

WEBSTAR[®]

**SERVER
SUITE**

www.starnine.com

**POWERFUL
SERVERS
FOR THE
MAC OS**



STARNINE

COPYRIGHT

Software and Manual Copyright © 1989-1999 StarNine Technologies, Inc. and their Licensors. Portions of the Software copyright © 1999 Blue World Communications, Inc. All rights reserved. Portions Copyright © 1998-1999 RSA Data Security, Inc. All rights reserved. This guide and the software described in it are copyrighted with all rights reserved. Neither the guide nor the software may be copied in whole or part without the written consent of StarNine Technologies, Inc., except as described in the license agreement included in this guide. To inquire about where you can purchase this product please contact us at:

StarNine Technologies, Inc.
2550 Ninth Street, Suite 112
Berkeley, CA 94710 USA

Tel: 510-649-4949 Fax: 510-548-0393

Internet: info@starnine.com

Written by Avi Rappoport, with portions by and help from Eric Zelenka, Stuart Gripman, Joe Kalash, CJ Holmes, David Wiester and Doug Finley. WebSTAR Lasso Publisher chapter written by Stuart Gripman. Special thanks to Luke van der Westhuyzen, Marc Eagle, Robert Ameet, Scott Steward, Kevin Rardin, and Hilary Nelson.

STARNINE® WEBSTAR® LICENSE AND LIMITED WARRANTY AGREEMENT

CAREFULLY READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT PRIOR TO USING THIS PACKAGE. USE OF ANY PORTION OF THIS PACKAGE INDICATES YOUR AGREEMENT TO THE FOLLOWING TERMS AND CONDITIONS. IF YOU DO NOT AGREE WITH SUCH TERMS AND CONDITIONS, YOU SHOULD PROMPTLY RETURN THIS PACKAGE BEFORE USING IT TO YOUR PLACE OF PURCHASE FOR A REFUND.

DEFINITIONS

The following definitions apply to the terms as they appear in this agreement:

- StarNine means StarNine Technologies, Inc. and its Licensors.
- You and Your refer to any person or entity that acquires or uses this package.
- Users refer to persons using the StarNine Software
- Package means the software, manual(s), and other items accompanying this agreement.
- Software means the computer programs contained in the Package, together with all codes, techniques, software tools, formats, designs, concepts, methods, and ideas associated with these computer programs.

PERMITTED USES

StarNine grants you a non-exclusive license to use the software in this package according to the terms set forth below. You may:

1. Install and operate the Software on only one computer at a time, except for those portions of the Software which StarNine specifically gives you permission to install and/or operate on more than one computer as described in the manual(s) and/or ReadMe file which are part of the Package. If the Software is licensed as an update or upgrade from a previous version you may use or transfer the Software only as an update or upgrade from the previous software version on the same computer, provided that the software was in use in accordance with the previous license agreement. Use of the Software shall be in accordance with this license, which supersedes the license for the previous version.
2. Make a reasonable number of copies of the Software solely for back-up or archive purposes, which automatically become the property of StarNine and are subject to this agreement. In any such copies, you must reproduce all copyright notices and other identifying or restrictive legends that appear on the Software as received.
3. Transfer, after providing written notification to StarNine, all (but no lesser portion) of the Software and related manuals to another person or entity, who in turn will be subject to this agreement.

PROHIBITED USES

You may not:

1. Modify the Software. Any modified or merged portion of the Software is subject to this agreement.
2. Reverse-engineer, disassemble, decompile, or make any attempt to discover the source code to the Software.
3. Translate or create derivative works based on the Software.
4. Remove, obscure, or alter any copyright notice or other proprietary rights related to the Software or Package including manuals.
5. Sub-license, sell, lend, rent, or lease any portions of the Software.
6. Copy any portion of the Software, except as described above under Permitted Uses.

7. Operate the Software with more Users than are allowed by the Keys supplied with this Software and/or other products licensed from StarNine. If you plan to have more than this number of Users, you will need to license additional copies of the Package or license a different StarNine product. Contact StarNine or the place where you purchased the Package if you want information on site licenses or other StarNine products.

8. Transfer the Software or any direct product to any person or entity in violation of the United States Export Administration Act.

The Software involves valuable proprietary rights of StarNine and others. StarNine retains title to and ownership of the Software and all copyright, trade secret, trade name, trademark, and other property rights related to the Software, regardless of the form that the original or other copies exist in. You may not violate these rights, and you must take appropriate steps to protect StarNine's rights. StarNine may at any time replace, modify, alter, improve, enhance, or change the Software.

Both the license and your right to use the Software terminate automatically if you violate any part of this agreement. In the event of termination, you must immediately destroy all copies of the Software or return them to StarNine.

EXPORT CONTROLS

None of the Software or underlying information or technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident of) Cuba, Iraq, Libya, Yugoslavia, North Korea, Iran, Syria or any other country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By downloading or using the Software, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list.

In addition, if the licensed Software is identified as a not-for-export product (for example, on the box, media or in the installation process), then the following applies: EXCEPT FOR EXPORT TO CANADA FOR USE IN CANADA BY CANADIAN CITIZENS, THE SOFTWARE AND ANY UNDERLYING TECHNOLOGY MAY NOT BE EXPORTED OUTSIDE THE UNITED STATES OR TO ANY FOREIGN ENTITY OR "FOREIGN PERSON" AS DEFINED BY U.S. GOVERNMENT REGULATIONS, INCLUDING WITHOUT LIMITATION, ANYONE WHO IS NOT A CITIZEN, NATIONAL OR LAWFUL PERMANENT RESIDENT OF THE UNITED STATES. BY DOWNLOADING OR USING THE SOFTWARE, YOU ARE AGREEING TO THE FOREGOING AND YOU ARE WARRANTING THAT YOU ARE NOT A "FOREIGN PERSON" OR UNDER THE CONTROL OF A FOREIGN PERSON.

LIMITED WARRANTY

StarNine warrants that, upon delivery by StarNine, the media (CD-ROMs and/or diskettes) on which the Software program is distributed will be free from defects in materials and workmanship and that the software will substantially conform to the specifications established by StarNine. StarNine does not warrant that the Software is free from all bugs, errors, and omissions.

If any of the Software fails to comply with the warranties set forth above, StarNine will replace the media or, at StarNine's option, make a reasonable effort to correct the program errors. To receive any such replacement Software, you must return all copies of the Software, along with a copy of your paid invoice, to your place of purchase within 90 days of the date you received the Software. If StarNine is unable to correct defective media or program errors, StarNine will refund all or a fair portion of the price you paid for the Package. The refund will fully satisfy your claims for software or disk failure. This limited warranty shall continue for any replacement software for the rest of the original 90-day warranty period or for 30 days from the date you receive the replacement, whichever is longer.

EXCEPT AS SPECIFICALLY SET FORTH ABOVE, STARNINE MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE SOFTWARE. STARNINE DOES NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME JURISDICTIONS. THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

EXCEPT AS SPECIFICALLY SET FORTH ABOVE, STARNINE AND ITS DIRECTORS, OFFICERS, SUPPLIERS, DISTRIBUTORS AND DEALERS (COLLECTIVELY STARNINE) WILL IN NO EVENT BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTIONS, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF STARNINE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

StarNine's liability to you for actual damages for any cause whatsoever, and regardless of the form of the action (whether in contract, tort (including negligence), product liability or otherwise), will be limited to the purchase price you paid for the Product.

STARNINE'S LICENSOR(S) MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE SOFTWARE. STARNINE'S LICENSOR(S) DOES NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME JURISDICTIONS. THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

IN NO EVENT WILL STARNINE'S LICENSOR(S), AND THEIR DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS (COLLECTIVELY STARNINE'S LICENSOR) BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTIONS, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THE USE OR

INABILITY TO USE THE SOFTWARE EVEN IF STARNINE'S LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

StarNine's Licensor's liability to you for actual damages for any cause whatsoever, and regardless of the form of the action (whether in contract, tort (including negligence), product liability or otherwise), will be limited to \$50.

GENERAL

Though StarNine is not responsible for maintaining or helping you use the Software, StarNine does at its discretion offer support. To receive support, you or the person who installed the Software for you must complete and return the enclosed user Registration Card.

This agreement constitutes the entire agreement and supersedes any prior agreement between StarNine and you concerning the contents of the Package. StarNine is not bound by any provision of any purchase order, receipt, acceptance, confirmation, correspondence, or otherwise, unless an authorized corporate officer of StarNine specifically agrees to the provision in writing and the writing includes the officer's signature. Any written or oral information or advice given by StarNine dealers, distributors, agents, or employees will in no way increase the scope of this warranty. Nor may you rely on any such oral or written communication. This agreement cannot be amended, modified, or waived, unless the change is written and signed by an authorized corporate officer of StarNine.

YEAR 2000 READINESS DISCLOSURE

STATEMENT ON THE YEAR 2000 AND WEBSTAR SERVER SUITE 4.0 FOR MAC OS

The information contained in this notice regarding StarNine's products and services are hereby designated as "Year 2000 Readiness Disclosures" under the Year 2000 Information and Readiness Disclosure Act of 1998. The contents of this Year 2000 Readiness Disclosure are subject to the Year 2000 Information Readiness Disclosure Act (112 stat. 2386). In the case of a dispute, the Year 2000 Information Readiness Disclosure Act may reduce your legal rights regarding the use of any such statements, unless otherwise specified by a contract with StarNine, or by tariff.

This Year 2000 Readiness Disclosure shall not be interpreted or construed as an amendment to or alteration of a contract or warranty. StarNine's obligations and responsibilities regarding StarNine products and services are governed solely by the agreements under which they are licensed or sold.

NO WARRANTY IS EXPRESS OR IMPLIED OTHER THAN IS INCLUDED IN THE SOFTWARE LICENSE AND LIMITED WARRANTY WHICH ACCOMPANIED THE PRODUCT.

YEAR 2000 READINESS DISCLOSURE FOR WEBSTAR SERVER SUITE 4.0 FOR MAC OS

With the WebSTAR Server Suite 4.0 upgrade, all issues known to StarNine Technologies as of March 1, 1999, directly related to the operation of WebSTAR Server Suite in the Year 2000 have been resolved. We believe that WebSTAR Server Suite will operate properly in the year 2000 and in the years immediately following 2000, with the currently available Apple Macintosh system software; Mac OS 8.1, Mac OS 8.5 and 8.5.1.

OTHER INFORMATION REGARDING THE YEAR 2000

WebSTAR Server Suite 4.0 uses the Mac OS System Toolbox functions for obtaining date information. According to Apple Computer, Inc., the date function in Mac OS 8.1, Mac OS 8.5 and 8.5.1 are Year 2000 compliant. Please see the information provided by Apple Computer, Inc. regarding official verification of Year 2000 compliance for Mac OS at <http://www.apple.com/about/year2000/index.html>.

SUPPORT

Though StarNine is not responsible for maintaining or helping you use the Software, StarNine does at its discretion offer support in the following ways:

- Our website: <<http://www.starnine.com/>>
- Our mail discussion lists:

Sign up at <<http://www.starnine.com/Address-List-Editor.html>> or send email to support@starnine.com for instructions

- Direct email to support@starnine.com
- Telephone: (510) 704-1272 or fax (510) 548-0393

Free for the first ninety (90) days after your purchase. Some charges may apply for additional telephone support.

- US Mail: StarNine Technologies, Inc. ATTN: Support
2550 Ninth Street, Suite 112 Berkeley, CA 94710 USA

TRADEMARKS

StarNine and WebSTAR are registered trademarks of StarNine Technologies, Inc. Lasso is a registered trademark of Blue World Communications, Inc. All other trade names referenced are the service mark, trademark or registered trademark of the respective manufacturer.

SUN MICROSYSTEMS COPYRIGHT AND LICENSE INFORMATION

JAVA™ web development products are owned and licensed exclusively by Sun Microsystems, Inc. Copyright © 1992-96 Sun Microsystems, Inc. All rights reserved. Java and all Java-based names and logos, including the Coffee Cup and Duke, are trademarks of Sun Microsystems, Inc. and refer to Sun's Java Technologies. Products bearing the authorized "JAVA-Compatible" Logo are based upon Sun's JAVA and technology, and are compatible with the API's for such technology.

Sun grants to you ("Licensee") a non-exclusive, non-transferable license to use the Java binary code version (hereafter, "Binary Software") without fee. Licensee may distribute the Binary Software to third parties provided that the copyright notice and this statement appear on all copies. Licensee agrees that the copyright notice and this statement will appear on all copies of the software, packaging, and documentation or portions thereof.

In the event Licensee creates additional classes or otherwise extends the Applet Application Programming Interface (AAPI), licensee will publish the specifications for such extensions to the AAPI for use by third party developers of Java-based software, in connection with licensee's commercial distribution of the Binary Software.

RESTRICTED RIGHTS: Use, duplication or disclosure by the government is subject to the restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software Clause as DFARS 252.227-7013 and FAR 52.227-19.

SUN MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE SUITABILITY OF THE BINARY SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SUN SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE BINARY SOFTWARE OR ITS DERIVATIVES.

By downloading, using or copying this Binary Software, Licensee agrees to abide by the intellectual property laws, and all other applicable laws of the U.S., and the terms of this License. Ownership of the software shall remain solely in Sun Microsystems, Inc.

Sun shall have the right to terminate this license immediately by written notice upon Licensee's breach of, or non-compliance with, any of its terms. Licensee shall be liable for any infringement or damages resulting from Licensee's failure to abide by the terms of this License.

The JDK 1.0.2 binary release is based in part on the work of the Independent JPEG Group.

BIIT INC. COPYRIGHT AND LICENSE INFORMATION

Copyright © Biit Inc. 1996-1998 All Rights Reserved.

Permission to use, copy, modify, and distribute this software [HeapManager], in both binary and source forms, and together with its documentation, for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Biit not be used in advertising or publicity pertaining to distribution of this software without specific, written permission.

BIIT DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL BIIT BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OPENSSL LICENSE INFORMATION

Copyright © 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

ERIC YOUNG COPYRIGHT AND LICENSE INFORMATION

Copyright ©1997 Eric Young (eay@cryptsoft.com) All rights reserved.

This package contains an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL. Redistribution and use of Eric Young's SSL implementation is permitted as long as the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Table of Contents

COPYRIGHT	2
STARNINE® WEBSTAR® LICENSE AND LIMITED WAR- RANTY AGREEMENT	2
YEAR 2000 READINESS DISCLOSURE.	4
SUPPORT.	4
TRADEMARKS	5

Chapter 1: Introduction

Welcome to WebSTAR.	.23
WebSTAR Features	.23
WebSTAR Web Serving.	.24
Mail Server	.24
FTP Server	.24
Proxy Server	.24
Secure Administration.	.25
About This Manual.	.25
Additional WebSTAR Information	.25
WebSTAR Information Online	.25
StarNine Technical Support.	.26
Developing CGIs and Plug-Ins for WebSTAR	.26
General Information	.27

Chapter 2: Installation

System Requirements	.29
Hardware	.29
System Software	.29
Memory Requirements	.29
Network Requirements	.30
Standard New Installation.	.32
Active Installer	.32
Installing Your WebSTAR Server	.32
Custom Installation.	.34
Custom Install	.34
Custom Install Location.	.34
Custom Install Items.	.35
Active Installer	.36
Installing SSL	.36
Upgrading your WebSTAR Server	.37
Upgrading SSL Versions of WebSTAR	.37
Using the WebSTAR Upgrade Installer	.38

About the Installed Files	40
WebSTAR 4.	40
WebSTAR Admin	40
About WebSTAR 4.	41
HTML files	41
Plug-Ins folder	41
CGI-BIN folder.	43
JRun Folder.	43
Documentation folder.	43
Restart Server Application	43
Tools & Examples Folder	44
Other Files	45

Chapter 3: Getting Started

Starting The WebSTAR Server Suite	47
Start Your Server.	48
WebSTAR Serial Number.	48
Admin Password	49
More About WebSTAR	49
Try Out Your Server	50
Connect To Your Web Server.	51
Browse the Documentation.	52
Administering WebSTAR	52
About the WebSTAR Admin Application	52
Accessing the Browser Admin Pages	55
Connect To Your FTP Server	57
Creating an FTP User Entry	57
Testing Your FTP Server	58
Start Your Mail Server	59
Setting the Mail Host Name	59
Creating a Mail User Account	59
Log Into Your Email Account	60
Allow Email Clients to Send Messages	61
Protect Your User Directory	62
Connect to Your Proxy Server.	63
Setting Up Your Web Site	64
URLs, HTTP and Your Web Server	64
Default Page	65
Folder Hierarchy.	65
Extending Your Web Server.	67

Chapter 4: New Features in WebSTAR 4

Upgrading	.69
What's New In WebSTAR 4	.69
Changes to The Web Server	.69
SSL (Secure Sockets Layer) Changes.	.70
Changes to the WebSTAR Admin	.70
New Mail Server Added to the Suite	.71
Changes to the WebSTAR FTP Server	.72
Changes to the WebSTAR Proxy Server	.72
New Features:	.73
Changes to the WebSTAR Plug-Ins.	.73
Core Plug-Ins Changes	.73
Additional Plug-Ins	.74
New Plug-Ins.	.75

Chapter 5: WebSTAR Server & Troubleshooting

WebSTAR Status and Monitor Windows	.77
Status Window Top Panel	.78
Minimized Window	.79
Status Window Monitor Pane	.80
FTP Monitor Window	.82
Mail Monitor Window	.82
Proxy Monitor Window	.83
WebSTAR Server Menus.	.83
File Menu	.83
Edit Menu.	.83
Options Menu	.85
Plug-Ins Menu	.86
Help Menu	.87
Server Application Issues	.87
Server Administration Responsibilities	.87
Application Memory and Connections	.88
Optimizing WebSTAR for Best Performance	.90
Restarting After Open Transport Errors.	.90
WebSTAR Background Server	.91
Running Multiple Servers On The Same Machine	.92
Log Archiving	.93
WebSTAR Security	.93
Physical Security	.93
WebSTAR Server and Admin Security	.93

SSL Security	94
CGI and Plug-In Security	94
Web File Security	95
FTP Security	95
Safe Passwords.	96
Identifying Your Site: IP, Host Name and DNS.	96
IP Addresses	97
Your Server's IP Address	97
Host Names	98
Your Server's Host Name.	99
DNS	100
Port Numbers	102
Important WebSTAR Files.	103
WebSTAR.Messages File	104
Web Server Files	104
FTP Server Files	105
Mail Server Files	105
Proxy Server Files	106
Server Troubleshooting	106
How to Get Help.	106
WebSTAR Debug Plug-In.	107
General Server Troubleshooting Guidelines	108

Chapter 6: Server Administration and Status

About the WebSTAR Admin Application	113
Connecting To A Server.	113
Disconnecting From a Server.	114
WebSTAR Admin Security	115
Admin Monitor Windows.	116
WebSTAR Admin Menus	118
File Menu	118
Edit Menu	118
Windows Menu	119
WebSTAR Admin Server Settings	120
Working With Admin Lists.	120
File Paths in WebSTAR Admin.	121
Log Archiving.	122
How Log Archiving Works.	122
Log Status Reporting	123
Log Archiving Settings	124
Status Reports	125

