

# Tru64 UNIX

---

## Compaq Secure Web Server Administration Guide

**November 2001**

**Product Version:** Compaq Secure Web Server Version 5.7 for Tru64 UNIX

This document describes the administration tasks for configuring and managing the Compaq Secure Web Server (based on Apache) for Compaq Tru64 UNIX operating system.

---

© 2001 Compaq Computer Corporation

Compaq, the Compaq logo, and AlphaServer Registered in U.S. Patent and Trademark Office. Tru64 is a trademark of Compaq Information Technologies Group, L.P. in the United States and other countries.

Microsoft, Windows, and FrontPage are trademarks of Microsoft Corporation in the United States and other countries. UNIX and The Open Group are trademarks of The Open Group in the United States and other countries. All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from Compaq required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

---

# Contents

## About This Manual

### 1 Overview

1.1	Accessing the Compaq Secure Web Servers .....	1-1
1.1.1	Managing the Administrator Password .....	1-2
1.2	Web Server Administration Functions .....	1-3
1.3	Dynamic Modules .....	1-3
1.4	Tomcat Java Servlet and JSP Engine .....	1-3
1.5	SSL and the Compaq Secure Web Server .....	1-4

### 2 Managing the Compaq Secure Web Server

2.1	Changing Configuration Parameters .....	2-1
2.1.1	Changing Server Tuning Parameters .....	2-3
2.1.2	Changing Access Control Entry Parameters .....	2-4
2.1.3	Changing Listening Port and IP Address Parameters .....	2-6
2.1.4	Changing Virtual Host Parameters for the Public Web Server ...	2-7
2.1.5	Changing URL Default Parameters for the Public Web Server ...	2-8
2.1.6	Changing HTML Directory Alias Parameters for the Public Web Server .....	2-9
2.1.7	Changing CGI Directory Alias Parameters for the Public Web Server .....	2-10
2.1.8	Changing Logging and Reporting Parameters .....	2-11
2.2	Changing Public Web Server User Accounts .....	2-12
2.3	Displaying Public Web Server Status .....	2-13
2.4	Displaying Public Web Server Information .....	2-14
2.5	Viewing Web Server Reports and Log Files .....	2-14
2.6	Refreshing the Administration Web Server Log Files .....	2-16
2.7	Starting and Stopping the Compaq Secure Web Server .....	2-16
2.8	Changing the Password for the Compaq Secure Web Server .....	2-17
2.9	Allowing Remote Access to the Administration Web Server .....	2-18

### 3 Using Dynamic Modules

3.1	Compaq Secure Web Server Support for Apache Dynamic Modules ..	3-1
3.1.1	Standard Modules Provided as DSO Modules .....	3-2
3.1.2	Non-Standard Modules Provided as DSO Modules .....	3-2
3.2	Activating the Apache DSO Modules .....	3-2
3.2.1	Using the LoadModule Directive .....	3-3
3.2.2	Using the AddModule Directive .....	3-3
3.2.3	Verifying the Configuration File .....	3-3
3.2.4	Activating an Apache DSO Module — Example .....	3-3
3.2.5	Web Server LDAP Authentication Requires LDAP Runtime Library .....	3-4

### 4 Implementing the Tomcat Java Servlet and JSP Engine

4.1	Tomcat Overview .....	4-1
-----	-----------------------	-----

4.2	Locating Tomcat Directories .....	4-1
4.3	Starting Tomcat .....	4-2
4.3.1	Restarting Tomcat in a Non-TruCluster Enviroment .....	4-2
4.3.2	Restarting Tomcat in a TruCluster Enviroment .....	4-2
4.3.3	Tomcat Log Files .....	4-2
4.4	Accessing the Tomcat Examples .....	4-3
4.5	Locating Additional Information .....	4-3

## 5 Enabling the Secure Socket Layer Protocol

5.1	SSL Concepts .....	5-1
5.2	Enabling SSL Support from the Web Server Administration Utility ..	5-2
5.3	Generating a Private Key .....	5-3
5.4	Generating a Certificate Request .....	5-3
5.5	Generating and Installing a Test Certificate .....	5-5
5.6	Installing a Digital Certificate .....	5-6
5.7	Viewing Certificate Details .....	5-7
5.8	Enabling and Disabling SSL for a Web Server .....	5-8
5.9	Testing Your SSL Connection .....	5-9
5.10	Specifying Public Web Server Access to HTTP and HTTPS Connections .....	5-9
5.11	Migrating Your Netscape Digital Certificate to the Compaq Secure Web Server .....	5-10
5.11.1	Prerequisites for Migration .....	5-10
5.11.2	Migrating the Netscape Digital Certificate .....	5-10

## A Compaq Secure Web Server Components and Modules

### Glossary

### Index

### Figures

1-1	Compaq Secure Web Server Main Menu .....	1-2
1-2	Secure Web Server Administration Menu .....	1-2
2-1	Change Configuration Parameters Menu .....	2-2
2-2	Change Tuning Parameters Form .....	2-3
2-3	Change Access Control Entries Form .....	2-4
2-4	Change Listening Ports and IP Addresses Form .....	2-6
2-5	Change Web Server Public Instance Virtual Hosts Form .....	2-7
2-6	Change Web Server Public Instance URL Defaults Form .....	2-8
2-7	Change Web Server Public Instance HTML Directory Aliases Form ..	2-9
2-8	Change Web Server Public Instance CGI Directory Aliases Form ....	2-10
2-9	Change Logging and Reporting Parameters Form .....	2-11
2-10	Manage the Public Web Server Form .....	2-13
2-11	Report and Log Files for the Public Web Server .....	2-14
2-12	Manage the Administration Web Server Menu .....	2-15
2-13	Report and Log Files for the Administration Web Server Menu .....	2-15
2-14	Start/Stop the Administration Web Server Server Form .....	2-17
2-15	Change the Password for All Administration Servers Form .....	2-17
2-16	Change Administration Web Server Configuration Parameters Menu .....	2-18

2-17	Modify Administration Web Server Access Control Entry Form .....	2-19
5-1	Manage SSL for the Public Web Server Menu .....	5-2
5-2	Generate a Private Key — Results .....	5-3
5-3	Generate a Certificate Request Form .....	5-4
5-4	Certificate Request Success Notice .....	5-5
5-5	Test Certificate Installation Success Notice .....	5-6
5-6	Manage SSL Main Menu with Additional Options .....	5-6
5-7	Install a Certificate Text Field .....	5-7
5-8	Certificate File in Readable Format .....	5-8
5-9	Enable SSL Confirmation Page .....	5-9
5-10	SSL Connections Error Message .....	5-9

## Tables

2-1	Configuration Files for Compaq Secure Web Servers .....	2-1
2-2	Server Tuning Parameters and Associated Directives .....	2-3
2-3	Access Control Parameters and Associated Directives .....	2-5
2-4	Listening Port/IP Address Parameters and Associated Directives ....	2-7
2-5	Virtual Hosts Parameters and Associated Directives .....	2-7
2-6	URL Default Parameters and Associated Directives .....	2-8
2-7	HTML Directory Alias Parameters and Associated Directives .....	2-10
2-8	CGI Directory Alias Parameter and Associated Directive .....	2-10
2-9	Logging and Reporting Parameters and Associated Directives .....	2-11
2-10	Activity Reports for the Compaq Secure Web Servers .....	2-16
3-1	Standard Compaq Secure Web Server Modules .....	3-2
4-1	Tomcat Log Files .....	4-3
A-1	Compaq Secure Web Server Components .....	A-1
A-2	Standard Compaq Secure Web Server Modules .....	A-2
A-3	Related Modules Provided with the Compaq Secure Web Server .....	A-3
A-4	Additional Modules Provided with the Compaq Secure Web Server ..	A-3



---

# About This Manual

This document describes the administration tasks for configuring and managing the Compaq™ Secure Web Server (based on Apache) for the Tru64™ UNIX operating system.

## Audience

This document is intended for the system administrator who manages Internet services on a Tru64 UNIX AlphaServer™ system.

## Organization

This document consists of the following chapters:

<i>Chapter 1</i>	Provides an overview of the Compaq Secure Web Server.
<i>Chapter 2</i>	Describes the general administration tasks for managing a Compaq Secure Web Server.
<i>Chapter 3</i>	Explains how to implement dynamic modules.
<i>Chapter 4</i>	Explains how to implement the Tomcat Java Servlet and JSP Engine.
<i>Chapter 5</i>	Describes how to enable the Secure Socket Layer (SSL) to provide secure Internet connections to your server.
<i>Appendix A</i>	Lists the Compaq Secure Web Server components and modules.

This document also contains a glossary and an index.

## Related Documents

Consult the following documentation for information on installing, configuring, and administering Internet solutions on Tru64 UNIX operating systems.

### Internet Express

For information on installing, configuring, and administering Open Source and other Web server-related software, see the Documentation Bookshelf provided with Internet Express. (Compaq includes the Internet Express CD-ROM with Tru64 UNIX AlphaServer systems.)

After installation of the Compaq Secure Web Server subset (IAEAPCH) and the Internet Express Documentation subset (IAEDOC), and after installation of the Internet Express Administration Utility (IAEADM subset), you can access the Administration utility for Internet Express and read the documentation following the link from the Web page at `http://hostname.domain:8081`.

You can also read the documentation without the Administration Utility using the public Web server (if you chose to configure one) by accessing the documentation index page at `http://hostname.domain/documents/bookshelf.html`.

If this URL does not work, verify that the Web server configuration file `/usr/internet/httpd/admin/conf/httpd.conf` contains the following line:

```
Alias /documents/ "/usr/internet/docs/IASS/"
```

In order for the links to reference pages to work correctly, you must enable the webman application. To do this, edit `/usr/internet/httpd/admin/conf/httpd.conf`. Add the following lines, if necessary:

```
ScriptAlias /webman/ "/usr/internet/webman/"
Alias /webman-content/ "/usr/internet/webman/"
```

Now, restart the Web Server, using the following command:

```
# /sbin/init.d/httpd_public restart
```

You can also read the installed documentation directly from the file system using a Web browser running on the same system by using the file URL: `file:/usr/internet/docs/IASS/bookshelf.html` but in this case you will not be able to use the reference page links.

You can also access the Documentation Bookshelf on the Internet Express CD-ROM. The documentation is available in the following formats:

- HTML
- PostScript
- Portable Document Format (PDF)

### **Tru64 UNIX Operating System Base Documentation**

The Documentation Overview describes the documentation that comes with the Compaq Tru64 UNIX operating system. The Compaq Tru64 UNIX documentation main page can be accessed from the following URL:

<http://www.tru64unix.compaq.com/docs/>

### **Tru64 UNIX Best Practices Documentation**

Compaq Tru64 UNIX Best Practices describe additional concepts and tasks, for Internet as well as other topics. You can find these documents at the following URL:

[http://www.tru64unix.compaq.com/docs/best\\_practices](http://www.tru64unix.compaq.com/docs/best_practices)

## **Reader's Comments**

Compaq welcomes any comments and suggestions you have on this and other Tru64 UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-884-0120. Attn: USPG Publications, ZKO3-3/Y32
- Internet electronic mail: [readers\\_comment@zk3.dec.com](mailto:readers_comment@zk3.dec.com)

A Reader's Comment form is located on your system in the following location:

```
/usr/doc/readers_comment.txt
```

- Mail:

```
Compaq Computer Corporation
USD Publications Manager
ZKO3-3/Y32
110 Spit Brook Road
Nashua, NH 03063-2698
```

Please include the following information along with your comments:

- The full title of the document
- The section numbers and page numbers of the information on which you are commenting
- The version of Tru64 UNIX and Internet Express that you are using
- If known, the type of processor that is running Tru64 UNIX

The Tru64 UNIX Publications Group cannot respond to system problems or technical support inquiries. Please address technical questions to your local system vendor or to the appropriate Compaq technical support office. Information provided with the software media explains how to send problem reports to Compaq.

## Conventions

The following typographical conventions are used in this document:

%	
\$	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells.
#	A number sign represents the superuser prompt.
% <b>cat</b>	Boldface type in interactive examples indicates typed user input.
<i>file</i>	Italic (slanted) type indicates variable values, placeholders, and function argument names.
[   ]	
{   }	In syntax definitions, brackets indicate items that are optional and braces indicate items that are required. Vertical bars separating items inside brackets or braces indicate that you choose one item from among those listed.
...	In syntax definitions, a horizontal ellipsis indicates that the preceding item can be repeated one or more times.
cat(1)	A cross-reference to a reference page includes the appropriate section number in parentheses. For example, cat(1) indicates that you can find information on the cat command in Section 1 of the reference pages.
<span style="border: 1px solid black; padding: 2px;">Return</span>	In an example, a key name enclosed in a box indicates that you press that key.
Ctrl/x	This symbol indicates that you hold down the first named key while pressing the key or mouse button that follows the slash. In examples, this key combination is enclosed in a box (for example, <span style="border: 1px solid black; padding: 2px;">Ctrl/C</span> ).



---

## Overview

The Compaq Secure Web Server (based on Apache) is an implementation of the Apache Software Foundation's (ASF) Apache **HTTP** server for Tru64 UNIX. It contains a packaged, integrated and tested version of many of the popular components of the Apache Web server (`mod_ssl`, PHP, `fastcgi`, and others) and the modules that are used with it.

