

---

Compaq Secure Web Server  
Version 1.0-1 for OpenVMS  
Alpha (*based on Apache*)

Installation and Configuration  
Guide

---

**January 2001**

**Distribution restrictions and disclaimer**

Customer agrees that he/she is not prohibited by the U.S. or other government export control regulations from receiving this software or technical data. This documentation contains links to external sites whose content is subject to change and for which Compaq Computer Corporation has no responsibility. Furthermore, the accuracy of such links cannot be guaranteed because of the dynamic nature of the web.

Copyright 2001 Compaq Computer Corporation

Compaq, VMS, and the Compaq logo

Registered in the U.S. Patent and Trademark Office.

OpenVMS and Tru64 are trademarks of Compaq Information Technologies Group, L.P.

Apache is a trademark of the Apache Software Foundation.

Includes RSA BSAFE cryptographic or security protocol software from RSA Security.

Netscape Navigator and Netscape Communicator are trademarks of Netscape Communications Corporation.

Internet Explorer is a trademark of Microsoft Corporation.

All other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

Confidential computer software. Valid license from Compaq or authorized sublicensor 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 subject to change without notice.

The information in this publication is subject to change without notice and is provided "AS IS" WITHOUT WARRANTY OF ANY KIND. THE ENTIRE RISK ARISING OUT OF THE USE OF THIS INFORMATION REMAINS WITH RECIPIENT. IN NO EVENT SHALL COMPAQ BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION), EVEN IF COMPAQ HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING SHALL APPLY REGARDLESS OF THE NEGLIGENCE OR OTHER FAULT OF EITHER PARTY AND REGARDLESS OF WHETHER SUCH LIABILITY SOUNDS IN CONTRACT, NEGLIGENCE, TORT, OR ANY OTHER THEORY OF LEGAL LIABILITY, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

The limited warranties for Compaq products are exclusively set forth in the documentation accompanying such products. Nothing herein should be construed as constituting a further or additional warranty.

This document was prepared using DECdocument, Version 3.3-1b.

---

# Contents

## 1 Installation Requirements and Prerequisites

1.1	Hardware Requirements .....	1-1
1.2	Software Requirements .....	1-1
1.2.1	Earlier Versions of OpenVMS Alpha .....	1-1
1.2.2	Support for MultiNet and TCPware .....	1-2
1.2.3	MOD_JSERV Requirements .....	1-2
1.2.4	MOD_PERL Requirements .....	1-2
1.2.5	Building the Apache HTTP Server from Source Code .....	1-3

## 2 Installation and Configuration

2.1	Read the Release Notes .....	2-1
2.2	Remove Older Versions of the Software (upgrade customers only) .....	2-1
2.3	Install the Server and Optional Modules .....	2-2
2.4	Configure the Server .....	2-4
2.5	Post Configuration Checklist .....	2-5
2.5.1	Configure MOD_JSERV .....	2-5
2.5.2	Configure MOD_PERL .....	2-6
2.5.3	Run AUTOGEN .....	2-6
2.5.4	Check Disk Quota .....	2-6
2.5.5	Check for SET TERMINAL/INQUIRE .....	2-6
2.6	Test the Installation .....	2-6
2.6.1	Browser Test .....	2-7
2.6.2	TELNET Test .....	2-7
2.6.3	Troubleshooting .....	2-7
2.7	What's Next .....	2-8
2.8	Merge HTTPD.CONF (upgrade customers only) .....	2-8
2.9	Installing Optional Modules at a Later Time .....	2-8

## 3 Running the Compaq Secure Web Server on OpenVMS

3.1	Starting and Stopping the Server .....	3-1
3.2	Server Log File .....	3-2
3.3	Performance Considerations .....	3-2
3.3.1	Limits and Quotas .....	3-2
3.3.2	Server Experiencing Medium to High Usage .....	3-4
3.3.3	Global Pages and Global Sections .....	3-4
3.3.4	Excessive File Build Up .....	3-4
3.4	Customizing the Server Environment .....	3-4
3.5	Modules and Directives .....	3-5
3.6	Supported and Unsupported Features .....	3-8
3.6.1	Modules Not Included .....	3-9
3.6.2	Unsupported Directives .....	3-9
3.6.3	Command Line Options .....	3-10

3.6.4	Virtual Host Support .....	3-11
3.6.5	Dynamic Shared Object Support .....	3-11
3.6.6	File Handlers .....	3-11
3.6.7	Content Negotiation .....	3-12
3.6.8	Apache API .....	3-12
3.6.9	suEXEC Support .....	3-12
3.6.10	Running MOD_OSUSCRIPT .....	3-12
3.7	File Formats .....	3-13
3.8	File Naming Conventions .....	3-14
3.9	File Transfer Process and Access Control List .....	3-14
3.10	Logical Names .....	3-15
3.11	Redefining Logical Names .....	3-16
3.12	OpenVMS Cluster Considerations .....	3-17
3.12.1	Individual System vs. Clusterwide Definition .....	3-17
3.12.2	Mixed-Architecture Cluster .....	3-18
3.13	Common Gateway Interface (CGI) .....	3-18
3.13.1	CGI Environment Variables .....	3-18
3.13.2	Referencing Input .....	3-19
3.13.3	Executing CGI .....	3-19
3.13.4	Logicals for Debugging CGI Scripts .....	3-19
3.13.5	Displaying Graphics with CGI Command Procedures .....	3-20

## 4 Security Information

4.1	Process Model .....	4-1
4.2	Privileged Images .....	4-1
4.3	Privileges Required to Start and Stop the Server .....	4-2
4.4	File Ownership and Protection .....	4-2
4.5	Server Extensions (CGI Scripts, Java Servlets, Perl Modules) .....	4-2
4.6	suEXEC Not Available for Protecting Script Execution .....	4-3
4.7	Protecting Server Certificate Keys .....	4-3

## 5 Open Source Licenses

### Tables

3-1	Sample Values for the APACHE\$WWW SYSUAF .....	3-3
3-2	HTTPD Command Line Options .....	3-11
3-3	System Defined Logical Names .....	3-15
3-4	User Defined Logical Names .....	3-15

---

# Installation Requirements and Prerequisites

Before you can install the Compaq Secure Web Server for OpenVMS Alpha Version 1.0-1 (*based on Apache*), you should verify that your system meets the minimum hardware and software requirements described below.

## 1.1 Hardware Requirements

You can install the Compaq Secure Web Server for OpenVMS on any AlphaServer system or Alpha workstation running OpenVMS Version 7.1-2 or higher.

## 1.2 Software Requirements

The Compaq Secure Web Server requires the following software:

- OpenVMS Alpha Version 7.1-2 or higher
- Compaq TCP/IP Services for OpenVMS Version 5.0A or higher

### 1.2.1 Earlier Versions of OpenVMS Alpha

Compaq Secure Web Server has not been thoroughly tested on versions of OpenVMS prior to Version 7.1-2 and is not supported on those earlier versions. However, if you are running a version of OpenVMS Alpha earlier than Version 7.1-2, you should apply an Engineering Change Order (ECO) for the DEC C Run Time Library (RTL).

For versions of OpenVMS Alpha earlier than Version 7.1-2, install the following ECOs:

- ALPACRT09\_071
- ALPBASE02\_071

You can obtain these ECOs from the Compaq support website at

<http://www.compaq.com/support/>

From the Compaq support website:

1. In the top left corner, click *Software and Drivers*.
2. In the center of the page, find *Software Patches* and click *OpenVMS*.
3. On the left, under *Associated Links*, click *Search Patches*.
4. Under *Released Patches*, click *OpenVMS*.
5. Use the Search function (end of the top line) to search for ALPACRT09\_071 and ALPBASE02\_071.

## Installation Requirements and Prerequisites

### 1.2 Software Requirements

#### 1.2.2 Support for MultiNet and TCPware

If you are using MultiNet or TCPware instead of Compaq TCP/IP Services for OpenVMS, you should be aware of the following information.

##### **MultiNet**

The Compaq Secure Web Server has been successfully tested with MultiNet Version 4.2A and higher.

MultiNet 4.1B works with the Compaq Secure Web Server with the following ECO kits installed:

- UCXDRIVER
- UCX\_LIBRARY\_EMULATION
- KERNEL\_UPDATE

These ECO kits can be obtained from:

##### **TCPware**

The Compaq Secure Web Server has been successfully tested with TCPware Version 5.3-3 and higher.

TCPware Version 5.3-3 works with the Compaq Secure Web Server with the DRIVERS\_V543022 kit installed.

This ECO kit can be obtained from:

---

##### **Note**

---

The MultiNet and TCPware ECO kits required for the Compaq Secure Web Server are subject to change. For the latest ECO kit information, contact Process Software and ask for the ECO kits required to run the Compaq Secure Web Server. Send network connectivity questions regarding the Compaq Secure Web Server for OpenVMS on TCPware and MultiNet via email to [support@process.com](mailto:support@process.com).