Browser-Based Admin	126
Chapter 7: Web Server Administration	
WebSTAR Admin Application	129
File Names and Paths	130
Default Names	130
Processors.	132
Connections Settings	134
Max Connections.	134
HTTP Port	135
Timeout	136
Buffer Size	136
Use DNS for Server and Client Lookups	136
Restrict CGIs to CGI-BIN	137
Persistent Connections	137
Performance	138
Caching	139
File Info Cache	139
Data Cache	140
Updating Caches.	143
Virtual Hosts	144
Editing Virtual Hosts Entries	144
Virtual Host Root Folders.	149
Virtual Host Options	150
Virtual Hosts Settings File	150
SSI	152
Suffix Mapping	154
Suffixes, Type and Creator Codes	154
How Suffix Mapping Works	155
Editing Suffix Mapping Table Entries	156
Fields in the Suffix Mapping Table	158
Suffix Mapping Example: Using SSI for All HTML Files	160
Actions	161
Editing Actions Entries	162
Using Actions	163
Security Realms	164
About Realms	164
Editing Realms Entries	165
Realms, Allow / Deny and User Names Work Together	167
Web Users and Passwords.	168

Editing User Entries	168
Importing and Exporting Large Users Lists	170
Allow / Deny.	172
Realms Access Control	172
Editing Allow / Deny Entries	173
Allow / Deny Examples	175

Chapter 8: About Web Serving

Web Serving and HTTP	179
HTTP Connections.	179
WebSTAR URL Processing	180
Responding To Errors.	182
WebSTAR URL Security Processing.	183
Folder Hierarchy, File Paths, and Names	186
Example Hierarchy and File Paths.	186
File Hierarchy and Virtual Hosting	187
Links to Subfolders and Parent Folders	187
Web File and Folder Name Rules	189
Redirection: Aliases and Redirect Files	190
Virtual Hosts: Hosting Multiple Web Sites	193
Routing to Virtual Hosts	193
Configuring Virtual Hosts	194

Chapter 9: Web Server Logging

Logging	199
Log Archiving	200
Log Formats.	200
About Log Formats: WLF, CLF and ExLF.	202
Log Format Tokens	203
Configuring the Log Format	207

Chapter 10: SSL Web Security

About SSL Security.	209
Secure Sockets Layer (SSL) Protocol.	209
Encryption Levels: US and International	209
How Browsers Access A Secure Server	211
SSL and Multiple Domains	212
Installing & Configuring SSL	213
Steps to Secure Serving	213
Performing the Installation	214
Obtaining and Installing Certificates.	215

Certificate Formats	215
Certificate Authorities	215
Creating Certificate Signing Requests	216
Using the VeriSign Certificate Authority	218
Using the Thawte Certificate Authority	220
Obtaining a Test Certificate	225
Installing Your Server Certificate	226
Using SSL in WebSTAR	229
Testing Your Secure Server	229
Access Control	230
Additional Privacy Considerations	230
SSL Server Performance Issues	231
SSL (Secure Socket Layer) Troubleshooting	231

Chapter 11: WebSTAR Plug-Ins

About WebSTAR Plug-Ins	235
Plug-In Memory Issues	235
Installing and Removing Plug-Ins	236
WebSTAR Plug-In Settings	237
WebSTAR Auto BinHex	238
Using Auto BinHex	238
Auto BinHex Settings	239
WebSTAR Byte Server	240
Example: Byte-Serving PDF files	240
WebSTAR Directory Indexer	241
Using Directory Indexer	241
Default Index Pages vs. Directory Index Listings	244
WebSTAR Directory Indexer Administration	244
WebSTAR File Upload	247
Using the WebSTAR File Upload Plug-In	247
WebSTAR File Upload Administration	248
WebSTAR Form Mail	249
Using WebSTAR Form Mail	249
WebSTAR Form Mail Examples	250
WebSTAR Form Mail Administration	251
Additional Form Mail Options	252
WebSTAR Image Map	253
Using the WebSTAR Image Map Plug-In	254
WebSTAR JRun Servlet Runner	255
System Requirements & Configuration	255

Using WebSTAR JRun Servlet Runner	255
Java Servlet Development Information	256
WebSTAR PowerKey Pro Tickler	256
WebSTAR QuickDNS Load Balancer	257
Fault Tolerance.	257
Load Balancing.	257
Load Balancing vs. Load Sharing	258
QuickDNS Configuration Page	258
HTTP Configuration.	259
WebSTAR Rebound! Assist	260
WebSTAR Search.	261
How the Searching Works	261
Search Results	263
Installation	264
Indexing and Index Files	266
Search Dictionaries	269
Web Tools For Searching	269
Search Plug-In Administration: Index Auto-Update	271
WebSTAR WebObjects Adaptor	272
How the WebObjects Adaptor Works.	273
WebObjects Configuration	273

Chapter 12: WebSTAR SSI

Using WebSTAR SSI Commands	275
SSI Command Structure	276
SSI Command Example.	279
SSI Command List	280
Echo Command	280
Include Command.	282
FSize Command	283
FLastMod Command	283
Counter Command	284
Hide and Show Commands	285
Exec Command	288
Store Command	291
PostArg Command	291
Config Command	292
SSI Troubleshooting.	295
SSI Administration & Security	296
SSI Security.	296
Editing Counters and Numeric Variables.	297

SSI and File Suffixes	298
Additional SSI Features and Options	298
WebSTAR SSI-WebInclude	299
WebInclude Security.	299
Legal Issues.	300
Installation	301
Using WebSTAR SSI-WebInclude	301
SSI WebInclude Commands	303
Nesting TAGEXTRACT Commands.	305
Extending WebSTAR SSI.	306
Tag Registry	306
WebSTAR SSI Extensions.	306
Chapter 13: WebSTAR Lasso Publisher	
Installation.	307
Files Installed.	307
How WebSTAR Lasso Publisher Works	308
WebSTAR Lasso Publisher vs. Lasso Web Data Engine. . .	308
What You Need to Know	309
HTML Editor Requirements	309
Preparing a Database for Web Publishing	310
Security	310
Create a Layout	310
Open in Browse Mode.	310
Using FileMaker Pro Server.	310
Instant Web Database Publishing.	311
Custom Web Database Publishing	312
LDML (Lasso Dynamic Markup Language)	313
FM Link	314
Creating a Search Form	314
Required Tags for a Search	314
Other Important Tags	316
Search Operators.	317
Displaying Search Results	318
Listing the Matched Record Data	318
Navigating the Found Set.	319
Showing Details	320
Creating a Form to Add Records	322
Add Record Example	322
Other Important Tags	323

WebSTAR Lasso Publisher Troubleshooting	324
Going Further	325
Advanced Topics	325
The LDML 3.5 Reference Database	325
Online Help	326
Purchasing the Lasso Web Data Engine.	326

Chapter 14: Web Server Troubleshooting

Chapter 15: WebSTAR FTP Server

About the WebSTAR FTP Server	337
FTP and Cache Flushing	337
FTP Security	337
FTP Data Types Supported	339
FTP and Multiple Hosts.	339
FTP Load Balancing	339
FTP URLs in HTML	339
FTP Standards and Conventions	340
FTP Specification.	340
FTP Ports	340

Chapter 16: FTP Server Administration

WebSTAR FTP Settings	341
Max Connections	341
Timeout	341
Reported Server Name	342
Use MacBinary for .bin files	342
Displaying Files with Resource Forks	342
Default Type & Creator Codes For Upload	343
Connection Messages	344
FTP Users: Access Control.	344
Making an FTP User Entry	345
User Name and Password	345
FTP Root Folder File Path.	346
Max Folder Size	346
Privileges	346
FTP Users Import & Export.	347
Anonymous FTP.	347

Chapter 17: FTP Monitors & Logging

FTP Monitor Windows.	349
FTP Logging Information	349

FTP Log Elements	349
FTP Activities.	350
FTP Commands	351
FTP Log Files	353
Logging Options	353
Log Archiving	353
Chapter 18: WebSTAR FTP Troubleshooting	
FTP Server Troubleshooting	355
The WebSTAR FTP Server Startup Errors.	355
Errors and Error Codes	356
Client Errors	356
Chapter 19: WebSTAR Mail Server Overview	
About the WebSTAR Mail Server.	357
WebSTAR Mail Files.	357
About Internet Email.	358
SMTP	358
POP	359
IMAP	360
Web Mail	360
LDAP	360
DNS Servers and Mail Hosts	362
Mail Exchange Records	362
Email Access from Web Browsers	363
Log In	363
Writing Messages	364
Viewing Messages	365
Acting on Messages	365
Mail Administrator Responsibilities	367
Mail Server Account Management.	367
Reading the Postmaster Messages	367
Tracking Mail Server Usage	368
Backing Up and Restoring Email Files.	370
Dealing With Spam (Unsolicited Email).	370
Chapter 20: WebSTAR Mail Settings	
Mail Defaults	373
Mail Storage	373
Alternate DNS Server	374
Web-Based Email	374
Backup Scheduling	374

Mail Hosts	375
Host Name	376
Unknown Address.	376
Copy To.	376
Redirect To	376
Mail Connections	377
About Connections	377
SMTP Connections	378
Relay Restrictions and Spam Prevention	380
IMAP Connections.	381
POP Connections	381
LDAP Connections	382
Mail Caching	382
RAM Cache.	383
Disk Cache	383
DNS Caching.	384
Mail Routing	384
Editing the Routing Entries	385
Routing Options	386
Mail Allow / Deny	387
Allow / Deny Services	387
Editing Allow / Deny Entries	388

Chapter 21: Mail Users & Accounts

Users & Accounts Settings.	391
Account ID	391
Password	392
E-Mail	392
Host	392
Message Limit	393
Forward To.	393
Forwarding To Groups	393
Storage Limit.	394
Require APOP	394
IMAP Privileges	394
Import and Export	395
WebSTAR Mail Export Formats	395
Import User Mailboxes	396
Exporting Mail Users and Messages.	397
Account Tips and Examples.	397
Postmaster Account	397

Characters Allowed in Names Addresses.	398
Creating Address Conventions.	398
Chapter 22: Mail Monitors, Logs, and Reports	
Mail Monitor & Queue Window	399
Connections	399
Activity Log	400
Queue	401
Logging Options Settings	403
Logging Options	403
Log Archiving	403
Reporting	404
Mail Server Report Format	404
Setting the Report Schedule.	405
Clear Report	405
Run Now	405
Chapter 23: Mail Server Troubleshooting	
Repairing Damaged Mail Files	407
Server Not Getting Messages.	407
Log Error Messages	408
Mail Trace File	408
Client Problems and Error Messages	408
Postmaster Problem Messages	410
Chapter 24: WebSTAR Proxy Server	
About the WebSTAR Proxy Server	411
Privacy Issues	411
Cache Issues	412
Browsers and the Proxy Server.	413
WebSTAR Proxy Server Design	414
Chapter 25: WebSTAR Proxy Server Settings	
Proxy Connections.	415
Upstream Proxy	416
Caching	416
Proxy Allow/Deny	418
Chapter 26: Proxy Server Monitor & Logs	
Proxy Status Window & Log File	421
Proxy Log Options	422
Logging Options	422
Log Archiving	422

Chapter 27: Proxy Server Troubleshooting

Proxy Server Troubleshooting	423
--	-----

Appendix A:Suffix Mapping Defaults

Default File Suffix Mappings	425
RAW Files	427
WebSTAR Plug-In Suffix Mappings	428

Appendix B:WebSTAR SSI Reference

SSI Command Reference Table	429
SSI Environmental Variables	431
SSI Field Descriptors for TimeFmt	433
Descriptors Not Supported	433

Appendix C:Lasso Tag Reference

Lasso Tag Table	435
---------------------------	-----

Appendix D:Extending WebSTAR: CGIs, Plug-Ins and Java

WebSTAR Development Information	443
Scripting Tools	444
MacPerl	444
Third-Party WebSTAR Add-Ons	445
Developing CGIs	445
ACGIs and Asynchronous Processing.	446
AppleScript CGI Issues	446
WebSTAR Apple Events	446
Apple Event Properties	450
Calling CGIs	451
CGIs and Virtual Hosts	454
More Information on CGIs	454
Developing WebSTAR API Plug-Ins	454
Theory of Operation.	454
Filter Plug-Ins	455
WebSTAR API Parameter Definitions.	455
Error Checking.	460
Additional information on WebSTAR API Plug-ins.	460
Using WebSTAR Plug-In Services	460
Calling WebSTAR Auto BinHex	460
Calling WebSTAR Data Cache	461
Calling WebSTAR Proxy	462
Calling WebSTAR Form Mail	463

Calling WebSTAR SSI	463
Developing Java Servlets for WebSTAR	464
Overview of JRun	464
Using JRun	465
Additional information on Java Servlets	465
Index	467

This chapter introduces you to the WebSTAR Server Suite and the documentation and support available.

WELCOME TO WEBSTAR

Welcome to WebSTAR™ Server Suite, the ultimate Mac OS™ Internet server package! And welcome to a vibrant community of Mac OS server administrators and developers.

First released in early 1995, the WebSTAR Web server became an instant success. The simplicity of WebSTAR makes it easy for any Mac user to create and serve a Web site. The many Plug-ins, CGIs and Java™ Servlets that run with WebSTAR offer a wealth of tools for serving dynamic content. WebSTAR FTP server provides fast industry-standard uploading and downloading. The WebSTAR Proxy server optimizes web access for local browsers. The WebSTAR Mail server is a full-featured email server, providing POP, IMAP, and Web-mail access.

WebSTAR Features

- World-class Web server is so fast, it can serve millions of connections a day.
- Serves multiple web sites, with different domain names and even multiple IP addresses from one Macintosh.
- Integrated SSL (Secure Sockets Layer) server lets you host a web store or serve confidential material using high-quality encryption.
- WebSTAR Admin application provides secure remote administration over TCP/IP.
- Web server works with third-party CGIs, Plug-In modules, and Java Servlets, to access databases, integrate mailing lists, customize sites, automate guestbook and email forms, and more.
- Integrated Search feature allows you to index and search your site using the same technology as Apple's "Find by Content" in Sherlock.
- WebSTAR Mail server supports SMTP mail transfer, mail clients using the POP and IMAP standards, and web browsers.
- LDAP server provides an online directory of names and email addresses.
- Integrated FTP server lets visitors to your site download or upload to specified folders.
- Caching Proxy server for optimizing network bandwidth and increased network security.

WebSTAR Web Serving

With a Macintosh and an Internet connection, WebSTAR will serve HTML documents, graphics, even QuickTime movies from your computer to web browsers all over the Internet. WebSTAR does much more than this as well, but you'll read about that later.



For information, see “Virtual Hosts: Hosting Multiple Web Sites” on page 193.

Virtual Domains and Multihoming

WebSTAR lets your single Mac serve several web sites using different IP addresses and/or host names. You can also have different hosts based on the browser's Language setting, providing websites in the native language of your visitors.

Extensible Architecture

WebSTAR allows you to extend the server using everything from simple CGIs written in AppleScript to Plug-In modules in C, C++ or Java. Many of WebSTAR's own features are implemented in the powerful Plug-In environment.

A large community of third-party developers provides a wide selection of turnkey solutions for everything from online stores and real-time conferencing through WebCams and streaming video.

Mail Server

The WebSTAR Mail server supports Internet standards such as SMTP for mail transfer, POP and IMAP for email clients, and LDAP for directory services. Web mail access allows users to read and send mail from any computer with a browser and Internet access. WebSTAR Mail and the WebSTAR Admin provide a complete suite of mail server functions, including account management, multiple email hosts and domains, DNS caching, routing control, spam prevention, and reporting.

FTP Server

The WebSTAR FTP server provides Internet-standard file uploading and downloading. You can arrange accounts with password access to certain folders, as well as anonymous downloading for public files.

Proxy Server

The WebSTAR Proxy server allows many browser clients to share a cache on the server, improving speed and efficiency of Internet access. Each browser designates the WebSTAR Proxy server to store the web

page data as it is received. If another browser accesses the same page, the Proxy server sends it from the cache, instead of requesting it from the original server.

In addition, the Proxy server allows schools and other sensitive institutions to limit access to specified IP addresses and host names.

Secure Administration

The WebSTAR Admin application can control the server from any Mac OS computer connected to the Internet. It communicates via an encrypted data stream, providing extraordinary security for your server. The intuitive but powerful interface makes it easy to control your server from any location, without having to remember cryptic codes or flags.

ABOUT THIS MANUAL

This manual is provided in two formats: Adobe Acrobat (PDF) for printing, and HTML for online access.

It covers installation, upgrading from version 3, using the WebSTAR server application, using the WebSTAR Admin application, IP Addresses, domain names and DNS, web server administration, web server issues such as virtual hosting and how the server handles HTTP requests, information about the WebSTAR Plug-Ins, the WebSTAR FTP server, the WebSTAR Mail server, the WebSTAR Proxy server, and an overview of writing CGIs and Plug-Ins for WebSTAR.

This document does not cover third-party CGIs and Plug-Ins, HTML editing, or web server design issues in detail.

ADDITIONAL WEBSTAR INFORMATION

WebSTAR Information Online

- The WebSTAR home page will always have current information about the program, as well as links to updates, third-party offers, and other useful information:

<http://www.starnine.com/webstar/>

- The Extending WebSTAR listing provides a searchable database of third-party CGIs and Plug-Ins for WebSTAR:

<http://www.starnine.com/extendingwebstar.html>

StarNine Technical Support

WebSTAR Support on the Web

The WebSTAR Support area contains Frequently Asked Questions, Technical Notes and additional online help, at:

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

WebSTAR-Talk Mailing list

The email discussion list, WebSTAR-Talk, provides an excellent resource for questions and discussions. In addition to StarNine support and engineering staff, other web administrators and third-party developers provide answers and advice.

Sign up for the WebSTAR-Talk list on the Web at:

<http://www.starnine.com/support/maillinglists/>

Or send an email message with the word “subscribe” in the subject to:

webstar-talk-request@starnine.com

You can search the archives of this mailing list as well. It's a great way to find immediate answers twenty-four hours a day:

<http://search.starnine.com/talklists.html>

Email and US Mail Technical Support

Technical questions may be sent to:

support@starnine.com

or

StarNine Technologies, Inc., ATTN: Support
2550 Ninth St. Suite 112
Berkeley, CA 94710 USA

Telephone and Fax Support

StarNine provides telephone support on weekdays between 8 am and 5 pm, Pacific Time. Telephone support is free for the first ninety (90) days after your purchase. Some charges may apply for additional telephone support.

phone: (510) 704-1272

fax: (510) 548-0393

Developing CGI's and Plug-Ins for WebSTAR

- The WebSTAR package includes a great deal of information about writing Plug-Ins for WebSTAR using the Mac web server standard **WebSTAR API**. To install the development information, launch the

the WebSTAR Server Suite Installer application, choose **Custom Install**, and then check the box marked **Development Resources**.

- The StarNine Development Services area, which includes links to various tutorials and references:

<http://dev.starnine.com/>

- ClearWay's WebSTAR Plug-In Cookbook:

<http://dev.clearway.com/>

General Information

- Internet Standards

<http://www.starnine.com/development/internetstd.html>

- Apple Email Discussion Lists, especially **Apple-Net-Authoring** and **Apple-Net-Servers**:

<http://www.lists.apple.com/>

- Tips for Mac Webmasters:

<http://mac-web-tips.clearway.com/>

- Providing Internet Services via the Mac OS (book and web site):

<http://www.pism.com>

- Net Professional Magazine web site:

<http://www.netprolive.com/>



For information on the changes in this version, see “New Features in WebSTAR 4” starting on page 69.



The WebSTAR server Suite includes Web, FTP, Mail and Proxy servers. The servers are installed on one computer, and cannot be divided among multiple machines.

This chapter describes the hardware and software requirements for installing WebSTAR Server Suite, the installation procedures, and the files that the installer places on your computer.