The Compaq Secure Web Server integrates other features beyond the core modules supplied by ASF, including:

- Support for Dynamic Shared Objects (DSO).
- Support for SSL connections (HTTPS) using a DSO module.
- Support for APXS, which allows third party modules to be built against and used with an installed Compaq Secure Web Server.
- Support for SUEXEC, once it is enabled in the server (an additional configuration is required to enable it).
- Support for the Atalla hardware accelerator cards.
- Support for the Tomcat Java Servlets and JSP Engine.

In addition, all modules provided with the Apache code base are built-in or provided as a DSO, except for the `auth_digest` module.

The Compaq Secure Web Server provides a Web-based administration interface that allows an administrator to perform common management tasks on the Web server. You access these administration pages from the Web Server Administration utility (see Section 1.1).

The Compaq Secure Web Server is available on the Associated Products CD-ROM, included with the Tru64 UNIX operating system distribution, and is also available with Internet Express for Tru64 UNIX. Compaq includes the Internet Express CD-ROM with Tru64 UNIX AlphaServer systems. If you need the Internet Express CD-ROM, you can contact your Compaq representative. The part number for the Internet Express product is QB-3NCAA-SA.

### 1.1 Accessing the Compaq Secure Web Servers

The Compaq Secure Web Server provides the following servers for managing Internet services:

- **Public** — The public web server is an instance of the Compaq Secure Web Server, listening on Port 80, that can be configured and used by anyone.
- **Administration** — The Web Server Administration Server is an instance of the Compaq Secure Web Server that listens on Port 8081 and Port 8089. It provides an administration interface for the Compaq Secure Web Servers accessible from a Web browser.

The URL takes the form:

```
http://host.domain.name:port
```

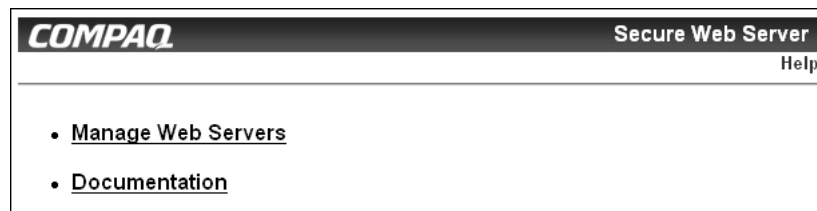
where *host.domain.name* represents the fully qualified host name of the local system (the system on which Internet Express is installed) and *port* represents either Port 80, 8081, or 8089.

The Web Server Administration Server is initially accessible from the local system only. To allow access from a remote system when running the Compaq Secure Web Server, see Section 2.9.

To access the Compaq Secure Web Servers, follow these steps:

1. From an HTML-based Web browser (such as Netscape Navigator Version 4.5 or later, or Microsoft Internet Explorer Version 4.0 or later), enter the URL, indicating either Port 80, 8081, or 8089. When you access the Administration server, you are prompted for a user name and password.
2. Enter a user name and password. The default user name for Web server administration is `admin`. During installation, the system administrator sets a password to be used for the Web server administration accounts. To change the password for the Administration Web server, see Section 1.1.1. Figure 1–1 shows the Compaq Secure Web Server main menu when you first log in.

**Figure 1–1: Compaq Secure Web Server Main Menu**



When you choose Manage Web Servers from the main menu, the Secure Web Server Administration menu is displayed, listing the available servers and providing a link for changing server passwords. Figure 1–2 shows the Secure Web Server Administration menu.

**Figure 1–2: Secure Web Server Administration Menu**



When you access the Web server, you are given access to privileged files and can perform system management tasks until exiting the browser. Do not leave an administration session unattended. Limit access to the `admin` account to those individuals authorized to perform Internet system management tasks.

### 1.1.1 Managing the Administrator Password

During installation of the Compaq Secure Web Server, a single Web administration user is created for accessing all Web Server Administration Server instances. The username is `admin`. The administrator password is set to the password that you entered during installation.

If you know the administrator password, you can change it using the Web Server Administration utility (Section 2.8).

If you received your Compaq Secure Web Server software preinstalled from Compaq or if you have forgotten your administrator password, the `/usr/internet/httpd/bin/dbmmange` command lets you create, view, add, and update the contents of the Administrator user database.

To run the `dbmanage` command and change the administrator password, follow these steps:

1. Login as the root user, then run the following command:  

```
# /usr/internet/httpd/bin/dbmanage /usr/internet/httpd/userdb/admin adduser admin
```
2. The `dbmanage` command initializes the database (if needed) and prompts you for a password for Web user administrator, `admin`. If the user administrator already exists, the following message is displayed:  

```
Sorry user 'admin' already exists !
```

If you receive this message, rerun the `dbmanage` command as follows (note that `adduser` is now `update`):

```
# /usr/internet/httpd/bin/dbmanage /usr/internet/httpd/userdb/admin update admin
```

The command prompts you for a password and updates the database.
3. After updating the database, if the Web Server Administration Server is already running, you should not have to restart it. If you do need to restart the Web Server Administration Server, run the following command:  

```
# sbin/init.d/httpd_admin start
```

## 1.2 Web Server Administration Functions

All Compaq Secure Web Server administration functions are performed using Port 8081. All activity is recorded in the associated log files (Section 2.5).

Management tasks available from the Compaq Secure Web Server administration menus include:

- Changing configuration parameters, including tuning parameters, access control entries, listening ports and addresses, virtual hosts, URL defaults, HTML directory aliases, CGI directory aliases, and logging and reporting parameters.
- Managing user accounts, displaying status, and viewing information for the public Web server
- Changing passwords for the Web Server Administration Server
- Allowing remote access to the Web Server Administration Server
- Viewing server activity reports, access log files, and error log files, and refreshing these files
- Starting and stopping the Compaq Secure Web Servers

These tasks are described in detail in Chapter 2.

## 1.3 Dynamic Modules

Dynamic modules, also called Dynamic Shared Objects (DSO) or shared libraries, are loaded into the server process space only when necessary to assure that overall memory usage is reduced. You can use DSO modules to customize the Compaq Secure Web Server. Chapter 3 describes how to activate the Apache DSO modules. Appendix A lists the standard Apache modules provided as dynamic modules and additional dynamic modules not provided by the Apache Software Foundation.

## 1.4 Tomcat Java Servlet and JSP Engine

Tomcat, provided with the Compaq Secure Web Server, is a Java Servlet and Java Server Pages (JSP) engine developed by the Apache Software Foundation's Jakarta project. The Tomcat engine is most commonly used with commercial grade Web servers such as Apache and can also be used as a standalone Web server.

Tomcat is provided as an optional Compaq Secure Web Server subset that, when installed, allows the public instance of the Compaq Secure Web Server to be configured to seamlessly pass requests for Java Servlet and JSP pages to the Tomcat engine. Although the Tomcat engine could be configured respond to these requests directly (on another port), the Compaq Secure Web Server provides certain capabilities such as access control, static pages handling, Secure Socket Layer (SSL), and legacy CGI programs that are superior to that those provided by Tomcat.

Chapter 4 describes how to start Tomcat, use the Tomcat examples, and locate Tomcat directories and files.

## 1.5 SSL and the Compaq Secure Web Server

The Compaq Secure Web Servers have built-in support for the Secure Socket Layer (SSL). Netscape's SSL protocol is the most widely-used method for performing secure transactions on the Web. The protocol is supported by most Web servers and clients including Netscape Navigator and Microsoft Internet Explorer.

SSL provides privacy, guaranteed through encryption. Although information can be intercepted by a third party, the perpetrator cannot read the information without a private encryption key. If the information received will not decrypt properly, the recipient can determine whether the information has been tampered with during transmission.

SSL also provides authentication through **digital certificates** that are generated for SSL, although the source of digital certificates might not always be credible for online payment transactions. Compaq Secure Web Server SSL encryption uses a secret key nested within **public key encryption** and authenticated through digital certificates.

Chapter 5 describes the administration functions that you perform to enable SSL on your server:

- Generating a private key.
- Generating a request for a digital certificate.
- Generating and installing a test certificate, installing an actual certificate, and then viewing its details.
- Enabling (or disabling) SSL capabilities.
- Testing your SSL connection.
- Limiting access to HTTPS connections.
- Special considerations for enabling SSL on public web servers.

---

## Managing the Compaq Secure Web Server

This chapter describes how to manage the Compaq Secure Web Server. From the administration Web server on port 8081, the following management tasks are available through the administration menus:

- Change configuration parameters for the Compaq Secure Web Servers (Section 2.1)
- Change public Web server user accounts (Section 2.2)
- Display public Web server status (Section 2.3)
- Display public Web server information (Section 2.4)
- View server activity reports or the access and error log files for the Web servers (Section 2.5)
- Refresh the access log and error log files for the Web servers (Section 2.6)
- Start and stop the Web servers (Section 2.7)
- Change the password for the administration Web server (Section 2.8)
- Allow remote access to the administration Web server (Section 2.9)

In addition, you can enable and manage the Secure Socket Layer (SSL) with the Compaq Secure Web Server (Chapter 5).

### 2.1 Changing Configuration Parameters

A configuration parameter is specified by a directive and is stored in one of the configuration files listed in Table 2-1.

**Table 2-1: Configuration Files for Compaq Secure Web Servers**

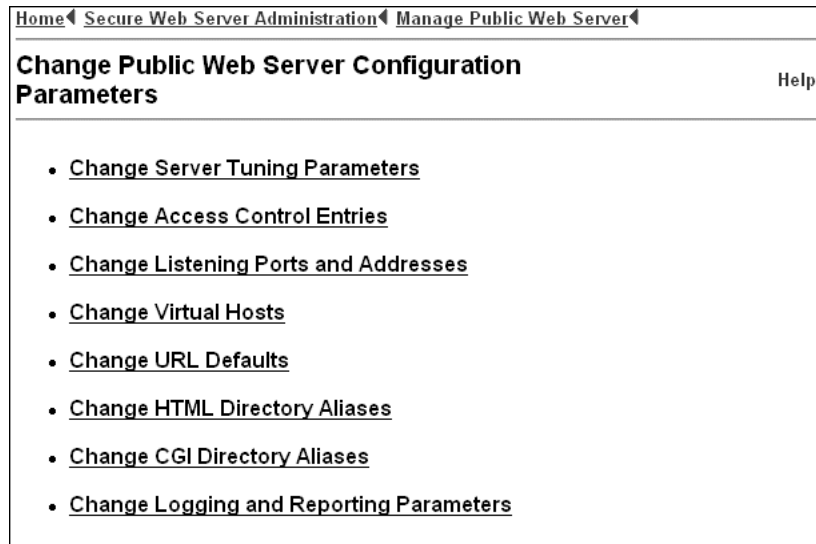
Server	Configuration File
Public Web server	<code>/usr/internet/httpd/conf/httpd.conf</code>
Administration Web server	<code>/usr/internet/httpd/admin/conf/httpd.conf</code>

You can specify the following types of configuration parameters:

- Server tuning parameters (Section 2.1.1)
- Access control entries (Section 2.1.2)
- Listening ports and addresses (Section 2.1.3)
- Virtual hosts (Section 2.1.4)
- URL defaults (Section 2.1.5)
- HTML directory aliases (Section 2.1.6)
- CGI directory aliases (Section 2.1.7)
- Logging and reporting parameters (Section 2.1.8)

Figure 2-1 shows the menu for changing the configuration parameters for the public Web server instance.

**Figure 2–1: Change Configuration Parameters Menu**



The Compaq Secure Web Server configuration files are read in the following order:

- `httpd.conf`
- `srm.conf`
- `access.conf`

---

**Note**

---

By default, the `access.conf` and `srm.conf` configuration files do not contain any directives. While they remain supported in Internet Express Version 5.7, all directives are defined in `httpd.conf`.

---

If you specify the same directive in more than one configuration file, the first directive found takes precedence.

In the tables in the following sections, a directive enclosed in angle brackets can be defined using multiple lines and must be delimited by a `<directive>...</directive>` pair, where *directive* is the directive name. The following example shows the proper syntax for a multiple-line directive:

```
<Limit GET POST>
order deny,allow
deny from all
allow from host1.domain.name domain2.name
</Limit>
```

Through the Change Configuration Parameters menu for each server, the Web Server Administration utility allows you to set many of the frequently used configuration parameters described in this section. If you want to take advantage of more specialized functionality, you must manually edit the Compaq Secure Web Server configuration files listed in Table 2–1. Avoid modifying the configuration parameters that are handled by the Administration utility when manually editing these files.

For a complete listing of Compaq Secure Web Server directives, see the following Web site:

<http://www.apache.org/docs/mod/directives.html>

## 2.1.1 Changing Server Tuning Parameters

To change the server tuning parameters, follow these steps:

1. On the Secure Web Server Administration menu, choose the link to the Web server on which you want to change the parameters. You can change the configuration parameters on either the public or administration Web server instances. For example, choose Manage the Public Web Server for the public Web server instance.
2. On the Manage the Public Web Server menu, choose Change Configuration Parameters.
3. On the Change Public Web Server Configuration Parameters menu, choose Change Server Tuning Parameters. Figure 2–2 shows the Change Tuning Parameters form for the public Web server instance. This form is also available from the Web Administration Server Instance menu (see Figure 2–12).

**Figure 2–2: Change Tuning Parameters Form**

4. On the Change Server Tuning Parameters form (Figure 2–2), change one or more of the parameters.

Table 2–2 shows which Compaq Secure Web Server directive is associated with each parameter field on the Change Tuning Parameters form and the type of value expected.

