/docs/senior-staff/";
deny (all)
    user = "anyone";
allow absolute (read,execute,list)
    group = "executives";
allow absolute (all)
    user = "ceo";
```

Restricting Access to a URI (Path)

This example uses a URI to control access to a single user's content on the web server. URIs are paths and files relative to the server's document root directory. Using URIs is an easy way to manage your server's content if you frequently rename or move all or part of it (for example, for disk space). It's also a good way to handle access control if you have additional document roots.

This example gives anyone read access to files and directories in the path specified by the URI `/my_directory`. Only one user ("me" in this example) has full access to the directories and files.

You might use this example if you have several users who publish their content on your server. The users want to have write access to their content, and they want anyone to have read/execute access.

To restrict access to a URI, perform the following steps:

1. In the Server Manager, choose **Server Preferences**.
2. Click the **Restrict Access** link.

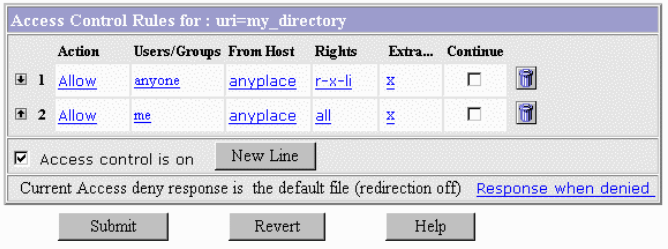
   The web server displays the Access Control List Management page.
3. In the **Type in the ACL name** section, type the URI you want to control. For example, type `uri=/my_directory`.
4. Click **Edit Access Control**.

   The two-frame pages appear.
5. Click **New Line** to create the first rule that allows all users read access.
6. Click the **Deny** link. In the bottom frame that appears, check **Allow**, and then click **Update**.
7. Click the **all** link in the top frame. Uncheck the **Write and Delete** access rights.

   This means users cannot add or remove files, but they can view them and run any applications in the directories. Click **Update**.
8. Click **New Line** to create a rule for the owner of the directory. Check **Allow** for the second rule.
9. Click **anyone**. In the bottom frame, type `me` in the User field. Click **Update**.
10. Uncheck **Continue** for both the first and second rules.

    This means that the server ignores any ACLs for other URIs, directories, or files under the URI you specified in Step 3. The frame should look like the one in Figure 12-7.

Figure 12-7 Restricting access to a URI (path) in the document root



11. Click **Submit** and save and apply your changes.

The entry in the `generated.https-`*serverid*`.acl` file for this example looks like this:

```
acl "uri=/my_directory";
allow absolute (read,execute,list,info)
    user = "anyone";
allow absolute (all)
    user = "me";
```

Restricting Access to a File Type

This example controls write and delete access to all files with the extension `.cgi`. You might use this example if you only want specific users to create programs that run on your server. In this example, anyone can run the programs, but only users in the “programmers” group can create or delete them.

To restrict access to a file type, perform the following steps:

1. In the Server Manager, choose **Server Preferences**.
2. Click **Restrict Access**.

   The web server displays the Access Control List Management page.
3. In the **Pick a resource** section, click **Wildcard**. In the prompt that appears, type `*.cgi` and click OK.

   This wildcard pattern matches any request that contains a file or directory with the `.cgi` extension.

4. Click **Edit Access Control**.

   The two-frame pages appear.

5. Click **New Line** to create the first rule that will allow all users read access.

6. Click **Deny**. In the bottom frame that appears, check **Allow**, and then click **Update**.

7. Click **all** in the top frame. Uncheck the **Write and Delete** access rights.

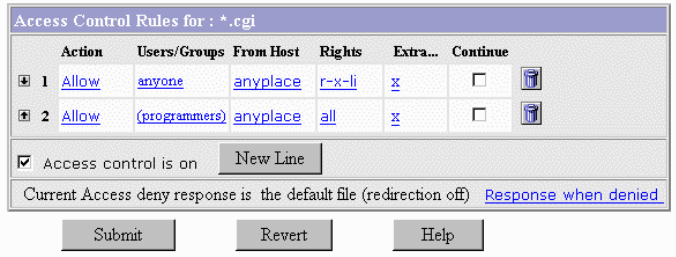
   This means users can't add or remove files or directories with the `.cgi` extension. Click **Update**.

8. Click **New Line** to create a rule that allows write and delete access to the "programmers" group. Check **Allow** for the second rule.

9. Click **anyone**. In the bottom frame, type `programmers` in the **Group** field. Click **Update**.

   The frame should look like the one in Figure 12-8.

Figure 12-8 Restricting access to a file type—in this case, to files with the .cgi extension



10. Click **Submit** and save and apply your changes.

In this example, both continue boxes are checked. This means that if a request for a file comes in, the server will first look at the ACL for the file type, and then it will continue to look for another ACL that matches (for example, am ACL on the URI or the path). The web server checks ACLs in the following order:

1. **Pathcheck functions in `obj.conf`**. For example, these could be wildcard patterns for files or directories. The entry in the ACL file would appear as follows: `acl "*.cgi";`

2. **URIs**. For example, a path relative to the document root. The entry in the ACL file would appear as follows: `acl "uri=/my_directory";`

3. **Pathnames**. For example, an absolute path to a file or directory. The entry in the ACL file would appear as follows:
   `acl “path=d:\netscape\suitespot\docroot1\sales/”;`

The entry in the `generated.https-`*`serverid`*`.acl` file for this example looks like this:

```
acl "*.cgi";
allow (read,execute,list,info)
  user = "anyone";
allow (all)
  group = "programmers";
```

Restricting Access Based on Time of Day

This example restricts write and delete access to the server during working hours. You might use this example if you don’t want people publishing documents at times when people might be accessing the files. This example allows users to publish during the evening during the week (between 6:00pm and 6:00am, Monday through Friday) and all time during the weekend.

To restrict access based on time of the day and day of the week, perform the following steps:

1. In the Server Manager, choose **Server Preferences**.
2. Click **Restrict Access**.
3. In the **Pick a Resource** section, select “The entire server” from the Editing drop-down list. (You can select any resource.) Click **Edit Access Control**.

   The server displays the two-frame pages.
4. Click **New Line**.
5. Click the **Deny** link. In the bottom frame that appears, check **Allow**, and then click **Update**.
6. Click the **all** link in the top frame. Uncheck the **Write and Delete** access rights.

   This means that if a user wants to add, update, or delete a file or directory, this rule won’t apply and the server will search for another rule that matches. Click **Update**.

7. Click **New Line** to create a rule that restricts the write and delete methods. Check **Allow** for the second rule.

8. Click the **X** link to create a customized expression. In the bottom frame, type the following lines:

```
user = "anyone" and
dayofweek = "sat,sun" or
(timeofday >= 1800 and
timeofday <= 600)
```

   You might want to select the entire text element and copy to memory—if there are errors, you'll have to reenter the text. Click **Update**. The top frame will display "Unrecognized expressions" in the Users/Groups and From Host fields because you created a custom expression.

9. Click **Submit**. If you made any errors in the custom expression, you'll get a JavaScript alert. Correct any changes and click Submit again.

Restart your server for the changes to take effect.

Appendix A

HyperText Transfer Protocol

This appendix provides a short introduction to a few HyperText Transfer Protocol (HTTP) basics. For more information on HTTP, see the Internet Engineering Task Force (IETF) home page at:

```
http://www.ietf.org/home.html
```

This appendix contains the following sections:

- About HyperText Transfer Protocol (HTTP)
- Requests
- Responses

About HyperText Transfer Protocol (HTTP)

The **HyperText Transfer Protocol (HTTP)** is a protocol (a set of rules that describe how information is exchanged on a network) that allows a web browser and a web server to "talk" to each other using the ISO Latin1 alphabet, which is ASCII with extensions for European languages.

HTTP is based on a request/response model. The client connects to the server and sends a request to the server. The request contains the following: request method, URI, and protocol version. The client then sends some header information. The server's response includes the return of the protocol version, status code, followed by a header that contains server information, and then the requested data. The connection is then closed.

The iPlanet Web Server 4.x supports HTTP 1.1. Previous versions of the server supported HTTP 1.0. The server is conditionally compliant with the HTTP 1.1 proposed standard, as approved by the Internet Engineering Steering Group (IESG) and the Internet Engineering Task Force (IETF) HTTP working group. For more information on the criteria for being conditionally compliant, see the Hypertext Transfer Protocol—HTTP / 1.1 specification (RFC 2068) at:

```
http://www.ietf.org/html.charters/http-charter.html
```

Requests

A request from a client to a server includes the following information:

- Request method
- Request header
- Request data

Request Method

A client can request information using a number of methods. The commonly used methods include the following:

- `GET`—Requests the specified document
- `HEAD`—Requests only the header information for the document
- `POST`—Requests that the server accept some data from the client, such as form input for a CGI program
- `PUT`—Replaces the contents of a server's document with data from the client

Request Header

The client can send header fields to the server. Most are optional. Some commonly used request headers are shown in Table A-1.

Table A-1 Common request headers

Request header	Description
`Accept`	The file types the client can accept.

Table A-1 Common request headers *(Continued)*

Request header	Description
`Authorization`	Used if the client wants to authenticate itself with a server; information such as the username and password are included.
`User-agent`	The name and version of the client software.
`Referer`	The URL of the document where the user clicked on the link.
`Host`	The Internet host and port number of the resource being requested.

Request Data

If the client has made a `POST` or `PUT` request, it can send data after the request header and a blank line. If the client sends a `GET` or `HEAD` request, there is no data to send; the client waits for the server's response.

Responses

The server's response includes the following:

- Status code
- Response header
- Response data

Status Code

When a client makes a request, one item the server sends back is a status code, which is a three-digit numeric code. There are four categories of status codes:

- Status codes in the 100–199 range indicate a provisional response.
- Status codes in the 200–299 range indicate a successful transaction.
- Status codes in the 300–399 range are returned when the URL can't be retrieved because the requested document has moved.
- Status codes in the 400–499 range indicate the client has an error.

- Status codes of 500 and higher indicate that the server can't perform the request, or an error has occurred.

Table A-2 contains some common status codes.

Table A-2 Common HTTP status codes

Status code	Meaning
200	OK; successful transmission. This is not an error.
302	Found. Redirection to a new URL. The original URL has moved. This is not an error; most browsers will get the new page.
304	Use a local copy. If a browser already has a page in its cache, and the page is requested again, some browsers (such as Netscape Navigator) relay to the web server the "last-modified" timestamp on the browser's cached copy. If the copy on the server is not newer than the browser's copy, the server returns a 304 code instead of returning the page, reducing unnecessary network traffic. This is not an error.
401	Unauthorized. The user requested a document but didn't provide a valid username or password.
403	Forbidden. Access to this URL is forbidden.
404	Not found. The document requested isn't on the server. This code can also be sent if the server has been told to protect the document by telling unauthorized people that it doesn't exist.
500	Server error. A server-related error occurred. The server administrator should check the server's error log to see what happened.

Response Header

The response header contains information about the server and information about the document that will follow. Common response headers are shown in Table A-3.

Table A-3 Common response headers

Response header	Description
`Server`	The name and version of the web server.
`Date`	The current date (in Greenwich Mean Time).
`Last-modified`	The date when the document was last modified.
`Expires`	The date when the document expires.
`Content-length`	The length of the data that follows (in bytes).
`Content-type`	The MIME type of the following data.
`WWW-authenticate`	Used during authentication and includes information that tells the client software what is necessary for authentication (such as username and password).

Response Data

The server sends a blank line after the last header field. The server then sends the document data.

Appendix B

ACL File Syntax

This appendix describes the access-control list (ACL) files and their syntax. ACL files are text files that contain lists that define who can access resources stored on your web server. By default, the web server uses one ACL file that contains all of the lists for access to your server. However, you can create multiple ACL files and reference them in the `obj.conf` file.

You need to know the syntax and function of ACL files if you plan on customizing access control using the access-control API. For example, you might use the access control API to interface with another database, such as an Oracle or Informix database. For more information on the API, see the iPlanet documentation site at:

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

This appendix contains the following sections:

- ACL File Syntax
- Referencing ACL Files in obj.conf

ACL File Syntax

All ACL files must follow a specific format and syntax. An ACL file is a text file containing one or more ACLs. All ACL files must begin with the version number they use. There can be only one version line and it can appear after any comment lines. For example:

```
version 3.0;
```

You can include comments in the file by beginning the comment line with the # sign.

Each ACL in the file begins with a statement that defines its type. ACLs can follow one of three types:

- **Path ACLs** specify an absolute path to the resource they affect
- **URI (Uniform Resource Indicator) ACLs** specify a directory or file relative to the server's document root.
- **Named ACLs** specify a name that is referenced in resources in the `obj.conf` file. The server comes with a "default" named resource that allows read access to anyone and write access to users in the LDAP directory. Even though you can create a named ACL from the iPlanet Web Server windows, you must manually reference the named ACLs with resources in the `obj.conf` file.

The type line begins with the letters `acl` and then includes the type information in double-quotation marks followed by a semicolon. Each type information for all ACLs must be a unique name--even among different ACL files. The following lines are examples of several different types of ACLs:

```
acl "path=C:/Netscape/server4/docs/mydocs/";
acl "*.html";
acl "default";
acl "uri=/mydocs/";
```

After you define the type of ACL, you can have one or more statements that define the method used with the ACL (authentication statements) and the people and computers who are allowed or denied access (authorization statements). The following sections describe the syntax for these statements.

Authentication Statements

ACLs can optionally specify the authentication method the server must use when processing the ACL. There are two general methods:

- Basic requires users to enter a username and password before accessing a resource.
- SSL requires the user to have a client certificate. For this method to work, the web server must have encryption turned on, and the CA must be in the list of trusted CAs.

By default, the server uses the Basic method for any ACL that doesn't specify a method.

Each authenticate line must specify what list (users, groups or both) the server should use when authenticating users. The following authentication statement, which would appear after the ACL type line, specifies basic authentication with users matched to individual users in the database or directory:

```
authenticate (user) {
     method = “basic”;
};
```

The following example uses SSL as the authentication method for users and groups:

```
authenticate (user, group) {
     method = “ssl”;
};
```

The following example allows any user whose username begins with the letters `sales`:

```
authenticate (user)
allow (all)
    user = sales*
```

If the last line was changed to `group = sales`, then the ACL would fail because there are no groups in the user lists.

Authorization Statements

Each ACL entry can include one or more authorization statements. Authorization statements specify who is allowed or denied access to a server resource. Use the following syntax when writing authorization statements:

```
allow|deny [absolute] (right[,right...]) attribute expression;
```

Start each line with either allow or deny. It’s usually a good idea to deny access to everyone in the first rule and then specifically allow access for users, groups, or computers in subsequent rules. This is because of the hierarchy of rules. That is, if you allow anyone access to a directory called `/my_stuff`, and then you have a subdirectory `/my_stuff/personal` that allows access to a few users, the access control on the subdirectory won’t work because anyone allowed access to the `/my_stuff` directory will also be allowed access to the `/my_stuff/personal` directory. To prevent this, create a rule for the subdirectory that first denies access to anyone and then allows it for the few users who need access.

However, in some cases if you set the default ACL to deny access to everyone, then your other ACL rules don’t need a “deny all” rule.

The following line denies access to everyone:

```
deny (all)
    user = "anyone";
```

Hierarchy of Authorization Statements

ACLs have a hierarchy that depends on the resource. For example, if the server receives a request for the document (URI) `/my_stuff/web/presentation.html`, the server first looks for an ACL that matches the file type or any other wildcard pattern that matches the request, then it looks for one on the directory, and finally it looks for an ACL on the URI. If there are more than one ACLs that match, the server uses the last statement that matches. However, if you use an absolute statement, then the server stops looking for other matches and uses the ACL containing the absolute statement. If you have two absolute statements for the same resource, the server uses the first one in the file and stops looking for other resources that match.

For example, using the ACL hierarchy with the request for the document `/my_stuff/web/presentation.html`, you could have an absolute ACL that restricts access to the file type `*.html`. Then the server would use that ACL instead of looking for one that matches the URI or the path.

```
version 3.0;
acl "default";
authenticate (user,group) {
     prompt="WebServer Server";
};
allow (read,execute,list,info)
     user = "anyone";
allow (write,delete)
     user = "all";
acl "*.html";
deny absolute (all)
     user = "anyone";
acl "uri=/my_stuff/web/presentation.html";
deny (all)
     user = "anyone";
allow (all)
     user = "anyone";
```

Attribute Expressions

Attribute expressions define who is allowed or denied access based on their username, group name, host name, or IP address. The following lines are examples of allowing access to different people or computers:

- `user = “anyone”`

- `user = “smith*”`
- `group = “sales”`
- `dns = “*.iplanet.com”`
- `dns = “*.iplanet.com,*.mozilla.com”`
- `ip = “198.*”`
- `ciphers = “rc4”`

You can also restrict access to your server by time of day (based on the local time on the server) by using the `timeofday` attribute. For example, you can use the `timeofday` attribute to restrict access to certain users during specific hours.

Note

Use 24-hour time to specify times (for example, use 0400 to specify 4 a.m. or 2230 for 10:30 p.m.).

The following example restricts access to a group of users called guests between 8 a.m. and 4:59 pm.

```
allow (read)
     (group="guests") and
     (timeofday<800 or timeofday=1700);
```

You can also restrict access by day of the week. Use the following three-letter abbreviations to specify days of the week: Sun, Mon, Tue, Wed Thu, Fri, and Sat.

The following statement allows access for users in the premium group any day and any time. Users in the discount group get access all day on weekends and on weekdays anytime except 8am-4:59pm.