SYSTEM REQUIREMENTS

Hardware

WebSTAR Server Suite 4 will run on any PowerPC-based Macintosh computer, from 6100s and clones to G3s and beyond.

For best performance in processor-intensive tasks such as encryption, use a G3 or better. For best response when serving busy sites or serving large files, make sure you have a fast hard drive.

A complete install with all possible options selected will require approximately 50 MB of free disk space. An Easy Install will require approximately 15 MB of free disk space.

System Software

WebSTAR Server Suite 4 requires Mac OS 8.0 or greater, with versions 8.5.1 or 8.6.x recommended.

It is compatible with the Mac OS Extended File Format (HFS Plus).

The server machine must have Open Transport version 1.1.1 or later enabled. If you plan to use IP Multihoming to support several websites, you must run Open Transport 1.3 or greater. You can use Virtual Domains with earlier versions of Open Transport.

Java Virtual Machine

To work with Java Servlets, you must install Apple’s MRJ (Mac OS Runtime for Java) version 2.1.1 or later.

The current MRJ Installer is included on the WebSTAR CD. You can also download it from:

<http://www.apple.com/java/>

Memory Requirements

- The WebSTAR server application uses 10 MB of RAM for its memory partition, when installed with default settings. The minimum is 5 MB (with Core Plug-Ins only).
- The WebSTAR Admin application requires 2.5 MB of RAM for its memory partition.

- If you plan to test your server with clients running on the same machine, you'll need enough RAM to run those applications as well.
- If you plan to run a database or other application, such as FileMaker Pro, on the same machine as the WebSTAR server, be sure the system has enough memory for all applications to run at once.

Suggested Memory Configurations

The default memory partition for WebSTAR is enough for most small to medium server requirements. The WebSTAR server application may require additional memory if you expect a very busy site, or many Proxy or email users.

Plug-Ins share the WebSTAR application's memory allocation. Third-party Plug-Ins often require additional memory as well: be sure to check the documentation before installing them.

Increasing the sizes of the various WebSTAR caches for performance also increases the amount of memory required.

Memory Suggestions

- Small to medium-sized site: 24 MB installed RAM. Of that, 10 MB will be used by the WebSTAR server application.
- Large and busy site: 72 MB installed RAM, depending on other applications running on the same machine. Of that, you may need to allocate 20 to 24 MB to the WebSTAR server application.

Network Requirements

The WebSTAR Server Suite requires a connection to the Internet or to an internal TCP/IP Intranet network.

Direct TCP/IP Internet connections, such as T3, T1, fractional T1, DSL, and cable modems, allow your server to respond very quickly. Dedicated ISDN and 56K connections are also reasonably fast, for smaller sites. A 28.8 bps modem connected via PPP or SLIP will also work, although it is not recommended.

Domain Name Service (DNS) is also required, either from your own DNS server on the local network, or from your ISP. See page 100 for more information.

IP Address

The WebSTAR server must run with a full TCP/IP connection to the Internet (or to a local network, for Intranet use). That means you need to obtain an IP address and configure it in the TCP/IP control panel.



For instructions, see "Server Application Issues" on page 87.



Make sure that your ISP allows you to run a server: cable modem providers in particular may not permit web or mail service.



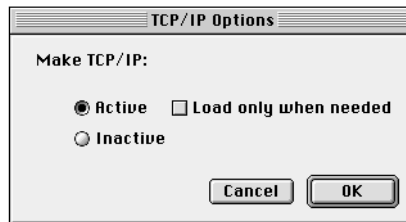
For more information, see "Identifying Your Site: IP, Host Name and DNS" on page 96.

To test WebSTAR without an Internet connection, see "Local Testing With a Temporary IP Address" on page 47.

Keep Open Transport Loaded

For best performance, you should configure Open Transport TCP/IP to remain loaded at all times. When Open Transport is installed, the default is to try to unload the TCP/IP module when not in use, to reduce the system overhead. While this setting may make sense for client machines, on a server machine it is not appropriate. You'll need to change the setting in Open Transport.

- 1 Open the TCP/IP Control Panel.
- 2 From the Edit menu, choose **User Mode**.
- 3 In the User Mode dialog box, click the **Advanced** radio button, then the **OK** button.
- 4 In the TCP/IP control panel, click on the new **Options** button at the lower right corner.
- 5 In the TCP/IP Options dialog, **uncheck** the **Load only when needed** checkbox, and click **OK**.



Be sure to repeat these steps if you move your WebSTAR server application onto a new machine or install a new version of the Mac OS.

Firewall Access

If you are installing WebSTAR within an organization network, and you want to open your server to the Internet, you may need to ask your network administrator to make some “holes” in the firewall for your server and administration ports. For more information, see “Port Numbers” on page 102.

Multiple Domains

WebSTAR Server Suite allows you to serve several Internet hosts and domains, with different names and/or IP addresses, on the same server. You must have your DNS records set up properly so that other servers can find your host: see “DNS” on page 100 for details.

For information on serving multiple web hosts see “Virtual Hosts: Hosting Multiple Web Sites” starting on page 193. For information on serving mail for multiple hosts, see “Mail Hosts” on page 375.

STANDARD NEW INSTALLATION

The Installer creates a new WebSTAR Server Suite folder and automatically places the correct files and folders in that folder.

The **Easy Install** sets up the the Web, FTP, Mail and Proxy servers, the Core WebSTAR Plug-Ins required for these servers, useful default files, and examples for you to use. For information, see “About the Installed Files” on page 40.

The **Custom Install** installs other optional Plug-Ins: for details see “Custom Installation” on page 34.

Active Installer

If you download the WebSTAR Server Suite Installer, you can download the smaller Active Installer version or the full version. The Active Installer contains all necessary files for the Easy Install, and will automatically download other files as needed.

Installing Your WebSTAR Server

- 1 Double-click the Installer application file.
- 2 When the splash screen appears, click the **Continue** button.
- 3 Read the Copyright and License Agreement information, and then click the **Accept** button. If you do not accept the license, you cannot install WebSTAR.
- 4 The Installer will put the WebSTAR Server Suite folder in the root folder of the startup disk by default.

You can specify an alternate location by using the **Select Folder** or disk names popup menu in the “Install Location” area at the lower left. Use this menu or button to choose the location you prefer.



- 5 In most cases, you can use the Easy Install: just click on the **Install** button to install the applications, documentation and examples.



For instructions on **upgrading from an existing WebSTAR system**, see “Upgrading your WebSTAR Server” on page 37.



If you install from the WebSTAR CD, you automatically get the secure Web Server as well: see “Installing SSL” on page 36.

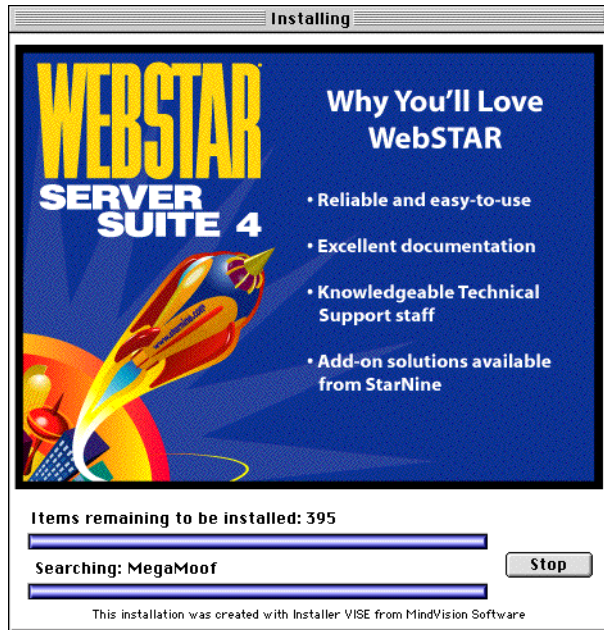


The WebSTAR folder will be installed **inside** the selected disk or folder.



Some Plug-In Modules are not installed by the **Easy Install**. See “Custom Installation” on page 34.

- 6 If you've downloaded the Active Installer, you'll see a message indicating that you can continue to install, or check the StarNine site for updates. If you are connected to the Internet, consider checking for updates; if not, continue installing now.
- 7 You'll see the Installer unpack and install all your files.



Keep your WebSTAR Server Suite Installer handy: you'll need it for extra Plug-Ins and other features.

Allow the Installer to continue until it is entirely finished: there may be pauses in the installation process.

- 8 The Installer will report that it is finished, and allow you to perform more installations or quit.
- 9 When you're done installing, you may want to make an alias to the WebSTAR application and place it in the *Startup Items* folder of the active System folder. This will automatically launch your WebSTAR server when your Mac starts up.



After installing WebSTAR, be sure to read the section "Getting Started" on page 47.

If you have problems with installation, you should check the system requirements, and try installing on another disk or machine. For troubleshooting, see "Server Troubleshooting" on page 106.

The WebSTAR Server Suite 4 Installer will install the Apple update files for Appearance Manager and Navigation Services on Mac OS 8.0 and 8.1. In those cases, it will bring up a Restart dialog. Your WebSTAR server will not work properly until you restart with these extensions enabled.

For newer versions of the Mac OS, you will not have to restart your machine after installation.

CUSTOM INSTALLATION

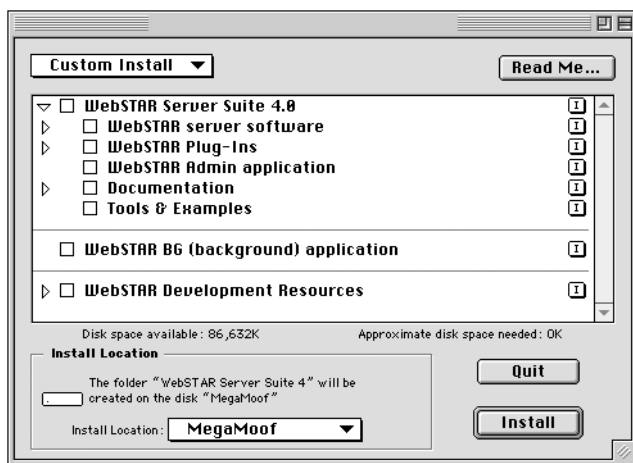
You can use the Custom Install options to choose a subset of the WebSTAR files. You may want to install additional WebSTAR Plug-In modules, the WebSTAR BG background server, the WebSTAR Admin application on remote machines, or to avoid installing documentation on secondary servers, and so on.



If you install a server, the Installer will also include the required support files.

Custom Install

To install, launch the WebSTAR Server Suite Installer and select Custom Install, the item or items you want to install.



Custom Install Location

The new items can be installed directly into your existing *WebSTAR Server Suite 4* folder (if you have not renamed it). To do this, click the **Install Location** popup menu, at the lower left, and choose **Select Folder**. Then choose the folder above the WebSTAR folder. The Installer will place the items you choose in that folder, replacing the older versions.

If you have renamed your WebSTAR folder, the Installer will make a new folder with the name *WebSTAR Server Suite 4* and place all files in that folder.

Custom Install Items



For information on these files, see “About the Installed Files” on page 40.



For information, see “WebSTAR Plug-Ins” starting on page 235 and “WebSTAR Debug Plug-In” on page 107.

■ WebSTAR Server Suite 4

- **WebSTAR server software** installs all the servers together. Additional checkboxes provide options to install the Web, FTP, Mail and Proxy servers separately.

■ WebSTAR Plug-Ins

- **Core Plug-In modules** installs the WebSTAR Plug-In modules Admin, Byte Server, Data Cache, Log Archiver, SSI and Virtual Hosts. If you open this section, you can select these Plug-In modules individually.
- **Extra Plug-in Modules** installs the WebSTAR Plug-In modules Auto BinHex, Directory Index, File Upload, Form Mail, Image Map, JRun Servlet Runner, Lasso Publisher, PowerKey Pro Tickler, QuickDNS Load Balancer, Rebound! Assist, Search, SSI-WebInclude, WebObjects 3 Adaptor, WebObjects 4 Adaptor and WebSTAR Debug. If you open this section, you can select these Plug-In modules individually.
- **WebSTAR Admin**—the WebSTAR Admin application, which can be used on the server machine or remotely.
- **Documentation**—Adobe Acrobat printable version and HTML version of this WebSTAR Technical Reference. If you open this section, you can choose the formats individually.
- **Tools & Examples**—useful applications, example HTML and other files.
- **WebSTAR BG**—background-only version of the server application. For more information, see “WebSTAR Background Server” on page 91. This is not included in the Easy Install.
- **WebSTAR Developer Resources**—WebSTAR API SDK and WebSTAR Developer Toolkit. for writing Plug-Ins and other server add-on programs. These are not included in the Easy Install.

When you click the **Install** button, you'll see the Installer unpack and install all your files. Allow the Installer to continue until it is entirely finished: do not be concerned by pauses in the installation process. The Installer will report that it is finished, and allow you to perform more installations or quit.

If you've installed a new WebSTAR application or WebSTAR BG, you may want to make an alias to it and place it in the *Startup Items* folder of the active System folder. This will automatically launch your WebSTAR server when your Mac starts up.

Active Installer

When you download the WebSTAR Server Suite Installer, you can download the smaller Active Installer version or the full version. The Active Installer may not contain all the files for the Custom Install, although it does have many of them. If you want to install one of the files not included, the Active Installer will automatically log into the StarNine site and download those files.

If you have to work through a proxy server, you can enter the host name at the dialog. Otherwise, leave it blank, and you'll see the download window:



Once the Active Installer downloads the needed files, it continues normally.

INSTALLING SSL

The WebSTAR Server Suite 4 CD will install a Web server with SSL (Secure Sockets Layer encryption) by default. This allows you to accept and serve private information, such as credit cards and personal records, using encryption to protect the data as it flows through the Internet.

Because the U.S. Commerce Department does not allow StarNine to distribute server encryption software online, all Installers you download from the StarNine site will not directly install a version of the server application with SSL support. When you purchase a copy of WebSTAR Server Suite from StarNine, you will receive a CD and can use it to upgrade your downloaded server to the full version with SSL. Just follow the instructions to upgrade your server, and SSL will install automatically.

 For information, see "SSL Web Security" starting on page 209.

 Some third-party Plug-Ins may not support HTTPS and SSL connections. If you have difficulties, contact those developers directly.

If you have WebSTAR/SSL on your machine already, a downloaded Installer will allow you to upgrade the SSL: see below for details.

UPGRADING YOUR WEBSTAR SERVER



For information on the changes in this version, see “New Features in WebSTAR 4” on page 69.

It's easy to upgrade from previous versions of WebSTAR: you will not have to change your site organization or HTML files at all. When you install the new WebSTAR server and WebSTAR Plug-Ins, they will read your old *WebSTAR Settings* file and serve your site exactly as it was before.

The WebSTAR Installer will automatically upgrade your server and WebSTAR Plug-Ins **without** disturbing the HTML files, CGIs, third-party Plug-Ins or other items in your server folder. It will make a new folder on the root level of the hard drive called *WebSTAR (old)* with all the files that have been superseded.

Upgrading SSL Versions of WebSTAR



See also “SSL Web Security” starting on page 209.

When you upgrade from the CD, SSL will automatically install as well. However, installers downloaded over the Internet will only upgrade an existing SSL set-up, and will not add SSL to a non-SSL site. This allows StarNine to distribute the Installer without breaking US export rules.

Combining WebSTAR and WebSTAR/SSL

WebSTAR version 2 and 3 had a separate application for SSL serving. This is no longer necessary, as the WebSTAR Server Suite 4 now includes HTTPS and the SSL security features in the main application. You no longer have to run two applications to provide encryption in your web store or other private space.

- If your previous installation included a **single folder** with both public and private pages, you do not have to make any major changes.
- If your previous installation had **separate folders** for public and private pages, you should consider combining the folders before upgrading. However, you can still run two copies of WebSTAR in separate folders on the same machine, or use Virtual Hosting (see page 193) with separate folders at the same level and unique IP addresses for both standard and SSL serving, so that private data is never accessible without SSL encryption.



For suggestions, see “Additional Privacy Considerations” on page 230.

When running the Installer to upgrade your SSL server, make sure you choose one of the SSL upgrade options, or your version 4 server will not include SSL.

Using the WebSTAR Upgrade Installer

- 1 Quit the WebSTAR server application.
- 2 If you do not have redundant backups, make a copy of your WebSTAR folder onto another disk now.
- 3 Make sure that you have at least 50 MB of free disk space on the working hard disk.
- 4 If you have increased the memory partition to support additional Plug-Ins, make sure you know how much memory to add to the new server. Select the older WebSTAR application and choose **Get Info** from the File Menu. If you are on Mac OS 8.5, choose the Memory item from the Show menu. Your current partition is in the **Preferred Size** field, so write down the difference between it and the **Suggested Size** field number.
- 5 Run the WebSTAR Installer, and click on the popup menu in the upper left corner of the Installer window:

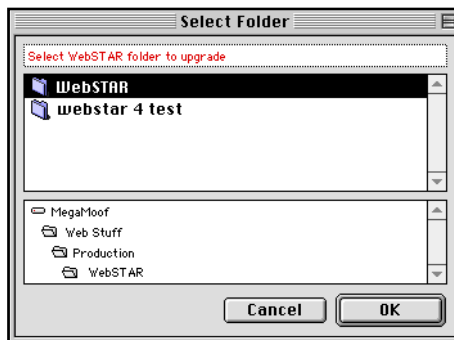


 Ignore the **Install Location** option when upgrading: your server will be upgraded in its current folder.

- If you do **not** have SSL (secure server) or you are installing from the CD:
Choose the **Upgrade** option to bring your server up to version 4.
 - If you **do** have SSL installed and are not installing from the CD:
If you are in the U.S. or Canada and are using 128-bit encryption, choose the **U.S. & Canada** SSL Upgrade option.
If you are in another country and are using 40-bit encryption, choose the **International** SSL Upgrade option.
The SSL installer will display another dialog confirming that you are installing from the CD and upgrading an existing version of WebSTAR SSL.
- 6 If you have downloaded the Active Installer, it may need to retrieve some files from the StarNine site. See "Active Installer" on page 32 for details.

 See "Encryption Levels: US and International" on page 209 for information on Web Server security and U.S. Government export restrictions.

- 7 Next, the Installer will locate all versions of the server on your disk, and let you choose which one to upgrade:



- 8 When you click **OK**, you'll see the Installer unpack and install all your files.
- 9 Allow the Installer to continue until it is entirely finished: do not be concerned by pauses in the installation process.
- 10 The Installer will report that it is finished, and allow you to perform more installations or quit.

The Installer has moved your old server files to a *WebSTAR (old)* folder on the root level of your disk.

- 11 Check your Plug-Ins folder: all the WebSTAR Plug-Ins will be replaced by new versions, and all other old files, including *SSI Settings* for counters, should still be there.

- WebSTAR QuickSend has been replaced by WebSTAR Form Mail: be sure to change any forms that use this Plug-In.
- If you have WebSTAR WebObjects Adaptor installed, it will be upgraded to WebSTAR WebObjects 3 Adaptor (compatible with WebObjects version 3). You can also install WebSTAR WebObjects 4 Adaptor (compatible with WebObjects version 4) using the Custom Install options. Future installers will automatically upgrade these Plug-Ins separately.

- 12 If you have any aliases to the old server, such as in the *Startup* folder, you must be sure to **delete** them and create new ones pointed at the new server. Your old server has not been deleted, so you could easily launch it by accident.

- 13 If you increased the memory allocation on the older WebSTAR server, add that amount of memory to the new one as well.

- 14 Double-click the new WebSTAR server application to launch it, and use a browser to visit your site and test all your pages and add-ons.



See "Server Application Issues" on page 87 for directions and information on memory usage. For more information about the installed files, see below.