**Table 2–2: Server Tuning Parameters and Associated Directives**

Parameter	Directive	Description
Minimum Spare Servers	MinSpareServers <i>number</i>	Minimum number of unused server child processes to maintain
Maximum Spare Servers	MaxSpareServers <i>number</i>	Maximum number of unused server child processes left running before additional child processes are killed
Start Servers	StartServers <i>number</i>	Initial number of server child processes
Maximum Connections	MaxClients <i>number</i>	Maximum number of server processes for client connections
Maximum Requests/Connection	MaxRequestsPerChild <i>number</i>	Number of requests handled before child process is terminated

**Table 2–2: Server Tuning Parameters and Associated Directives (cont.)**

Parameter	Directive	Description
Connection Timeout (secs)	Timeout <i>number</i>	Time (seconds) to wait for response before terminating a connection
Enable Keepalive	KeepAlive on   off	Whether or not to hold open a connection after the initial connection is lost
Keepalive Timeout (secs)	KeepAliveTimeout <i>number</i>	Time (seconds) to wait for subsequent connection on a KeepAlive connection
Maximum Keepalive Retries	MaxKeepAliveRequests <i>number</i>	Number of times to re-use a connection

### 2.1.2 Changing Access Control Entry Parameters

You can change access control entries for any of the Compaq Secure Web Server instances that are installed. The steps in this section describe changing access control entries for the public Web server instance.

From the Change Public Web Server Configuration Parameters form (Figure 2–1), choose Change Access Control Entries. Figure 2–3 shows the Change Access Control Entries form for the Web Server Administration Server instance. This form is also available for the Web Server Public Instance.

**Figure 2–3: Change Access Control Entries Form**

Home > Secure Web Server Administration > Change Public Web Server Configuration Parameters

### Change Public Web Server Access Control Entries Help

**New Access Control Entry:** Directory [ ] [ ] Add

**Existing Access Control Entries:**

- Directory /
- Directory /usr/internet/httpd/htdocs
- Directory /usr/internet/httpd/icons
- Directory /usr/internet/horde
- Directory /usr/internet/httpd/cgi-bin

Modify Delete

By default, each Web server instance has one main access control entry that controls access to most pages for that server. In general, this entry should be the only entry you might want to change, though many access control entries are listed. The main access control entries are as follows:

- /usr/internet/httpd/htdocs (public Web server).
- /usr/internet/httpd/admin/htdocs (administration Web server)

You can also change access control entries for the following locations (for the public Web server only):

- /server-status
- /server-info

You can also add an access control entry for a directory or location.

Table 2–3 shows which Compaq Secure Web Server directive is associated with each parameter field on the Change Access Control Entries form and the type of value expected.

**Table 2–3: Access Control Parameters and Associated Directives**

Parameter	Directive	Description
Type and Specification	<Directory <i>path</i> >   <Location <i>name</i> >   <Files <i>filename</i> >	<i>path</i> , <i>name</i> , and <i>filename</i> can contain wildcards.
Limit Access Methods	<Limit <i>method</i> >	Specify one of the following Limit Access Methods: <ul style="list-style-type: none"> <li>• GET—Standard HTML access; parameters can be passed as part of the URL.</li> <li>• POST—Form access; parameters are passed separately.</li> <li>• GET POST</li> <li>• All Methods</li> </ul> When you choose All Methods (the default), the Limit directive is not specified in the <code>access.conf</code> file for this Type and Specification (directory, location, or file).
Precedence	order <sup>a</sup> deny,allow   order allow,deny	Specifies the order in which to process the deny from and allow from directives.
Hosts Allowed Access	allow from <sup>a</sup> all   allow from <i>host_list</i>	List of fully or partially qualified host or domain names, separated by spaces. You cannot use wildcards and you must use complete DNS fields (for example, <code>domain.com</code> does not match <code>mydomain.com</code> ).
Hosts Denied Access	deny from <sup>a</sup> all   deny from <i>host_list</i>	List of fully or partially qualified host or domain names, separated by spaces. You cannot use wildcards and you must use complete DNS fields (for example, <code>domain.com</code> does not match <code>mydomain.com</code> ).
User Authentication and Selected Users	require <i>user_list</i>	To authenticate only specific users, set User Authentication to For Selected Users, and select one or more users from the Selected Users list. (These users are defined in the file specified by the <code>AuthDBMUserFile</code> directive. To add a user to this list, use the Change Web Server User Accounts form.)  To authenticate all users, set User Authentication to For All Valid Users.  If no Compaq Secure Web Server user accounts exist, Authentication is disabled.
Authentication Prompt Name	AuthName <i>string</i>	Portion of the string displayed in the Username/Password dialog box that prompts for user name (“Enter username for <i>name</i> at <i>host:port</i> :”)
CGI Execution	Options ExecCGI <sup>b</sup>	When the Enable CGI Script Execution check box is selected, allows CGI scripts to be executed from within the specified directory.

<sup>a</sup> The Administration utility expects this directive to be defined within the context of the Limit directive.

<sup>b</sup> The Administration utility expects this directive to be defined within the context of the Directory directive.

In the following example, the `Limit` directive allows access to the specified domain and host only:

```
<Limit GET POST>
order deny, allow
deny from all
allow from host1.domain1.name domain2.name
</Limit>
```

In the following example, access is allowed to everyone except the specified host and domain:

```
<Limit GET POST>
order allow, deny
allow from all
deny from host1.domain1.name domain2.name
</Limit>
```

### 2.1.3 Changing Listening Port and IP Address Parameters

Normally, the public Web server listens on all known IP addresses on a system and uses Port 80 for each address. The Change Listening Ports and Addresses form allows you to limit which IP addresses are used by the public Web server and allows you to provide alternate paths to your server by specifying additional IP addresses on which the public Web server (Port 80) listens for HTTP requests.

From the Change Public Web Server Configuration Parameters form (Figure 2–1), choose Change Listening Ports and Addresses. Figure 2–4 shows the Change Listening Ports and Addresses form for the Web Server Public Instance. This form is also available from the Web Administration Server Instance menu (see Figure 2–12).

**Figure 2–4: Change Listening Ports and IP Addresses Form**

The screenshot shows a web form titled "Change Public Web Server Listening Ports and Addresses" with a "Help" link. Under "Known IP addresses", the values "127.0.0.1" and "16.141.0.86" are listed. Below this is a table with two columns: "Active IP Address (blank means all addresses)" and "Active Port (required)". The "Primary" row has an empty IP address field and a port field containing "80". There are three "Additional:" rows, each with empty IP address and port fields. At the bottom of the form are "Submit" and "Reset" buttons.

Table 2–4 shows which Compaq Secure Web Server directive is associated with each parameter field on the Change Listening Ports and Addresses form and the type of value expected.

**Table 2–4: Listening Port/IP Address Parameters and Associated Directives**

Parameter	Directive	Description
Active IP Address and Active Port (Primary and Additional)	Listen [ <i>IP address:</i> ] <i>port</i>	Specifies one or more ports or IP addresses to listen on
Active IP Address and Active Port (Primary only)	Port <i>port</i>	Defines the <code>SERVER_PORT</code> environment variable used by CGI scripts.

For example, if your system has eight IP addresses configured, but you want the public Web server to listen on only two of those ports, you can explicitly define these two addresses as the Active IP Addresses for the server. Optionally, you can specify a different port for each address. (Port 80 is normally used.)

If you want to listen to all known IP addresses on more than one port (for example, Ports 80 and 81), specify Active Port 80 and Active Port 81 and leave the Active IP Address field blank for both ports.

## 2.1.4 Changing Virtual Host Parameters for the Public Web Server

You can specify virtual host parameters for the public Web server only.

From the Change Public Web Server Configuration Parameters form (Figure 2–1), choose Change Virtual Hosts. Figure 2–5 shows the Change Web Server Public Instance Virtual Hosts form.

**Figure 2–5: Change Web Server Public Instance Virtual Hosts Form**

The first time you access the Change Web Server Public Instance Virtual Hosts form (Figure 2–5), the only choice is to add a new virtual host. Thereafter, each virtual host you add is displayed on this form in the Existing Virtual Hosts list box. To change the configuration for an existing virtual host, select the virtual host from the list box and click on Modify.

Table 2–5 shows which Compaq Secure Web Server directive is associated with each field on the Change Public Web Server Virtual Hosts form and the type of value expected.

**Table 2–5: Virtual Hosts Parameters and Associated Directives**

Parameter	Directive	Description
Host Name or IP Address and Port Number	<i>hostname[:port]</i>   <i>IP address[:port]</i>	Host name or IP address of the virtual host; port number is optional.
Server Name	ServerName <sup>a</sup> <i>hostname</i>	Host name; used in URL parsing.
Document Root	DocumentRoot <sup>a</sup> <i>path</i>	Full path of the directory containing the default Web homepage for the specified Host Name or IP Address.
Server Admin Mail Address	ServerAdmin <sup>a</sup> <i>e-mail address</i>	E-mail address of the Web system administrator.

**Table 2–5: Virtual Hosts Parameters and Associated Directives (cont.)**

Parameter	Directive	Description
Error Log	ErrorLog <sup>a</sup> <i>path</i>	Full path of error log file; the default is /usr/internet/httpd/logs/error_log.
Access Log	TransferLog <sup>a</sup> <i>path</i>	Full path of access log file; the default is /usr/internet/httpd/logs/access_log.

<sup>a</sup> When an instance of this directive is specified outside the context of the Virtual Host directive, the directive applies to the server as a whole and its value is used as the default for the instance within the Virtual Host directive.

For a comprehensive document on virtual host support, see the following Web site:

<http://www.apache.org/docs/vhosts/index.html>

## 2.1.5 Changing URL Default Parameters for the Public Web Server

You can specify the URL default parameters for the public Web server only.

From the Change Public Web Server Configuration Parameters form (Figure 2–1), choose Change URL Defaults. Figure 2–6 shows the Change Public Web Server URL Defaults form.

**Figure 2–6: Change Web Server Public Instance URL Defaults Form**

Use the Change Public Web Server URL Defaults form (Figure 2–6) to specify the default HTML directory and default homepage (index page) for users on your system. By convention, on UNIX systems the default HTML directory is `public_html` and the default homepage is `index.html`.

When the Recognize .cgi Files As CGI Scripts parameter is enabled, files with the `.cgi` extension in the user's default HTML directory (or in a directory where CGI script execution is enabled) are executed as CGI scripts.

Table 2–6 shows which Compaq Secure Web Server directive is associated with each field on the Change URL Defaults form and the type of value expected.

**Table 2–6: URL Default Parameters and Associated Directives**

Parameter	Directive	Description
User's HTML Home Directory	UserDir <i>path</i>	Path relative to a user's home directory for the user's HTML home directory. The default is <code>public_html</code> .

**Table 2–6: URL Default Parameters and Associated Directives (cont.)**

Parameter	Directive	Description
Directory Index Page Name	DirectoryIndex <i>filename list</i>	One or more file names, separated by spaces, that define the default page displayed when an HTTP request specifies a directory path only (without a file name).
Recognize .cgi Files As CGI Scripts	AddHandler cgi-script.cgi	When this field is enabled, the comment character in this line is removed from the <code>srn.conf</code> file. When this field is disabled, the line is commented out.

## 2.1.6 Changing HTML Directory Alias Parameters for the Public Web Server

You can specify the HTML Directory Alias parameters for the public Web server only.

From the Change Public Web Server Configuration Parameters form (Figure 2–1), choose Change HTML Directory Aliases. Figure 2–7 shows the Change Public Web Server HTML Directory Aliases form.

**Figure 2–7: Change Web Server Public Instance HTML Directory Aliases Form**

Home Secure Web Server Administration  
Change Public Web Server Configuration Parameters

**Change Public Web Server HTML Directory Aliases** Help

HTML Aliases

New Alias Name:  Add

Existing Alias Names: 

- /icons/
- /horde/
- /imp/
- /webmail/
- /documents/

 Modify Delete

URL paths are rooted only by aliases, not by actual directories. The system-defined aliases are as follows:

- `icons`—Defines the directory to search for browser-specific icons  
When an HTTP request specifies a directory other than the user's HTML home directory (Table 2–6), the icons used in the resulting display to identify subdirectories and files are obtained from the directory associated with the `icons` alias.
- `copyrights`—Defines the directory in which the copyright information is installed.
- `documents`—Defines the directory in which the book files are installed.

Normally, these aliases should not be changed or deleted. However, you can specify a new HTML alias for any directory by providing an alias name and the full path name of the directory you want to associate with the alias. To add a new HTML alias, follow these steps:

1. On the Change HTML Directory Aliases form, enter the new alias name in the New Alias Name field and click on Add.
2. On the Add HTML Directory Alias form, specify the full pathname for the directory associated with the new alias in the Actual Directory field.

- Click on Submit.  
The Web Server Administration utility displays a confirmation message indicating that the configuration file has been successfully updated.
- Click on Submit to have the public Web server on the indicated port reread its configuration file. Wait a few seconds before using the navigation bar.

When you determine that an alias is no longer useful, you can remove it by selecting the alias name from the Existing Alias Names list box and clicking on Delete.

Table 2–7 shows which Compaq Secure Web Server directive is associated with each field on the Change Public Web Server HTML Directory Aliases form and the type of value expected.

**Table 2–7: HTML Directory Alias Parameters and Associated Directives**

Parameter	Directive	Description
Alias Specification and Actual Directory	Alias <i>alias path</i>	Alias Specification (New Alias Name) specifies the <i>alias</i> part of the directive and Actual Directory specifies the <i>path</i> .