---

#### 1.2.3 MOD\_JSERV Requirements

The Compaq Secure Web Server for OpenVMS supports an optional kit, CSWS\_JSERV, which includes MOD\_JSERV and JSSI modules that enable you to execute Java servlets. The CSWS\_JSERV kit requires the following software:

- OpenVMS Alpha Version 7.1 or higher
- Compaq Java Development Kit Version 1.1.8-3 or higher for OpenVMS Alpha
- Any patches required for the Compaq Java Development Kit Version 1.1.8-x for OpenVMS Alpha

#### 1.2.4 MOD\_PERL Requirements

Perl has become the premier scripting language of the Web, as most CGI programs are written in Perl. The Compaq Secure Web Server for OpenVMS supports an optional kit, CSWS\_PERL. This kit includes MOD\_PERL, an interface between Perl and the Compaq Secure Web Server which lets you write modules entirely in Perl. The CSWS\_PERL kit requires the following software:

- OpenVMS Alpha Version 7.2 or higher

- Perl Version 5.5-3

---

**Note**

---

The Compaq Secure Web Server for OpenVMS works with a specific version of Perl. You can have more than one version of Perl installed on your system as long as you are careful about how you define logical names. Make sure the Compaq Secure Web Server can only see its required version of Perl.

---

### **1.2.5 Building the Apache HTTP Server from Source Code**

The Compaq Secure Web Server for OpenVMS is based on Apache 1.3.12. Source code and instructions for building an Apache HTTP server for OpenVMS can be found at

<http://www.openvms.compaq.com/openvms/products/ips/apache/csws.html>

By itself, the source code does not include Secure Socket Layer (SSL) functionality. Download MOD\_SSL and OpenSSL source kits if you wish to include this feature in your Apache HTTP server.

If you are building an Apache HTTP Server from source code, you also need:

- Compaq C Version 6.2

Informal support for a customer built Apache HTTP Server can be obtained through the `comp.os.vms` or `comp.infosystems.www.servers.unix` internet news groups.

---

## Installation and Configuration

Read this chapter to install and configure the Compaq Secure Web Server for OpenVMS. Installation and configuration consists of the following steps:

1. Read the release notes
2. Remove older versions of the software (upgrade customers only)
3. Install the server and optional modules
4. Configure the server
5. Review the post configuration checklist
6. Test the installation

Detailed instructions for completing each of these steps are provided below.

### 2.1 Read the Release Notes

Before you begin the installation, you should read the release notes provided with the kit. See the *Compaq Secure Web Server for OpenVMS Alpha Release Notes* at

[http://www.openvms.compaq.com/openvms/products/ips/apache/cs\\_ws\\_relnotes.html](http://www.openvms.compaq.com/openvms/products/ips/apache/cs_ws_relnotes.html)

### 2.2 Remove Older Versions of the Software (upgrade customers only)

If you have Apache Version 1.3-12 (or any Apache beta kit) installed, you must use the POLYCENTER Software Installation Utility (PCSI) to remove it before you can install your new kit. Do the following:

1. Preserve files you have customized.

The PCSI utility removes only the files and directories it previously installed. Any files you have created will not be affected, but you must preserve any PCSI-installed files you have edited. Copy the following files to another location (these files are deleted during the remove operation):

- [APACHE]LOGIN.COM
- [APACHE.HTDOCS]INDEX.HTML

The new kit contains an updated version of HTTPD.CONF. You will need to save your current version of HTTPD.CONF and merge it with the new version. Copy the following file to another location for safekeeping:

```
[APACHE.CONF]HTTPD.CONF
```

2. If Apache is running, shut it down now.

Use the following command for **Apache T1.3-12A2 and later**:

```
$ @SYS$STARTUP:APACHE$SHUTDOWN
```

## Installation and Configuration

### 2.2 Remove Older Versions of the Software (upgrade customers only)

Use the following command for **Apache T1.3-12A1 and earlier**:

```
$ @APACHE_ROOT:APACHE_DAEMON SHUTDOWN
```

3. Enter the following command:

```
$ PRODUCT REMOVE APACHE
```

4. If you have APACHE\_JSERV installed, enter the following command to remove it:

```
$ PRODUCT REMOVE APACHE_JSERV
```

5. If you have APACHE\_PERL installed, enter the following command to remove it:

```
$ PRODUCT REMOVE APACHE_PERL
```

You are now ready to install the newest version of the server. You can restore your preserved files after you have tested the installation.

### 2.3 Install the Server and Optional Modules

The following kits are provided with this release:

- Compaq Secure Web Server for OpenVMS (CSWS)
- CSWS\_JSERV
- CSWS\_PERL

CSWS\_JSERV and CSWS\_PERL are optional modules. You can install the Compaq Secure Web Server by itself or you can install it with one or both of the optional modules. You can install the optional modules later, if you choose.

Before you begin, do the following:

1. Decide what you want to install.
2. Review the software requirements in Section 1.2 for the server and each optional module you are installing.
3. Decide where you want to install the kit. Please note:
  - The Compaq Secure Web Server, CSWS\_JSERV, and CSWS\_PERL are all installed in the same directory (required).
  - By default, they are installed in SYS\$COMMON but you should specify another location.

Follow these instructions to install the Compaq Secure Web Server by itself or with one or both of the optional modules:

1. The Compaq Secure Web Server for OpenVMS kit is provided as a compressed, self-extracting file. To download it from the Internet, fill out and submit the registration form at:

```
http://www.openvms.compaq.com/openvms/products/ips/apache/csws.html
```

At this time you should also download any optional modules you want to install.

CSWS\_JSERV for the Compaq Secure Web Server for OpenVMS Alpha is located at:

```
http://www.openvms.compaq.com/openvms/products/ips/apache/csws\_modjserv\_relnotes.html#down
```

## Installation and Configuration

### 2.3 Install the Server and Optional Modules

CSWS\_PERL for the Compaq Secure Web Server for OpenVMS Alpha is located at:

[http://www.openvms.compaq.com/openvms/products/ips/apache/csws\\_modperl\\_relnotes.html#down](http://www.openvms.compaq.com/openvms/products/ips/apache/csws_modperl_relnotes.html#down)

2. Make sure you are logged in as a privileged OpenVMS user (for example, SYSTEM).
3. You need to select UIC group and member numbers for the APACHE\$WWW account that will be created by the installation procedure. Compaq recommends that you use an empty or new UIC group (without current members). Servers typically use the highest unused UIC group (for example, [370,1]).

To ensure that the UIC you chose for APACHE\$WWW has READ and WRITE access to the intended login device, use the SHOW DEVICE/FULL command. For example:

```
$ SHOW DEVICE/FULL DKB0:

Disk $DKB0:, device type RZ56, is online, mounted, file-oriented
device, shareable, error logging is enabled.

Error count          0  Operations completed          392750
Owner process        " "  Owner UIC                      [1,4]
Owner process ID    00000000  Dev Prot          S:RWPL,O:RWPL,G:R,W
Reference count      317  Default buffer size          512
Total blocks         1299174  Sectors per track          54
Total cylinders      1604  Tracks per cylinder         15

Volume label "SYSTEM_DISK"  Relative volume number          0
Cluster size      3  Transaction count          278
Free blocks        367632  Maximum files allowed        162396
Extend quantity    5  Mount count                  1
```

4. Decompress the server kit with the following command:

```
$ RUN CPQ-AXPVMS-CSWS-V0100-1-1.PCSI-DCX-AXPEXE
```

The system displays information about the file compression version and help information about the command syntax. When you see the following prompt:

```
Decompress into (file specification):
```

press ENTER.

The system expands the file and names it. Do not rename this file.

- a. To decompress CSWS\_JSERV, enter the following command:

```
$ RUN CPQ-AXPVMS-CSWS_JSERV-V0100--1.PCSI-DCX-AXPEXE
```

At the Decompress into (file specification): prompt, press return. The system expands the file and names it. Do not rename this file.

- b. To decompress CSWS\_PERL, enter the following command:

```
$ RUN CPQ-AXPVMS-CSWS_PERL-V0100--1.PCSI-DCX-AXPEXE
```

At the Decompress into (file specification): prompt, press return. The system expands the file and names it. Do not rename this file.

5. Start the installation with the PRODUCT INSTALL command. Use the /DESTINATION qualifier to specify a target device and directory for the installation (recommended). If you don't specify a destination, the software will be installed in SYS\$COMMON. Choose the appropriate PRODUCT INSTALL command from the following list.

## Installation and Configuration

### 2.3 Install the Server and Optional Modules

---

#### Important

---

Review the software requirements for the server and each optional module you are about to install. To prevent installation problems, make sure the required software is installed **before** you enter the PRODUCT INSTALL command.

---

**To install the server, use the following command:**

```
$ PRODUCT INSTALL CSWS /DESTINATION=device:[directory-name]
```

**To install the server and CSWS\_JSERV, use the following command:**

```
$ PRODUCT INSTALL CSWS, CSWS_JSERV /DESTINATION=device:[directory-name]
```

**To install the server and CSWS\_PERL, use the following command:**

```
$ PRODUCT INSTALL CSWS, CSWS_PERL /DESTINATION=device:[directory-name]
```

**To install the server, CSWS\_JSERV, and CSWS\_PERL, use the following command:**

```
$ PRODUCT INSTALL CSWS, CSWS_JSERV, CSWS_PERL /DESTINATION=device:[directory-name]
```

The installation proceeds and displays product information as well as post-installation instructions. The installation is finished when you see the DCL prompt (\$).