- 15** If you are upgrading a WebSTAR/SSL server, the first time you launch the new server, it will recognize the old Certificate format and update it to the new format.

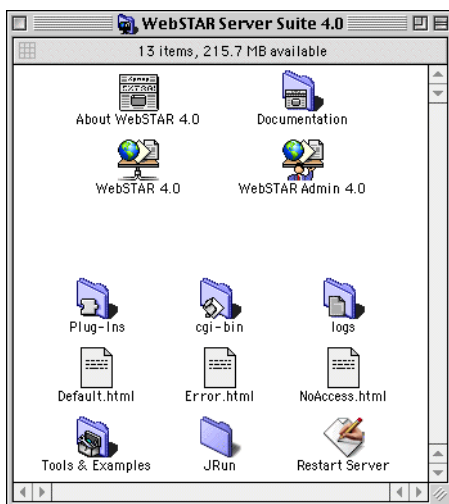
Although we have made every effort to retain compatibility with earlier versions of third-party CGIs and Plug-Ins, it is possible that some may no longer work. You should test all your add-on programs to make sure that they are compatible, and contact the developers if you notice additional problems.

ABOUT THE INSTALLED FILES

The WebSTAR folder contains the WebSTAR applications, WebSTAR Plug-Ins, default files, examples, and more. You'll add HTML and other files to this folder to serve web and FTP data.



See also: "Important WebSTAR Files" starting on page 103.



WebSTAR 4

This is the main **server application**. It serves web pages, runs the Plug-In modules, displays the status of your server, and provides an interface for the Administration Password and your WebSTAR Serial Number. The WebSTAR application does the actual serving, while the WebSTAR Admin application allows you to configure the server.

WebSTAR Admin

This application provides an **administration interface** for you to change the settings for your Web, Mail, FTP and Proxy servers, and to



See "WebSTAR Server & Troubleshooting" on page 77.



See also: “About the WebSTAR Admin Application” on page 113 and for web-specific instructions, “Web Server Administration” on page 129.

monitor the status of your servers. It does not have to be running at all times: you can launch it when you need to make changes, then quit when you’re done.

WebSTAR Admin communicates with the WebSTAR server application via TCP/IP, so you can run it on **any** Macintosh system that has access to the Internet. The password and encrypted communications mean that no one else can access your server.

To install the WebSTAR Admin application on a remote machine, use the **Custom Install** option in the WebSTAR Installer.

About WebSTAR 4

This file contains release information and last-minute changes that you should know about.

HTML files

The Installer automatically places these useful HTML files in your WebSTAR web server’s default root folder. You should change them to include information about your server in particular.

Default.html is a temporary starter web page, which appears when a browser contacts your site. You’ll want to replace this shortly, following the instructions in “Default Page” on page 65. To change the default index name, see “Index File Name” on page 131.

Error.html is an HTML page with a brief message that appears when there’s a request for data that can’t be served. For more information, see “Error File Path” on page 131.

NoAccess.html is the page displayed when a browser can’t connect to the server, because that host is denied access to the entire site using the “Global” option. For more information see “No Access File Path” on page 132.

Plug-Ins folder

WebSTAR Plug-Ins are modules which provide functionality to the WebSTAR server. Many WebSTAR features, including the Mail, FTP and Proxy servers, are implemented as Plug-Ins.

The WebSTAR server will find **only** those Plug-Ins in the *Plug-Ins* folder, or a subfolder within that folder. Do not move the files or rename the folder. Some Plug-Ins have Extensions and Data folders, storing

additional data used by that Plug-In. Do **not** delete or remove these folders unless you are deleting the associated Plug-In.

There are many third-party Plug-Ins available to extend your server: for more information, see the StarNine Store at store.starnine.com and the Extending WebSTAR Pages at

www.starnine.com/extendingwebstar.html

Mail, FTP, and Proxy Server Plug-Ins

The WebSTAR Plug-In architecture is so powerful that the Mail, FTP and Proxy servers are implemented as Plug-Ins. If you do not intend to use these features of WebSTAR, you can remove them from the *Plug-Ins* folder and they will not be loaded.

- *WebSTAR Mail* and the *WebSTAR Mail Data* folder (described starting at page 357).
- *WebSTAR FTP* and the *WebSTAR FTP Data folder* (described starting at page 247).
- *WebSTAR Proxy* and the *WebSTAR Proxy Extensions* folder (described starting at page 411).

Core WebSTAR Plug-Ins

The **Core Plug-Ins**, listed below, are important for WebSTAR—you should not remove them.

- *WebSTAR Admin* (used by the WebSTAR Admin application and the Browser admin), also has a *WebSTAR Admin Data* folder which stores the data required for the Browser Admin.
- *WebSTAR Byte Server*, used for HTTP 1.1 byte-range serving, most notably of Adobe Acrobat's PDF pages.
- *WebSTAR Data Cache*, used by the web server and many different Plug-Ins to improve Web server responsiveness.
- *WebSTAR Log Archiver*, used by all the servers to schedule and save log archive files.
- *WebSTAR SSI*, required by the Browser Admin and used by several third-party Plug-Ins.
- *WebSTAR Virtual Hosts*, required for virtual domains, IP multihoming and processing multiple index file names.

Additional WebSTAR Plug-Ins

The other WebSTAR Plug-Ins provide additional functionality to the web server. These are not required by the web server and are not installed by default: you must install them separately (see “Custom Installation” on page 34).



If you ever need to re-install the WebSTAR Plug-Ins, use the WebSTAR Installer.



For information on Plug-Ins, see “WebSTAR Plug-Ins” starting on page 235.

- *WebSTAR Auto BinHex*
- *WebSTAR Directory Indexer*
- *WebSTAR File Upload*
- *WebSTAR Form Mail*
- *WebSTAR JRun Servlet Runner*.
- *WebSTAR Lasso Publisher* and the *WebSTAR Lasso Publisher Data* folder.
- *WebSTAR Search*, the *Search Indexer* application, and the *WebSTAR Search Data* folder, containing Search Dictionaries.
- *WebSTAR SSI -WebInclude*
- *WebSTAR WebObjects Adaptor* (version 3 or 4) and the *WebSTAR WebObjects Adaptor Data* folder, storing the WebObjects configuration file.

Other Plug-In files provide support for third-party products:

- *PowerKey Pro Tickler* and *Rebound! Assist* work with the automated restart hardware from Sophisticated Circuits.
- *QuickDNS Load Balancer* works with the QuickDNS server from Men & Mice.

CGI-BIN folder

CGIs (Common Gateway Interface scripts) are another way to extend the power and flexibility of your WebSTAR web server. The *cgi-bin* folder is a standard place to store CGIs, so do **not** rename this folder. CGIs may be stored in other folders as well. WebSTAR includes several example CGIs in the *Tools & Examples* folder.

JRun Folder

The WebSTAR JRun Servlet Runner allows WebSTAR to support JavaSoft's Java Servlet API. For more information, see page 255 and "Developing Java Servlets for WebSTAR" on page 464.

Documentation folder

The *Documentation* folder contains WebSTAR's documentation, including this manual, in Adobe Acrobat (PDF) format for printing, and HTML format for online viewing using your favorite web browser.

Restart Server Application

The Restart Server Application is automatically launched when WebSTAR receives certain TCP/IP errors or settings are changed. For



You can use WebSTAR Search to index the WebSTAR HTML manual and search it locally.

information on this program, see “Restarting After Open Transport Errors” on page 90.

Tools & Examples Folder

This folder contains helpful tools, example files and instructions for using WebSTAR and writing extensions to it. If you have trouble accessing this folder in your browser, encode the space and ampersand for HTTP, like this:

`http://www.domain.com/Tools%20%26%20Examples/tools_and_examples.html`

(be sure to change "www.domain.com" to your server's host name)

Files

- *tools_and_examples.html* links to some of the example files in this folder.
- *Make Redirect File* is a tool for making files that redirect from one URL to another. For information, see “Redirect Files” on page 191.

Folders

- *Mail Tools* includes a *Mailbox Extraction Tool* which copies account messages from the AIMS and EIMS server programs to WebSTAR Mail. For more information, see “Import User Mailboxes” on page 396.
- *SSL Tools* includes two programs for creating SSL keys and certificates. For more information, see “Installing & Configuring SSL” starting on page 213.
- *AppleScript CGI* folder includes source code and information about CGI add-ons for the web server. For more information, see the instructions in the folder and “Developing CGIs” on page 445.
- *File Upload* folder contains HTML example pages for WebSTAR File Upload (described on page 247).
- *Form Mail* folder contains HTML example pages for the form-sending Plug-In, WebSTAR Form Mail (described on page 249).
- *Image Map* folder contains example files for server-side image maps for the WebSTAR Image Map (described on page 253).
- *Lasso Instant Publishing* contains HTML and graphics files for the WebSTAR Lasso Publisher (described on page 307).
- The *Search Examples* folder provides example pages and files to help you use WebSTAR Search. You must index the test collection before using the search examples. For more information, see “WebSTAR Search” on page 261.

- *SSI Demo* demonstrates the powerful features of WebSTAR SSI (described on page 275).
- *SSI-WebInclude* shows how to include the contents of a remote page within a web page using WebSTAR SSI-WebInclude (described on page 299).

Other Files

WebSTAR Mailing Lists File

This file, automatically installed on your desktop, contains a link to the sign-up page for the StarNine email-based discussion lists, including WebSTAR-Talk. If you have any questions about using WebSTAR or related CGIs and Plug-Ins, the WebSTAR-Talk list, and its associated archive of messages, is a great resource for you.

IP Secondary Addresses

This file, installed in the *System Folder, Preferences* folder, is used for a particular form of virtual hosting: see “IP Multihoming: Special Configuration” on page 195 for details. If a file with this name already exists, the WebSTAR Server Suite Installer will not replace it.

Extensions for Mac OS 8.0 and 8.1

WebSTAR will install the Apple update files for Appearance Manager and Navigation Services on Mac OS 8.0 and 8.1.

This chapter covers the basics you need to know to start your server. It will help you launch the server, and access it for the first time via a browser, an FTP client and send some email. In addition, we'll give you a little background on setting up a web site, default pages, and server folder hierarchy.

STARTING THE WEBSTAR SERVER SUITE

Before starting up, make sure that your machine has access to the Internet, and has a static IP address so other machines can see it. If you're not sure about your IP address, look in your TCP/IP Control Panel, and write down the address you see there. If you find a number, skip to "Try Out Your Server" on page 50, otherwise, follow these instructions for testing.



See also: "Identifying Your Site: IP, Host Name and DNS" on page 96.

Local Testing With a Temporary IP Address

If you have a machine that is not currently on the Internet and want to try out WebSTAR, you can follow these instructions. Your server machine and any clients on your local network must already have TCP installed. No one on the larger Internet can see your server until you get a static IP address, but you can test your server.

Setting the Temporary IP Address

- 1 Open the TCP/IP control panel.

If there's an IP address entered, **stop**. Try out your server as described on page 48. Only if that doesn't work should you try the temporary address (and be sure to save the previous address in the Note Pad or other convenient place).

- 2 Select **Configurations** from the File menu and make a new configuration. This will allow you to switch back to your normal system when you're done testing.

You may have to select **User Options** from the Edit menu to enable **Advanced Mode**, to enable the Configurations command.

- 3 If you are using a local AppleTalk network or a single computer, set:

- **Connect via** to App leTa lk (MacIP)
- **Configure** to USING MacIP Manually
- If necessary, click the **Select Zone** button and select the local AppleTalk zone.

All other fields can be blank.

- 4 If you are using an Ethernet network, set:

- **Connect via** to Ethernet

- **Configure** to Manually
- **Subnet mask** to 255.255.255.0.

All other fields can be blank.

- 5 Enter the **test IP address**: 192.168.0.2, and save your changes.
- 6 Double-click to launch WebSTAR. You'll know the test address is working, because the server application will not launch unless there's a working IP address. See below for more details.
- 7 Use a browser on this machine to try accessing the server using the test IP address 192.168.0.2, by entering this number as a URL.

Client Temporary IP Addresses

If you have a network with TCP connectivity, but without access to the Internet, configure all clients to use the same connection method (LocalTalk/AppleTalk or Ethernet). Make sure they have different IP addresses, higher than the server, such as 192.168.0.3 and 192.168.0.4.

Then launch a web browser, and give it the test IP address of the web server to access the default page on your WebSTAR server.

Start Your Server

To start the WebSTAR server, double-click the WebSTAR application. You'll see the WebSTAR splash screen with the status area at the lower left side. This shows what is loading, and can be useful for troubleshooting. If it launches correctly, go on to "WebSTAR Serial Number".



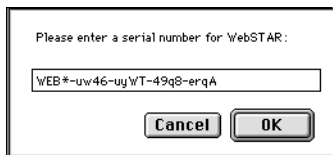
If you have any trouble launching the server, see "Server Troubleshooting" starting on page 106.

WebSTAR Serial Number

Because this is first time you are using WebSTAR, you are prompted to enter your serial number:



See also "Serial Numbers" on page 84.



This number is included in your WebSTAR package, or in some cases sent from StarNine via email. The number must be a WebSTAR 4 Serial Number: serial numbers for older versions will not work.

Type your serial number: be sure to enter the number exactly as you see it on the serial number sheet or message, with dashes, capital



To avoid losing your serial number, write it in your WebSTAR manual. You can also save it in a clipping file or on your Mac's Note Pad.

letters, numbers and no spaces. You can also paste your serial number into this field. Then click **OK**. If you make a mistake in typing, WebSTAR will show you an error message and let you try again.

Temporary Serial Number

You can request a temporary evaluation serial number from StarNine to test WebSTAR: these last approximately one month. Send email to info@starnine.com for more information.

Testing Without a Serial Number

For a very short test, you can press **Cancel** in the serial number dialog. You'll see a dialog with a simple math problem: if you answer the problem correctly, WebSTAR will work for two hours, and for a limited number of connections.

Admin Password

Your next step is to enter a password for the WebSTAR Admin program. This allows you to configure WebSTAR using the Admin program from any Mac on the Internet.

If you don't see a password dialog, choose **Admin Password** from the Edit menu to enter the password. Create a password you can remember but no one else will guess.

More About WebSTAR

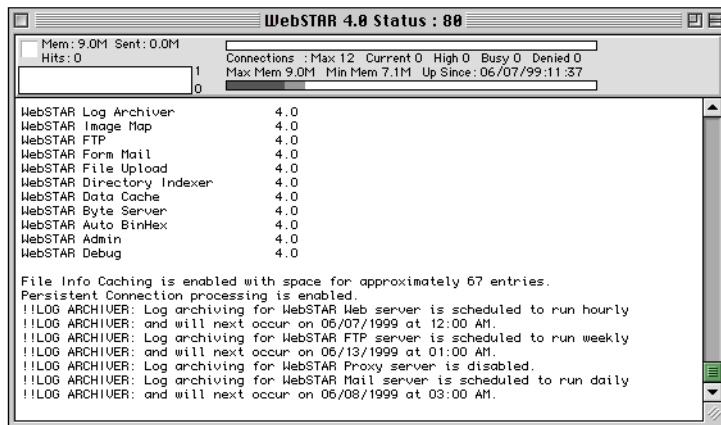
When WebSTAR starts up as installed, you'll see four windows: the Status window with the Web monitor, the FTP monitor window, the



For password guidelines, see "Safe Passwords" on page 96.

CHAPTER 3: GETTING STARTED

Mail window and the Proxy monitor window. The Status window is the most important:



For more information, see “WebSTAR Status and Monitor Windows” on page 77.

The Status window will display information about the number of connections and the amount of data served. The same window includes a log of web activity, with information about each HTTP request and the results. The separate FTP, Mail, and Proxy monitors each show a log of activity on those servers.

You can use the WebSTAR menus to open and close the windows, update the serial number and Admin password, control the server, and view Plug-In module status windows. For more information, see “WebSTAR Server Menus” on page 83.

TRY OUT YOUR SERVER

Now that you have your WebSTAR server running, you need to use client applications to try it out. A **client** is simply an application that requests data from a server: web browsers can be clients for Web (HTTP/HTTPS), FTP and Proxy servers and their message components can be clients of the Mail server. WebSTAR is compatible with browsers on all platforms. There are also stand-alone FTP clients (such as Anarchie and Fetch on the Macintosh), and email clients (such as Eudora, Mailsmith and Emailer): your server should be compatible with clients on Mac, Windows, Unix and other platforms.

WebSTAR comes with a simple set of web pages, so you can try out your server right away. Once you’ve tested it, you’ll want to set up your own Web pages and files, and let other people try it out. You can



WebSTAR is compatible with all Web browsers, FTP clients, and email programs which follow the Internet standards.

test on the server machine, or using any machine that has access to your server machine.

If you don't know the name or IP address of your server, open the TCP/IP control panel. If you see an active field labeled "IP Address", write down that number. You can also ask your Network Administrator about the host name.

If you do not have an IP address, see "Local Testing With a Temporary IP Address" on page 47 before connecting.

Connect To Your Web Server

- 1 Launch your web browser software.

If you run your test on the server machine, expect some delays in communication. The system is designed to work across the network, rather than talking to itself.

- 2 Use the **Open URL** or **Open Location** menu command or the Location field, and enter your host name like this:

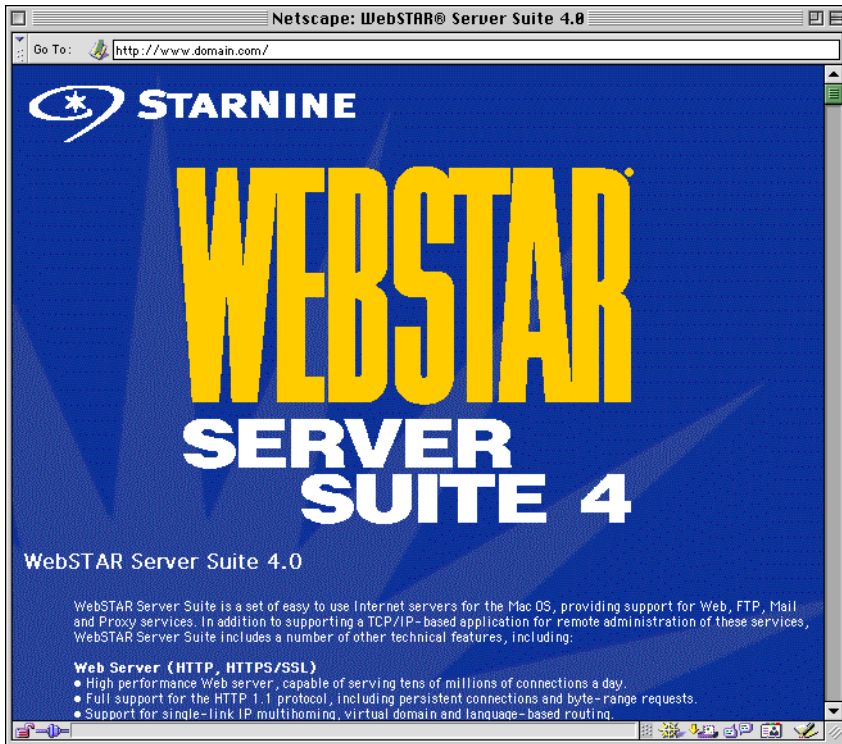
`http://www.domain.com/`

but be sure to replace "www.domain.com" with the host name or IP address of your WebSTAR server,



If you don't have a static IP address, see "Local Testing With a Temporary IP Address" on page 47.

- 3 You'll see the default page that WebSTAR installs for you:



- 4 Check the Status window on the WebSTAR Server: you should see an entry for the HTTP request for the default page.