```
allow (read) (group="discount" and dayofweek="Sat,Sun") or
(group="discount" and (dayofweek="mon,tue,wed,thu,fri" and
(timeofday<0800 or timeofday=1700)))
or
(group="premium");
```

Operators For Expressions

You can use various operators in attribute expressions. You can use parentheses to delineate the order of precedence of the operators. With `user`, `group`, `dns`, and `ip`, you can use the following operators:

- `and`
- `or`
- `not`

- = (equals)
- != (not equal to)

With `timeofday` and `dayofweek`, you can use the following additional operators:

- greater than
- < less than
- = greater than or equal to
- <= less than or equal to

The Default ACL File

After installing the server, the server uses the default settings in the file `server_root/httpacl/generated.https-serverid.acl`. There is also a file called `genwork.https-serverid.acl` that is a working copy the server uses until you save and apply your changes when working with the user interface. When editing the ACL file, you might want to work in the `genwork` file and then use the iPlanet Web Server to save and apply the changes.

The following text is from the default file:

```
# File automatically written
#
# You may edit this file by hand
#
version 3.0;
acl "agents";
authenticate (user,group) {
          prompt = "WebServer Server";
};
deny (all)
    user = "anyone"
allow absolute (all)
    user = "all";
acl "default";
allow (read,execute,list,info)
    user = "anyone";
allow (write,delete)
    user = "all";
```

The default ACL file is referenced in `magnus.conf` as follows:

```
ACLFile absolutepath/generated.https-serverid.acl
```

You can reference multiple ACL files in magnus.conf and then use their ACLs for resources in `obj.conf`. However, the server uses only the first ACL file when evaluating access control for objects that don't have specific ACLs listed in `obj.conf`. If you're using the iPlanet Web Server windows to do some access control, the first ACL file in magnus.conf should point to the file `generated.https-serverid.acl`. See the section "Referencing ACL Files in obj.conf" on page 265 for more information.

General Syntax Items

Input strings can contain the following characters:

- Letters a through z
- Numbers 0 through 9
- Period and underscore

If you use any other characters, you need to use double-quotation marks around the characters.

A single statement can be placed on its own line and be terminated with a semicolon. Multiple statements are placed within braces. A list of items must be separated by commas and enclosed in double-quotation marks.

Referencing ACL Files in obj.conf

If you have named ACLs or separate ACL files, you can reference them in the `obj.conf` file. You do this in the `PathCheck` directive using the `check-acl` function. The line has the following syntax:

```
PathCheck fn="check-acl" acl="aclname"
```

The `aclname` is a unique name of an ACL as it appears in any ACL file.

For example, you might add the following lines to your `obj.conf` file if you want to restrict access to a directory using the acl named `testacl`:

```
<Object ppath="/usr/ns-home/docs/test/*"
PathCheck fn="check-acl" acl="testacl"
</Object
```

In the previous example, the first line is the object that states which server resource you want to restrict access to. The second line is the `PathCheck` directive that uses the `check-acl` function to bind the name ACL (`testacl`) to the object in which the directive appears. The `testacl` ACL can appear in any ACL file referenced in `magnus.conf`.

Internationalized iPlanet Web Server

The internationalized version of the iPlanet Web Server contains special features tailored for the non-U.S. environment. These features include a choice of user-interface language (Japanese, French, or German) and a choice of search engines that allow you to use text search on a variety of languages.

This appendix contains the following sections:

- General Information
- Server-side JavaScript Information
- Search Information
- Getting Support for Accented Characters in Filenames

General Information

The following information covers the international considerations for general server capabilities.

This section includes the following topics:

- Installing the Server
- Entering 8-bit Text
- Using the Accept Language Header
- Language Settings in Configuration Files

Installing the Server

When you install the server, you choose what user-interface language to use, as well as what search engines to install.

For information on installing the international version of the server, see the iPlanet Web Server, FastTrack Edition 4.1 *Release Notes.* You can access the *Release Notes* online via the link provided in the `README` file.

Entering 8-bit Text

If you want to type 8-bit data into the Server Manager or the administration server forms, you need to be aware of the issues in this section.

File or Directory Names

If a file or directory name is to appear in a URL, it cannot contain 8-bit or multi-byte characters.

LDAP Users and Groups

For email addresses, use only those characters permitted in RFC 822 (`ftp://ds.internic.net/rfc/rfc822.txt`). User ID and password information must be stored in ASCII.

If you use a local database, you can enter 8-bit and multi-byte characters, but you should standardize on one character set. If you use more than one character set in the same database, it can cause display and search problems.

If you must use 8-bit or multi-byte characters in your directory database, you should store them in UTF-8 for future compatibility with the Netscape Directory Server version 4.x. To make sure you enter characters in the correct format, use a UTF-8 form-capable client (such as Netscape Communicator) to input 8-bit or double-byte data.

If you let users access their own user and group information, they will need to use a UTF-8 form-capable client.

NOTE iPlanet Web Server 4.x no longer packages the `ldapsearch` and `ldapmodify` utilities. Earlier versions of Enterprise Server included them, since those versions employed local LDAP database support. iPlanet Web Server 4.x now uses an LDAP server all the time which includes these utilities.

NOTE The default maximum number of parallel LDAP sessions is now set to 8. There is a way to override this limitation. In addition to the `binddn` and `bindpw` properties that a LDAP connection listed in `dbswitch.conf` may have, iPlanet Web Server 4.x now includes a `sessions` property. The value is numeric and this property sets the maximum number of parallel connections in the LDAP session pool.

Using the Accept Language Header

When clients contact a server using HTTP 1.1, they can send header information that describes the various languages they accept. You can configure your server to parse this language information.

For example, suppose this feature is set to *on*, and a client configured to send the accept language header sends it with the value `en,fr`. Now suppose that the client requests the following URL:

`http://www.`*someplace*`.com/`*somepage*`.html`

The server first looks for:

`http://www.`*someplace*`.com/en/`*somepage*`.html`

If it does not find that, it looks for:

`http://www.`*someplace*`.com/fr/`*somepage*`.html`

If that is not available either, and a `ClientLanguage` (call it `xx`) is defined in the `magnus.conf` file, the server tries:

`http://www.`*someplace*`.com/xx/`*somepage*`.html`

If none of these exist, the server tries:

`http://www.`*someplace*`.com/`*somepage*`.html`

Language Settings in Configuration Files

The following directives in the `magnus.conf` file affect languages:

Table C-1 International settings in magnus.conf

Directive	Values	Description
`ClientLanguage`	`en`, `fr`, `de`, `ja`	Specifies the language in which client messages, such as "Not Found" or "Access denied" are to be expressed. This value is used to identify a directory containing `ns-https.db`.
`DefaultLanguage`	`en`, `fr`, `de`, `ja`	Specifies the language used if a resource cannot be found for the client language or the administration language.
`AcceptLanguage`	`on`, `off`	Enables or disables the Accept language header parsing.

The following directives in the `ns-admin.conf` file affect languages:

Table C-2 International settings in ns-admin.conf

Directive	Values	Description
`ClientLanguage`	`en`, `fr`, `de`, `ja`	If the client does not send an accept language header, `ClientLanguage` defines the language of the Directory Server User Information and Password pages. The two-letter value code is used to find the directory containing `ns-admin.db`.
`AdminLanguage`	`en`, `fr`, `de`, `ja`	Sets the language used for administrative pages that are accessed through the administration server.
`DefaultLanguage`	`en`, `fr`, `de`, `ja`	The language used if a value cannot be found for the client or admin languages.

Server-side JavaScript Information

When you use server-side JavaScript with the international version of the server, you have additional things to consider when compiling applications and using databases. For example, you can specify the language of the JavaScript application one of two ways: using the compiler, or using the HTML `<META>` tag.

Specifying the Character Set for the Compiler

For the international version, the server-side JavaScript compiler (`jsac`) has a `-l` option called *charSet*. This option specifies the character set being used in the input HTML files. The value for *charSet* is one of the following character set names.

Table C-3 Valid values for charSet

Language	Value for *charSet*
Western European	`iso-8859-1`
Central European	`iso-8859-2`
Cyrillic	`iso-8859-5`
Japanese	`iso-2022-jp`, `x-sjis`, `x-euc-jp`
Korean	`iso-2022-kr`, `x-euc-kr`
Simplified Chinese	`x-gb2312`
Traditional Chinese	`x-big5`, `x-euc-ch`
Greek	`iso-8859-7`
Turkish	`iso-8859-9`

Usage

To use this option, use the following format:

```
jsac [-cdv] [-l charSet] -o binaryFile [-i] inputFile1 [-i]
inputFile2 ...
```

```
jsac [-cdv] -o binaryFile -f includeFile
```

```
jsac -h
```

Options

The following table shows the options for the compiler.

Table C-4 Options for the jsac compiler

Option	Usage
`-c`	Check only; do not generate *binaryFile*
`-v`	Enable verbose output
`-d`	Enable debug output

Table C-4 Options for the jsac compiler *(Continued)*

Option	Usage
`-o`	Name of *binaryFile* (output file).
`-i`	Name of *inputFile* (use if the input filename starts with a switch character)
`-f`	Name of *includeFile* (has input filenames, separated by white space)
`-l`	Name of *charSet* (for example, `iso-8859-1`, `x-sjis`, `euc-kr`)
`-h`	Display this help

The possible filename extensions are summarized in the following table:.

Table C-5 File extensions

Extension	File type
`.html` or `.htm`	HTML source file (may include JavaScript)
`.js`	JavaScript source file
`.web`	Binary output file

When you specify the language using the compiler option, you can only specify one language. If you want to specify multiple languages, you can use the `<META>` tag in the individual files.

Specifying the Character Set With the <META> Tag

You can also use the `<META>` tag to specify the character set information. For example, if you put the following statement into the header (between `<HEAD>` and `</HEAD>`) in a JavaScript program, the server-side JavaScript compiler (`jsac`) considers the file to be written in `x-sjis`.