### 2.1.7 Changing CGI Directory Alias Parameters for the Public Web Server

You can specify the CGI Directory Alias configuration parameters for the public Web server only.

From the Change Public Web Server Configuration Parameters form (Figure 2–1), choose Change CGI Directory Aliases. Figure 2–8 shows the Change Public Web Server CGI Directory Aliases form.

**Figure 2–8: Change Web Server Public Instance CGI Directory Aliases Form**

You can also specify a new alias by providing an alias name and the full path name of the directory you want to associate with the alias.

Table 2–8 shows which Compaq Secure Web Server directive is associated with each field on the Change Web Server Public Instance CGI Directory Aliases form (Figure 2–8) and the type of value expected.

**Table 2–8: CGI Directory Alias Parameter and Associated Directive**

Parameter	Directive	Description
Alias Specification and Actual Directory	ScriptAlias <i>alias path</i>	Alias Specification (New Alias Name) specifies the <i>alias</i> part of the directive and Actual Directory specifies the <i>path</i> .

## 2.1.8 Changing Logging and Reporting Parameters

Use the Change Logging and Reporting Parameters form to specify the following:

- The host name associated with an IP address in the log file. (Server performance can decrease when you enable host name lookup.)
- E-mail address for mail intended for the server administrator (if not specified anywhere else in the configuration files).
- The URL of the HTML page to display when the browser receives any of the following error codes:
  - Unauthorized—Usually caused by an incorrect user name or password.
  - Forbidden—Access to the directory, location, or file is explicitly prohibited or the file is protected.
  - File Not Found—File or path name alias does not exist.
  - Server Error—Usually caused by a malformed HTTP header generated by a CGI script.

From the Change Public Web Server Configuration Parameters form (Figure 2–1), choose Change Logging and Reporting Parameters. Figure 2–9 shows the Change Logging and Reporting Parameters form for the public Web server. This form is also available for the Web Administration Server Instance.

**Figure 2–9: Change Logging and Reporting Parameters Form**

Table 2–9 shows which Compaq Secure Web Server directive is associated with each field on the Change Logging and Reporting form (Figure 2–9) and the type of value expected.

**Table 2–9: Logging and Reporting Parameters and Associated Directives**

Parameter	Directive	Description
Hostname Lookups	HostnameLookups on   off	When set to on, the server performs DNS lookups on IP addresses to include host names in logging records.
Server Admin Mail Address	ServerAdmin <i>e-mail address</i>	E-mail address displayed with some error pages.

**Table 2–9: Logging and Reporting Parameters and Associated Directives (cont.)**

Parameter	Directive	Description
“Unauthorized” Error Response URL	ErrorDocument 401 <i>URL</i>   <i>string</i>	Specifies a page or text string to display upon receiving a “bad password” error. If specified, the URL for 401 errors must be local (The <code>http://host.domain.name</code> prefix is not permitted).
“Forbidden” Error Response URL	ErrorDocument 403 <i>URL</i>   <i>string</i>	Specifies a page or string to display upon receiving a “no authorization” or “file access” error.
“File Not Found” Error Response URL	ErrorDocument 404 <i>URL</i>   <i>string</i>	Specifies a page or text string to display upon receiving a “file not found” error.
“Server Error” Error Response URL	ErrorDocument 500 <i>URL</i>   <i>string</i>	Specifies a page or text string to display upon receiving an internal error or CGI format error (most likely related to a problem with HTTP header information).

## 2.2 Changing Public Web Server User Accounts

You can establish Compaq Secure Web Server user accounts to control access to the public Web server. You can enable a different level of access to each combination of user name and password that you specify. The password you specify for a Compaq Secure Web Server user account is not a UNIX system password; that is, you will not find these passwords in the `/etc/passwd` file.

The first time you access the Change Web Server User Accounts menu, the only option is to add a new Compaq Secure Web Server user account. Thereafter, each user account you create is displayed on this menu in the Existing Web Server Users list box, allowing you to change the password for the account or delete the account.

To add a Compaq Secure Web Server user account to control access to the public Web server, follow these steps:

1. On the Compaq Secure Web Server Administration menu, choose Manage the Public Web Server. Figure 2–10 shows the Manage the Public Web Server menu and available options.

**Figure 2–10: Manage the Public Web Server Form**



2. On the Manage the Public Web Server menu, choose Change Web Server User Accounts.
3. On the Change Public Web Server User Accounts form, enter the account name in the New Web Server User field.
4. Click on Add. The Add Public Web Server User Account form is displayed.
5. Enter a password in the New Password field.
6. Verify the password for the user by typing the same password in the Verify Password field.
7. Click on Submit.

The Web Server Administration utility displays a confirmation message indicating that the new user account has been successfully created. You can use the navigation bar at the top of the page to return to the Change Public Web Server User Accounts form.

To change a user's password, select the user name from the Existing Web Server Users list box and click on Modify. Specify a new password, verify the password, and click on Submit.

To delete a user account, select the user name from the Existing Web Server Users list box and click on Delete.

## 2.3 Displaying Public Web Server Status

To display the status of the public Web server on Port 80, on the Manage the Public Web Server menu, choose Display Web Server Status. The Web Server Status page allows you to see how well your server is performing. The current server statistics are displayed in an easy-to-read form.

The Display Server Status and Display Server Information links under Manage the Public Web Server menu return a "Forbidden server" error if you try to access them from a remote web browser after opening up access controls to remote systems on the Administration server. To avoid this problem, open access controls on the Location `/server-info` and Location `/server-status` entries for the public Web server in the Change Access Control Entries form under Change Configuration Parameters.

For more information on the data displayed on the Web Server Status page, go to the following URL for Apache Web site:

[http://www.apache.org/docs/mod/mod\\_status.html](http://www.apache.org/docs/mod/mod_status.html)

## 2.4 Displaying Public Web Server Information

To display information for the public Web server on Port 80, on the Manage the Public Web Server menu, choose Display Web Server Information. The Web Server Information page displays a comprehensive overview of the server configuration, including all installed modules and directives in the configuration files.

The Display Server Status and Display Server Information links under Manage the Public Web Server menu return a “Forbidden server” error if you try to access them from a remote web browser after opening up access controls to remote systems on the Administration server. To avoid this problem, open access controls on the Location `/server-info` and Location `/server-status` entries for the public Web server in the Change Access Control Entries form under Change Configuration Parameters.

For more information on the data displayed on the Web Server Information page, go to the following URL for the Apache Web site:

[http://www.apache.org/docs/mod/mod\\_info.html](http://www.apache.org/docs/mod/mod_info.html)

## 2.5 Viewing Web Server Reports and Log Files

During its normal operation, the Compaq Secure Web Server puts information in two log files. The access log keeps track of requests for use of this server and the information requested. The error log maintains a record of errors that occurred since the log file was last refreshed. You should periodically save and recreate these log files so they do not get too large (see Section 2.6).

To view the access log file or error log file for a Web server, follow these steps:

1. On the Secure Web Server Administration menu, select the server for which you want to view the access log or error log, for example, the public Web server. The Manage the Public Web Server menu is displayed (see Figure 2–10).
2. From the Manage the Public Web Server menu, choose View Server Reports and Log Files. The Report and Log Files for the Public Web Server menu is displayed (Figure 2–11).

**Figure 2–11: Report and Log Files for the Public Web Server**



3. Select the item corresponding to the log file you want to view.

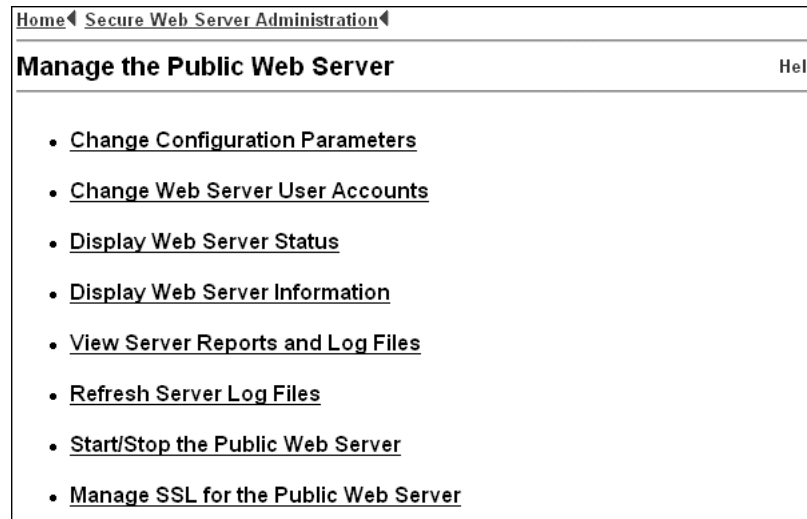
The entries in the chosen log file are shown 100 lines at a time with the most recent entries first.

You can use the navigation bar at the top of each page to return to the Reports and Log Files menu or the Compaq Secure Web Server Administration menu.

To generate the activity reports for any one of the Compaq Secure Web Server instances, follow these steps:

1. On the Secure Web Server Administration menu, select the server for which you want to generate activity statistics, for example, the administration Web server. The Manage the Administration Web Server menu is displayed (Figure 2–12).

**Figure 2–12: Manage the Administration Web Server Menu**



2. On the Manage the Administration Web Server menu, choose View Server Reports and Log Files. The Report and Log Files for the Administration Web Server menu is displayed (Figure 2–13). This menu contains additional reports than listed on the Report and Log Files menu for the Web Server Public Instance.

**Figure 2–13: Report and Log Files for the Administration Web Server Menu**



3. On the Reports and Log Files menu, click on Generate a Summary Report. (For your convenience, a link to the Analog HTML documentation is also provided at the bottom of the page; look for This analysis was produced by analogx.xx, where x.x.x indicates the version number.)

The activity reports are generated using analog, an Open Source utility that analyzes log files. The analog configuration file is located in /usr/internet/httpd/admin/analog/analog.cfg.

Table 2–10 describes the various activity reports that you can generate for the public and administration instances of the Compaq Secure Web Server:

**Table 2–10: Activity Reports for the Compaq Secure Web Servers**

Report	Description
Summary Report	For the time period shown at the top of the page, the following statistics are shown: the total requests that were completed, failed, and redirected; the number of distinct hosts served; the number of corrupt log file entries; and the total bytes transferred.
Monthly Report	Shows how many requests were processed, by month.
Daily Summary Report	Shows how many requests were processed each day since the last time the server was started.
Hourly Summary Report	Shows how many requests were processed each hour.
Domain Report	Shows all domains with any traffic, sorted by amount of traffic.
Directory Report	Shows all directories to depth 1 with at least 0.01% of the traffic, sorted by amount of traffic.

For more information, visit the analog Web site at:

<http://www.statslab.cam.ac.uk/~sret1/analog/>

## 2.6 Refreshing the Administration Web Server Log Files

To refresh the access log, the error log, or both, follow these steps:

1. On the Secure Web Server Administration menu, select the server for which you want to refresh the log files, for example, the administration Web server. The Manage the Administration Web Server menu is displayed (see Figure 2–12).
2. On the Manage the Administration Web Server menu, choose Refresh Server Log Files.
3. On the Refresh Server Log Files form, select the check box corresponding to the log file you want to refresh. You can select one file or more files.
4. Click on Submit.

For each log file you select, the Web Server Administration utility makes a backup copy of the log file and creates an empty file to replace it. The Administration utility also restarts the `httpd` server daemon.

## 2.7 Starting and Stopping the Compaq Secure Web Server

To stop or restart the Compaq Secure Web Server, follow these steps:

1. On the Secure Web Server Administration menu, select the server you want to start or stop, for example, the administration Web server. The Manage the Administration Web Server menu is displayed (see Figure 2–12).
2. On the Manage the Administration Web Server menu, choose Start/Stop the Administration Web Server Server.
3. If the server is running, the Web Server Administration utility shows you the current status of the server and offers the following operations:

- Stop—Shuts down the server daemon listening on the port shown in the title of the form. Use this operation to prevent the server from responding to requests.
- Restart—Restarts the server daemon listening on the port shown in the title of the form. Use this operation to enable any change to the server configuration files.

Figure 2–14 shows the Start/Stop form when the server is running.

**Figure 2–14: Start/Stop the Administration Web Server Server Form**

If the server is not running, the utility offers the following control operations:

- Start—Starts the server daemon listening on the port shown in the title of the form.
  - Restart—Stops and restarts the server daemon listening on the port shown in the title of the form. Use this operation to enable any change to the server configuration files.
4. Click on the button corresponding to the operation you want to perform. The Web Server Administration utility confirms the request and performs the operation.

## 2.8 Changing the Password for the Compaq Secure Web Server

To change the password used for the Compaq Secure Web Server, follow these steps:

1. On the Secure Web Server Administration menu, choose Change the Password for All Administration Servers. The Change the Password for All Administration Servers form is displayed (Figure 2–15).

**Figure 2–15: Change the Password for All Administration Servers Form**

2. Enter the new password in the New Password field and again in the Verify New Password field.
3. Click on Submit.

The new password takes effect immediately.

If you decide not to change the password, cancel the operation by clicking on one of the following:

- The Clear button at the bottom of the form
- One of the links on the navigation bar at the top of the form to go to another Administration menu

## 2.9 Allowing Remote Access to the Administration Web Server

The installation procedure installs the administration Web server on Port 8081 and initially allows access to the server from the local system only.