Browse the Documentation

When you first access your server, you'll see the default home page, which describes how to access other sites and the WebSTAR documentation. Go ahead and open the WebSTAR manual. It includes this book, additional materials and links to the StarNine web site. We hope you'll find it useful as you work with your server.

ADMINISTERING WEBSTAR

About the WebSTAR Admin Application

The WebSTAR Admin application allows you to monitor and configure your WebSTAR Server. You can use this application on any PowerPC Mac with access to the Internet. The data communications between

i If you have trouble accessing the server, you can still read the HTML documentation in your browser software. Use the "Open File" command to open the *manual.html* file in the *Documentation* folder locally. .



For more information, see “Web Server Administration” starting on page 129.

the WebSTAR Admin and the WebSTAR server are encrypted, so access is secure.

You can also administer some of the server functions, and all the Plug-Ins, from a browser on any machine connected to the Internet. For more information, see “Accessing the Browser Admin Pages” on page 55.

Connecting with WebSTAR Admin

- 1 Launch the WebSTAR Admin application.

You'll see the New Connection dialog:

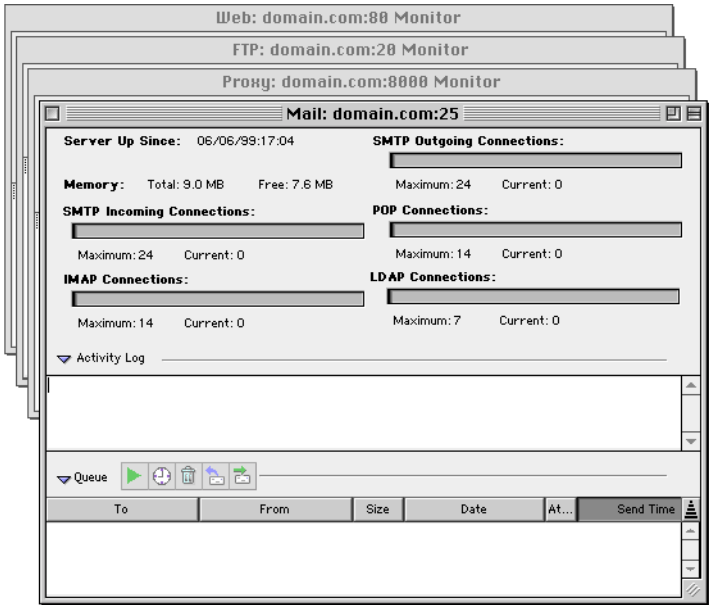
The screenshot shows a 'New Connection' dialog box. It has a title bar with the text 'New Connection'. Inside the dialog, there are three input fields: 'IP/Domain Name:' with a dropdown menu showing 'domain.com', 'Port:' with a text box containing '80', and 'Password:' with an empty text box. Below the password field is a checkbox labeled 'Save Password' which is unchecked. At the bottom right are two buttons: 'Cancel' and 'Connect'.

- 2 Type in your host name or IP address, leave the port number at 80, and enter the password. This is the password that you set in the WebSTAR Server: if you didn't set it before, see “Admin Password” on page 49.

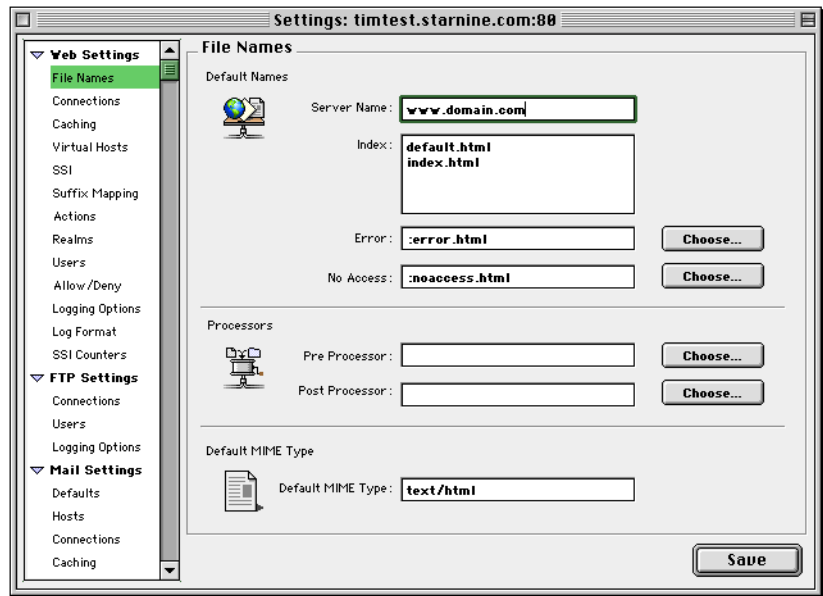
- 3 You'll see the Web, FTP, Mail and Proxy Monitor windows. They will display log information about what's happening on your server, with an entry for each client request.



See also: "Admin Monitor Windows" on page 116.



- 4 Choose **Server Settings** from the Edit menu to see the WebSTAR Admin Settings Window.



- 5 Type your server's host name into the Server Name field. This is used to resolve certain URLs and is checked by the FTP server.
- 6 Click **Save** to send the information back to the server.

There are a lot of options here for tuning your web server, setting up Virtual Hosts, defining Security Realms, and configuring Log Formats. For detailed instructions, see “Web Server Administration” starting on page 129. You can also configure the WebSTAR FTP Server (described on page 337), the WebSTAR Mail Settings (described on page 373) and the WebSTAR Proxy Server (described on page 411)

Accessing the Browser Admin Pages

The browser admin pages allow you to use any web browser, on any system on the Internet, to administer many of the functions and Plug-ins on your server. The browser admin pages are protected by a WebSTAR **security realm**, so that no one else can change your settings. You'll need to create a password to access these pages.

Setting the Browser Admin Password

When you install WebSTAR for the first time, the default administration security realm, **ADMINISTRATION** is already set up. This limits access



See also: “Security Realms” on page 164.

to the Browser Admin pages, so no one else can change your server settings. You must add a user name and password, so that you can use the Browser Admin.

- 1 Launch the WebSTAR Admin application and connect to your server, as described above.
- 2 Bring up the settings window by choosing **Server Settings** from the Edit menu.
- 3 Select the **Users** option from the list at the left, to see the User Name and Password list.
- 4 Click on the **New** button to make a new entry.
- 5 Enter a User Name and Password for browser administration. Make sure to keep the name shorter than 16 letters. For security information, see “Safe Passwords” on page 96.
- 6 The realm on the popup **Realms** menu on the lower left should be **ADMINISTRATION**. If it's not, click on the menu and select that Realm.



See also: “Web Users and Passwords” on page 168.

User Name	Realm	Password
tim	administration	Hc19x

Users: 1 User Selected: 1

User Name: Password:

Realm: ☒ ADMINISTRATION
☐ LOGS

- 7 Click the **Save** button to send the new entry back to the server.

Using the Browser Admin Pages

From your web browser, enter the browser admin URL, which is your server's name followed by “pi_admin.admin”, for example:

`http://www.domain.com/pi_admin.admin`

Now enter the Administration User Name and Password for access. You'll be able to administer many of the server features, as well as

many Plug-Ins using this interface. You may want to bookmark the page for future reference.

If you use a specific machine or group of machines to do your administration, you can set up an “Allow” entry for this realm to avoid the password. Follow the instructions in the section “Allow/Deny” on page 172.



See also: “WebSTAR FTP Server” on page 337 and “WebSTAR FTP Trouble-shooting” on page 355.



Anonymous users don't have a password. They usually send their email address as their password.

CONNECT TO YOUR FTP SERVER

Once you've connected to the web server, connecting to the FTP server is quite easy. WebSTAR FTP always “listens” for FTP requests, but will not respond until you create FTP Users and specify the root folder.

Creating an FTP User Entry

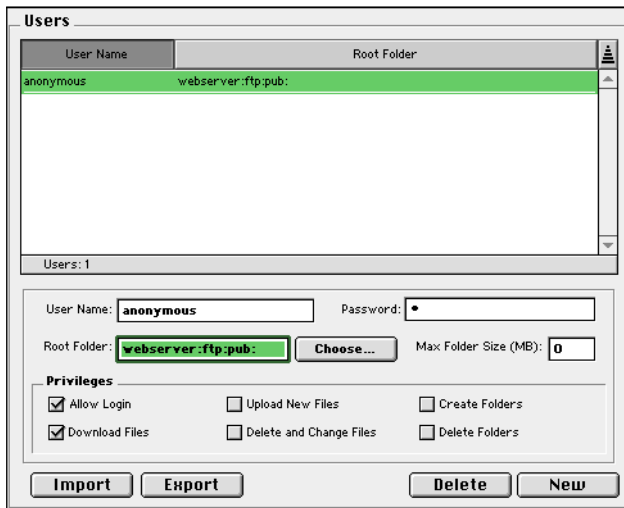
- 1 On the server machine, create a folder named *pub* (this is a common FTP name for a publications or public folder). For convenience, you can create it in your *WebSTAR* folder.
- 2 Put a temporary test file in your *pub* folder.
- 3 Launch the WebSTAR Admin application and connect to your server, as above.
- 4 Bring up the settings window by choosing **Server Settings** from the Edit menu.
- 5 Choose the FTP Settings section, and the **FTP Users** item.
- 6 Click the **New** button to create a new user.
- 7 Set the User Name to anonymous, and enter * in the Password field.
- 8 Use the **Choose** button to set the root folder for this user to the *pub* folder.

Notice that the path for the root folder starts at the name of the hard drive, and includes the entire folder hierarchy getting to your folder. The FTP server always requires full path names, although the user can only see their root folder and any subfolders.

- 9 In the **Access Controls** options at the bottom of the panel, notice that the checkboxes are all checked. Uncheck all the options except for **Allow Login** and **Download Files**.



Be careful in allowing uploads—some users may abuse the privilege.



- 10 Click the **Save** button at the bottom right of the window to send your changes back to the server.

Testing Your FTP Server

- 1 Open your favorite FTP client, or web browser with FTP client functions.
- 2 Type the URL with the FTP prefix, like this:

`ftp://www.domain.com/`

but be sure to replace “www.domain.com” with the host name or IP address of your server.

- 3 If you are using an FTP, leave the name and password blank.
- 4 You'll see a listing of the *pub* folder, with your test file in it.

When you look at the FTP Monitor Window, you'll see a log of that FTP request from your test machine.

WebSTAR's FTP server lets you create user names, passwords and disk folders for FTP access. For more information, see “WebSTAR FTP Server” starting on page 337.

Now you can try out your Mail server or skip to “Connect to Your Proxy Server” on page 63. If you are interested in Web serving primarily, go to “Setting Up Your Web Site” on page 64.

START YOUR MAIL SERVER



Your DNS entry must be set up for mail service: see “DNS” on page 100 for details.

To use your WebSTAR Mail server, you must give it the host name and create at least one email account. For much more detailed information, including background on what it means to act as a mail administrator, see “WebSTAR Mail Server Overview” on page 357 and the following chapters.

Setting the Mail Host Name

- 1 Launch the WebSTAR Admin application and connect to your server.
- 2 Bring up the settings window by choosing **Server Settings** from the Edit menu.
- 3 Select the **Hosts** option from the **Mail Settings** section in list at the left.
- 4 Click on the **New** button to make a new entry.
- 5 Type this server's host name in the Host Name field.
- 6 Type your email address in the Unknown Address field. Messages for names without user entries will go to this address, so it's a way to catch problems rather than missing them. You can change this address later.



For more information on these fields, see “Mail Hosts” starting on page 375.

Host Name	Unknown Address	C...	Redirect To
domain.com	postmaster@example.com		

Action: 1 1

Host Name: Unknown Address:

Copy To: Redirect To:

- 7 Click on the **Save** button to send the information back to the server.

Creating a Mail User Account

To conform to Internet conventions, you should always have a Postmaster account. If anyone has an urgent need to contact someone in your domain, they are likely to send a message to this account. For

more information, see “Reading the Postmaster Messages” on page 367.

- 1 In the WebSTAR Admin application, choose the **Users & Accounts** item.
- 2 Type in a **User Name**, such as Postmaster. You will use this to log in from your email client program.
- 3 Type in a **Password**.
- 4 Type in the public email name in the **E-Mail** field: this is the part before the @ in the email address. If you want to set up the Postmaster account, just type postmaster here.
- 5 The **Host** popup menu lets you select a specific email host and domain name. The default, **Any**, will accept mail for this user name at any of the hosts served by this machine. For example, you could have one Postmaster entry for all hosts.

Account ID	E-mail	Storage	APOP	Messages
Postmaster	postmaster	0	false	0

Accounts 1

Account ID: Password:

E-mail Name: Host: Message Limit:

Forward To: Storage Limit (K): ☐ Require APOP

IMAP Privileges

☐ Create Mailboxes ☐ Delete Mailboxes ☐ Rename Mailboxes



For more information on the fields and options, see “Mail Users & Accounts” starting on page 391.

- 6 Ignore the other settings: the default values will work fine.
- 7 Click on **Save** to send the settings to the server.

Log Into Your Email Account

The easiest way to test your email is to use the Web Mail option.

- 1 Type a URL into your browser's location field that ends in .mail, such as
`http://www.domain.com/web.mail`
(replacing “domain.com” with your web host name).
- 2 You'll see a simple login screen. Type the User Name and Password that you created above.

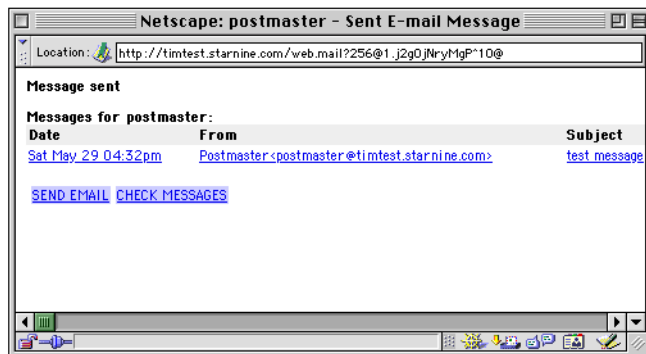
- 3 You'll see the main page for web mail, but you have no messages yet, so it's pretty empty.



- 4 Click on the **SEND EMAIL** link to create a new message, address it to yourself, and send it. Be sure to send it to the postmaster account at your host name, for example "postmaster@mail.domain.com".
- 5 If you look at the Mail Monitor on the server or the WebSTAR Admin, you'll see some messages indicating that the message was sent, and then received.
- 6 You'll see the message from yourself waiting in the mailbox.



For more information on the Mail server log entries, see "Activity Log" on page 400.



Allow Email Clients to Send Messages



See also "Dealing With Spam (Unsolicited Email)" on page 370.

As shipped, WebSTAR Mail only allows the Web Mail to use the server to send messages. This protects your server from being used by "spammers" to send their unsolicited messages to thousands of people.

However, you probably want to allow users to send messages from their email client programs, such as Eudora and Netscape Messenger. You can allow the server to send messages based on when they logged in and read messages.

- 1 Open the WebSTAR Admin and choose the Mail Server Connections item in the list at the left.
- 2 If it's not already checked, click on the checkbox **Enable SMTP Forwarding**.

This allows people to send email using this server as their SMTP server.

- 3 Click on the checkbox **Require prior client login**, and type a small number, such as 10, into the **minutes** field.

This protects you from the case where users share machine IP addresses when they use dialup accounts, and a spammer might be able to send messages through your server from the same machine after your user has closed their modem connection.
- 4 Click the **Save** button.

Now users will be able to send messages via the WebSTAR Mail SMTP server. However, they will get a “we do not relay” error if they send messages more than 10 minutes after checking their mail. You can increase that interval if your users prefer to send mail without checking every 10 minutes, and you are comfortable with the risk.

Protect Your User Directory

Before continuing, you should limit access to your LDAP server, which provides a directory of the server user names and email addresses. Unfortunately, spammers could access this directory to harvest addresses and send unsolicited messages to your users.

- 1 Open the WebSTAR Admin and choose the Mail Server **Allow/Deny** item in the list at the left.
- 2 Select **LDAP** from the Services menu in the upper left corner.
- 3 Click the **New** button to make a new entry.
- 4 Select the **Allow** radio button on the left side.
- 5 Type your domain name in the Address field, with a star to allow all hosts in the domain:

*.domain.com

All other domains are now denied access to the LDAP Server. Creating one or more “Allow” entries automatically denies all non-allowed domains.

- 6 Click the **Save** button to send the information back to the server.
- 7 To test the LDAP server and the security, go to your client, such as the Eudora email application or the Netscape or Microsoft browsers.

You will need to add a link to the WebSTAR LDAP Server: for example, in Netscape Communicator 4, open the Address Book and choose **New Directory** from the File menu. Just give your LDAP server a name, and

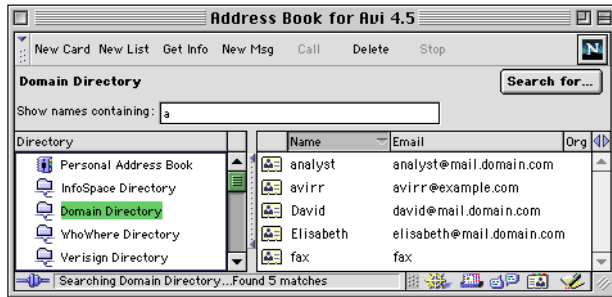


Set the login time delay by balancing security considerations against convenience. See also “Relay Restrictions and Spam Prevention” on page 380.



See also “LDAP” on page 360 and “Mail Allow/Deny” on page 387.

enter your server host name, and you'll be able to select it in the Address Book window:



- 8 Go to another machine, outside your domain, and try it again. You should get an error that the LDAP server will not respond. This protects your directory from outsiders.

CONNECT TO YOUR PROXY SERVER

WebSTAR Proxy is a caching HTTP server that runs as a Plug-In to WebSTAR. Unlike a regular web server, a proxy server is intended to reduce bandwidth consumption and improve Net access speed for users within your organization. Your users can receive all HTTP traffic via WebSTAR Proxy (by configuring the proxy settings in their browsers). When they request a URL on the Internet, their connection is actually to WebSTAR Proxy, which then retrieves the page from the target server and relays it to your user. Proxy also improves security by only requiring one IP address on your network to have HTTP access to the outside world (keeping firewall administration simple), and allows you to restrict access from your internal machines to certain sites and locations on the net. WebSTAR Proxy is particularly useful for schools and small- to medium-sized businesses.

The WebSTAR Proxy Server caches web pages in RAM. This means that the first time a page is requested by a user, it is stored in cache, and relayed to the user. On subsequent requests of the same page from any user, WebSTAR Proxy simply retrieves the page out of its local cache, and passes it to the user. These repeat transactions are faster because they take place on your own network instead of going out on the Internet. This is especially helpful if you have a crowded or slow network connection.



See also: "WebSTAR Proxy Server" on page 411.

You can try out your Proxy server right away., as long as it's installed in your *Plug-Ins* folder. You'll need access to some other machines on your network to test this feature.

- 1 On another machine, open the web browser, and find the proxy panel in the "Preferences" or "Options" window.

Set the HTTP Proxy option to use the host name or IP address of your WebSTAR server, using the default port, 8000.

- 2 Repeat the previous step on a another machine (Mac or any other OS).
- 3 Have each machine access a site with a lot of graphics, such as www.starnine.com.

There's not much to see: the first machine will get the page in the normal time, but all other browsers configured to use the Proxy Server will get the same page much more quickly.