```
<META HTTP-EQUIV="Content-Type" CONTENT="test/html;
CHARSET=x-sjis">
```

If the character set specified in the `<META>` tag is different from the character set specified by the compiler's *charSet* option, the character set specified by the compiler option is used.

Using Server-side Javascript With Oracle's Japanese Database

To use server-side JavaScript with Oracle's Japanese database, you need to install Oracle and set up your environment, verify the connection, and verify the language setup. follow these overall steps. This section discusses these topics:

- Installing Oracle and Setting Up Your Environment
- Verifying the Connection
- Verifying the Language Setup

Installing Oracle and Setting Up Your Environment

You must first install the Japanese Oracle database. For instructions, see the documentation that came with your database. Next, you must set up your environment variables using the following information. Note that the environment variable syntax assumes C Shell.

Server-side JavaScript library:

- `setenv LD_LIBRARY_PATH` *server_root*`/bin/https:$LD_LIBRARY_PATH`

Environment variables for Oracle:

- `setenv ORACLE_HOME` *oracle_root*
  for example, `/usr/oracle7`
- `setenv ORACLE_SID` *oracle_service_ID*
  for example, `WG73`
- `setenv TNS_ADMIN` *path_to_tnsnames.ora*
  `for example, /.../tnsnames.ora`

Environment variable for NLS (National Language Support) in Oracle:

- `setenv NLS_LANG` *language_charset_info*
  for example, `japanese_japan.JA16EUC`

  (This example sets up `x-euc-jp`)

Environment variable for the path:

- `setenv PATH` *server_root*`/bin/https:$ORACLE_HOME/bin:$PATH`

Restart the web server from the command line.

Verifying the Connection

1. At the Application Manager, select and run `dbadmin`.
2. Click **Connect to Database Server**.
3. Enter the following information in the window, and click Connect. If your server identifier, user ID, or password is different from these default values, enter your actual values here.

Table C-6

Field	Value
Server Type	`ORACLE`
Server Identifier	`WG73`
User ID	`system`
Password	`manager`
Database	

Unless you see an error indicating otherwise, you are now connected.

Verifying the Language Setup

Use the `videoapp` sample application to verify the language setup.

1. If your ORACLE installation has a server identifier, user ID, or password that is different from the default values shown in the previous table, be sure to specify the actual values in the `start.htm` file at the following line:

   ```
   project.sharedConnections.pool =
   new DbPool("ORACLE","WG73", "system", "manager", "", 2, false)
   ```

2. Run the build script in the directory to recompile the JavaScript code.
3. At the Application Manager, select and run **`vidoeapp`**.
4. Click **Add New Customer** and enter data in the character set you specified.
5. Click **Home** to go back to the `videoapp` home page, and then click **Save Changes**.
6. Click **Delete a Customer**.
7. Check to see if the data you entered appears in the table. If the data appears in the database in the correct language, you've set up the languages correctly.

Putting the Oracle Client and Database Server On Separate Hosts

To put the Oracle client (with server-side JavaScript database service) and the Oracle database server on separate hosts, follow these steps:

1. On the client side, define the `SERVER SID` alias to refer to the server in `tnsnames.ora`.
2. Set the `TWO_TASK` environment variable to the `SERVER SID` alias defined in the `tsnames.ora` file. For example:

   ```
   setenv TWO_TASK SERVER SID alias
   ```

3. Set the `NLS_LANG` environment variable to the correct client language and character set information.
4. Using the sample application `videoapp`, edit the `start.htm` file as shown below. (In this example, assume that the `SERVER SID` alias is `remoteDB`.)

   ```
   project.sharedConnections.pool = new DbPool("ORACLE","remoteDB",
   "system", "manager", "", 2, false)
   ```

5. Click **Add New Customer** and enter data in the character set you specified.
6. Click **Home** to go back to the `videoapp` home page, and then click **Save Changes**.
7. Click **Delete a Customer**.
8. Check to see if the data you entered appears in the table. If the data appears in the database correctly, you've configured your system properly.

Search Information

Search capabilities are supported for the following languages:

- English
- German
- French
- Italian
- Spanish
- Swedish
- Dutch

- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

You choose which search engines to install when you install the international version of the server.

International Search and Auto Catalog

If your server contains documents in various character set encodings, the search collections and / or auto catalog for the documents will inherit the same encodings as the originals. To view documents in different character set encodings, users must change the character set encoding for their browsers. In addition, since the text search and auto catalog features work with one character set encoding at a time, you might receive inaccurate results when using those features. For best results, use one specific character set for all documents.

Searching in Chinese, Japanese, and Korean

The following information is specific to searching in Japanese, Korean, and Chinese.

Query Operators

This release supports the following query operators for Japanese, Korean and Chinese languages:

Table C-7 Query operators for Japanese

Operator	J/C/K Character
AND	Yes
CONTAINS	No
ENDS	Yes
MATCHES	Yes
NEAR	Yes
NEAR/N	Yes

Table C-7 Query operators for Japanese

Operator	J/C/K Character
NOT	Yes
OR	Yes
PHRASE	Yes
STARTS	Yes
STEM	English only
SUBSTRING	Yes
WILDCARD *	Yes
WILDCARD ?	Yes
WILDCARD {}	No
WILDCARD []	No
WILDCARD ^	No
WILDCARD -	No
WORD	Yes

Document Formats

This release supports the following document formats for the Japanese, Korean, and Chinese languages:

- HTML
- ASCII
- NEWS
- MAIL

Searching in Japanese

The following sections give additional information about searching in the Japanese character set.

Document Codes

This release supports the following document codes for the Japanese language:

- euc

- `sjis`
- `jis` (7-bit)

Search Words

This release supports the following search words:

- Kanji
- hirakana
- katakana (full-width and half-width)
- ascii-string (full-width and half-width)

The search engine translates half-width katakana to full-width katakana, and translates full-width ascii-string to half-width ascii-string. Users can use full-width and half-width as the same characters.

This release also supports phrase and sentence search.

Getting Support for Accented Characters in Filenames

If the filenames on your server contain accented characters, for instance elninõ.html, you can get support for them by specifying the 8859 character set as the internal coding for search collections. To specify 8859, you need to modify the file `language.conf` in the directory `<serverRoot>\plugins\search\admin`. This file is used by the Search Engine and the document indexing features of the server.

The `language.conf` file contains the following lines for the English language. These lines direct the server to configuration files that use 8859 as the default character set. The configuration files are located in the directory `<serverRoot>\plugins\search\common`.