---

### Note

---

Using a Web server on a remote system to manage user accounts and other system services poses a security risk. That is, unless the Secure Socket Layer (SSL) is enabled on your Web server, all data, including passwords, is transmitted between the Web server and the browser in clear text. This unencrypted data is subject to interception by network snooping.

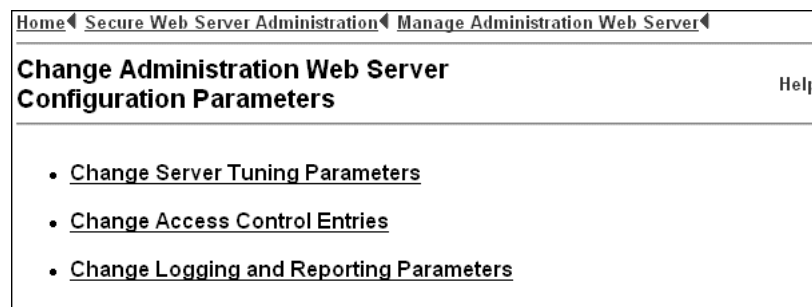
Carefully evaluate the security risks to your system before you enable remote access to the Administration utility or other server administration. See Chapter 5 for information on setting up your Web server with SSL.

---

To allow access to the administration Web server from remote systems, follow these steps:

1. On the Secure Web Server Administration menu, choose Manage the Administration Web Server. The Manage the Administration Web Server menu is displayed (see Figure 2–12).
2. On the Manage the Administration Web Server menu, choose Change Configuration Parameters. The Change Administration Web Server Configuration Parameters menu is displayed (Figure 2–16).

**Figure 2–16: Change Administration Web Server Configuration Parameters Menu**



3. On the Change Administration Web Server Configuration Parameters menu, choose Change Access Control Entries (see Figure 2–3).
4. On the Change Access Control Entries menu, select `Directory /usr/internet/httpd/admin/htdocs` from the Existing Access Control Entries list box, then click on Modify. The Modify Administration Web Server Access Control Entry form is displayed (Figure 2–17).

**Figure 2–17: Modify Administration Web Server Access Control Entry Form**

Home ◀ Secure Web Server Administration ◀  
Change Administration Web Server Configuration Parameters ◀  
Change Administration Web Server Access Control Entries ◀

---

**Modify Administration Web Server Access Control Entry** Help

---

**Type:** Directory    **Specification:** /usr/internet/httpd/admin/htdocs

**Host Access**

**Limit Access Methods:** All Methods ▾

**Precedence:** Process Deny First ▾

**Hosts Denied Access:** all

**Hosts Allowed Access:** all

**Authentication**

**User Authentication:** For Selected Users ▾

**Selected Users:** admin

**Authentication Prompt Name:** Web Server Administration Server Ac

5. In the Hosts Allowed Access field, enter one of the following:
  - *host.domain.name* for a specific host
  - *.domain.name* for a specific domain
  - all for any remote host

For more information on the Allow command, see the Apache documentation at the following Web site:

<http://www.apache.org/>

6. Click on Submit.
7. On the confirmation page, click on Submit to reload the administration Web server configuration file.



---

## Using Dynamic Modules

**Dynamic modules** provide a means of allowing developers and third parties to extend the capabilities of the Compaq Secure Web Server. When properly configured in the server configuration file, these modules will be loaded into the Web server at startup time. As the Secure Web Server is based on Apache, modules conforming to the Apache DSO API can be use with the Compaq Secure Web Server.

The Compaq Secure Web Server can be customized using dynamic modules provided from Apache and other sources. Table 3–1 lists the dynamic modules available with the Compaq Secure Web Server software. For a complete list of the Compaq Secure Web Server modules (DSO and integrated), see Appendix A.

This chapter provides the following information:

- Compaq Secure Web Server support for dynamic modules (Section 3.1).
- Activating the Apache dynamic modules (Section 3.2).

### 3.1 Compaq Secure Web Server Support for Apache Dynamic Modules

Apache dynamic modules can be obtained from many sources. These include:

- Modules that are part of the Apache distribution.
- Modules from the Apache Module Register on the Web: <http://modules.apache.org>. The Module registry contains a list of modules that are available for use with Apache based servers. These modules derive from a variety of sources, and can often be easily built and used with the Compaq Secure Web Server.
- Custom-written modules from various sources. Occasionally, a Website has special needs that cannot be easily addressed using the existing Compaq Secure Web Server functionality of and are not readily available from existing modules. In these cases, a Web site can create custom modules based on the Apache DSO API that extends the functionality of the Compaq Secure Web Server.

The Compaq Secure Web Server integrates many Apache modules and provides many other modules as dynamic shared objects (DSO). The DSO modules are not integrated because they are not usually part of the default configuration of an Apache server. Section 3.1.1 lists the standard Apache modules provided as DSO modules. Section 3.1.2 lists non-standard DSO modules provided in the Compaq Secure Web Server kit. (Non-standard DSO modules are modules not from the Apache Foundation.)

Administrators can build Apache modules for use with the Compaq Secure Web Server. The standard Apache `apxs` utility (`/usr/internet/httpd/bin/apxs`) is provided with the Compaq Secure Web Server to assist you during compilation and installation of the Apache modules.

Instructions for compiling modules using the `apxs` utility are usually included with the source code for that particular module. Instructions can also be found in the standard Apache documentation on the Web: <http://www.apache.org>.

Standard Apache documentation is also included with the Compaq Secure Web Server in the `IAEAPDOCxxxxsubset`, installed in `/usr/internet/httpd/apdocs`.

### 3.1.1 Standard Modules Provided as DSO Modules

The Compaq Secure Web Server provides several standard Apache modules as DSO modules. These are modules that are included in source form as part of the Apache source distribution. Although there are many modules that are included in the distribution, many of them are not included in the default server configuration. The optional modules are provided in the form of DSO modules so they can be activated if needed. Table 3–1 lists and describes these modules.

**Table 3–1: Standard Compaq Secure Web Server Modules**

DSO Module	Description
<code>mod_auth_anon</code>	Anonymous user access to authenticated areas
<code>mod_auth_db</code>	User authentication using Berkeley DB files
<code>mod_cern_meta</code>	Support for HTTP header metafiles
<code>mod_digest</code>	MD5 authentication
<code>mod_expires</code>	Apply Expires: headers to resources
<code>mod_headers</code>	Add arbitrary HTTP headers to resources
<code>mod_log_agent</code>	Logging of User Agents
<code>mod_log_referer</code>	Logging of document references
<code>mod_mime_magic</code>	Determining document types using “magic numbers”
<code>mod_mmap_static</code>	Experimental file caching, mapping files into memory to improve performance
<code>mod_proxy</code>	Caching proxy abilities
<code>mod_rewrite</code>	Powerful URI-to-file name mapping using regular expressions
<code>mod_speling</code>	Automatically correct minor typos in URLs
<code>mod_unique_id</code>	Generate unique request identifier for every request
<code>mod_usertrack</code>	User tracking using Cookies (replacement for <code>mod_cookies.c</code> )
<code>mod_vhost_alias</code>	Support for dynamically configured mass virtual hosting

### 3.1.2 Non-Standard Modules Provided as DSO Modules

In addition to the standard Apache modules, the Compaq Secure Web Server provides DSO modules from sources outside the Apache Foundation

See Table A–3 and Table A–4 for a list of nonstandard Apache DSO modules.

## 3.2 Activating the Apache DSO Modules

To activate an Apache DSO module, you must modify the `httpd.conf` server configuration file, as follows:

1. Add a `LoadModule` directive.
2. Add an `AddModule` directive, if the `ClearModule` directive is used.
3. Add additional module configuration-specific directives.
4. Restart the server for the configuration changes to take effect.

Usually, an Apache DSO module will not perform any useful function until the module-specific configuration directives activate the module’s functionality. The

module-specific documentation explains the module configuration directives. For Apache DSO modules provided with the Compaq Secure Web Server, refer to either the Apache documentation provided with the Compaq Secure Web Server kit, or the documentation available on the Apache Web site:

<http://httpd.apache.org>)

### 3.2.1 Using the LoadModule Directive

The `LoadModule` directive enables dynamic module loading by the Web server. This directive must occur before any other configuration directive for the module being loaded.

The `LoadModule` directive has the following form:

```
LoadModule module_identifier filename
```

The `module_identifier` variable is the internal module definition variable name, that is documented in the module documentation.

The `filename` parameter is the loadable module on disk that the server will load. The file name can be an absolute path or a path relative to the server root as defined by the `httpd.conf` file.

If the `ClearModule` directive is present, it signals the server that the list of loaded modules needs to be reordered. The `ClearModule` directive begins the process by clearing the internal list of modules, thus providing the configuration file with a complete list of all modules (integrated and DSO). Each module is readded to the module list with an `AddModule` directive (Section 3.2.2).

### 3.2.2 Using the AddModule Directive

The `AddModule` directive is used by the Web server to build a list of modules in order or precedence. The directive is only needed if the `ClearModule` directive is used to zero out the module list. If the `ClearModule` directive is not used, then the module precedence is in the order that they were loaded.

The `AddModule` directive has the form:

```
AddModule source_file
```

The `source_file` is the file name of the compilation unit that contained the module declaration. To determine the proper file name to use, see the module-specific documentation.

### 3.2.3 Verifying the Configuration File

After adding the configuration directives to the `httpd.conf` file, the file syntax can be reviewed prior to restarting the server. The following command directs the server to verify the specified configuration file:

```
#!/usr/internet/httpd/bin/httpd -t -f /usr/internet/httpd/conf/httpd.conf
```

### 3.2.4 Activating an Apache DSO Module — Example

The example in this section shows how to activate the `mod_usertrack` Apache DSO module, which uses Cookies to track users. To activate the module, use the `httpd.conf` configuration file for the default public server `/usr/internet/httpd/conf/httpd.conf` and follow these steps:

1. Define the `LoadModule` directive as follows:

```
LoadModule usertrack_module libexec/mod_usertrack.so
```

2. If the `ClearModule` directive is defined, add the module to the module list with an `AddModule` directive:

```
AddModule mod_usertrack.c
```

3. Define the module-specific directives, for example:

```
CookieName OurTestCookie  
CookieTracking on
```

4. Track the generated cookies by using a directive for another Apache module (that is, one that is integrated in the Compaq Secure Web Server). This directive will cause the cookies to be logged into a file called `clickstream`, in the `logs` directory relative to the server root. For example:

```
CustomLog logs/clickstream "%{cookie}n %r %t"
```

### 3.2.5 Web Server LDAP Authentication Requires LDAP Runtime Library

Before enabling the Compaq Secure Web Server's LDAP authentication module (`libauth_ldap.so`) you must install the Internet Express Netscape LDAP Runtime subset (`IAELDRT`).

If you enable the Compaq Secure Web Server's LDAP authentication module (`libauth_ldap.so`) in the web server's configuration file using the `LoadModule` directive without installing the `IAELDRT` subset, the Web server will fail to start, returning the following error:

```
Cannot load /usr/internet/httpd/libexec/libauth_ldap.so into server:  
dlopen: cannot load /usr/internet/httpd/libexec/libauth_ldap.so
```

Note that the Web Server's LDAP authentication module is separate and distinct from and not to be confused with the Internet Express System Authentication LDAP Module (`IAELDAM` subset).

---

# Implementing the Tomcat Java Servlet and JSP Engine

This chapter contains the following information:

- Overview of Tomcat (Section 4.1)
- Locating Tomcat directories (Section 4.2)
- Starting Tomcat (Section 4.3)
- Accessing the Tomcat examples (Section 4.4)
- Locating additional information (Section 4.5)

## 4.1 Tomcat Overview

Tomcat is a Java Servlet and Java Server Pages (JSP) engine provided through the Apache Software Foundation Jakarta project. The Tomcat engine is most commonly used with commercial grade Web servers such as Apache. It can also be used as a standalone Web server.

Tomcat is provided with the Compaq Secure Web Server as an optional subset (`IAETOMCATxxx`, where `xxx` is the version number of the Compaq Secure Web Server release). When this subset is installed, the public instance of the Compaq Secure Web Server will be configured to seamlessly pass requests for Java Servlet and JSP to the Tomcat engine. Although the Tomcat engine could be configured respond to these requests directly (on another port), the Compaq Secure Web Server provides certain capabilities such as access control, static pages handling, and Secure Socket Layer (SSL) and legacy CGI programs that are superior to those provided by Tomcat.

The Tomcat subset creates a Cluster Application Availability (CAA) resource when it is used in a TruCluster environment. Tomcat is configured as a single instance resource so that it can take advantage of sessions and other capabilities of a Java Servlet environment. The public instances of the (multi-instance) Compaq Secure Web Server are configured to communicate with the Tomcat instance and will handle the failover of the Tomcat resource.

For more information on developing and installing servlets and JSPs, see Section 4.5. After installing or updating an application, the Tomcat engine and the public Web server may need to be restarted. For information on starting Tomcat, see Section 4.3.

## 4.2 Locating Tomcat Directories

After installation, Tomcat resides in the `/usr/internet/httpd/tomcat` directory. Applications (Java Servlets and JSPs) are installed under the `/usr/internet/httpd/tomcat/webapps` directory.

Tomcat-specific configuration information is installed in the `/usr/internet/httpd/tomcat/conf` directory.

## 4.3 Starting Tomcat

The Tomcat engine creates a number of configuration files each time it is started. These configuration files contain directives that determine the information the Compaq Secure Web Server will serve and the requests that should be directed to the Tomcat engine.