SETTING UP YOUR WEB SITE

The purpose of a web server is to respond to browser requests and display information. WebSTAR has some structures and shortcuts to make that easier for you.

URLs, HTTP and Your Web Server

If you are new to web serving, read the following notes on how the browser and the server are communicating. Otherwise, skip to "Default Page" on page 65.

URL (Universal Resource Locator) messages are the basis for the transactions between the client (the browser) and the web server (WebSTAR). When someone enters a URL for data on your site, your browser sends an **HTTP** (HyperText Transfer Protocol) request to your computer, which is received by WebSTAR.

If you just ask for the site, WebSTAR knows to serve the *default.html* file from the default host root folder (in this case, the same folder as the WebSTAR server application).

Behind the scenes

In this example URL, we can see how the browser and the server work together to show you a useful file:

http://www.starnine.com/webstar/webstar.html			
protocol	host name	folder	file name



See also: "Web Serving and HTTP" starting on page 179.



For information on suffixes, see “Suffix Mapping” on page 154.

- 1 **http://** tells the browser what **protocol** to use (other protocols for URLs include “ftp” and “gopher”).
- 2 **www.starnine.com** is the server host name. The browser will look up the host name in the DNS system, find the IP address and contact the machine with that address directly.
- 3 **/webstar/** is the folder name. You can have a deep hierarchy of folders, such as “/webstar/new/test/”.
- 4 **webstar.html** is the file name.

When a URL like this comes in, WebSTAR first looks at the suffix of the file being requested. In the default configuration, WebSTAR itself handles all files which end in “.html”. Your server looks for the file and, if it exists, returns it to the browser. If a file of that name doesn’t exist at that location, WebSTAR will return an error message to the browser.

For a more detailed explanation of this process, see “WebSTAR URL Processing” on page 180.



The WebSTAR default page has useful links to the manual and examples. To keep it as a reference, make a copy.

Default Page

When a browser contacts your website without requesting a specific file, the server will return a page with a special name: the **default index file name** (also known as the **default page**). The name is set to default.html when WebSTAR is installed.

The first thing you’re likely to do on your website is create your own default page: the front door that the world will see.

If you’re new to the web, you can simply take the *default.html* file that comes with WebSTAR and change it in an HTML editor such as Adobe GoLive CyberStudio, Claris HomePage, Macromedia Dreamweaver, or Bare Bones’ BBEdit.

If you already have a website somewhere else, you can move it to your WebSTAR folder. Replace *default.html* with your home page, and prepare to update the links to your other pages. For more information, see “Moving a Web Site to WebSTAR” on page 66.



To change the default file name, see “Index File Name” on page 131.

Folder Hierarchy

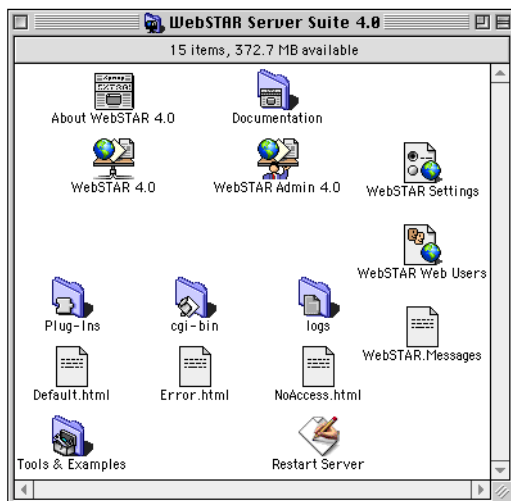
To set up your site, you need to organize your data in a folder hierarchy within the WebSTAR folder. When you are moving documents into the folders that can be served by WebSTAR, you need to make decisions about who can access the files, how they should be

CHAPTER 3: GETTING STARTED

transferred to clients, whether there are links within the documents to other local files, and more.

Default WebSTAR 4 Arrangement

This is what your WebSTAR folder will look like after you have run the program for the first time. It includes the files that are installed with WebSTAR, described in “About the Installed Files” on page 40. It also shows some of the files that WebSTAR creates, described in “Important WebSTAR Files” on page 103.



 To simplify future upgrades, don't change the name of your WebSTAR folder.

WebSTAR Root Folder

The WebSTAR folder is your **root folder**. All references to your main host begin from this folder. You should place all files to be served in this folder or subfolders within this folder. For information on linking, see “Links to Subfolders and Parent Folders” on page 187.

The names of your subfolders are particularly important if you expect to protect some parts of your site. For more information, see “Security Realms” on page 164.

There are times when you may want to direct URLs to another file or folder: for information, see “Redirection: Aliases and Redirect Files” on page 190.

Moving a Web Site to WebSTAR

If you already have a working web site, you'll be able to move the files and hierarchy to your WebSTAR server fairly easily, even if it's coming from Windows or Unix. If you are using SSI commands in your pages, they will be fairly compatible as well. However, most CGIs and server-side functions will have to be changed to Mac versions.

 See also: “Virtual Hosts: Hosting Multiple Web Sites” on page 193.

 For SSI details, see “WebSTAR SSI” on page 275.

If your Mac is on a network with your WebSTAR server machine, you can use Apple's Personal File Sharing. See your Macintosh manual for information on copying files using File Sharing.

You can also download your site from your old service provider using an FTP client or a browser on the WebSTAR server machine. Put the HTML pages from the top level of your old site into the WebSTAR folder. If you have subdirectories or subfolders on your old site, make folders with the same names in the WebSTAR folder and download the HTML pages into the correct folder.

You can also upload data to the WebSTAR Server: see "WebSTAR FTP Server" on page 337 and "WebSTAR File Upload" on page 247 for details on using these services.

About File Names and URLs

WebSTAR itself, and the Mac OS, are not **case-sensitive** (it doesn't distinguish between upper and lower-case letters) for file names. For example, WebSTAR treats

`WWW.DOMAIN.COM/DOCUMENTATION/MANUAL.HTML`

the same as

`www.domain.com/documentation/manual.html`



The Internet is much less flexible than the Mac OS in handling non-English characters, and even punctuation.

Some browsers and other servers are case-sensitive, however, so it's a good idea make sure all links and filenames are in lower case.

Special Characters in File Names

One of the advantages of Macs is that you can use spaces and all sorts of punctuation in file names. The Web is much less flexible, so you should be very careful in naming your files. For information, see "Web File and Folder Name Rules" on page 189.

EXTENDING YOUR WEB SERVER

WebSTAR's support for CGIs and Plug-Ins allows you to serve much more than just HTML. You can send email forms, provide a search interface, connect databases to your web server, add guestbooks and conferencing, even set up a online store.

Using WebSTAR Plug-Ins

StarNine's WebSTAR Plug-Ins are automatically installed with WebSTAR. For more information see "WebSTAR Plug-Ins" starting on page 235.

Third-Party CGIs and Plug-Ins

Third-party CGIs and Plug-Ins provide many excellent tools to make your web server do more. The documentation for each program will explain how to install and use it. For information on CGIs and Plug-Ins, see:

<http://www.starnine.com/extendingwebstar.html>

Writing Your Own CGIs and Plug-Ins

WebSTAR provides development support for writing CGIs in AppleScript, Perl and C, and W*API Plug-Ins in C, C++, and Java.

For more information, use the WebSTAR Server Suite Installer, choose Custom Install, and select the WebSTAR Development Resources item. This will install both the WebSTAR API SDK and the WebSTAR Developer Toolkit. The WebSTAR CD includes other developer resources as well.



See also : “Extending WebSTAR: CGIs, Plug-Ins and Java” starting on page 443.

This chapter covers the changes in WebSTAR Server Suite 4, and explains the changes in the WebSTAR server application, WebSTAR Admin, and the Plug-Ins since version 3.

Upgrading



Be sure to back up your *WebSTAR Settings* file before upgrading. WebSTAR 4 changes the structure of the file, so you can't "downgrade" that file. The rest of your site is still compatible with the old version of WebSTAR.

WebSTAR version 4 is compatible with your existing files and Plug-Ins from versions 2 and 3, although you can't use the new settings file with old servers. To set it up, just follow the instructions in "Upgrading your WebSTAR Server" on page 37.

Webstar 4 will read your WebSTAR settings and passwords files, automatically! All your pages will be served as before, and you do not have to change any files on your site. WebSTAR Plug-Ins will all work, although you should check with third-party developers about their Plug-Ins and CGIs.

After upgrading, check out the new version of the WebSTAR Admin application, and use it to set up the new WebSTAR Mail server, as described in "Getting Started" starting on page 47.

WHAT'S NEW IN WEBSTAR 4

WebSTAR 4's new features build on the power and flexibility of WebSTAR, giving you more tools to extend your web presence and build superior sites, with even more Mac ease-of-use.

For a complete description of all the changes in WebSTAR since the initial release, see the notes on the StarNine web site:

<http://www.starnine.com/webstar/webstar.html>

CHANGES TO THE WEB SERVER

WebSTAR is a high performance Web server, capable of serving tens of millions of connections a day.

- High performance file info and data caching architecture.
- Server provides facilities for Plug-Ins to support persistent connections. The Data Cache and the SSI Plug-Ins take advantage of this new feature in WebSTAR, allowing Plug-In-processed requests to take advantage of HTTP/1.1 pipelining.
- Now supports multiple index file names (e.g. index.html, default.html, index.htm) in the main host and all virtual hosts.
- Improved WebSTAR Data Cache reduces number of files open at one time.

- Persistent CGI connections option will greatly speed up CGI interactions.
- For increased server performance, the WebSTAR application reserves more processor cycles by default. This will slow down CGIs, but speed up the server and Plug-In processing. You can override this in the WebSTAR Admin: see “Performance” on page 138.
- Improved error handling: if a Plug-In returns an error indicating that the file was not found, the WebSTAR Web server will now handle normal Plug-In processing of the error file (instead of just returning a 404 status code).
- Removed a “No Access” warning message that was displayed when an Error file was mapped to an Action.
- Updated default Suffix Mapping entries to provide support for Cascading Style Sheets and several new Microsoft application MIME Types.
- User names and passwords file now named *WebSTAR Web Users* instead of *WebSTAR.pass*.
- Three new WebSTAR Log Format logging tokens: STATUS for logging of HTTP header result codes, HOSTFIELD for logging of the hostname requested by the client, CS-SIP to print out the server IP address (multihome aware).
- Server Suite and Web server log information now in the *WebSTAR Web.log* file in the *logs* folder by default. Archived copies are stored in the *archived_logs* folder by default.
- WebSTAR Admin browser pages have been re-designed and no longer have a text version.

SSL (Secure Sockets Layer) Changes

- Now supports SSLv3 as well as SSLv2, with code based on OpenSSL.
- Allows multiple certificates, one for each IP address.
- Support for multiple X509, X509v3, PKCSv7Netscape, and Server Gated Cryptography (SGC) style certificates
- RC4-128, 3DES-112, DES-56, DES-40, RC4-40 and MAC (message authentication only) encryption ciphers.
- Improved SSL random number generator is much faster and avoids a great number of extra hashing functions.
- New SSL Security panel in the WebSTAR Admin application.

CHANGES TO THE WEBSTAR ADMIN

The WebSTAR Admin program has been updated for WebSTAR 4. It now allows you to administer the Mail server, as well as FTP and Proxy



For information, see “About the WebSTAR Admin Application” on page 113 and “Web Server Administration” starting on page 129.

servers. It has an improved interface for displaying and configuring the WebSTAR settings.

The WebSTAR Admin requires the *WebSTAR Admin Plug-In* file in the *Plug-Ins* folder.

The WebSTAR Admin browser pages are still available, but they do not display all the server options.

- Admin Connection dialog now saves server information about the last 10 servers you've connected to, including an option to save the password.
- Added SSL Security panel for configuration of HTTPS/SSL settings.
- Adds support for configuration of Better Server Performance vs. Better CGI Performance settings.
- New area to enter several index file names for folder URLs.
- Data cache file modification date control.
- New SSI Counters administration panel.
- Standard Log Archiving part for all servers, with a **Choose** button for setting the log file locations.
- New features in Web, FTP and Proxy monitor windows including server uptime and server-specific data such as number of web hits and cache efficiency.
- Confirmation dialogs for Suspend Logging and Refuse New Web Connections.

NEW MAIL SERVER ADDED TO THE SUITE



See “WebSTAR Mail Server Overview” starting on page 357.

The WebSTAR Mail server provides Internet-standard email services, allowing you to host email accounts as well as Web pages.

- SMTP (Simple Mail Transfer Protocol) and some ESMTP (Extended SMTP) support, such as the EHLO command.
- IMAP4 (Internet Message Access Protocol)
- POP3 (Post Office Protocol)
- APOP (Authenticated Post Office Protocol)
- MIME (Multipurpose Internet Mail Extensions)
- limited LDAP (Lightweight Directory Access Protocol) for email alias and address lookups.
- Support for multiple domains and user accounts on individual or multiple domains.
- Web-browser access to user account mailboxes.
- Robust routing options for outgoing SMTP messages.

- Advanced relay blocking and Allow/Deny security for the prevention of unsolicited email (“spam”).
- Remote viewing and control of the outgoing mail queue.
- Full support for 8-bit messages.
- SMTP/ETRN support for intermittent Internet connections.

CHANGES TO THE WEBSTAR FTP SERVER

The WebSTAR FTP server provides standard FTP services to clients and web browsers so you can allow visitors and publishers on your site to download and upload files using the standard FTP protocol.

- Now supports limiting of folder content size on a per-user basis.
- Support for MacBinary II and III encoding standards.
- Supports resuming of FTP file transfers using the REST FTP command.
- Now supports the APPE FTP command for appending of uploaded data to a preexisting file.
- Improved communication with users via log-on, log-out and folder message file displays.
- Now returns an error message to the FTP client when the maximum number of FTP connections has been reached.
- Disconnects if attacked by long control strings.
- Option to automatically append “.bin” for files with resource forks.
- Better compatibility with Anarchie FTP client from Stairways Software.
- Settings information is now stored in the *WebSTAR FTP Settings* file, and is now stored in the new *WebSTAR FTP Data* folder within the *Plug-Ins* folder.
- Server log information is now stored in the *WebSTAR FTP.log* file in the *logs* folder.
- *FTP Users* file has been renamed *WebSTAR FTP Users* and is stored in the *WebSTAR FTP Data* folder.



See “WebSTAR FTP Server” on page 337.

CHANGES TO THE WEBSTAR PROXY SERVER

The Proxy server for WebSTAR allows you to cache and filter HTTP requests for browsers within your internal network. This improves responsiveness when several browsers access the same URL. In addition, if you are in a school laboratory, kiosk, or other controlled setting, you can use the WebSTAR Proxy server to limit access to the Web based on server host name, IP address, and more.



See “WebSTAR Proxy Server” on page 411.

New Features:

- Support for upstream Proxy servers.
- Security architecture for preventing Proxy access from and Proxy access to individual hosts and web sites.
- Added AppleEvents for getting and setting of the log file name and location.
- Server log information is now stored in the *WebSTAR Proxy.log* file in the *logs* folder.

CHANGES TO THE WEBSTAR PLUG-INS



For more information, see “WebSTAR Plug-Ins” starting on page 235.

The new versions of the WebSTAR Plug-Ins are more stable and flexible. All WebSTAR Plug-Ins now return HTTP “head” requests. Some take advantage of new W*API features to display information windows on the server machine.

Core Plug-Ins Changes

WebSTAR Byte Server



See “WebSTAR Byte Server” on page 240.

- WebSTAR Byte Server now runs as the Default Byte Server and will now process any GET or `CONDITIONAL_GET` byte-range request that is not handled by other Plug-Ins. You don't have to edit the Suffix Map to byte-serve specific types of files, although you can if you want.
- Now tells the server “not handled” when it can't find a file, so the server does normal error handling.

WebSTAR Data Cache

The caching architecture of WebSTAR Server Suite has been completely redesigned. No longer will the server experience the pausing problem caused by flushing large data caches, and no longer will the entire cache need to be flushed to update a single entry.

- The Data and File caches will automatically include all file requests, including requests for files that do not exist. This allows the server to handle multiple default and index file names.
- Supports HTTP/1.1 persistent connections.
- Now tells the server “not handled” when it can't find a file, so the server does normal error handling.
- More strict about checking modification dates. A “not modified” response is returned only if the mod-dates of the request and the file match **exactly**.

- Always refreshes file info when the cache's external API is used. This reduces the efficiency somewhat, but ensures up-to-date data.
- Now handles the no-cache Pragma and Cache-Control: request header fields — the file will be read off disk rather than being served out of RAM. This means that you no longer need to use third-party utilities to flush WebSTAR's cache, you can just do a Super-Reload in the browser.



See “Data Cache” on page 140.

WebSTAR Log Archiver

- Now the standard archiver for Web, FTP, Mail and Proxy servers, configured using the WebSTAR Admin application.
- Improved log archiving automation reduces server disruption.



See “Log Archiving” on page 93, and the logging chapters.

WebSTAR SSI

- Now tells the server “not handled” when it can't find a file, so the server does normal error handling.
- Added support for the SSI environmental variable HTTP_COOKIE.
- New SSI Counter panel in WebSTAR Admin.
- The improved check-pointing of the counter data. A crash won't cause all of your counters to disappear. At most, you could lose the previous 20 minutes of data.
- Now supports #include references to 30 levels (increased from 3 levels).
- Enhanced Server-Side-Includes featuring an extensible architecture allowing Plug-Ins to register custom HTML tags. When the SSI Plug-In encounters these tags, it will call the registered Plug-In which can generate the data in that part of the page.



See “WebSTAR SSI” starting on page 275.

WebSTAR Virtual Hosts

- Works with the new Index File Name system to allow multiple default index file names.
- Settings information is now stored in the *WebSTAR Virtual Hosts* file in the *Plug-Ins* folder.



See “Virtual Hosts” on page 144.

Additional Plug-Ins

These Plug-Ins are provided as part of the WebSTAR Server Suite. If you choose the Upgrade option, the Installer will upgrade any older versions of these Plug-Ins to the newest version. However, these Plug-Ins are not installed by the Easy Install; you must use the Custom Install option to add them to a server.

WebSTAR Auto BinHex

- Improved error messages.



See “WebSTAR Auto BinHex” on page 238



See “WebSTAR Directory Indexer” on page 241.



See “WebSTAR File Upload” on page 247.



See “WebSTAR Form Mail” on page 249.



See “WebSTAR Search” on page 261.



See “WebSTAR WebObjects Adaptor” on page 272.



See “WebSTAR Debug Plug-In” on page 107.



See “WebSTAR Lasso Publisher” on page 307.



See “WebSTAR PowerKey Pro Tickler” on page 256.

- Improved compatibility with already-binhexed files.

WebSTAR Directory Indexer

- Fixes a problem referencing subdirectories with URL-encodable chars in the parent names.
- Improved HTML generation.

WebSTAR File Upload

- Corrected problems preventing file uploads to different volumes.
- Fixed problems uploading extremely large files.

WebSTAR Form Mail (formerly QuickSend).

- Name has been changed, and form action changed to `x.formmail`.

WebSTAR Search

- Added support for 2-byte characters.

WebSTAR WebObjects Adaptor

- Now compatible with WebObjects 4
- Two versions
 - WebSTAR WebObjects 3 Adaptor
 - WebSTAR WebObjects 4 Adaptor

New Plug-Ins

WebSTAR Debug

- Logs server information for tracking down recurring problems. Use this Plug-In when instructed by StarNine Technical Support.

WebSTAR Lasso Publisher

- Now includes WebSTAR Lasso Publisher, a lightweight version of the Lasso Web Data Engine from Blue World Communications.