```
# [en-ns]
# name = English NS 8859 (ISO-8859-1)
# lang = english-ns;8859
# charset = iso-8859-1
# cjk = N
# encode850 = N
```

To specify 8859, you need to activate these lines in `language.conf` by removing the comment characters (#).

If you make this change to the `language.conf` file after a collection has been created, to support accented characters in filenames for that collection you need to delete the collection, make this change to the file, recreate the collection choosing “English NS 8859 (ISO-8859-1” from the “Documents are in” drop-down list, and reindex all the documents in the collection.

Glossary

Access Control Entries (ACEs) A hierarchy of rules which the web server uses to evaluate incoming access requests.

Access Control List (ACL) A collection of ACEs. An ACL is a mechanism for defining which users have access to your server. You can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users and groups.

admpw The username and password file for the Enterprise Administrator Server superuser.

agent Software that runs the network-management software in a network device, such as a router, host, or X terminal. See also intelligent agents.

authentication Allows client to verify that they are connected to an SSL-enabled server, preventing another computer from impersonating the server or attempting to appear SSL-enabled when it isn't.

authorization The granting of access to an entire server or particular files and directories on it. Authorization can be restricted by criteria including hostnames and IP addresses.

browser See client.

cache A copy of original data that is stored locally. Cached data doesn't have to be retrieved from a remote server again when requested.

certification authority (CA) A third-party organization that issues digital files used for encrypted transactions.

certificate A nontransferable, nonforgeable, digital file issued from a third party that both communicating parties already trust.

Certificate revocation list (CRL) CA list, provided by the CA, of all revoked certificates.

Compromised key list (CKL) A list of key information about users who have compromised keys. The CA also provides this list.

CGI Common Gateway Interface. An interface by which external programs communicate with the HTTP server. Programs that are written to use CGI are called CGI programs or CGI scripts. CGI programs handle forms or parse output the server does not normally handle or parse.

ciphertext Information disguised by encryption, which only the intended recipient can decrypt.

client Software, such as Netscape Navigator, used to request and view World Wide Web material. Also known as a browser program.

collection A database that contains information about documents, such as word list and file properties. Collections are used by the search function to retrieve documents matching specified search criteria.

Common LogFile Format The format used by the server for entering information into the access logs. The format is the same among all major servers, including the iPlanet FastTrack and Enterprise servers.

DHCP Dynamic Host Configuration Protocol. An Internet Proposed Standard Protocol that allows a system to dynamically assign an IP address to individual computers on a network.

daemon (Unix) A background process responsible for a particular system task.

DNS Domain Name System. The system that machines on a network use to associate standard IP addresses (such as 198.93.93.10) with hostnames (such as `www.netscape.com`). Machines normally get this translated information from a DNS server, or they look it up in tables maintained on their systems.

DNS alias A hostname that the DNS server knows points to a different host—specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as `www.`*`yourdomain.domain`* might point to a real machine called `realthing.`*`yourdomain.domain`* where the server currently exists.

document root A directory on the server machine that contains the files, images, and data you want to present to users accessing the server.

drop word See stop word.

encryption The process of transforming information so it can't be decrypted or read by anyone but the intended recipient.

Enterprise Administration Server A web-based server that contains the Java and JavaScript forms you use to configure all of your Netscape Enterprise Servers

expires header The expiration time of the returned document, specified by the remote server.

extranet An extension of a company's intranet onto the Internet, to allow customers, suppliers, and remote workers access to the data.

file extension The last part of a filename that typically defines the type of file. For example, in the filename `index.html` the file extension is `html`.

file type The format of a given file. For example, a graphics file doesn't have the same file type as a text file. File types are usually identified by the file extension (`.gif` or `.html`).

firewall A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. Firewalls are commonly used to protect information such as a network's email and data files within a physical building or organization site.

flexible log format A format used by the server for entering information into the access logs.

FORTEZZA An encryption system used by U.S. government agencies to manage sensitive but unclassified information.

FTP File Transfer Protocol. An Internet protocol that allows files to be transferred from one computer to another over a network.

GIF Graphics Interchange Format. A cross-platform image format originally created by CompuServe. GIF files are usually much smaller in size than other graphic file types (BMP, TIFF). GIF is one of the most common interchange formats. GIF images are readily viewable on Unix, Microsoft Windows, and Apple Macintosh systems.

hard restart The termination of a process or service and its subsequent restart. See also soft restart.

home page A document that exists on the server and acts as a catalog or entry point for the server's contents. The location of this document is defined within the server's configuration files.

hostname A name for a machine in the form *machine.domain.dom*, which is translated into an IP address. For example, `www.netscape.com` is the machine `www` in the subdomain `netscape` and `com` domain.

HTML Hypertext Markup Language. A formatting language used for documents on the World Wide Web. HTML files are plain text files with formatting codes that tell browsers such as the Netscape Navigator how to display text, position graphics and form items, and display links to other pages.

HTTP HyperText Transfer Protocol. The method for exchanging information between HTTP servers and clients.

HTTP-NG The next generation of HyperText Transfer Protocol.

HTTPD An abbreviation for the HTTP daemon or service, a program that serves information using the HTTP protocol. The iPlanet FastTrack Server is often called an HTTPD.

HTTPS A secure version of HTTP, implemented using the Secure Sockets Layer, SSL.

imagemap A process that makes areas of an image active, letting users navigate and obtain information by clicking the different regions of the image with a mouse. Imagemap can also refer to a CGI program called "imagemap," which is used to handle imagemap functionality in other HTTPD implementations.

inittab (Unix) A Unix file listing programs that need to be restarted if they stop for any reason It ensures that a program runs continuously. Because of its location, it is also called `/etc/inittab`. This file isn't available on all Unix systems.

intelligent agent An object within a server that performs various requests (such as HTTP, NNTP, SMTP, and FTP requests) on behalf of the user. In a sense, the intelligent agent acts as a client to the server, making requests that the server fulfills.

IP address Internet Protocol address. A set of numbers, separated by dots, that specifies the actual location of a machine on the Internet (for example, 198.93.93.10).

ISDN Integrated Services Digital Network.

ISINDEX An HTML tag that turns on searching in the client. Documents can use a network navigator's capabilities to accept a search string and send it to the server to access a searchable index without using forms. In order to use <ISINDEX>, you must create a query handler.

ISMAP ISMAP is an extension to the IMG SRC tag used in an HTML document to tell the server that the named image is an imagemap.

ISP Internet Service Provider. An organization that provides Internet connectivity.

Java An object-oriented programming language created by Sun Microsystems used to create real-time, interactive programs called applets.

JavaScript A compact, object-based scripting language for developing client and server Internet applications.

JavaServer Pages Extensions that enable all JavaServer page metafunctions, including instantiation, initialization, destruction, access from other components, and configuration management. JavaServer pages, are reusable Java applications that run on a web server rather than in a web browser.