---

### Note

---

To take full advantage of the generated configuration files, the Compaq Secure Web Server must be restarted whenever you change the Tomcat configuration and restart the Tomcat server.

---

The Compaq Secure Web Server startup script is designed to detect the presence of Tomcat and start the Web server with additional command-line directives that enable the communication with Tomcat and cause the dynamic configuration files generated by Tomcat to be used.

Starting or restarting Tomcat is different if you are running your Compaq Secure Web Server in a Trucluster environment. Section 4.3.1 describes how to restart Tomcat when it is not in a Trucluster environment. Section 4.3.2 describes how to restart Tomcat in a Trucluster environment. Section 4.3.3 gives the location of the Tomcat log files.

### 4.3.1 Restarting Tomcat in a Non-TruCluster Environment

To start Tomcat and the Compaq Secure Web Server that is not part of a TruCluster environment:

1. If Tomcat is running, use the `stop` command to stop the server:  

```
/sbin/init.d/tomcat stop
```
2. Restart the Tomcat server using the `start` command:  

```
/sbin/init.d/tomcat start
```
3. Restart the public instance of the Compaq Secure Web Server using the `restart` command:  

```
/sbin/init.d/httpd_public restart
```

### 4.3.2 Restarting Tomcat in a TruCluster Environment

To restart Tomcat and the Compaq Secure Web Server in a TruCluster environment:

1. If Tomcat is running, use the `caa_stop` command to stop the server:  

```
#caa_stop tomcat
```
2. Restart the Tomcat Server using the `caa_start` command:  

```
#caa_start tomcat
```
3. Restart (on all cluster members) the public instance of the Compaq Secure Web Server using the `cluster-restart` command:  

```
#!/sbin/init.d/httpd_public cluster-restart
```

### 4.3.3 Tomcat Log Files

Tomcat records log files in the `/usr/internet/httpd/logs` directory. Table 4-1 lists the log files Tomcat creates and provides a description of each file.

**Table 4–1: Tomcat Log Files**

Log File	Description
tomcat_startup.log	Tomcat startup log
tomcat.log	Tomcat general log
servlet.log	Servlet log
jasper.log	JSP log
access_log	Access requests log, shared with the Compaq Secure Web Server
error_log	Failed access requests log, shared with the Compaq Secure Web Server

## 4.4 Accessing the Tomcat Examples

The Tomcat subset includes several example servlets and JSPs. When Tomcat is installed for the first time, the `examples.war` file will be linked into the `webapps` directory for you. If the examples are not present, then they can be easily installed.

To install the examples, link them into place and then restart Tomcat. Follow these steps:

1. Use the `ln -s` command to link the examples, as follows:

```
#ln -s /usr/internet/httpd/tomcat/samples/examples.war \  
/usr/internet/httpd/tomcat/webapps/
```

2. Restart Tomcat and the Compaq Secure Web Server (Section 4.3).

After restarting Tomcat and Compaq Secure Web Server, Tomcat opens the `examples.war` file in the `webapps/examples` directory.

- Access the Servlet examples by specifying the name of your host domain using the following URL:

```
http://yourhost.domain/examples/servlets
```

- Access the JSP examples by specifying the name of your host domain using the following URL:

```
http://yourhost.domain/examples/jsp
```

## 4.5 Locating Additional Information

Additional information about Tomcat can be found in the following locations:

- The Jakarta Project Web site: <http://jakarta.apache.org>
- Tomcat documentation Web site: <http://jakarta.apache.org/tomcat/tomcat-3.2-doc/index.html>
- Tomcat Development Guide and User Guide (part of the IAEAPDOCxxx subset):  
`/usr/internet/httpd/tomcat/doc`



---

## Enabling the Secure Socket Layer Protocol

To enhance the security of communications between your Web browser and administrative instances of the Compaq Secure Web Server, the Compaq Secure Web Servers have built-in support for the Secure Socket Layer (**SSL**) protocol. This chapter describes how SSL provides secure Internet connections and how to use Internet Express to enable SSL on your server.

### 5.1 SSL Concepts

Netscape's SSL protocol is a widely used method for performing secure transactions on the Web. This protocol is supported by most Web servers and clients including Netscape Navigator and Microsoft Internet Explorer.

SSL provides privacy, guaranteed through encryption. Although information can be intercepted by a third party, the perpetrator cannot read the information without the private encryption key (**session key**). If the information is received and will not decrypt properly, the recipient can determine that the information has been tampered with during transmission. Authentication is provided through digital **certificates** generated for SSL, though the source of digital certificates might not always be credible for online payment transactions.

SSL encryption uses a secret key nested within **public key encryption**, authenticated through certificates. Secret key encryption provides faster access than public-key encryption alone. Initially, the client and server exchange public keys, and then the client generates a session key for a specific transaction. The client encrypts the session key with the server's public key and sends the information to the server. Then, and for the remainder of the transaction, the client and the server use the session key for private key encryption.

Completing a transaction with an SSL-enabled server follows this general procedure:

1. A client sends a request for a document to be transmitted using the **https:** protocol by prefixing the URL with `https://`.
2. The server sends the client its certificate.
3. The client verifies that the certificate was issued by a trusted **Certificate Authority** (CA). If the client does not verify the CA, it gives the user the option to continue or to terminate the transaction.
4. The client compares information in the certificate with information received concerning the site; specifically, the domain name and the public key. If the information matches, the client accepts the site as authentic.
5. The client tells the server what ciphers (encryption algorithms) it uses to communicate.
6. The client generates a session key using the agreed-upon cipher.
7. The client encrypts the session key with the server's public key and sends the information to the server.
8. The server receives the encrypted session key and decrypts the information with the session key.

9. The client and the server then use the session key for the remainder of the transaction.

For additional information about SSL, see the `mod-ssl` Web site:

<http://www.modssl.org/docs>

## 5.2 Enabling SSL Support from the Web Server Administration Utility

Using the Web Server Administration utility, you can manage support for SSL connections. Follow these steps:

1. On the Secure Web Server Administration menu, select the Web server for which you want to enable (or disable) SSL support, for example, the public Web server. The Manage the Public Web Server menu is displayed (see Figure 2–10).
2. Choose Manage SSL for the Public Web Server. The SSL menu options are displayed (Figure 5–1), initially showing the following options:
  - Generate a private key (Section 5.3)
  - Generate a certificate request (Section 5.4)
  - Generate and install a test certificate (Section 5.5)
  - Install a certificate (Section 5.6)
3. Proceed to generate a private key (Section 5.3) and request a digital certificate (Section 5.4).

---

### Note

---

The steps for managing SSL that are described in this chapter use public Web server examples. Steps for managing SSL for the administration Web server are identical.

---

**Figure 5–1: Manage SSL for the Public Web Server Menu**



When you enable SSL for the first time, you must generate a private key and then generate a certificate request. A Certificate Authority (CA), such as **VeriSign** (<http://www.verisign.com>), processes the request and provides you with an official digital certificate. While waiting for your official digital certificate, you can generate and install a test certificate. These steps are described in Section 5.3 through Section 5.5.

For information on setting up an Apache Web server with SSL without using the Compaq Secure Web Server Administration utility, visit the Apache Web site at the following URL:

<http://www.apache.org/>

## 5.3 Generating a Private Key

SSL uses an asymmetric key encryption to encode and decode data that is transmitted to and from the Web server. SSL key encryption requires two keys: a private key and a public key. The private key resides on the Web server system and must be kept secure. Before you can perform other steps to set up an SSL connection, you must generate a private key.

To generate a private key, perform these steps:

1. From the server administration menu, choose Manage SSL for the desired server. For example, from the Manage the Public Web Server menu, choose Manage SSL for the Public Web Server. The Manage SSL for the Public Web Server menu is displayed.
2. Choose Generate a Private Key. The Generate a Private Key menu is displayed, informing you whether a private key already exists.
3. Click Submit to generate a private key. When you generate a private key, the key is saved to following file for each server:

```
/usr/internet/httpd/server/conf/ssl.key/server.key
```

Where *server* is the name of the server you are modifying for SSL, as follows:

- Public Web server —/usr/internet/httpd/conf/ssl.key/server.key
- Administration Web server —/usr/internet/httpd/admin/conf/ssl.key/server.key

If a private key already exists, the existing key is saved in a separate `server.n.key` file where *n* is an integer incrementing from 1.

Figure 5–2 shows that a private key has been generated for the public Web server and the location of the `server.key` file. Note that you can generate a certificate request directly from this page, from which you can display the Generate a Certificate Request form. See Section 5.4 for complete steps for generating a certificate request.

**Figure 5–2: Generate a Private Key — Results**



## 5.4 Generating a Certificate Request

After you have generated a private key (Section 5.3), you can generate a certificate request that provides information about your company and private key to a Certificate Authority (CA). From this request, an X.509 certificate signing request (CSR) is created.

To generate a certificate request, perform these steps:

1. From the server administration menu, choose Manage SSL for the desired server. For example, from the Manage the Public Web Server menu, choose Manage SSL for the Public Web Server. The Manage SSL for the Public Web Server menu is displayed.
2. Choose Generate a Certificate Request. The Generate a Certificate Request form is displayed (Figure 5–3).

**Figure 5–3: Generate a Certificate Request Form**

The screenshot shows a web browser window with the following content:

- Navigation bar: Home < Secure Web Server Administration < Manage SSL for the Public Web Server <
- Page title: **Generate a Certificate Request for the Public Web Server** Help
- Instruction: **Enter information needed to generate a certificate request.**
- Form fields:
  - Country Code:
  - State Or Province Name:
  - Locality Name (City/Town):
  - Organization Name:
  - Organizational Unit Name:
  - Common Name (Fully Qualified Domain Name):
  - Email Address:
- Submit button: Submit

3. Enter your company data in the text fields.

A two-character country code is required by your CA. For the country code, enter an official ISO standard two-character country code as defined in *ISO Standard 3166-1*:  
<http://www.din.de/gremien/nabd/iso3166ma/index.html>

For the Common Name field, use the fully qualified domain name of your server (for example, `www.server.wyxcorp.com`).
4. Click on Submit. From the information you provided, an X.509 certificate signing request (CSR) is created. The certificate request displays in your browser window and is saved in the `/usr/internet/httpd/server/conf/ssl.csr/server.csr` file, where `server` is the name of the server you are modifying. For the the Web Server Public Instance, the certificate request file is saved in `/usr/internet/httpd/conf/ssl.csr/server.csr`.
5. To complete the certificate request process, copy information from the browser window or copy the contents from the CSR file and send the information (along with required paperwork and payment) to a Certificate Authority (CA) such as VeriSign (<http://www.verisign.com>). The highlighted text in Figure 5–4 shows the information that you send to your CA.

Note that you can generate a test certificate directly from this page. See Section 5.5 for complete steps for generating a test certificate.