WebSTAR PowerKey Pro Tickler

- Works with PowerKey Pro from Sophisticated Circuits to monitor the server status and restart the system if the WebSTAR server crashes or freezes.

WebSTAR QuickDNS Load Balancer

- Works with QuickDNS server from Men & Mice to provide server load information.
- Updated to provide native PowerPC Open Transport support.
- Now sends the IP address for all Virtual Hosts.
- Default values are now listed on the HTML administration page.

- Works with WebSTAR FTP to provide FTP load balancing.

WebSTAR Rebound Assist

- Works with Rebound! from Sophisticated Circuits to monitor the server status and restart the system if the WebSTAR server crashes or freezes.

WebSTAR SSI-WebInclude

- Dynamically reads data from other web pages, reformats and includes the text in your pages.



See “WebSTAR QuickDNS Load Balancer” on page 267.



See “WebSTAR Rebound! Assist” on page 260.



See “WebSTAR SSI-WebInclude” on page 299.



The WebSTAR server application acts as an umbrella under which all WebSTAR Plug-Ins are loaded. The FTP, Mail and Proxy servers are actually implemented as Plug-In modules.

The WebSTAR server application is responsible for serving all Web (HTTP), Mail, FTP and Proxy connection requests. It is the core application and must be running for your server to be available. For configuration information, see “Server Administration and Status” starting on page 113.

This chapter provides information on configuring and using the WebSTAR Server Suite application. It covers the server status reporting panel and monitor windows, passwords, serial numbers, and the Restart Server application. It also gives you important background information on server security, IP addresses, domain names, host names, DNS, important files, and more.

For information on individual servers in the suite, see “About Web Serving” starting on page 179; “WebSTAR FTP Server” starting on page 337; “WebSTAR Mail Server Overview” starting on page 357 and “WebSTAR Proxy Server” starting on page 411.

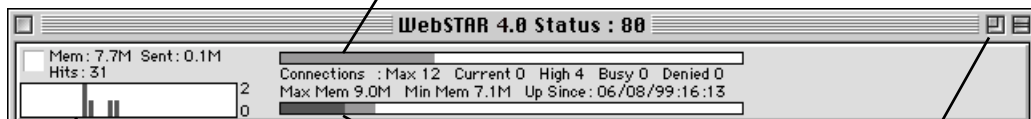
WEBSTAR STATUS AND MONITOR WINDOWS

The WebSTAR Status window has two parts: a top panel which displays important information about the status of the server as a whole, and a monitor panel which displays initialization messages, error messages, and Web requests. The FTP, Mail and Proxy servers have separate monitor windows, so you can track those interactions as well.

Status Window Top Panel

The **LED heartbeat** gives you quick reading of the status. Slowly flashing green shows that the server is idle, flashing green shows it's busy, flashing red shows a connection refused, and solid red shows no connections accepted.

The **Connection Meter** displays the percentage of available connections currently used. The light grey bar is the "high-water mark" since the server was launched, the dark grey bar is the current status. If the bar fills up, you should consider increasing the number of connections (see "Max", below).



The **Load Histogram** displays the average load on the server. The top number on the right indicates the number of open connections in the recent past. When this window is updated, according to the Status Report Delay (described on page 200), each bar moves left.

The **Memory Meter** displays the total amount of RAM currently used by WebSTAR and any installed Plug-Ins. The light grey bar is the "high-water mark" since the server was launched, the dark grey bar is the current status. If the bar fills up, you should consider increasing the amount of RAM allocated to the WebSTAR server application.

Zoom box to switch to the minimized view.

The title of the WebSTAR Server Status window shows you the web server port number (80, by default).

Summary Status

The text at the top left corner of the Status window displays the following information:

- **Mem:** The amount of free memory (in megabytes) currently available in the WebSTAR server. If this number is less than 500K, you will want to increase the RAM allocation to the WebSTAR server application.
- **Sent:** The total amount of data (in megabytes) sent since the server was last launched.
- **Hits:** The total number of connections served since the server was last launched.

Connections

- **Max:** The maximum number of simultaneous incoming connections this server can handle.
- **Current:** The total number of web connections currently active.
- **High:** The "high-water mark" of simultaneous connections. Use this value to verify that you have set the maximum number of connections correctly.



Some of these elements are also displayed in the Browser Admin Monitor page.



To change this setting, see "Max Connections" on page 134.

- **Busy:** The number of connection requests refused by WebSTAR because the server was too busy.
- If this number is greater than zero, you may need to increase the number of connections you have allocated to the server. However, if you are on a slow-speed network or have a slow server, you may find that limiting the number of connections enhances performance by keeping the server and network from getting swamped by too many requests
- **Denied:** the number of connections that have been denied access to pages protected by your server's Security Realms and User Names settings. When a browser is denied automatic entry and required to enter a name and password, this number will be increased by one.



The current memory status is shown in the both memory meter bar and in the "Mem" status, described above.

Memory

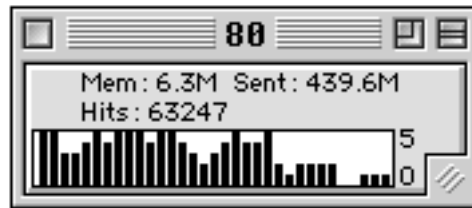
- **Max Mem:** A "high-water" mark indicating the maximum amount of memory (in megabytes) used by the WebSTAR server in the current session.
- **Min Mem:** A "low-water" mark indicating the smallest amount of free memory (in megabytes) used by the WebSTAR server in the current session.

Up Since

- The date and time when the server was last launched.

Minimized Window

The Zoom Box () on the right side of the title bar lets you toggle between standard and **minimized** modes of this window (as shown above). In minimized mode it will show you the heartbeat LED, the "Mem", "Sent", and "Hits" data, and the Load Histogram.

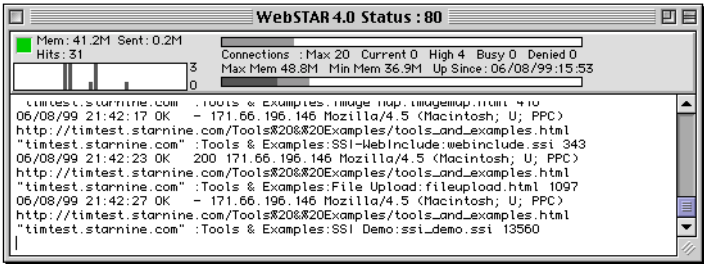


To speed up your server's responses, keep this window closed and use the Admin Status Window.

Log monitoring of HTTP requests and responses is only displayed in the monitor panel when the Status window is at the standard size: the data is not stored when the window is minimized. However, log data is always stored in the log file.

Status Window Monitor Pane

The Web Monitor pane (below the Server Status Panel) displays server initialization data, error messages, and Web server HTTP and HTTPS requests and responses.



Startup Messages

On initialization, you'll see copyright information, status, and initialization information.

- List of Virtual Hosts and routing information (see “Virtual Hosts” on page 144).
- List of Plug-Ins Installed (see “Web Server Administration” on page 129 and “WebSTAR Plug-Ins” starting on page 235)
- Web Server File Caching and Persistent Connections (see “Caching” on page 139 and “Use Persistent CGI connections” on page 138).
- Status of WebSTAR Lasso Publisher (described on page 307)
- Status of the WebSTAR FTP Server (described on page 337)
- WebSTAR Log Archiver status (see “Log Archiving” on page 122).

 These messages are not stored in the log file or displayed in the Admin monitor windows.

PowerPC (CW) Server is running on port 80.

WebSTAR Virtual Hosts

```
=====
* knickknacks.domain.com * -> :kkn:
* www.tchotchkeys.com * -> :tch:
* widgets.domain.fr * -> :mechanisme:
192.168.0.4 * es -> :cositas
192.168.0.4 * fr -> :mechanisme:
* widgets.domain.com * -> :widgets:
* www.domain.com * -> :widgets:
192.168.0.4 * * -> :widgets:
192.168.0.3 * * -> :kkn:
```

Initialized Plug-ins:

```
=====
WebSTAR Virtual Hosts          4.0
WebSTAR SSI-WebInclude        4.0
WebSTAR SSI                    4.0
```


WebSTAR Search	4.0
WebSTAR QuickDNS Load Balancer	4.0
WebSTAR Mail	4.0
WebSTAR Log Archiver	4.0
WebSTAR Lasso Publisher	4.0
WebSTAR JRun Servlet Runner	4.0
WebSTAR Image Map	4.0
WebSTAR FTP	4.0
WebSTAR Form Mail	4.0
WebSTAR File Upload	4.0
WebSTAR Directory Indexer	4.0
WebSTAR Data Cache	4.0
WebSTAR Byte Server	4.0
WebSTAR Admin	4.0

File Info Caching is enabled with space for approximately 41 entries.
 Persistent Connection processing is enabled.
 WebSTAR Lasso Publisher: Loading Tag Modules
 Loaded " Lasso_Tags.mod" module successfully.
 Loaded "DB_Info_Tags.mod" module successfully.
 WebSTAR Lasso Publisher: 4/22/1999 1:45:43 PM New Lasso Tag Parser is ON.
 Loaded "NewParser_On.mod" module successfully.
 WebSTAR Lasso Publisher: Loading DataSource Modules
 Loaded "FM_DataSource.mod" module successfully.
 Loaded "Send_Mail_DataSource.mod" module successfully.
 Load Balancing for FTP turned off
 !!LOG ARCHIVER:Log archiving for WebSTAR Web server is scheduled to run daily
 !!LOG ARCHIVER:and will next occur on 04/23/1999 at 11:00 AM.
 !!LOG ARCHIVER:Log archiving for WebSTAR FTP server is disabled.
 !!LOG ARCHIVER:Log archiving for WebSTAR Proxy server is disabled.
 !!LOG ARCHIVER:Log archiving for WebSTAR Mail server is scheduled to run hourly
 !!LOG ARCHIVER:and will next occur on 04/22/1999 at 03:00 PM.

Web Server Monitoring

Most of the data in the Status window Monitor Panel will be requests using the HTTP protocol. For example, the line:

```
06/01/99 19:18: 200 OK 200 leslie.domain.com Mozilla/4.5 (Macintosh; U; PPC) "www.example.com" :knickknacks:index.html
```

is in the default format (see "WebSTAR Log Format" on page 202). It shows that on June 1, 1999 at 7:18 pm, the server successfully returned a file to the browser on the machine "leslie.domain.com", that the browser was Netscape version 4.5 for the Mac, that the host requested was `www.example.com` and that the file served was named *index.html* and stored in the *knickknacks* folder.



This information is also stored in the Web Log file (see "Logging" on page 199).

When you change your log file format, the monitor window will change too. For more information, see "Log Formats" on page 200.

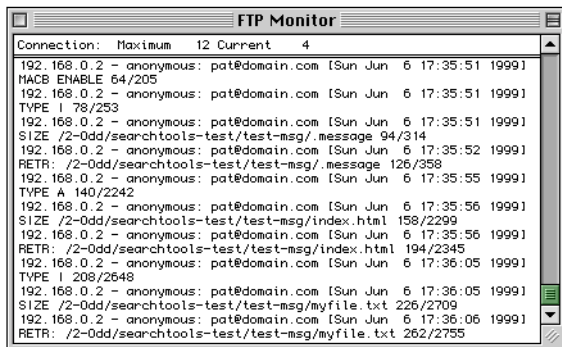
If your server has errors, you'll see an entry with "ERR!" in the Monitor Panel. If the server cannot find a file, or there's a problem with Plug-In that should handle a URL, it will display information about these errors. For more information, see Chapter Running H/F 3: Running H/F 1.

As you use more Plug-Ins and CGIs, the messages in this window will be more complex, but they are designed to help you understand what is going on and how to best configure your server.

If you're having trouble with your server, you can specify more detailed messages by selecting Verbose Messages (described on page 85).

FTP Monitor Window

The FTP monitor window shows you information about current connections in the top panel. The monitor panel shows logins, uploads, downloads, and errors. For complete information, see "FTP Monitors & Logging" on page 349.



Mail Monitor Window

The Mail monitor window displays all mail transactions, including logons, logoffs, incoming and outgoing messages, LDAP requests and so on. It does not show the connections or queue information, although the Admin Mail Monitor window shows that information.



For more information, see "Mail Monitor & Queue Window" on page 399.

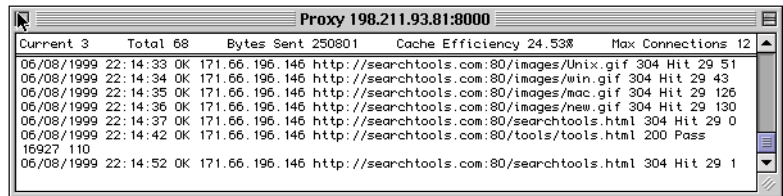


Proxy Monitor Window

The Proxy monitor window displays information about connections and caching. The logging panel displays each transaction, with information about the URL and the cache status. For complete description, see “Proxy Status Window & Log File” on page 421.

WEBSTAR SERVER MENUS

The WebSTAR server application is responsible for serving all Web (HTTP or HTTPS), FTP and Proxy connection requests. It includes menu commands for the basic setup of your WebSTAR server. However, to configure and administer the WebSTAR server, you will use the WebSTAR Admin application and the Browser Admin described in “Server Administration and Status” starting on page 113.



Proxy 198.211.93.81:8000									
Current 3		Total 68	Bytes Sent 250801		Cache Efficiency 24.53%		Max Connections 12		
06/08/1999	22:14:33	OK	171.66.196.146	http://searchtools.com:80/images/Unix.gif	304	Hit	29	51	
06/08/1999	22:14:34	OK	171.66.196.146	http://searchtools.com:80/images/win.gif	304	Hit	29	43	
06/08/1999	22:14:35	OK	171.66.196.146	http://searchtools.com:80/images/mac.gif	304	Hit	29	126	
06/08/1999	22:14:36	OK	171.66.196.146	http://searchtools.com:80/images/new.gif	304	Hit	29	130	
06/08/1999	22:14:37	OK	171.66.196.146	http://searchtools.com:80/searchtools.html	304	Hit	29	0	
06/08/1999	22:14:42	OK	171.66.196.146	http://searchtools.com:80/tools/tools.html	200	Pass			
16927 110									
06/08/1999	22:14:52	OK	171.66.196.146	http://searchtools.com:80/searchtools.html	304	Hit	29	1	

File Menu

The Server's File menu lets you open the Status window and the FTP, Mail and Proxy Monitor windows, as well as **Quit** the server application.

Edit Menu

The Undo, Cut, Copy, and Paste commands in this menu mainly work in dialog text fields. In addition, you can select text in the Status window and Copy it to the clipboard.

Admin Password

This dialog allows you to set the password for access to the WebSTAR Admin Application. You can only have one Admin Password: if you open this dialog and enter a new password, you will not be able to use the old password. Note that this password is case-sensitive, so you must always match the upper and lowercase letters. For information on keeping your server secure, see “Safe Passwords” on page 96.



The Admin password is not the same as the Administration Realm password. See “Accessing the Browser Admin Pages” on page 55.

Serial Numbers

You must have a unique serial number to enable WebSTAR. If you need to edit or change your serial number, use this menu item to bring up the Serial Number dialog. WebSTAR serial numbers will start with WEB*. Localized versions may have other prefixes for the serial number.

You may store up to five serial numbers, including expiring demonstration numbers and older version serial numbers. Having more than five numbers may cause error messages at startup.

You must have a different serial number for each WebSTAR server machine that you are running. If you launch a second copy on another machine, you must enter a different serial number.

The serial number is stored in the *Web Server Files*, so if you remove your settings file, or it becomes corrupted, you will have to re-enter your serial number.

Entering and Editing WebSTAR Serial Numbers

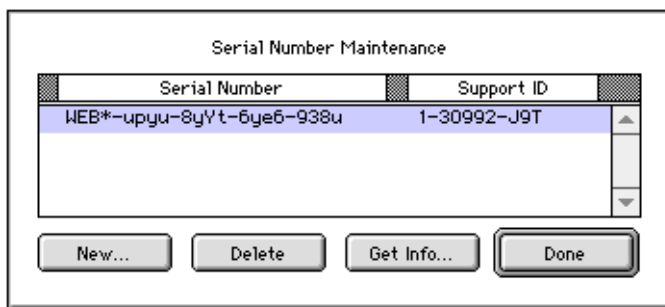
The “Serial Numbers” command in the WebSTAR server’s Edit menu opens a dialog in which you can view, add, or delete serial numbers for WebSTAR. The buttons in the Serial Number Maintenance window let you add, delete, or get more information about a number.



For information on testing without a permanent serial number, see “Temporary Serial Number” on page 49.



To avoid losing your serial number, write it in your WebSTAR manual and save it in your Mac’s Note Pad.



- **New** opens the Serial Number Entry dialog.

Type your serial number and then press the “OK” button. Be sure to type the number exactly as you see it on the serial number sheet or message, with dashes, capital letters, numbers and no spaces. If you make a mistake in typing, WebSTAR will show you an error message and let you try again.

If you have the serial number in a message or on the Note Pad, you can copy and paste it into this dialog (be sure to delete any new line or return characters).

- **Delete** removes the selected serial number. Use this to remove expired evaluation serial number.

- **Get Info** displays more information about the selected serial number: the serial number, support ID, expiration date, and start date (if applicable). Use this to check when your evaluation serial numbers will expire.
- **Done** closes this dialog.

Options Menu

Options	
Verbose Messages	⌘M
Suspend Logging	⌘L
Hide Window In Background	⌘H
Refuse New Web Connections	⌘R
Restrict CGIs to CGI-BIN	⌘B
Flush Cache	⌘F

Items in the Options menu let you change the behavior of the server. All selections made in this menu are saved in the server's *WebSTAR Settings* file and restored the next time the server is launched. The Options menu in WebSTAR Admin and the WebSTAR server application are almost identical.

Verbose Messages

When this option is checked, WebSTAR displays additional connection and diagnostic information. The information is displayed in the Status window but not recorded in the log. You can also set this in the Browser Admin, Controls Page.

Many of the messages produced by checking this option pertain to low-level HTTP, FTP, Proxy or TCP/IP internal state information. If you are not familiar with these protocols, these messages may seem quite obscure. However, some of the verbose messages can be useful for watching the details of client requests and for troubleshooting.

Errors reported with Verbose Messages enabled should **not** be reported to StarNine Technical Support.

Suspend Logging

When this option is checked, WebSTAR temporarily closes its log file, allowing you to open and examine the file with a text editor. No incoming connection data will be logged to the file while this option is checked. You can also set this in the Browser Admin, Controls Page.



Displaying the Verbose Messages makes the server run more slowly. For normal operations, make sure this option is **not** checked.

Hide Window in Background

When this option is checked, the WebSTAR Status window is hidden when other applications are active in the foreground.

 Monitor windows and Plug-In status windows will not be hidden.

Refuse New Web Connections

When you check this option, WebSTAR will refuse all new HTTP requests, until the option is unchecked. However, it will finish servicing all currently queued requests.

Incoming connections are still reported in the statistics area of the Status window, but those connections are just “knocking at the door”—they are not being allowed in and the clients are notified that their connection is refused.

This option is useful for gracefully shutting down a server, without causing those who are currently receiving data to get errors.

 You can also set this in the Browser Admin Controls page

Restrict CGIs to CGI-BIN

This menu command works just like the checkbox in WebSTAR Admin: see “Restrict CGIs to CGI-BIN” on page 137.

Flush Cache

Forces WebSTAR to flush the memory caches. You can also flush the caches in the Browser Admin Controls page.