Java Servlets Extensions that enable all Java servlet metafunctions, including instantiation, initialization, destruction, access from other components, and configuration management. Java servlets are reusable Java applications that run on a web server rather than in a web browser.

last-modified header The last modification time of the document file, returned in the HTTP response from the server.

magnus.conf The main Enterprise Server configuration file. This file contains global server configuration information (such as, port, security, and so on). This file sets the values for variables that configure the server during initialization. Enterprise Sever reads this file and executes the variable settings on startup. The server does not read this file again until it is restarted, so you must restart the server every time you make changes to this file.

MD5 A message digest algorithm by RSA Data Security. MD5 can be used to produce a short digest of data that is unique with high probability. It is mathematically extremely hard to produce a piece of data that produces the same message digest email.

MD5 signature A message digest produced by the MD5 algorithm.

MIB Management Information Base.

MIME Multi-Purpose Internet Mail Extensions. An emerging standard for multimedia email and messaging.

mime.types The MIME (Multi-purpose Internet Mail Extension) type configuration file. This file maps file extensions to MIME types, to enable the server to determine the type of content being requested. For example, requests for resources with `.html` extensions indicate that the client is requesting an HTML file, while requests for resources with `.gif` extensions indicate that the client is requesting an image file in GIF format.

MTA Message Transfer Agent. You must define your server's MTA Host to use agent services on your server.

Netscape Console A Java application that provides server administrators with a graphical interface for managing all Netscape servers from one central location anywhere within your enterprise network. From any installed instance of Netscape Console, you can see and access all the Netscape servers on your enterprise's network to which you have been granted access rights.

NIS (Unix) Network Information Service. A system of programs and data files that Unix machines use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computers.

network management station (NMS) A machine users can use to remotely manage a network. A managed device is anything that runs SNMP such as hosts, routers, and Netscape/iPlanet servers. An NMS is usually a powerful workstation with one or more network management applications installed.

NNTP Network News Transfer Protocol for newsgroups. You must define your news server host to use agent services on your server.

NSAPI See Server Plug-in API.

obj.conf The server's object configuration file. This file contains additional initialization information, settings for server customization, and instructions that the server uses to process requests from clients (such as browsers). FastTrack Server reads this file every time it processes a client request.

password file (Unix) A file on Unix machines that stores Unix user login names, passwords, and user ID numbers. It is also known as `/etc/passwd`, because of where it is kept.

primary document directory See document root.

protocol A set of rules that describes how devices on a network exchange information.

private key The decryption key used in public-key encryption.

public key The encryption key used in public-key encryption.

public information directories (Unix) Directories not inside the document root that are in a Unix user's home directory, or directories that are under the user's control.

Quality Feedback Agent An error-handling mechanism that enables you to automatically send error information (stack and register dump) to Netscape.

RAM Random access memory. The physical semiconductor-based memory in a computer.

rc.2.d (Unix) A file on Unix machines that describes programs that are run when the machine starts. This file is also called `/etc/rc.2.d` because of its location.

redirection A system by which clients accessing a particular URL are sent to a different location, either on the same server or on a different server. This system is useful if a resource has moved and you want the clients to use the new location transparently. It's also used to maintain the integrity of relative links when directories are accessed without a trailing slash.

resource Any document (URL), directory, or program that the server can access and send to a client that requests it.

RFC Request For Comments. Usually, procedures or standards documents submitted to the Internet community. People can send comments on the technologies before they become accepted standards.

root (Unix) The most privileged user on Unix machines. The root user has complete access privileges to all files on the machine.

server daemon A process that, once running, listens for and accepts requests from clients.

Server Plug-in API An extension that allows you to extend and/or customize the core functionality of Netscape servers and provide a scalable, efficient mechanism for building interfaces between the HTTP server and back-end applications. Also known as NSAPI.

server root A directory on the server machine dedicated to holding the server program, configuration, maintenance, and information files.

SOCKS Firewall software that establishes a connection from inside a firewall to the outside when direct connection would otherwise be prevented by the firewall software or hardware (for example, the router configuration).

soft restart A way to restart the server that causes the server to internally restart, that is, reread its configuration files. A soft restart sends the process the HUP signal (signal number one). The process itself does not die, as it does in a hard restart.

SSL Secure Sockets Layer. A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP.

stop word A word identified to the search function as a word not to search on. This typically includes such words as *the*, *a*, *an*, *and*. Also referred to as *drop words*.

strftime A function that converts a date and a time to a string. It's used by the server when appending trailers. `strftime` has a special format language for the date and time that the server can use in a trailer to illustrate a file's last-modified date.

superuser (Unix) The most privileged user available on Unix machines (also called root). The superuser has complete access privileges to all files on the machine.

Sym-links (Unix) Abbreviation for symbolic links, which is a type of redirection used by the Unix operating system. Sym-links let you create a pointer from one part of your file system to an existing file or directory on another part of the file system.

TCP/IP Transmission Control Protocol/Internet Protocol. The main network protocol for the Internet and for enterprise (company) networks.

telnet A protocol where two machines on the network are connected to each other and support terminal emulation for remote login.

timeout A specified time after which the server should give up trying to finish a service routine that appears hung.

top (Unix) A program on some Unix systems that shows the current state of system resource usage.

top-level domain authority The highest category of hostname classification, usually signifying either the type of organization the domain is (for example, `.com` is a company, `.edu` is an educational institution) or the country of its origin (for example, `.us` is the United States, `.jp` is Japan, `.au` is Australia, `.fi` is Finland).

uid (Unix) A unique number associated with each user on a Unix system.

URI Uniform Resource Identifier. A file identifier that provides an additional layer of security by using an abbreviated URL. The first part of the URL is substituted with a URL mapping that hides the file's full physical pathname from the user. See also URL mapping.

URL Uniform Resource Locator. The addressing system used by the server and the client to request documents. A URL is often called a location. The format of a URL is *`protocol://machine`*`:`*`port/document`*.

A sample URL is `http://www.netscape.com/index.html`.

URL database repair A process that repairs and updates a URL database that has been damaged by a software failure, a system crash, a disk breakdown, or a full file system.

URL mapping The process of mapping a document directory's physical pathname to a user-defined alias so that files within the directory need only refer to the directory's alias instead of the file's full physical pathname. Thus, instead of identifying a file as `usr/Netscape/SuiteSpot/docs/index.html`, you could identify the file as `/myDocs/index.html`. This provides additional security for a server by eliminating the need for users to know the physical location of server files.

Windows CGI (Windows NT) CGI programs written in a Windows-based programming language such as Visual Basic.

Index

SYMBOLS

NUMERICS

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X