After the installation you must configure the Compaq Secure Web Server. Do not attempt to start the server or configure any optional modules before you have configured the server.

## 2.4 Configure the Server

After you have installed the Compaq Secure Web Server, you are ready to configure it.

The installation wrote values, such as the name of the directory where the Compaq Secure Web Server is installed, to the file:

```
SYS$COMMON:[SYSMGR]APACHE$CONFIG_DEFAULT.DAT
```

The information stored in this file provides the default values you see during configuration. Do not try to modify the contents of this file.

The configuration procedure gives you the opportunity to separate the server components -server application, server system files, and server content files - and store them wherever it is most appropriate in your environment. By default they are all configured in SYS\$COMMON or the destination you specified on the PRODUCT INSTALL command line. During configuration you are asked if you would like to specify different locations.

If you have an OpenVMS Cluster, read Section 3.12 before you continue with the configuration.

To configure the server, enter the following command:

```
$ @SYS$MANAGER:APACHE$CONFIG
```

The configuration utility, APACHE\$CONFIG.COM, asks you to provide the following information:

- If this is the first time you are installing the server, you are asked to provide user account information for APACHE\$WWW. Use the UIC you chose during the installation procedure.
- The device and directory for the Compaq Secure Web Server (the server application files).
- The device and root directory for the server system files.
- The device and root directory where HTML documents and images (content files) will be stored. The ownership of these files will be set to the APACHE\$WWW UIC.
- Whether or not you want to enable MOD\_SSL.
- Whether or not you want to specify command line arguments when the server is started. For more information, see the *Compaq Secure Web Server SSL User Guide* at

[http://www.openvms.compaq.com/openvms/products/ips/apache/setup\\_ssl.html#configoptions](http://www.openvms.compaq.com/openvms/products/ips/apache/setup_ssl.html#configoptions)

The values you enter are written to:

SYS\$MANAGER:APACHE\$CONFIG.DAT

You need a valid server certificate to run the Compaq Secure Web Server in SSL mode. Configuration creates a self-signed certificate and installs it. If you want to view the certificate before starting the server, use the OpenSSL Certificate Tool as described in the *Compaq Secure Web Server SSL User Guide* at:

[http://www.openvms.compaq.com/openvms/products/ips/apache/using\\_the\\_ui.html#Startthetool](http://www.openvms.compaq.com/openvms/products/ips/apache/using_the_ui.html#Startthetool)

**After configuring the Compaq Secure Web Server, do not start the server.** Follow the instructions in the Section 2.5.

## 2.5 Post Configuration Checklist

After you configure the Compaq Secure Web Server, perform the following tasks to ensure a successful startup:

1. Configure MOD\_JSERV, if you've just installed it. You can configure MOD\_PERL now or later.
2. Run AUTOGEN.
3. Check disk quota.
4. Check for SET TERMINAL/INQUIRE.

Each of these tasks is explained below. Once you have completed them, you can test the installation by starting the Compaq Secure Web Server.

### 2.5.1 Configure MOD\_JSERV

If you installed the MOD\_JSERV module, you must configure it before you can start the server. For instructions, see *MOD\_JSERV for the Compaq Secure Web Server for OpenVMS Alpha Installation Guide and Release Notes* at

[http://www.openvms.compaq.com/openvms/products/ips/apache/csws\\_modjserv\\_relnotes.html](http://www.openvms.compaq.com/openvms/products/ips/apache/csws_modjserv_relnotes.html)

## Installation and Configuration

### 2.5 Post Configuration Checklist

#### 2.5.2 Configure MOD\_PERL

You are not required to configure MOD\_PERL before starting the server. MOD\_PERL is preconfigured with default values that let you execute PERL scripts. If you want to change the default configuration, you should do so now, before you start the server. To change the default configuration, edit APACHE\$ROOT:[CONF]MOD\_PERL.CONF. For more information, see

*MOD\_PERL for Compaq Secure Web Server for OpenVMS Alpha Installation Guide and Release Notes* at

[http://www.openvms.compaq.com/openvms/products/ips/apache/cswws\\_modperl\\_relnotes.html](http://www.openvms.compaq.com/openvms/products/ips/apache/cswws_modperl_relnotes.html)

#### 2.5.3 Run AUTOGEN

After the installation, run SYSSUPDATE:AUTOGEN.COM (AUTOGEN) to evaluate your system parameters and make adjustments based on your hardware configuration and system workload. On the Compaq Secure Web Server for OpenVMS, AUTOGEN will probably increase the page file size and the number of swap file pages.

#### 2.5.4 Check Disk Quota

If the disk quota is too low, the Compaq Secure Web Server will not start. Either raise the disk quota for the user account APACHE\$WWW, or grant the account the EXQUOTA privilege, thus allowing it to bypass disk quota restrictions. Use the following commands:

```
$ SHOW QUOTA/USER=[server-uic]/DISK=device-name
$ SET PROCESS/PRIVILEGES=EXQUOTA node-name::APACHE$WWW
```

#### 2.5.5 Check for SET TERMINAL/INQUIRE

When the Compaq Secure Web Server for OpenVMS is started, the following login files are executed:

- SYLOGIN.COM (system login file)
- LOGIN.COM (login file for APACHE\$WWW)

Check these files to make sure that any SET TERMINAL/INQUIRE statements are executed only in INTERACTIVE mode. For example:

```
$ IF F$MODE() .eqs "INTERACTIVE" then $ SET TERMINAL/INQUIRE
```

Failure to do so might result in ill-formed HTML intermittently being returned to clients. This problem might also appear when executing CGI scripts.

## 2.6 Test the Installation

Now you will manually start the Compaq Secure Web Server to verify the installation and configuration of the server. Enter the following command:

```
$ @SYSS$STARTUP:APACHE$STARTUP
```

### 2.6.1 Browser Test

You can test the installation using your web browser. Replace *host.domain* in the following URL with the information for the Compaq Secure Web Server you just installed:

```
HTTP://host.domain/
```

If this is a new installation, the browser should display the standard introductory page with the following bold text at the top:

```
"If you see this, it means that the installation of the Apache web server software on this system was successful."
```

The Apache logo is displayed at the bottom.

### 2.6.2 TELNET Test

You can also use TELNET on the local host to test the installation. Note: If you are running Compaq TCP/IP Services Version 5.1 for OpenVMS, user input is not echoed. However, the resulting output is the same for Version 5.0A and 5.1.

Use the following procedure to test the installation:

1. Enter the following command:

```
$ TELNET 0 80
```

The following text is displayed:

```
%TELNET-I-TRYING, Trying ... 127.0.0.1
%TELNET-I-SESSION, Session 01, host localhost, port 80
-TELNET-I-ESCAPE, Escape character is ^]
```

2. Press ENTER and enter the following HTTP command:

```
HEAD / HTTP/1.0
```

3. Press ENTER **twice**.

Text similar to the following is displayed:

```
HTTP/1.1 200 OK
Date: Tue, 23 May 2000 17:05:05 GMT
Server: Apache/1.3.12 (OpenVMS)
Last-Modified: Mon, 22 May 2000 15:33:27 GMT
ETag: "33dfec-681-39295347"
Accept-Ranges: bytes
Content-Length: 1665
Connection: close
Content-Type: text/html

%TELNET-S-REMCLOSED, Remote connection closed
-TELNET-I-SESSION, Session 01, host localhost, port 80
```

You should receive several lines of text from the Compaq Secure Web Server.

### 2.6.3 Troubleshooting

If you do not receive a response from the Compaq Secure Web Server, check the following:

- Look in your SYLOGIN.COM file and make sure there is no SET TERMINAL/INQUIRE statement for NETWORK processes.
- Make sure the APACHESWWW account exists and is not disabled.

## Installation and Configuration

### 2.6 Test the Installation

- Look for the following files:
  - APACHE\$ROOT:[000000]APACHE\$SERVER.LOG
  - APACHE\$ROOT:[LOGS]ERROR\_LOG

### 2.7 What's Next

After you have successfully tested the installation, perform any of the following tasks that are relevant for you:

- If you were upgrading, you can restore your preserved files now and merge the previous version of HTTPD.CONF with the new version of HTTPD.CONF. See Section 2.8.
- If you enabled MOD\_SSL, follow the instructions for verifying SSL in the *Compaq Secure Web Server SSL User Guide* at [http://www.openvms.compaq.com/openvms/products/ips/apache/setup\\_ssl.html#startserver](http://www.openvms.compaq.com/openvms/products/ips/apache/setup_ssl.html#startserver)
- Read Chapter 3 for information on starting and stopping the server, using HTTPD.CONF to customize the server environment, and other OpenVMS specific topics.