Figure 5–4: Certificate Request Success Notice

Home ◀ Secure Web Server Administration ◀ Manage SSL for the Public Web Server ◀

## Generate a Certificate Request for the Public Web Server Help

✔ Success

Successfully generated a certificate request for the Public Web Server  
The certificate request file is `/usr/internet/httpd/conf/ssl.csr/server.csr`:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB3TCCAUYCAQAwgZwxCzAJBgNVBAYTA1VTMRYwFAYDVQQIEW1NYXNzYWNoeXN1
dHRzMQ8wDQYDVQQHEwZCb3N0b24xEDAOBgNVBAoTB3h5emNvcnAxDTALBgNVBAst
BHVuaXgxGzAZBgNVBAMTEuN1cnZlcj54eXpjb3JwLmNvbTEuMCQGCSqGSIb3DQEJ
ARYXcm9vdEBzZXJ2ZXIueH16Y29ycC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAJ3MSfkoP7DjGhtJyGVaMQM/fNmuAfiksJa8QKN7a11JwkG6gsLhPw5M
G677cmc11vNL9FgAhb0VbyGdPctSR4C5h1FiRuFZPMyGyBQOEKfSmaEs0Jnwefgd
8EUOp3VCUtns8moY0uYLWEKzpLnaAarUTk5XTUwh/OK8HG+4ou7tAgMBAAGgADAN
BgkqhkiG9w0BAQQFAA0BgQAUEBCTSQ435/OfMFJETve4LixxRH/6XDaQpKt4HzMy
yK/gOH7rg21nLZozQWcdWy/Cn58c8KwH5k8dfepNczj8buuAy2FvINK0/A5jCgxe
f0wLxhrl9AyEY2sJsIWwqlspH7VdWxbsBUjELCgE2CGY/cyzjAULxgN2uKK60jxo
kA==
-----END CERTIFICATE REQUEST-----
```

Provide this certificate request data (including the BEGIN and END lines) when requesting a certificate from a Certificate Authority.

You may now generate a test certificate using the key and certificate request.

## 5.5 Generating and Installing a Test Certificate

Before you receive your official certificate, you can generate a self-signed certificate and test establishing secure connections from your server.

To generate and install a test certificate, perform these steps:

1. From the server administration menu, choose **Manage SSL for the desired server**. For example, from the **Manage the Public Web Server** menu, choose **Manage SSL for the Public Web Server**. The **Manage SSL for the Public Web Server** menu is displayed.
2. Choose **Generate and Install a Test Certificate**. The **Generate and Install a Test Certificate** form is displayed.
3. Click on **Submit**. The test certificate is saved in the `/usr/internet/httpd/server/conf/ssl.csr/server.crt` file, where `server` is the name of the server you are modifying. When you generate and install an official certificate, it is saved in the same file.

For example, for the public Web server, the test certificate or official certificate is stored in `/usr/internet/httpd/conf/ssl.csr/server.crt`. If you had a previous certificate, the new certificate overwrites the `server.crt` file. However, existing certificates are saved under a new name, as shown in Figure 5–5.

**Figure 5–5: Test Certificate Installation Success Notice**



With a test certificate in place, you can now try enabling SSL on the server.

4. On the Generate and Install Test Certificate form (Figure 5–5), click on the Manage SSL button to enable SSL using the installed test certificate. The Manage SSL for the Public Web Server form will be displayed as shown in Section 5.8. See Section 5.8 for instructions on enabling and disabling SSL for a Web server using this form.

When you generate a test certificate, it is automatically installed. The Manage SSL main menu changes to show two additional options, as shown in Figure 5–6.

**Figure 5–6: Manage SSL Main Menu with Additional Options**



With a test certificate in place, you can now try connecting to the SSL-enabled system. Note that when you make an SSL connection to a server using a self-signed test certificate, you are warned that the certificate is signed by an untrusted source. The system gives you the option to accept the certificate and connect to the Web server.

To view the contents of the certificate, see Section 5.7.

## 5.6 Installing a Digital Certificate

When you receive a digital certificate from your Certificate Authority, you must then install it to the proper location.

To install a certificate, perform these steps:

1. Determine that the certificate you received is compatible with the private key you created in Section 5.3. The key and certificate must be compatible for the certificate to install properly.

2. From the server administration menu, choose Manage SSL for the desired server. For example, from the Manage the Public Web Server menu, choose Manage SSL for the Public Web Server. The Manage SSL for the Public Web Server menu is displayed.
3. Choose Install a Certificate. The Install a Certificate form is displayed.
4. Cut and paste the contents from the official certificate into the Install a Certificate text field, shown in Figure 5–7.

**Figure 5–7: Install a Certificate Text Field**

Home < Secure Web Server Administration < Manage SSL for the Public Web Server <

**Install a Certificate for the Public Web Server** Help

**Enter the certificate text you received from your Certificate Authority.**

Certificate:

Submit

5. Click on Submit. The certificate file is copied to the `/usr/internet/httpd/server/conf/ssl.csr/server.csr` file, where `server` is the name of the system you are modifying.

If you generated and installed a test certificate (Section 5.5), the test certificate file (`server.csr`) is overwritten with the official certificate file and is saved under a new name (for example, `server.2.csr`).

After successfully installing the certificate, the Manage SSL main menu provides two additional options that let you:

- View certificate details (Section 5.7)
- Enable or disable SSL capabilities (Section 5.8)

These options also appear on the Manage SSL main menu when you generate and install a test certificate (Figure 5–6).

## 5.7 Viewing Certificate Details

The View Certificate Details option enables you to display certificate information in a readable format. This certificate file includes information you provided when you requested the certificate (Section 5.4), information from the CA, and information about your public key.

1. From the server administration menu, choose Manage SSL for the desired server. For example, from the Manage the Public Web Server menu, choose Manage SSL for the Public Web Server. The Manage SSL for the Public Web Server menu is displayed.

2. Choose View Certificate Details. The certificate stored in `/usr/internet/httpd/server/conf/ssl.csr/server.csr` is displayed in readable format. Figure 5–8 shows the information in an example certificate.

**Figure 5–8: Certificate File in Readable Format**

```

Home ◀ Secure Web Server Administration ◀ Manage SSL for the Public Web Server ◀
View Certificate Details for the Public Web Server Help
File: /usr/internet/httpd/conf/ssl.crt/server.crt
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 0 (0x0)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=US, ST=Massachusetts, L=Boston, O=xyzcorp, OU=unix, CN=server.
    Validity
      Not Before: May 31 14:15:39 2001 GMT
      Not After : May 31 14:15:39 2002 GMT
    Subject: C=US, ST=Massachusetts, L=Boston, O=xyzcorp, OU=unix, CN=server
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:9d:cc:49:f9:28:3f:b0:e3:1a:1b:49:c8:65:5a:
        31:03:3f:7c:d9:ae:01:f8:a4:b0:96:bc:40:a3:7b:
        6a:5d:49:c2:41:ba:82:c2:e1:3f:0e:4c:1b:ae:fb:
        72:67:35:d6:f3:4b:f4:58:00:85:bd:15:6f:21:9d:
        3d:cb:52:47:80:b9:87:51:62:46:e1:59:3c:cc:86:
        c8:14:0e:10:a7:d2:99:a1:2c:d0:99:f0:79:f8:1d:
        f0:45:0e:a7:75:42:52:d9:ec:f2:6a:18:d2:e6:0b:
        58:42:b3:a4:b9:da:01:aa:d4:4e:4e:57:4d:4c:21:
        fc:e2:bc:1c:6f:b8:a2:ee:ed
  
```

## 5.8 Enabling and Disabling SSL for a Web Server

After obtaining a private key and an official certificate, you can enable (or disable) SSL capabilities for your Web server. When you enable SSL, the Web server’s runtime configuration file (`/usr/internet/httpd/server/conf/.httpdrc`) is revised to instruct the Web server to use SSL when it restarts. Enabling SSL affects the public and administration servers as follows:

- For the public Web server instance, you can connect to the secure Port 443 using the `https:` prefix. Note that you also can continue connecting to Port 80 using a non-secure connection using the `http:` prefix.
- For the administration Web server instance, the port defined for each server is changed. You can only connect as a secure port using the `https:` prefix and the same port number. Once you connect to one of the administration servers, the Administration utility manages the connection to the other servers, using the proper type of connection.

To enable (or disable) SSL capabilities for a Web server:

1. From the server administration menu, choose Manage SSL for the desired server. For example, from the Manage the Public Web Server menu, choose Manage SSL for the Public Web Server. The Manage SSL for the Public Web Server menu is displayed.
2. Choose the Enable button or the Disable button at the bottom of the form to enable or disable SSL for the server, respectively.

Figure 5–9 shows the confirmation page after SSL has been enabled on the server.

**Figure 5–9: Enable SSL Confirmation Page**



## 5.9 Testing Your SSL Connection

Test your secure connection after enabling SSL for public and administration servers, as follows:

- For a public Web server, the standard `https:` port is 443. When you specify a URL as `https://www.xxx.com/`, for example, it automatically uses Port 443. Also test access to the nonsecure public server Port 80 by using `httpd:` after enabling SSL. (See Section 5.10 for additional considerations when enabling SSL for public Web servers.)
- For an administration server, the same port is used for all connections, regardless of whether SSL is enabled. With SSL enabled, you can only access this server using `https://www.xxx.com:8081/`. Using `http:` will produce an error message asking you to specify `https:` (Figure 5–10). The administration server menus determine which protocol to use, `http:` or `https:`, and will advise you when you first connect.

**Figure 5–10: SSL Connections Error Message**



### Note

After enabling SSL and changing a connection from nonsecure to secure, you might not be able to use the Back button of your browser to navigate to pages viewed prior to enabling SSL. Similarly, disabling SSL and changing a connection from secure to nonsecure might affect use of the Back button. This happens because the saved prefix might no longer be valid.

## 5.10 Specifying Public Web Server Access to HTTP and HTTPS Connections

After enabling SSL for the Web Server Public Instance, the data hierarchy you created (by default, `/usr/internet/httpd/htdocs`) will be accessible either using the standard `http:` protocol or the SSL-enabled `https:` protocol.

To limit access just to `https:` connections, perform these steps:

1. From the Secure Web Server Administration menu, choose Manage the Public Web Server.
2. Choose Change Configuration Parameters.
3. Choose Change Listening Ports and Addresses and remove Port 80 from the list of active ports and make Port 443 the primary port.
4. Click Submit to update the configuration file and restart the public Web server.

If you want the public Web server to respond to both `http:` requests on Port 80 and `https:` requests on Port 443 while maintaining separate data hierarchies, you must manually change the public Web server configuration file `/usr/internet/httpd/conf/httpd.conf`. Any `https:` directories must be defined within the SSL VirtualHost directive. (In the configuration file, search for the line `<VirtualHost _default_:443>`.)

Directory, Location, or File directives placed within the SSL VirtualHost directive, as well as Alias and ScriptAlias directives placed within the SSL VirtualHost directive, can only be accessed when SSL is enabled and when `https:` connections are used. By changing the value of the DocumentRoot directive within the SSL VirtualHost directive, you can specify a default location specific to `https:` connections.

## 5.11 Migrating Your Netscape Digital Certificate to the Compaq Secure Web Server

This section describes how to migrate a Netscape Web Server digital certificate to the Compaq Secure Web Server, which will then allow you to migrate Netscape (iPlanet) Web Server SSL users to an SSL-enabled Compaq Secure Web Server.

### 5.11.1 Prerequisites for Migration

Before you can migrate your Netscape digital certificate to the Compaq Secure Web Server, you must first access the Netscape Web Server's private key. You use this key as the Compaq Secure Web Server's private key when installing the digital certificate. You must also save a copy of the Netscape Web Server's digital certificate in order to install it in the Compaq Secure Web Server.

The Compaq Secure Web Server must have the same Common Name and IP address as the Netscape Web Server. This data was used when creating the Certificate Signing Request that you sent to your Certificate Authority when requesting the digital certificate. The Common Name is usually the same as the fully qualified host name of the server.

### 5.11.2 Migrating the Netscape Digital Certificate

Follow these steps to migrate your Netscape Web Server private key and digital certificate to the Compaq Secure Web Server:

1. Login as root on the system where you installed both Web servers and start the Netscape Communicator 4.X Web browser:

```
#su root
#/usr/bin/X11/netscape &
```

2. Create a backup copy of the Web browser certificate file and the private key database file in the root user's `$HOME/.netscape` directory:

```
#cp -pf /.netscape/key3.db /.netscape/key3.db.orig
#cp -pf /.netscape/cert7.db /.netscape/cert7.db.orig
```

3. Copy the Netscape Web Server digital certificate file and private key database file from the Web server root to the `/.netscape` directory, overwriting the Web browser certificate file and key database file:

```
#cp -pf Netscape server root/alias/server key database name-key3.db /.netscape/key3.db
#cp -pf Netscape server root/alias/server certificate database name-cert7.db \
    /.netscape/cert7.db
```

4. Export the Web Server private key database to a PKCS#12 (PFX) format certificate file using Netscape Communicator, as follows:
  - a. Under the Communicator pull down menu, select the Security Info option in the Tools menu. (Alternately, click on the padlock icon in the bottom left hand corner of the Web browser.) The Security Info dialog box is displayed.
  - b. Select the Yours option under Certificates in the Security Info dialog box. The Server-Cert certificate appears in the displayed list.
  - c. Select the Server-Cert certificate and click on the Export button.

---

**Note**

---

You must use the same password you used for the Netscape Web Server key database when prompted to enter the passwords for accessing and exporting the certificate.

---

- d. Export the certificate to the PKCS#12 format certificate file by entering the name of the file (for example, `cert.p12`) in the Save As pop-up menu, then click on OK.
5. Extract the private key from the PKCS#12 format certificate file (`cert.p12`) using the OpenSSL `pkcs12` command. Save the private key to a PEM-format private key file, using the same password you entered for the import password and PEM pass phase:

```
#!/usr/internet/httpd/bin/openssl pkcs12 -nocerts -in
/.netscape/cert.p12 -out /.netscape/key.pem
Enter Import Password: password
MAC verified OK
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase: password
```

6. Remove the PEM pass phase from the private key file using the OpenSSL `rsa` command:

```
#!/usr/internet/httpd/bin/openssl rsa -in /.netscape/key.pem
-out /.netscape/keyout.pem
read RSA key
Enter PEM pass phrase: password
writing RSA key
```

7. Create the Compaq Secure Web Server Private Key directory and copy the private key file to the `server.key` file into the directory:

```
#mkdir -p /usr/internet/httpd/server name/conf/ssl.key
#chown root:system /usr/internet/httpd/server name/conf/ssl.key
#chmod 640 /.netscape/keyout.pem
#chown root:nobody /.netscape/keyout.pem
#cp -pf /.netscape/keyout.pem /usr/internet/httpd/server
name/conf/ssl.key/server.key
```

---

**Note**

---

The *server name* directory should be omitted when creating the private key file for the Public Web Server instance.

---

8. Copy back the original Web browser certificate file and key database file overwriting the Web Server certificate file and key database file, then remove the files you created:

```
#cp -pf /.netscape/key3.db.orig /.netscape/key3.db
#cp -pf /.netscape/cert7.db.orig /.netscape/cert7.db
#rm -f /.netscape/cert.p12 /.netscape/key.pem /.netscape/keyout.pem
```

9. Using the copy of the Netscape Web Server server certificate you received back from your Certificate Authority, install the digital certificate into the Compaq Secure Web Server using the Install a Certificate form provided in the Compaq Secure Web Server Administration server (see Section 5.6).

---

## Compaq Secure Web Server Components and Modules

Table A–1 lists the major components of the Compaq Secure Web Server kit, along with a URL for more information about each component.

Table A–2 lists the Apache source distribution standard modules that are provided with the Compaq Secure Web Server. Modules are either provided built in to the `httpd` image or as Dynamic Shared Objects.

Table A–3 lists modules that are part of the `mod_ssl` distribution that is integrated in the Compaq Secure Web Server kit.

Table A–4 lists other modules provided with the Compaq Secure Web Server.

**Table A–1: Compaq Secure Web Server Components**

Component	Description	URL
Apache HTTPD Version 1.3.14	Apache HTTP Server.	<a href="http://www.apache.org">http://www.apache.org</a>
<code>mod_ssl</code> Version 2.7.1-1.3.14	An Open Source toolkit that implements the Secure Sockets Layer (SSL Version 2/Version 3) and Transport Layer Security (TLS Version 1) protocols, as well as a complete, general purpose cryptography library.	<a href="http://www.openssl.org">http://www.openssl.org</a>
PHP Version 4.0.3	A server-side, cross-platform HTML embedded scripting language.	<a href="http://www.php.net">http://www.php.net</a>
<code>fastcgi</code> Version 2.2.8	A language-independent, scalable, open extension to CGI that provides high performance without the limitations of server-specific APIs.	<a href="http://www.fastcgi.com">http://www.fastcgi.com</a>
<code>auth_ldap</code> Version 1.4.5	An LDAP authentication module for Apache.	<a href="http://www.rudedog.org/auth_ldap/">http://www.rudedog.org/auth_ldap/</a>
Jakarta Tomcat Version 3-1	A world-class implementation of the Java Servlet 2.2 and JavaServer Pages 1.1 Specifications.	<a href="http://jakarta.apache.org">http://jakarta.apache.org</a>
Analog Version 4.03	A popular log file analyzer.	<a href="http://www.stat-slab.cam.ac.uk/~sret1/analog/">http://www.stat-slab.cam.ac.uk/~sret1/analog/</a>

**Table A-2: Standard Compaq Secure Web Server Modules**

<b>Module</b>	<b>DSO or Integrated</b>	<b>Description</b>
mod_access	Integrated	Access control based on client host name or IP address
mod_actions	Integrated	Execute CGI scripts based on media type or request method
mod_alias	Integrated	Map different parts of the host file system in the document tree, and URL redirection
mod_asis	Integrated	Send files which contain their own HTTP headers
mod_auth	Integrated	User authentication using text files
mod_auth_anon	DSO	Anonymous user access to authenticated areas
mod_auth_db	DSO	User authentication using Berkeley DB files
mod_auth_dbm	Integrated	User authentication using DBM files
mod_autoindex	Integrated	Automatic directory listings
mod_cern_meta	DSO	Support for HTTP header metafiles
mod_cgi	Integrated	Invoke CGI scripts
mod_digest	DSO	MD5 authentication
mod_dir	Integrated	Basic directory handling
mod_expires	DSO	Apply Expires: headers to resources
mod_headers	DSO	Add arbitrary HTTP headers to resources
mod_imap	Integrated	The image map file handler
mod_include	Integrated	Server-parsed documents
mod_info *	Integrated	Server configuration information
mod_log_agent	DSO	Log of user agents
mod_log_config	Integrated	User-configurable logging replacement for mod_log_common
mod_log_referer	DSO	Log document references
mod_mime	Integrated	Determine document types using file extensions
mod_mime_magic	DSO	Determining document types using "magic numbers"
mod_mmap_static	DSO	Experimental file caching, mapping files into memory to improve performance
mod_negotiation	Integrated	Content negotiation
mod_proxy	DSO	Caching proxy abilities
mod_rewrite	DSO	Powerful URI-to-file name mapping using regular expressions
mod_setenvif	Integrated	Set environment variables based on client information
mod_so *	Integrated	Support for loading modules at run time
mod_spelling	DSO	Automatically correct minor typos in URLs

**Table A–2: Standard Compaq Secure Web Server Modules (cont.)**

<b>Module</b>	<b>DSO or Integrated</b>	<b>Description</b>
mod_status	Integrated	Server status display
mod_unique_id	DSO	Generate unique request identifier for every request
mod_userdir	Integrated	User home directories
mod_usertrack	DSO	User tracking using Cookies (replacement for mod_cookies.c)
mod_vhost_alias	DSO	Support for dynamically configured mass virtual hosting

**Table A–3: Related Modules Provided with the Compaq Secure Web Server**

<b>Module</b>	<b>DSO or Integrated</b>	<b>Description</b>
mod_ssl	DSO	Provide SSL connections
mod_define	DSO	Support for variables in configuration directives

**Table A–4: Additional Modules Provided with the Compaq Secure Web Server**

<b>Module</b>	<b>DSO or Integrated</b>	<b>Description</b>
mod_auth_ldap	DSO	Support for authentication with an LDAP database
mod_fastcgi	DSO	Supports connections to FastCGI processes
mod_frontpage	DSO	Support for Microsoft's FrontPage extensions
mod_jserv	DSO	Interface to Java Servlet engines
mod_php4	DSO	The PHP processing engine



---

# Glossary

## **Apache Web Server**

A freely available UNIX-based Web server. It is currently the most commonly used server on Internet connected sites. Compaq's implementation of the Apache Web Server is called the Compaq Secure Web Server.

## **certificate authority**

A third party organization that confirms the relationship between a party to the **https** transaction and that party's public key. Certification authorities may be widely known and trusted institutions for Internet-based transactions. Where https is used on a company's internal network, an internal department within the company may fulfill this role.

## **digital certificate**

A token which underpins the principle of trust in SSL-encrypted transactions. The information within a certificate includes the issuer (the Certificate Authority that issued the certificate), the organization that owns the certificate, the public key, the validity period (usually one year) of the certificate, and the host name for which the certificate was issued. It is digitally signed by the Certificate Authority so that none of the details can be changed without invalidating the signature. See also **certificate authority**, **digital signature**.

## **digital signature**

A use of public key cryptography to authenticate a message. Digital signatures use a private key to indicate that the signature was made by the owner of that key. See also **public key cryptography**, **private key**.

## **distinguished name**

Also called DN. A sequence of relative distinguished names (RDNs). See also **relative distinguished name**.

## **DN**

See **distinguished name**.

## **DNS**

Domain Name System. A general-purpose, distributed, replicated data query service chiefly used on the Internet to translate host names into Internet addresses. See also **fully qualified domain name**.

## **Domain Name System**

See **DNS**.

## **dynamic module**

A module that provides the means for building program code in a format that can be loaded into the address space of an executable program at run time. Dynamic modules are loaded into the server process space only when necessary and assure that overall memory usage is reduced.

## **firewall**

Hardware and software that lies between two networks, such as an internal network and an Internet service provider. The firewall protects your network by blocking unwanted users from gaining access and by disallowing messages to specific recipients outside the network.

## **FQDN**

See **fully qualified domain name**.

**fully qualified domain name**

Also called FQDN. The full name of a system, consisting of its local host name and its domain name. A fully qualified domain name is usually precise enough to determine an Internet address for any host on the Internet.

**HTTP**

Hyper Text Transfer Protocol. The protocol used between a Web browser and a server to request a document and transfer its contents. The specification is maintained and developed by the World Wide Web Consortium. See also **HTTPS**.

**HTTPS**

Ordinary HTTP exchanged over an **SSL**-encrypted session.

**port**

A logical channel in a communications system.

**private key**

The part of the key in a public key system that is kept secret and is used only by its owner. This is the key used for decrypting messages, and for making **digital signatures**. Compare with **public key**.

**public key**

The part of the key in a public key system which is distributed widely and is not kept secure. This is the key used for encryption (as opposed to decryption) or for verifying signatures. Compare with **private key**.

**public key cryptography**

Public key cryptography uses a key for encryption and a different key for decryption. Although the keys are related, it is not possible to calculate the decryption key from only the encryption key in any reasonable amount of computation time. In most practical systems, the public key system is used for encoding a **session key** which is used with a symmetric system to encode the actual data. RSA is an example of a public key algorithm.

**RDN**

See **relative distinguished name**.

**relative distinguished name**

Also called RDN. One or more attribute/value pairs stored on an LDAP server that uniquely identify an entry from its sibling in an object tree.

**secret key**

Part of a symmetric cipher in which the same key is used for encryption and decryption. SSL encryption uses a secret-key nested within a **public key** and authenticated through certificates. Secret-key encryption provides faster access than public-key encryption alone. See also **public key cryptology**.

**Secure Socket Layer**

See **SSL**.

**session key**

A key used for one message or set of messages. In a typical system, a random session key is generated for use with a symmetric algorithm to encode the bulk of the data. Only the session key is communicated using public key encryption. See also **public key cryptology**.

**SSL**

Secure Socket Layer. A protocol developed by Netscape for encrypted transmission over TCP/IP networks. SSL sets up a secure end-to-end link over which **http** or any other application protocol can operate. The most common application of SSL is **https** for SSL-encrypted HTTP.

**TCP/IP**

Transmission Control Protocol/Internet Protocol. Ethernet protocols incorporated into 4.2 BSD UNIX. While TCP and IP specify two protocols, the combined term is used to refer to the entire Department of Defense protocol suite, including Telnet and FTP.

**Telnet**

The Internet standard protocol for remote logins. UNIX BSD includes the telnet program, which uses the protocol, and acts as a terminal emulator for remote login sessions.

**VeriSign**

A dominant **certificate authority** on the internet, though many of its certificates are signed as RSA Data Security. Early versions of Microsoft and Netscape browsers had RSA Data Security configured as the only trusted certificate authority. This mandated that users who want to use certificates on the internet must obtain them from VeriSign and use server software accredited by VeriSign. Current versions of the Microsoft and Netscape browsers allow users to add new certificate authorities. As older versions of the browsers are replaced, new certificate authorities (such as Thawte) have emerged.

**virtual host**

An alias name assigned to an FTP server.

**Web server**

A server process, running at a Web site, that sends out Web pages in response to HTTP requests from remote browsers.



## A

---

**AddModule directive**, 3–3  
**administration account**  
  default ports, 1–1

## C

---

**certificate**  
  generating request, 5–3  
  installing, 5–6  
  viewing, 5–7  
**Compaq Secure Web Server**  
  additional modules, A–3  
  administration, 1–1  
  changing password, 2–17  
  components and modules, A–1  
  configuration files, 2–1  
  generating activity reports, 2–14  
  generating server reports, 2–14  
  managing, 1–3  
  migrating Netscape certificate, 5–10  
  modules in mod-ssl distribution, A–3  
  refreshing access log, 2–16  
  refreshing error log, 2–16  
  remote access to, 2–18  
  restarting public, 2–16  
  SSL, 5–1  
  standard Apache modules, A–2  
  stopping public, 2–16  
  user account, 2–12  
  using dynamic modules, 3–1  
  viewing access log, 2–14  
  viewing error log, 2–14  
**configuration file**  
  verification, 3–3  
**configuration files**, 2–1  
**configuration parameters**  
  access control entries, 2–4  
  adding HTML directory aliases, 2–9  
  address, 2–6  
  CGI directory aliases, 2–10  
  deleting HTML directory aliases, 2–10  
  HTML directory aliases, 2–9  
  listening port, 2–6  
  logging and reporting, 2–11  
  tuning, 2–3  
  URL defaults, 2–8  
  virtual hosts, 2–7

## D

---

**daemons**  
  httpd, 2–16  
**DSO**  
  ( *See* dynamic module )  
**DSO module**  
  ( *See* dynamic module )  
**dynamic module**, 1–3, 3–1  
  activating, 3–2  
  activating an Apache DSO, 3–3  
  non-standard Apache, 3–2  
  standard Apache, 3–2  
  support for, 3–1  
  using AddModule directive, 3–3  
  using LoadModule directive, 3–3  
  verifying configuration file, 3–3

## E

---

**encryption**, 1–4, 5–1

## J

---

**Java Servlet**, 1–3, 4–1  
**JSP Engine**, 1–3, 4–1

## L

---

**LoadModule directive**, 3–3  
**log file**  
  Tomcat, 4–2

## N

---

**Netscape**  
  SSL, 1–4, 5–1

## P

---

**password**  
  changing Compaq Secure Web Server,  
    2–17  
  managing administrator, 1–2  
**private key encryption**, 5–3  
**public Web server**  
  displaying information, 2–14  
  displaying server status, 2–13

## R

---

**remote access**, 2–18

## S

---

### **Secure Socket Layer**

( *See* SSL )

### **security**

SSL, 5–1

### **server activity reports**, 2–14

### **SSL**, 1–4, 2–18

authentication, 1–4

concepts, 5–1

considerations for public Web servers,  
5–9

disabling, 5–8

enabling, 5–8

enabling from Administration utility,  
5–2

generating a certificate request, 5–3

generating a private key, 5–3

generating a test certificate, 5–5

installing a certificate, 5–6

migrating Netscape Server certificate,  
5–10

overview, 1–4

performing authentication, 5–1

performing encryption, 5–1

prerequisites for migrating Netscape  
Server certificate, 5–10

steps for enacting, 5–1

steps for migrating Netscape Server  
certificate, 5–10

testing secure connections, 5–9

using private keys, 5–1

viewing certificate details, 5–7

## T

---

### **test certificate**

generating, 5–5

installing, 5–5

### **Tomcat**, 4–1

additional information, 4–3

examples, 4–3

locating files and directories, 4–1

log files, 4–2

overview, 1–3

restarting in non-TruCluster

environment, 4–2

restarting in TruCluster environment,  
4–2

starting, 4–2

understanding, 4–1

### **TruCluster**

restarting Tomcat, 4–2

## U

---

### **user account**

adding, 2–12

deleting, 2–13

modifying, 2–13

## W

---

### **Web server LDAP authentication**, 3–4