### 2.8 Merge HTTPD.CONF (upgrade customers only)

With this version of the Compaq Secure Web Server kit, the following changes were made to HTTPD.CONF:

- References to APACHE\_ROOT were changed to either APACHE\$ROOT or APACHE\$COMMON. APACHE\$COMMON is used in instances where you want to refer to a clusterwide specification. For example: APACHE\$COMMON:[HTDOCS].
- The User directive refers to APACHE\$WWW instead of Apache.
- The following line has been added:

```
Include /apache$root/conf/mod_ssl.conf
```

You can merge your previous version of HTTPD.CONF with the latest version in one of the following ways:

- Transfer your edits in the previous version of HTTPD.CONF to the new version.
- Update your previous version of HTTPD.CONF with the changes listed above.

Choose the method that best fits your situation.

### 2.9 Installing Optional Modules at a Later Time

If you didn't install the optional modules (MOD\_JSERV or MOD\_PERL) when you installed the server, follow these instructions for installing them at a later time. Before you begin, make sure:

- You have installed the required software.
- You have already installed the Compaq Secure Web Server.
- You install CSWS\_JSERV and CSWS\_PERL in the same directory as you installed the server.

Use the appropriate command from the list below.

## Installation and Configuration

### 2.9 Installing Optional Modules at a Later Time

**To install CSWS\_JSERV, use the following command:**

```
$ PRODUCT INSTALL CSWS_JSERV /DESTINATION=device:[directory-name]
```

**To install CSWS\_PERL, use the following command:**

```
$ PRODUCT INSTALL CSWS_PERL /DESTINATION=device:[directory-name]
```

**To choose from a list of products, use the following command:**

```
$ PRODUCT INSTALL * /DESTINATION= device:[directory-name]
```

The installation procedure displays a list of all PCSI kits in the current directory.

For example:

```
1 - CPQ AXPVMS CSWS V1.0-1           Layered Product
2 - CPQ AXPVMS CSWS_JSERV V1.0       Layered Product
3 - CPQ AXPVMS CSWS_PERL V1.0        Layered Product
4 - All products listed above
5 - Exit
```

Choose one or more items from the menu separated by commas:

Enter the appropriate number(s). If you enter more than one number, use a comma as a separator. The installation procedure asks you to confirm your choices, then displays installation and configuration information for the products you have selected.

The installation is complete when the dollar sign prompt (\$) is displayed.

After you install MOD\_JSERV, you must configure it. For more information, see Section 2.5.1. MOD\_PERL is preconfigured, but you can change the configuration. For more information, see Section 2.5.2.

---

## Running the Compaq Secure Web Server on OpenVMS

In general, you can run the Compaq Secure Web Server on OpenVMS as you would run Apache with MOD\_SSL on any platform. However, there are some exceptions. This chapter describes the functions that behave differently or are not available, as well as any enhancements that are specific to OpenVMS.

### 3.1 Starting and Stopping the Server

Starting and stopping the Compaq Secure Web Server requires enhanced privileges (DETACH, SYSNAM, WORLD, etc.). Start and stop the server from a privileged account such as SYSTEM.

Start the Compaq Secure Web Server with the following command:

```
$ @SYS$STARTUP:APACHE$STARTUP [parameter1]
```

where *parameter1* is optional and can have the following values:

Value	Description
START	Creates the Compaq Secure Web Server as a detached network process; default value
RESTART	Sends a restart signal to the server to have it reread APACHESROOT:[CONF]HTTPD.CONF
RUN	Runs the server on the current process

To automate the startup of the Compaq Secure Web Server when the system is booted, add the following commands to the SYS\$MANAGER:SYSTARTUP\_VMS.COM file:

```
$ FILE := SYS$STARTUP:APACHE$STARTUP.COM
$ IF F$SEARCH("FILE") .NES. "" THEN @'FILE'
```

You can shut down the Compaq Secure Web Server with the following command:

```
$ @SYS$STARTUP:APACHE$SHUTDOWN [parameter1]
```

where *parameter1* is optional and can have the following values:

Value	Description
SHUTDOWN	Stops the detached network process; default value
RESTART	Sends a restart signal to the server to have it reread APACHESROOT:[CONF]HTTPD.CONF

## Running the Compaq Secure Web Server on OpenVMS

### 3.1 Starting and Stopping the Server

To automate the shutdown of the Compaq Secure Web Server when the system is shut down, add the following commands to the SYSSMANAGER:SYSHUTDOWN.COM file:

```
$ FILE := SYS$STARTUP:APACHE$SHUTDOWN.COM
$ IF F$SEARCH(" 'FILE' ") .NES. "" THEN @'FILE'
```

---

#### Note

---

The Compaq Secure Web Server will not shut down as long as the APACHE\$WWW process is running. If you have a problem with shutting down the server, use the following command to see if APACHE\$WWW is running:

```
$ SHOW SYSTEM/PROC=APACHE$WWW
```

If APACHE\$WWW is still running, use the following command to stop it. You should then be able to shut down the server.

```
$ STOP PROCESS/ID=<apache-pid>
```

---

### 3.2 Server Log File

The server log file for APACHE\$WWW is written to:

```
APACHE$SPECIFIC:[000000]APACHE$SERVER.LOG
```

### 3.3 Performance Considerations

You should have prior experience tuning the performance of the OpenVMS operating system. For general information on OpenVMS performance, see the *OpenVMS Performance Management Manual* at

<http://www.openvms.digital.com:8000/72final/6491/6491pro.html>

Recommendations for improving performance on a Compaq Secure Web Server are provided below and in the See the *Compaq Secure Web Server for OpenVMS Alpha Release Notes* at

[http://www.openvms.compaq.com/openvms/products/ips/apache/cswws\\_relnotes.html](http://www.openvms.compaq.com/openvms/products/ips/apache/cswws_relnotes.html)

#### 3.3.1 Limits and Quotas

The following table shows sample values for the APACHE\$WWW system user account (SYSUAF) from a working and exercised Compaq Secure Web Server with a light to moderate load. These values are presented as an example of a system performing well within its context. If you should experience performance difficulties, refer to this table for guidelines in making adjustments. For heavier loads, we point out which values, in our experience, need to be increased as load increases. Keep in mind that no one set of values will be appropriate for all situations.

## Running the Compaq Secure Web Server on OpenVMS 3.3 Performance Considerations

**Table 3–1 Sample Values for the APACHE\$WWW SYSUAF**

Parameter	Default	On Compaq Secure Web Server
<b>ASTLM (NonPooled)</b> Total number of asynchronous system trap (AST) operations and scheduled wake-up requests the user can have queued at one time	250	610 Or BIOLM + DIOLM + 10
<b>BIOLM (NonPooled)</b> Number of outstanding buffered I/O operations permitted for a user's process	150	300 You might also need to increase the SYSGEN parameter CHANNELCNT because it limits BIOLM,DIOLM, and FILLM.
<b>BYTLM (Pooled)</b> Amount of buffer space a user's process can use	64000	200000 Increase this value for a heavy load.
<b>DIOLM (NonPooled)</b> Number of outstanding direct I/O operations permitted to a user's process	150	300 You might also need to increase the SYSGEN parameter CHANNELCNT because it limits BIOLM,DIOLM, and FILLM.
<b>ENGLM (Pooled)</b> Specifies the lock queue limit	2000	2000
<b>FILLM (Pooled)</b> Number of files a user's process can have opened at one time. Includes the number of network logical links that can be active at the same time	100	300 Increase this value for a heavy load. You might also need to increase the SYSGEN parameter CHANNELCNT because it limits BIOLM,DIOLM, and FILLM.
<b>JTQUOTA (Pooled)</b> Byte quota for the job-wide logical name table	4096	8192
<b>PGFLQUO (Pooled)</b> Number of pages the user's process can use in the system page file	50000	250000 If you increase PGFLQUO, you should monitor the free size of the system page and swap files; they may need to be increased.
<b>PRCLM (Pooled)</b> Number of subprocesses a user's process can create	8	20 You should increase this value for a heavy load.
<b>TQELM (Pooled)</b> Number of entries a user's process can have in the timer queue or the number of temporary common event flag clusters a user's process can have	10	610 Or BIOLM + DIOLM + 10

To change the quotas for the APACHE\$WWW SYSUAF, use the system manager account and run the AUTHORIZE utility. For example:

## Running the Compaq Secure Web Server on OpenVMS

### 3.3 Performance Considerations

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF> SHOW APACHE$WWW
Username: APACHE$WWW                               Owner: APACHE WEBSERVER
...
Maxjobs:      0 Fillm:      100 Byt1m:      64000
Maxacctjobs:  0 Shrfillm:   0 Pbyt1m:      0
Prclm:        8 DI01m:     150 WSdef:      2000
...
UAF> MODIFY APACHE$WWW/FILLM=300/PRCLM=20
%UAF-I-MDFYMSG, user record(s) updated
UAF> EXIT
$
```

#### 3.3.2 Server Experiencing Medium to High Usage

After you install the server and have been running it, look in the log file for errors of the "cannot open" variety. Errors of this type often indicate you need to modify system parameters. Try the following:

- Set FILLM to limit the number of files a user's process can have open.
- Set the SYSGEN parameter CHANNELCNT to 1024 (unless it is already set to a higher value).

---

#### Note

---

Whenever you change system parameters, you must reboot the system to enable the new settings.

---

#### 3.3.3 Global Pages and Global Sections

If a browser installation stalls, this could be an indication that the number of global pages or global sections is too low. Run AUTOGEN to evaluate the number of global pages and global sections you need. Some browsers might need more.

#### 3.3.4 Excessive File Build Up

A large number of .LOG and .PID files can amass over time in the directories APACHE\$ROOT:[0000000] and APACHE\$ROOT:[LOGS]. Purging these files can become a burden on application or system managers.

System managers should manually use explicit SET DIRECTORY/VERSION commands on these two directories.

### 3.4 Customizing the Server Environment

The installation procedure creates a file named HTTPD.CONF and places it in APACHE\$ROOT:[CONF]. The HTTPD.CONF file stores information that the Compaq Secure Web Server uses to set up the server environment. HTTPD.CONF has been tailored to use OpenVMS syntax, but its overall functionality is essentially identical to HTTPD.CONF on the UNIX platform.

HTTPD.CONF contains an explanation for each line that it can execute. You can refer to these explanations when customizing the file for your environment. You can also refer to any generally available Apache documentation on HTTPD.CONF.

## Running the Compaq Secure Web Server on OpenVMS

### 3.4 Customizing the Server Environment

Note the following about HTTPD.CONF on OpenVMS:

- No directives have been deleted or added to the Apache template except an Include directive for MOD\_SSL. Installing CSWS\_JSERV or CSWS\_PERL will also append Include directives specific to these modules.
- MOD\_OSUSCRIPT has been added to enable CGI scripts originally written for the OSU server.
- UNIX style path names are recognized by OpenVMS. You can use either UNIX style or OpenVMS style path names in the configuration file. However, you cannot intermix the two styles within a specification.
- In an OpenVMS Cluster, you can specify either clusterwide or system-specific files. For more information, see Section 3.12.1.

### 3.5 Modules and Directives

Following is a list of the modules included in the Compaq Secure Web Server for OpenVMS distribution kit. The list shows the directives supported in each module. All supported modules and directives function as documented by the Apache Software Foundation at

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

#### **HTTP\_CORE.C**

AccessConfig  
AccessFileName  
AllowOverride  
AuthName  
AuthType  
BindAddress  
CoreDumpDirectory  
DefaultType  
<Directory>  
<DirectoryMatch>  
DocumentRoot  
ErrorDocument  
ErrorLog  
<Files>  
<FilesMatch>  
HostnameLookups  
IdentityCheck  
<IfDefine>  
<IfModule>  
Include  
KeepAlive  
KeepAliveTimeout  
<Limit>  
<LimitExcept>  
LimitRequestBody  
LimitRequestFields  
LimitRequestLine  
Listen  
ListenBacklog

## Running the Compaq Secure Web Server on OpenVMS

### 3.5 Modules and Directives

<Location>  
<LocationMatch>  
LogLevel  
MaxClients  
MaxKeepAliveRequests  
MaxRequestPerChild  
MaxSpareServers  
MinSpareServers  
NameVirtualHost  
Options  
PidFile  
Port  
Require  
ResourceConfig  
Satisfy  
SendBufferSize  
ServerAdmin  
ServerAlias  
ServerName  
ServerPath  
ServerRoot  
ServerSignature  
ServerTokens  
ServerType  
StartServers  
TimeOut  
UseCanonicalName  
User  
VirtualHost

#### **MOD\_ACCESS.C**

allow  
deny  
order

#### **MOD\_ACTIONS.C**

Action  
Script

#### **MOD\_ALIAS.C**

Alias  
AliasMatch  
Redirect  
RedirectMatch  
RedirectTemp  
RedirectPermanent  
ScriptAlias  
ScriptAliasMatch

#### **MOD\_ASIS.C**

## Running the Compaq Secure Web Server on OpenVMS 3.5 Modules and Directives

### **MOD\_AUTH.C**

AuthGroupFile  
AuthUserFile

### **MOD\_AUTOINDEX.C**

AddAlt  
AddAltByEncoding  
AddAltyByType  
AddDescription  
AddIcon  
AddIconByEncoding  
AddIconByType  
DefaultIcon  
FancyIndexing  
HeaderName  
IndexIgnore  
IndexOptions  
IndexOrderDefault  
ReadmeName

### **MOD\_CGI.C**

ScriptLog  
ScriptLogBuffer  
ScriptLogLength

### **MOD\_DIR.C**

DirectoryIndex

### **MOD\_ENV.C**

SetEnv  
UnsetEnv

### **MOD\_IMAP.C**

ImapBase  
ImapDefault  
ImapMenu

### **MOD\_INCLUDE.C**

### **MOD\_INFO.C**

AddModuleInfo

### **MOD\_LOG\_CONFIG.C**

CustomLog  
LogFormat  
TransferLog

## Running the Compaq Secure Web Server on OpenVMS

### 3.5 Modules and Directives

#### **MOD\_MIME.C**

- AddCharset
- AddEncoding
- AddHandler
- AddLanguage
- AddType
- DefaultLanguage
- ForceType
- RemoveHandler
- SetHandler
- TypesConfig

#### **MOD\_NEGOTIATION.C**

- CacheNegotiatedDocs
- LanguagePriority

#### **MOD\_OSUSCRIPT.C** (OpenVMS specific)

#### **MOD\_SETENVIF.C**

- BrowserMatch
- BrowserMatchNoCase
- SetEnvIf
- SetEnvIfNoCase

#### **MOD\_SO.C**

- LoadModule

#### **MOD\_STATUS.C**

- ExtendedStatus

#### **MOD\_UNIQUE\_ID.C**

#### **MOD\_USERDIR.C**

- UserDir

## 3.6 Supported and Unsupported Features

The server documentation from the Apache Software Foundation at

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

provides most of the information needed to run your Compaq Secure Web Server for OpenVMS. Information specific to the OpenVMS operating system is provided below.

## Running the Compaq Secure Web Server on OpenVMS

### 3.6 Supported and Unsupported Features

#### 3.6.1 Modules Not Included

The following modules are **not** included in this version of the Compaq Secure Web Server for OpenVMS kit:

- MOD\_AUTH\_ANON
- MOD\_AUTH\_DB
- MOD\_AUTH\_DBM
- MOD\_AUTH\_DIGEST
- MOD\_CERN\_META
- MOD\_DIGEST
- MOD\_EXAMPLE
- MOD\_EXPIRES
- MOD\_HEADERS
- MOD\_ISAPI
- MOD\_LOG\_AGENT
- MOD\_LOG\_REFERERER
- MOD\_MIME\_MAGIC
- MOD\_MMAP\_STATIC
- MOD\_PROXY
- MOD\_REWRITE
- MOD\_SPELING
- MOD\_USERTRACK
- MOD\_VHOST\_ALIAS

#### 3.6.2 Unsupported Directives

The following directives are **not** supported:

- AgentLog
- AllowCONNECT
- Anonymous
- Anonymous\_Authoritative
- Anonymous\_LogEmail
- Anonymous\_MustGiveEmail
- Anonymous\_NoUserID
- Anonymous\_VerifyEmail
- AuthDBAuthoritative
- AuthDBGroupFile
- AuthDBMAuthoritative
- AuthDBMGroupFile
- AuthDBUserFile
- AuthDBMUserFile
- AuthDigestFile
- CacheDefaultExpire
- CacheDirLength
- CachedirLevels
- CacheForceCompletion
- CacheGcInterval
- CacheLastModifiedFactor
- CacheMaxExpire
- CacheRoot
- CacheSize
- CheckSpelling
- CookieExpires
- CookieTracking
- Example

## Running the Compaq Secure Web Server on OpenVMS

### 3.6 Supported and Unsupported Features

ExpiresActive  
ExpiresByType  
ExpiresDefault  
Header  
Metadir  
MetaFiles  
MetaSuffix  
MimeMagicFile  
MMapFile  
NoCache  
ProxyBlock  
ProxyDomain  
ProxyPass  
ProxyPassReverse  
ProxyReceiveBufferSize  
ProxyRemote  
ProxyRequests  
ProxyVia  
RefererIgnore  
RefererLog  
RewriteBase  
RewriteCond  
RewriteEngine  
RewriteLock  
RewriteLog  
RewriteLogLevel  
RewriteMap  
RewriteOptions  
RewriteRule  
RLimitCPU  
RLimitMEM  
RLimitNPROC  
ScriptInterpreterSource  
VirtualDocumentRoot  
VirtualDocumentRootIP  
VirtualScriptAlias  
VirtualScriptAliasIP

#### 3.6.3 Command Line Options

This section describes the HTTPD command line options supported on the Compaq Secure Web Server. Before you can use them you must first define HTTPD as a symbol, as follows:<sup>1</sup>

```
$ HTTPD ::= $APACHE$ROOT:[000000]APACHE_HTTPD.EXE_ALPHA
```

Then you can use the following format to enter a command line option:

```
$ HTTPD -option
```

---

<sup>1</sup> If needed, you can define HTTPD in SYSS\$MANAGER:LOGIN.COM.

## Running the Compaq Secure Web Server on OpenVMS

### 3.6 Supported and Unsupported Features

where *-option* is one of the following:

**Table 3–2 HTTPD Command Line Options**

Option	Description
<b>-v</b>	Displays the HTTPD version and its build date.
<b>-"V"</b>	Displays the HTTPD base version, its build date, and a list of compile settings that influence the behavior and performance of the server.
<b>-h</b>	Displays a list of the HTTPD options.
<b>-l</b>	Displays a list of all modules compiled into the server.
<b>-"L"</b>	Displays a list of directives with expected arguments and places where the directive is valid.

The following example shows how to enter the L option to list the available configuration directives:

```
$ HTTPD -"L"
```

#### 3.6.4 Virtual Host Support

The term *virtual host* refers to the practice of maintaining a single server to serve pages for multiple virtual hosts. Both IP-based and name-based virtual host support are available on the Compaq Secure Web Server for OpenVMS.

---

**Note**

---

On OpenVMS, the security profile of the running server is the same on all virtual hosts.

---

For more information, see the Apache Software Foundation documentation at

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

#### 3.6.5 Dynamic Shared Object Support

Dynamic shared object support provides a way to format code so that it will load into the address space of an executable program at run time. This functionality is supported on OpenVMS. For more information, see the Apache Software Foundation documentation at

<http://www.apache.org/docs/dso.html>

#### 3.6.6 File Handlers

The Compaq Secure Web Server for OpenVMS supports the ability to use file handlers explicitly. For more information, see the Apache Software Foundation documentation at

<http://www.apache.org/docs/handler.html>

## Running the Compaq Secure Web Server on OpenVMS

### 3.6 Supported and Unsupported Features

#### 3.6.7 Content Negotiation

The MOD\_NEGOTIATION module provides content negotiation. This module lets you specify language variants of HTML files. To specify language variants on OpenVMS, use an underscore instead of a period before the language extension.

For example:

- On UNIX, *filename.html.fr* is the French variant of *filename.html*.
- On OpenVMS, *filename.html\_fr* is the French variant of *filename.html*.

For more information, see the Apache Software Foundation documentation at

<http://www.apache.org/docs/content-negotiation.html>

#### 3.6.8 Apache API

You can use the standard Apache API to write your own modules that will run on the Compaq Secure Web Server for OpenVMS. For more information, see the Apache Software Foundation documentation at

<http://www.apache.org/docs/misc/API.html>

#### 3.6.9 suEXEC Support

The suEXEC feature provides the ability to run CGI programs under user IDs different from the user ID of the calling web server; this is **not** supported by the Compaq Secure Web Server for OpenVMS.

#### 3.6.10 Running MOD\_OSUSCRIPT

The Compaq Secure Web Server for OpenVMS Alpha provides a CGI script environment. However, it also includes MOD\_OSUSCRIPT, an optional module that enables the server to run scripts that were written for the OSU http server's script environment (which is not CGI).

MOD\_OSUSCRIPT does not need to communicate with a running OSU server to work properly. It needs only the following OSU http distribution files:

- WWWEXEC.COM
- INVCACHE.COM

You can download and install these files to run and test OSU scripts, as follows:

1. Create a directory for the OSU script files with the following command. The APACHE\$WWW username must be able to read this directory and its files.

```
$ CREATE/DIRECTORY device:[directory.BIN]
```

2. Create a logical name pointing to the OSU script root directory, as follows:

```
$ DEFINE/SYSTEM WWW_ROOT:[ directory.]/TRANS=CONCEAL
```

3. Copy INVCACHE.COM and WWWEXEC.COM from

```
http://www.er6.eng.ohio-state.edu/tarserv/http\_server\_3-8.tar/
```

to the following locations:

```
WWW_ROOT:[BIN]INVCACHE.COM
```

```
APACHE$ROOT:[000000]WWWEXEC.COM
```

4. Use the SHOW SECURITY command to ensure that APACHE\$WWW can read these files. If needed, use the SET SECURITY command to change the security settings.

## Running the Compaq Secure Web Server on OpenVMS 3.6 Supported and Unsupported Features

5. Edit HTTPD.CONF to add the following lines:

```
<Location /htbin>
    SetHandler osuscript-handler
    OSUscrip 0::"0=WWWEXEC" www_root:[bin]
    Order allow,deny
    Allow from all
</Location>
```

6. Enter the following commands to add the DECnet proxy. Replace *node* with your DECnet Phase IV node name.

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF> ADD/PROXY node::APACHE$WWW APACHE$WWW/DEFAULT
UAF> EXIT
```

If you are running DECnet-Plus, replace *namespace:.abc.xyz* with your system's full name, for example, DEC:.ZKO.NODE22::APACHE\$WWW.

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF> ADD/PROXY namespace:.abc.xyz::APACHE$WWW APACHE$WWW/DEFAULT
UAF> EXIT
```

7. To test, execute the simple OSU script INVCACHE.COM. To do this, replace *myhostname* in the following URL with your server's domain name:

```
HTTP://myhostname/INVCACHE.COM
```

MOD\_OSUSCRIPT does the following:

1. Opens a DECnet connection using task 0 for the APACHE\$WWW username entered in the proxy command.
2. Executes WWWEXEC.COM using the default HTTPD.CONF directives.
3. Searches the WWW\_ROOT:[BIN] directory for the script name entered in the URL.

MOD\_OSUSCRIPT supports all of the script server protocol commands, except the following:

- <DNETREUSE> Reuse logical link for subsequent scripts.
- <DNETINVCACHE> Invalidate internal cache (the Compaq Secure Web Server does not have a cache).
- <DNETMANAGE> Send management command, OSU server specific.
- <DNETFORCEKA> Put client link in keep-alive mode.

### 3.7 File Formats

All file formats are supported. However, the Web browser status bar will not show page loading progress for Variable or VFC format files larger than 8K.

Page loading progress relies on an accurate byte count. Accurate byte count is not readily available for files in Variable or VFC format. For files in these formats, the Compaq Secure Web Server must count the bytes as the files load. The counting process can slow performance so it has been turned off in this situation.

## Running the Compaq Secure Web Server on OpenVMS

### 3.8 File Naming Conventions

### 3.8 File Naming Conventions

In general, users running the Compaq Secure Web Server for OpenVMS can specify either UNIX style file names or OpenVMS style file names. The Compaq Secure Web Server usually displays UNIX style file names.

The ODS-5 volume structure, introduced in OpenVMS Alpha Version 7.2, supports long file names, allows the use of a wider range of characters within file names, and preserves case within file names. However, the DEC C RTL shipped with OpenVMS Alpha Version 7.2 does not provide full support for extended file names on ODS-5 devices. This lack of full support imposes certain restrictions on users running the Compaq Secure Web Server for OpenVMS Alpha.

Because mixed UNIX and OpenVMS style extended file names are not yet supported by the DEC C RTL, you might be required to use UNIX style syntax when interacting with the Compaq Secure Web Server. An example would be appending additional directories or a file name to a root.

The following examples illustrate mixed UNIX and OpenVMS style file names that are not supported in OpenVMS Alpha Version 7.2:

```
doc/foo.bar.bar
./tmp/foo.bar.b^_ar
~foo^.bar
```

You can, however, modify the last example so that it will work as an OpenVMS extended file name that has a tilde (~) as the first character. Precede the leading tilde (~) with the Extended File Specifications escape character (^). For example:

```
^~foo^.bar
```

For more information about using the tilde (~) in OpenVMS extended file names, see the *OpenVMS Guide to Extended File Specifications* at

<http://caedmon.zko.dec.com/72final/6536/6536pro.html>

Mixed UNIX and OpenVMS style file names will be supported in a future release of the DEC C RTL for OpenVMS Alpha.

### 3.9 File Transfer Process and Access Control List

When performing a File Transfer Process (FTP) operation, make sure the Access Control List (ACL) for the target directory on the Compaq Secure Web Server allows FTP access, as follows:

When transferring new files:

```
$ SET SECURITY/ACL=(IDENTIFIER=yourFTPname,ACCESS=READ+WRITE) [directory]
```

When replacing existing files:

```
$ SET SECURITY/ACL=(IDENTIFIER=yourFTPname,ACCESS=READ+WRITE)
[directory]*.*
```

## 3.10 Logical Names

The Compaq Secure Web Server for OpenVMS creates the following logical names.

**Table 3–3 System Defined Logical Names**

Logical Name	Description
APACHE\$COMMON	Concealed logical name that defines clusterwide files in APACHE\$ROOT (device:[APACHE])
APACHE\$FIXBG	System executive mode logical name pointing to installed, shareable images. Not intended to be modified by the user.
APACHE\$HTTDPD_SHR	System executive mode logical name pointing to installed, shareable images. Not intended to be modified by the user.
APACHE\$INPUT	Used by CGI programs for PUT/POST methods of reading the input stream.
APACHE\$PLV_ENABLE_<username>	System executive mode logical name defined during startup and used to control access to the services provided by the APACHE\$PRIVILEGED image. Not intended to be modified by the user.
APACHE\$PLV_LOGICAL	System executive mode logical name defined during startup and used to control access to the services provided by the APACHE\$PRIVILEGED image. Not intended to be modified by the user.
APACHE\$PRIVILEGED	System executive mode logical name pointing to installed, shareable images. Not intended to be modified by the user.
APACHE\$ROOT	System executive mode logical name defined during startup that points to the top-level directory. (device:[APACHE], device:[APACHE.SPECIFIC.node-name])
APACHE\$SPECIFIC	Concealed logical name that defines system-specific files in APACHE\$ROOT (device:[APACHE.SPECIFIC.node-name])

**Table 3–4 User Defined Logical Names**

Logical Name	Description
APACHE\$CGI_MODE	System logical name that controls how CGI environment variables are defined in the executing CGI process. There are three different options. Note that only one option is available at a time.
	0            Default. Environment variables are defined as local symbols and are truncated at 970 (limitable with DEC C).
	1            Environment variables are defined as local symbols unless they are greater than 970 characters. If the environment value is greater than 970 characters, it is defined as a multi-item logical.
	2            Environment variables are defined as logicals. If the environment value is greater than 512 characters, it is defined as a multi-item logical.

(continued on next page)

## Running the Compaq Secure Web Server on OpenVMS

### 3.10 Logical Names

Table 3–4 (Cont.) User Defined Logical Names

Logical Name	Description
APACHE\$DEBUG_DCL_CGI	If defined, this system logical name enables APACHE\$VERIFY_DCL_CGI and APACHE\$SHOW_CGI_SYMBOL.
APACHE\$VERIFY_DCL_CGI	If defined, this system logical name provides information for troubleshooting DCL command procedure CGIs by forcing a SET VERIFY before executing any DCL CGI. Use with APACHE\$DEBUG_DCL_CGI.
APACHE\$SHOW_CGI_SYMBOL	If defined, this system logical name provides information for troubleshooting the CGI environment by dumping all of the symbols and logicals (job/process) for a given CGI. Use with APACHE\$DEBUG_DCL_CGI.
APACHE\$PREFIX_DCL_CGI_SYMBOLS_WWW	If defined, this system logical name prefixes all CGI environment variable symbols with "WWW_". By default no prefix is used.
APACHE\$CREATE_SYMBOLS_GLOBAL	If defined, this system logical name causes CGI environment symbols to be defined globally. They are defined locally by default.
APACHE\$CGI_USE_DCLCOM_FOR_IMAGES	If defined, this system logical name forces CGI images to execute within a DCL process. The default is to execute CGI images directly. (Note: Direct execution of CGI images is not currently supported.)
APACHE\$DL_NO_UPPERCASE_FALLBACK	If defined to be true (1, T, or Y), this system logical name disables case-insensitive symbol name lookups whenever case-sensitive lookups fail. See APACHE\$DL_FORCE_UPPERCASE.
APACHE\$DL_FORCE_UPPERCASE	If defined to be true (1, T, or Y), this system logical name forces case-sensitive dynamic image activation symbol lookups. By default, symbol lookups are first done in a case-sensitive manner and then, if failed, a second attempt is made using case-insensitive symbol lookups. This fallback behavior can be disabled with APACHE\$DL_NO_UPPERCASE_FALLBACK.

### 3.11 Redefining Logical Names

You cannot manually redefine these logical names defined during configuration:

- APACHE\$ROOT
- APACHE\$SPECIFIC
- APACHE\$COMMON

If you need to change the definition of these logical names, rerun the configuration with the following command:

```
$ @SYS$MANAGER:APACHE$CONFIG
```

## 3.12 OpenVMS Cluster Considerations

An OpenVMS Cluster is a group of OpenVMS systems that work together as one virtual system. The Compaq Secure Web Server runs in an OpenVMS Cluster so you can take advantage of the resource sharing that increases the availability of services and data. Keep the following points in mind:

- The Compaq Secure Web Server is supported on OpenVMS Alpha Version 7.1-2 or higher.
- The Compaq Secure Web Server runs in an Alpha or a mixed-architecture cluster.

The configuration procedure lets you specify where you want to store the server software, the server system files (configuration, startup, and shutdown files), and your HTML files (content). By default, everything will go in SYSSCOMMON or the device and directory you specified with the PRODUCT INSTALL command.

Where you put each server component depends on your OpenVMS cluster environment and how much you want to integrate or segregate the Compaq Secure Web Server and its activities. You can install the server once on a disk that is visible to multiple systems in the cluster. You have the option of:

- Using one configuration for all systems, or
- Configuring individual systems, provided they all share a common system disk

In the latter case, a common system disk is needed so that all the systems have access to the server system files on the system disk. If a system has access to a clusterwide directory where the Compaq Secure Web Server is installed, but does not share a system disk with the other systems, you might need an additional installation.

If you have more than one installation, you must make sure that the APACHE\$WWW account has the same UIC across the entire cluster. The installation procedure automatically assigns the APACHE\$WWW UIC to all the files under [APACHE], regardless of their actual physical locations. One UIC definition for APACHE\$WWW for all installations ensures that all files are visible at all times.

### 3.12.1 Individual System vs. Clusterwide Definition

To define clusterwide vs. individual configuration files, APACHE\$ROOT uses the following concealed logical names:

- APACHE\$COMMON defines clusterwide files.
- APACHE\$SPECIFIC defines system-specific files.

When reading a file, the server first looks for a system-specific version of the file in APACHE\$SPECIFIC:[directory]. If it doesn't find one, it looks for a clusterwide file in APACHE\$COMMON:[directory].

To avoid confusion, always use the appropriate concealed logical name to specify the file you want to edit. For example, to edit a clusterwide version of HTTPD.CONF, refer to:

```
$ EDIT APACHE$COMMON:[CONF]HTTPD.CONF
```

## Running the Compaq Secure Web Server on OpenVMS

### 3.12 OpenVMS Cluster Considerations

If you referred to:

```
$ EDIT APACHE$ROOT:[CONF]HTTPD.CONF
```

the server would open the clusterwide file but save it as a system-specific version. The latest version of HTTPD.CONF would then be visible only to the individual node it was saved on.

Within HTTPD.CONF itself, you should make this distinction whenever you refer to a path or file location. This improves performance and ensures the server will return a complete directory listing. For example, you should specify APACHE\$COMMON or APACHE\$SPECIFIC (instead of APACHE\$ROOT) with Directory directives.

The following extract, from the HTTPD.CONF file distributed with the OpenVMS kit, refers to APACHE\$COMMON because the content for the default web page is in the clusterwide directories.

```
DocumentRoot "/apache$common/htdocs"

. . .

<Directory "/apache$common/htdocs">
  Options Indexes FollowSymLinks Multiviews
  AllowOverride None
  Order allow,deny
  Allow from all
</Directory>
```

If there were content for one specific node in a cluster, the APACHE\$SPECIFIC logical name would be used.

#### 3.12.2 Mixed-Architecture Cluster

In a mixed-architecture cluster, do not use a cluster alias IP address with the Compaq Secure Web Server. Because the VAX systems will not have the Compaq Secure Web Server running, they won't be able to service HTTP requests.

## 3.13 Common Gateway Interface (CGI)

Common Gateway Interface (CGI) programs execute within the DCL shell on the Compaq Secure Web Server for OpenVMS. Please note the following OpenVMS specific information.

#### 3.13.1 CGI Environment Variables

By default, an environment variable symbol takes the form designated by the name of the environment variable. You can determine how environment variables are set when the server executes a CGI program.

You can define the APACHE\$PREFIX\_DCL\_CGI\_SYMOBLS\_WWW logical name to prefix all environment variable symbols with "WWW\_". By default, no prefix is used.

The APACHE\$CGI\_MODE logical name controls how CGI environment variables are defined in the executing CGI program, as follows:

```
APACHE$CGI_MODE option
```

# Running the Compaq Secure Web Server on OpenVMS

## 3.13 Common Gateway Interface (CGI)

where *option* can have **one** of the following values at a time:

- 0 Default. Environment variables are defined as local symbols and are truncated at 970 (limitable with DEC C).
- 1 Environment variables are defined as local symbols unless they are greater than 970 characters. If the environment value is greater than 970 characters, it is defined as a multi-item logical.
- 2 Environment variables are defined as logicals. If the environment value is greater than 512 characters, it is defined as a multi-item logical.

APACHE\$DCL\_ENV is a foreign symbol that lets you define CGI environment variables, as follows:

```
APACHE$DCL_ENV [-c] [-d] [-e env-file]
```

where:

- c Default. Indicates create environment variables.
- d Indicates delete environment variables.
- e env-file Specifies an alternate environment file. The environment file does not need to be specified by the caller because the parent derives it (it is easily be determined by default).

The following example deletes the environment and then recreates it:

```
Example: diff_mode.cgi.com
$ APACHE$DCL_ENV -d
$ Define APACHE$PREFIX_DCL_CGI_SYMBOLS_WWW 1
$ APACHE$DCL_ENV -c
```

### 3.13.2 Referencing Input

CGI scripts that reference input to the Compaq Secure Web Server must refer to APACHE\$INPUT.

### 3.13.3 Executing CGI

On OpenVMS, CGI images execute within a DCL process. You cannot execute CGI images directly.

### 3.13.4 Logicals for Debugging CGI Scripts

Use the following logical to debug CGI scripts.

Logical Name	Description
APACHE\$DEBUG_DCL_CGI	If defined, this system logical name enables APACHE\$VERIFY_DCL_CGI and APACHE\$SHOW_CGI_SYMBOL.
APACHE\$VERIFY_DCL_CGI	If defined, this system logical name provides information for troubleshooting DCL command procedure CGIs by forcing a SET VERIFY before executing any DCL CGI. Enabled by APACHE\$DEBUG_DCL_CGI.
APACHE\$SHOW_CGI_SYMBOL	If defined, this system logical name provides information for troubleshooting the CGI environment by dumping all of the symbols and logicals (job/process) for a given CGI. Enabled by APACHE\$DEBUG_DCL_CGI.

## Running the Compaq Secure Web Server on OpenVMS

### 3.13 Common Gateway Interface (CGI)

#### 3.13.5 Displaying Graphics with CGI Command Procedures

To display a graphics file with a CGI command procedure, use the `APACHE$DCL_BIN` foreign symbol in the following format:

```
APACHE$DCL_BIN [-s bin-size] bin-file
```

where:

`-s bin-size` Specifies the actual or approximate file size in bytes. Bin-size is automatically determined if the image file is larger than 32768K (default value). If the image file is smaller than 32768K, you can provide an approximate (or actual) size (this will boost performance).

`bin-file` Specifies the file to be displayed.

For example:

```
$ SAY := WRITE SYS$OUTPUT
$ SAY "Content-type: image/gif"
$ SAY ""
$ APACHE$DCL_BIN APACHE$ROOT:[ICONS]APACHE_PB.GIF
$ EXIT
```

---

## Security Information

The Compaq Secure Web Server for OpenVMS is a non-privileged, user-mode, socket-based network application. TMPMBX and NETMBX are the only privilege requirements. The server runs under its own unique UIC and user account (APACHESWWW).

### 4.1 Process Model

The Compaq Secure Web Server runs as a single job which consists of:

- A master process (APACHESWWW)  
and
- Several subprocesses

Subprocesses are created to service incoming HTTP requests and execute CGI scripts (APACHESWWW\_x). The MOD\_JSERV Java servlet engine creates subprocesses (apache\_Jserv\_x) to execute Java programs. MOD\_PERL does not create any sub processes.

Because the server runs as a single job, the OpenVMS security profile for each process is identical and no enhanced mechanism is required for these processes to communicate with one another. Resource utilization is controlled by a single user account (APACHESWWW) where pooled quotas are defined.

### 4.2 Privileged Images

The Compaq Secure Web Server performs three operations that require additional privilege:

- Binding to a port below 1024 (privileged ports)  
By default, the server binds to port 80 (HTTP) and 443 (HTTPS) which are privileged ports.
- Fetching path information for other users  
The server provides a replacement for the getpwnam C RTL routine to allow the server to fetch default path information for other users (required by MOD\_UTIL and MOD\_USERDIR).
- Changing the "carriage-control" attribute on socket (BG) devices  
The server also enables/disables the carriage-control attribute on BG (socket) devices for certain stream operations.

Two protected shareable images are installed at startup to allow the server to perform these functions:

- APACHES\$PRIVILEGED.EXE\_ALPHA (exec-mode services)
- APACHES\$FIXBG.EXE\_ALPHA (kernel-mode services)

## Security Information

### 4.2 Privileged Images

The APACHE\$PRIVILEGED.EXE\_ALPHA image provides exec-mode services for binding to privileged sockets and fetching a user's default path information. Access to these services is limited to processes running under the APACHE\$WWW username and is controlled by the APACHE\$PLV\_ENABLE\_APACHE\$WWW logical name. This logical name is defined as:

```
"APACHE$PLV_ENABLE_APACHE$WWW" = "3,80,1023"
```

The "3,80,1023" string represents three parameters where:

- The first parameter (3) is a bit-mask which enables/disables the two services:
  - Bit 0 controls binding to privileged ports.
  - Bit 1 controls fetching user default path information.
- The second and third parameters are the minimum and maximum port allowed to be bound.

When a call to either service is made, the service code:

1. Temporarily enables the privileges SYSPRV, OPER, SYSNAM, and NETMBX.
2. Performs the function.
3. Restores the process' original privileges.

The APACHE\$FIXBG.EXE\_ALPHA image provides a kernel-mode service for manipulating the carriage-control attribute for BG devices owned by the calling process. There is no special access control on this service. This function can also be performed using a setsocketopt C RTL run-time call, but it is not supported by all TCP/IP stack vendors, which is the reason this service exists. This service does not enable privileges, but executes in kernel mode.

### 4.3 Privileges Required to Start and Stop the Server

The Compaq Secure Web Server runs under the APACHE\$WWW username and UIC and is started as a detached, network process. During startup, protected images are installed and logical names are placed in the system logical name table. Shutdown is accomplished by sending a KILL signal to the master process and its subprocess.

These actions require enhanced privileges (DETACH, SYSNAM, WORLD, etc.) and are usually performed from a suitably privileged account.

### 4.4 File Ownership and Protection

All of the server's files reside under its root directories pointed to by the APACHE\$ROOT logical name. During installation, file protection is set to (S:RWED, O:RWED, G, W). During configuration, all files are set to be owned by APACHE\$WWW.

### 4.5 Server Extensions (CGI Scripts, Java Servlets, Perl Modules)

Server extensions, such as CGI scripts, Java servlets, and Perl modules, run within the context of the Compaq Secure Web Server's process or its subprocesses. These extensions have complete control over the server environment. You can configure the server to allow execution of arbitrary user scripts, but standard practice is to limit such activity to scripts written by completely trusted users. The Compaq Secure Web Server includes directives that allow a web

## 4.5 Server Extensions (CGI Scripts, Java Servlets, Perl Modules)

administrator to control script execution and client access. The use of these directives is described in numerous books and is not duplicated here.

### 4.6 suEXEC Not Available for Protecting Script Execution

The Compaq Secure Web Server for OpenVMS does not currently support the suEXEC method of executing scripts under the username that owns the script. Many sites like to use this feature to allow execution of arbitrary, user-written scripts without the fear of compromising the server's environment.

### 4.7 Protecting Server Certificate Keys

The Compaq Secure Web Server's certificate keys must be protected against disclosure. The keys, by default, are owned by APACHESWWW, and protected as (S:RWED, O:RWED, G, W). As an additional measure of security, the keys can be encrypted. When using encrypted keys, a password must be entered during startup to decrypt the keys.

Keys must be kept out of directories accessible by clients (such as document directories!).

A second threat for key disclosure exists during script execution because scripts run in the context of the server and have complete access to key files no matter where they exist (as long as they exist in a directory accessible to APACHESWWW). Therefore, it is not advisable to allow the execution of arbitrary user scripts when using SSL.

---

## Open Source Licenses

This chapter provides open source license acknowledgements and license references.

### Apache

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). You can view the license at

[http://www.openvms.compaq.com/openvms/products/ips/apache/apache\\_license.txt](http://www.openvms.compaq.com/openvms/products/ips/apache/apache_license.txt)

### Mod\_Jserv

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (<http://www.java.apache.org/>). You can view the license at

[http://www.openvms.compaq.com/openvms/products/ips/apache/jserv\\_license.txt](http://www.openvms.compaq.com/openvms/products/ips/apache/jserv_license.txt)

### Mod\_SSL

This product includes software developed by Ralf S. Engelschall <[rse@engelschall.com](mailto:rse@engelschall.com)> for use in the Mod\_SSL Project (<http://www.modssl.org/>). You can view the license at

[http://www.openvms.compaq.com/openvms/products/ips/apache/modssl\\_license.txt](http://www.openvms.compaq.com/openvms/products/ips/apache/modssl_license.txt)

### OpenSSL

This product includes software developed by the OpenSSL Project (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (<http://eay@cryptsoft.com/>). You can view the license at

[http://www.openvms.compaq.com/openvms/products/ips/apache/openssl\\_license.txt](http://www.openvms.compaq.com/openvms/products/ips/apache/openssl_license.txt)

### Mod\_Perl

This product includes software developed by the Apache/Perl Integration Project (<http://perl.apache.org/>). You can view the license at

[http://www.openvms.compaq.com/openvms/products/ips/apache/modperl\\_license.txt](http://www.openvms.compaq.com/openvms/products/ips/apache/modperl_license.txt)

### Perl

This product includes software developed by the Perl Project (<http://www.perl.org/>). You can view the license at

[http://www.openvms.compaq.com/openvms/products/ips/apache/perl\\_license.txt](http://www.openvms.compaq.com/openvms/products/ips/apache/perl_license.txt)