Flushing the cache flushes the file, data and DNS caches, and sends a message to Plug-Ins to flush their caches as well (although not the Proxy Cache). For more information, see “Flushing the Caches” on page 143.

Plug-Ins Menu

The Plug-Ins menu displays the names of all installed WebSTAR server Plug-Ins. When you select a Plug-In from this menu, it may display a configuration interface, status information or version information. The exact action will depend on the Plug-In.

Most WebSTAR Plug-Ins display their version and copyright information, along with a contact URL. WebSTAR Data Cache and WebSTAR SSI will display their information windows. WebSTAR Mail, WebSTAR FTP and WebSTAR Proxy will bring up their monitor windows.

Help Menu

WebSTAR help is in the form of this document, available for printing in Acrobat PDF format and viewing in HTML. To view locally, open your Web browser and choose Open from the File menu, then open this manual from the Documentation folder.

SERVER APPLICATION ISSUES

Server Administration Responsibilities

As the administrator of an Internet server, you must protect your data and make sure that you, your server, and your users do not interfere with the rights of others.

If you plan to provide hosting services for others, you should create a Terms of Service agreement, detailing what you will provide to your users and what behavior you do and do not allow. A careful contract will allow you to enforce reasonable behavior, remove those who do not comply, and help you protect yourself from legal challenges.

Your ISP institution's IS department will probably have similar Terms of Service, so you should familiarize yourself with them and make sure that they will not cut off your service.

For Web servers, you should define what kind of content you allow: in particular, think about copyright infringements and pirated software, as well as controversial issues such as politics, religion, and adult content. You should also define in advance how much server disk space each user may have, and how much traffic you will support. Even if you do not check that in many cases, you may need to invoke it, if a user's content becomes overwhelmingly popular.

For FTP servers, unauthorized software distribution, content of files, disk space and traffic are important issues. In addition, you should reserve the right to change FTP passwords periodically, for improved security.

For Mail servers, you should make clear what behavior is acceptable and what is not. Have defined policies on threats, harassment and spam, as well as protection for free speech. This allows you to remove users who break these rules under your own process. If you do not remove these users, you may find that others will blacklist your server and cut off your email access.

 For background, see RFC1173: Responsibilities of Host and Network Mangers and RFC 1123: Requirements for Internet Hosts.

 You also have the responsibility to keep your server and data secure: see "WebSTAR Security" on page 93 for more details.

For Proxy servers, be sure that users understand the implications of the proxy system. There are logistic issues of making sure that all web browsers use the server rather than attempting to connect to the Internet directly. In addition, if you filter sites based on IP address or host name, you should make sure that your users understand why these sites are not available to them.

Application Memory and Connections

WebSTAR Server Suite 4, with default settings, is set to a preferred size of 10 MB (slightly higher if you are not running Virtual Memory). The default setting allows 12 connections, each, for the HTTP, FTP and Proxy servers, SMTP outgoing, SMTP incoming, POP and IMAP, 6 connections for LDAP, 50 K for the default the File Info cache, and 256 K for the default Data Cache.

Connections

You should check the Connections bar on all the monitor windows regularly. If they are often full, or the Web Connections “Busy” number is greater than zero, you may need to increase the number of connections you have allocated to the server.

There is a limit of 500 total connections on a single machine, so be sure you track how many you use for each kind of server, and leave a few for the WebSTAR Admin application. Each additional connection requires additional memory and there is a small system overhead for each open connection.

If you are on a slow-speed network or have a slow server, you may find that limiting the number of connections enhances performance, by keeping the server and network from getting swamped by too many requests.

To change connections, use the WebSTAR Admin application:

- Web server: Max Connections (described on page 134)
- FTP server: Max Connections (described on page 341)
- Mail server: Connections (described on page 78)
- Proxy server: Proxy Connections (described on page 415)

Rules for Increasing Memory Allocation

Be sure to look at the information in **About This Computer** (under the Apple Menu) to see if you have enough memory on the machine to handle all your applications.



See “Rules for Increasing Memory Allocation” on page 88.



WebSTAR requires at least 2048 K of memory to run. If your machine does not have enough memory free, WebSTAR will not run.

Web

- Increase the memory allocation by 100K for **each HTTP connection** assigned to the server above the default of 12. For example, add 1000K for 10 additional Web connections.
- Increase the memory allocation by 1K for each additional 1K assigned to the **file info cache**.
- Increase the memory allocation by 32K for each additional 32K assigned to the **data cache**.

FTP

- Increase the memory allocation by 32K for **each FTP connection** assigned to the server above the default of 12. For example, add 320K for 10 additional FTP connections.
- If you are not running the FTP server, you can reduce the memory by 384K.

Proxy

- Increase the memory allocation by 50K for **each Proxy connection** assigned to the server above the default of 12. For example, add 600K for 12 additional Proxy connections.
- If you are not running the Proxy server, you can reduce the memory by 600K.

Plug-Ins

WebSTAR Search may require you to allocate additional memory to the server, if you are indexing very large collections.

Depending on configuration, some Plug-Ins may require additional RAM be allocated to the server application. Consult relevant documentation.

How to Change WebSTAR's Memory Allocation

- 1 Quit the WebSTAR server if it is running.
- 2 Select the WebSTAR icon and choose Get Info from the File menu.
- 3 Increase or decrease the number in the "Preferred Size" field. To have a noticeable effect, increment by at least 100K.
- 4 Close the Get Info window.
- 5 Double-click the WebSTAR application to launch the server.

When you restart WebSTAR, it will request the larger amount of memory from the Mac OS. If that memory is not available, the application will take what it can get.

Optimizing WebSTAR for Best Performance

As shipped, WebSTAR provides very good performance for medium-sized sites. However, you may wish to optimize your server for your particular site.

For maximum performance, make sure all of the core Plug-Ins are installed, that the Web File Info and Data Caches have enough RAM allocated to them, that you set Persistent Connections (described on page 137) to at least the default settings, that WebSTAR Mail Cache settings are high enough to handle the amount of server load, and so on.

For general information on hardware, software and networking, see “System Requirements” on page 29; for memory allocation guidelines, see “Server Application Issues” on page 87; and to set the Web file and data cache sizes, see “Caching” on page 139.

In addition, the online WebSTAR Tech Note will give you updated suggestions for the most current techniques to optimize your server:

<http://www.starnine.com/support/technotes/wsperformance.html>

Restarting After Open Transport Errors

WebSTAR servers (including WebSTAR BG) will automatically shut down if they get errors from Open Transport. They will try to launch a **Restart Server** application, if there is one in the WebSTAR folder, by sending an Apple event.

Once launched, the included Restart Server application will quit the WebSTAR server and wait for 30 seconds. Once the 30 seconds are up, the Restart Server application will re-launch WebSTAR and then gracefully quit itself.

You can use the included *Restart Server* application, write an AppleScript restart script, or install a third-party replacement application for more flexibility and power, and to automatically restart after other problems.

Developing a Restart Server Application

You can create your own Restart Server application using whatever programming tools you have available. The easiest way is to write one in AppleScript.



For information on other server restart applications that are not limited to Open transport errors, see the [Extending WebSTAR](#) page.

For instance, you could develop a custom Restart Server application to backup your server whenever a TCP/IP error occurs, quit other server applications running on the same machine, etc.

Make sure that any replacement for this application is named *Restart Server*, has a creator code starting with “www”, and is located in the WebSTAR folder. In addition to launching an application called *Restart Server* in the same folder as WebSTAR, the server also sends an AppleEvent to the “Restart Server” application. This allows a single application to perform multiple tasks (and already be running when the server sends the restart event). The event WebSTAR sends passes the FSSpec as a parameter, but expects no reply. It’s simply intended as a trigger for applications that can restart the server which may already be running. The event class is WebSTAR’s www and the event code is REST. The application’s creator has been changed from “apLt” to “wwwΣ” for security reasons (you don’t want someone requesting a script named “Restart Server”). If your replacement Restart Server file is an AppleScript applet, you need to change the creator code back to “apLt” to edit it, and then back to a creator starting with “www”.

WebSTAR Background Server

The background-only version of the WebSTAR Server Suite, “WebSTAR BG”, runs in the background, providing no access to the server’s menus or other interface elements. Because there is no user interface, others cannot access the background-only applications, so they can’t change or quit the server by accident. The background server will respond to Web, Mail, FTP and Proxy requests just like the standard WebSTAR server.

To install WebSTAR BG, launch the WebSTAR Installer and choose “Custom Install”. Then choose “WebSTAR BG” from the list of options and install it in the same folder as the WebSTAR application.

Before you can use WebSTAR BG, you must first run the WebSTAR foreground server to enter the product’s serial number, and admin password. This initial launch and configuration of the foreground server creates a valid *WebSTAR Settings* file in the same folder as the WebSTAR application. WebSTAR BG will not run properly without a preconfigured Settings file.

After launching and configuring the foreground server, you can begin using the background-only server by quitting the foreground server and launching WebSTAR BG. Both applications can reside in the same

folder, but you **cannot** run them both at the same time. Typically, you would place an alias to WebSTAR BG in your Startup Items folder so it is launched automatically when you start your computer.

Once the WebSTAR BG application is running, you can communicate with it and configure it further by using the Admin application: see “About the WebSTAR Admin Application” on page 113.

To quit WebSTAR BG, use the WebSTAR Admin, and choose the Options menu **Quit WebSTAR** command.

There are no server monitor windows, although you can view server activity in WebSTAR Admin. To report server errors the WebSTAR BG application writes information in the WebSTAR.Messages File (described on page 104).

Running Multiple Servers On The Same Machine

If you want to have a Web site that has some public and some private pages and you don't want to use security realms, you can run multiple WebSTAR servers on a single computer, using a different TCP/IP port number. One server can be set up with no access restrictions, while another restricts access to specified hosts.

Web Port Numbers

All port numbers lower than 1024 are reserved for well-known services, such as Web requests, email, FTP and so on. WebSTAR uses the standard port 80 for the web server by default. If you are running multiple servers, you need to assign a different port number for the additional servers. Although you can use any unreserved, available port numbers, the convention is to use ports in the 8500 range (such as 8501) for additional WebSTAR servers.

See “HTTP Port” on page 135 for details on specifying an alternate port number for a selected Web server. When multiple servers are set up, URLs to the alternate servers (those not using port 80) must specify the appropriate port number. For example:

```
http://www.domain.com:8502/privatedoc.html
```

would use the same machine as “www.domain.com”, but an alternate web server.

FTP, Mail and Proxy Servers: Single Instance

Although WebSTAR allows you to run multiple copies of the server application, you **cannot run multiple FTP, Mail or Proxy servers**.



See also: “Virtual Hosts: Hosting Multiple Web Sites” on page 193.



See also: “WebSTAR Default Port Numbers” on page 102.



If you want to run multiple servers on different computers, they each need a unique serial number.

Therefore, to reduce memory usage and avoid confusion, you should remove the FTP and Proxy Plug-Ins from the alternate web server's *Plug-Ins* folder.

Log Archiving

WebSTAR servers (Web, FTP, Mail and Proxy) all use the same Log Archiver processing to make copies of their associated log file at scheduled intervals. This roll-over is disabled by default: you must use the WebSTAR Admin application to start or change the schedule. For more information, see "Log Archiving" on page 122.

WEBSTAR SECURITY



Open Transport versions 1.3 and later reduces the system's vulnerability to certain network attacks

Your Web, Mail and FTP servers present you to the Internet, and it's important that no one should change your site or modify your server settings without permission. While the Macintosh is one of the most secure server operating systems available, you still have to be careful to keep your server safe. For additional helpful information, see:

<http://www.w3.org/Security/Faq/www-security-faq.html>

Physical Security

The server machine runs the WebSTAR Server Suite application, which controls the Admin password, and the hard drive stores the *WebSTAR Settings* and the user names and passwords files. Make sure that your WebSTAR server machine is in a secure location. This may be your office, a closet, or a server room with locks or other controls. If you cannot lock the machine away, you should consider locking it to a desk or wall, so it can't be easily stolen.

WebSTAR Server and Admin Security

On your server machine, you can use software that controls access to the disk and applications, such as Apple's At Ease or the commercial Folder•Bolt. In addition, if you use the WebSTAR Background Server (described on page 91), there will be no application visible on the server machine. This reduces the chances of someone else quitting the server by accident.

The WebSTAR Admin application always encrypts communications with the server. That is how it can be secure, although the messages are sent via TCP/IP. You set the WebSTAR Admin password in the

WebSTAR server application (see “Admin Password” on page 83). Be sure to follow the guidelines in “Safe Passwords” on page 96.

The web browser administration pages are protected by the Administration Realm, and require a password to access. However, unlike WebSTAR Admin, commands sent to the server from a browser are not encrypted. If you use the Browser Admin, track your pages carefully and change your Administration Realm password often (using the WebSTAR Admin application).



For more information, see “Browser-Based Admin” on page 126

Firewall Security

Firewalls are security applications which check for unauthorized use of the server. They are not always required for WebSTAR Servers, because Macintosh systems are not vulnerable to the same kinds of attacks as other platforms. However, firewalls provide substantial additional protection, and allow you to track any attempts to break into your server.

Some routers provide firewall security. For software firewalls, see Open Door Systems

<http://www.opendoor.com/>

SSL Security

To provide a secure web site for an online store, confidential discussion area, access to proprietary databases, or other private services, you can use the **SSL** (Secure Sockets Layer) portion of the WebSTAR Server Suite. With a special certificate, this allows the server to work with browsers to send encrypted data, rather than plain text, over the Internet.



For more information, see “About SSL Security” on page 209.

CGI and Plug-In Security

WebSTAR provides several levels of security for CGIs, Plug-Ins and WebSTAR SSI commands. Even if you allow others to upload files to your server, you can use special folders to control what code runs on your machine.

CGIs

You may limit CGIs to the *cgi-bin* folder, so any uploaded CGIs cannot run. Set this limit by checking the option Restrict CGIs to CGI-BIN (described on page 137).

Plug-Ins

Plug-Ins can only be run from the *Plug-Ins* folder in the WebSTAR folder. WebSTAR will not serve any files from the *Plug-Ins* folder, although Plug-Ins can read and write to that folder.

WebSTAR SSI Security

The WebSTAR SSI Plug-In allows you to use SSI commands to run programs and include other files. You can use the options in the WebSTAR Admin panel SSI (described on page 152) to disable these commands, restrict the files used to those in the SSI folder in the CGI-BIN folder, or allow these commands to access all mounted volumes. The default setting is the most secure: the commands are disabled.

Web File Security

The WebSTAR servers will never serve any of the WebSTAR applications or settings files (these have a Creator Code beginning with “www”). In addition, WebSTAR will not serve any files from the *Plug-Ins* folder.

Security Realms



Your WebSTAR log file is automatically protected as a realm. No one can view it unless you give them access (see “Security Realms” on page 164).

WebSTAR has several options for limiting access to the site, or to parts of the site using the browser machine host name or a user name and password system. For more information, see “Security Realms” starting on page 164.

You should set up a log file analysis program and use it regularly to check who is accessing your security realms.

Robots.txt

Webcrawlers, spiders and robots may access your site to index it for search services. They follow all links on the default index page and linked pages. These agents can only read the files that are publicly accessible (not secured under WebSTAR’s access controls). The **Robot Exclusion** standard allows you work with the agents using a *robots.txt* file. For more information, see:

<http://info.webcrawler.com/mak/projects/robots/norobots.html>

FTP Security

Within the WebSTAR Admin application, you can define user names and passwords, along with the root folder for that user and whether or

not they can download or upload files, create and delete folders, and more.

You should limit access to FTP: set up your FTP folder hierarchy carefully, keep track of the users who can upload, and check your FTP logs carefully.



For detailed information, see “FTP Security” on page 337.

Safe Passwords

Passwords are only safe if no one can guess them—and if you remember them! You must be careful in setting and storing passwords, and change them regularly. In addition, you should have a password control system so that if you cannot reach your system, someone you trust can work with your server.

Make sure you have a secure storage area for your most important passwords, such as a safe, a safety deposit box, or a secure area in your supervisor’s office.

When you make a password, follow these guidelines:

- never use a word that can be found in a dictionary
- never use a family member’s name or birthdate
- never use a product or company name
- never write your password in your Scrapbook, Note Pad, or tape it to the bottom of your desk
- passwords you use for email clients, web site registration and file sharing are often visible to administrators: never use an important private password for a public site
- always make the password at least 6 characters long
- always mix letters and numbers
- make the password something you can remember
- change your important passwords periodically, at least every few months

If you follow these guidelines, it is unlikely that anyone will guess your password and be able to break into your site.

IDENTIFYING YOUR SITE: IP, HOST NAME AND DNS

To access your server, browsers and other clients have to know how to find you. The Internet (including the World Wide Web) has set up global standards that allow all systems to work together and find every other computer on the Internet. These consist of unique **IP addresses** for every computer on the Internet, **host names** such as



IP stands for “Internet Protocol”: the overall set of standards defining communications for the Internet.

TCP stands for “Transmission Control Protocol”, which is how computers send messages back and forth.

TCP/IP is used to refer to Internet networking in general.

“www.starnine.com” so we don’t all have to remember the IP addresses, and **Domain Name Servers (DNS)** which hook them all together.

WebSTAR version 3 can also support multiple web sites on one server. For more information, see “Virtual Hosts: Hosting Multiple Web Sites” starting on page 193.

IP Addresses

The Internet uses unique ID numbers called **IP Addresses** to identify each individual computer on the Internet.

These addresses are represented as four sets of 8-bit numbers (numbers from 0 to 255), with periods between them. For example, StarNine’s main web page is at:

198.211.93.9

There’s a hierarchy from left to right roughly organizing the entire Internet, so that some networks can contain other networks. The last number on the right is the **host ID** number: it identifies the individual computer.

Your Server’s IP Address

To serve data from WebSTAR, you must get at least one **static IP address** for your server machine, to identify yourself to the Internet. You may have one already: check your TCP/IP control panel. If there’s an IP Address filled in, write it down for future reference.

If you don’t have an IP address, you need to get one. Your process for doing so depends on your network connection:

If you dial up to your ISP at intervals, you probably have access to a set of **shared, dynamic IP addresses**. That’s fine while you’re browsing the Web or sending email, but it doesn’t work for WebSTAR, because no one can find you. You must arrange for a more continuous connection to your ISP and get a static IP address.

If your network doesn’t yet have TCP/IP access and you have to use a modem, you must either work with your Network Administrator to add TCP/IP support, or follow the instructions from your ISP to get a static IP address, and enter that in your TCP/IP Control Panel for your dialup connection.



You can have more than one IP address for a single WebSTAR server: see “Virtual Hosts: Hosting Multiple Web Sites” on page 193.

Host Names

Because numbers are difficult to remember, the Internet evolved **domain names** for organizations and **host names** for individual computers. These are the familiar names you see when browsing, such as `www.starnine.com`, `ftp.apple.com`, and so on.

To be exact, the first part is the computer's unique "host name", the second part is the "domain name", and the last part is the "top level domain". This section will explain each of these elements in detail.

First Element: Host Name

The **Host Name** is the unique name for a computer within its domain. It's always the first element of a full name, and, with its domain and top-level domain suffix, creates the unique name of that computer on the Internet. For example, the StarNine website is `www.starnine.com`. "www" is not unique on the web, but it is unique within StarNine.

For example, the StarNine main web server is:

`www.starnine.com`

and the server running the search engine is:

`search.starnine.com`

Both of these are host names in the "starnine.com" domain.

Defining your server host name requires you to work with your ISP or Network Administrator: see "Your Server's Host Name" on page 99 for details.

Middle Elements: Domain Name

The middle part of the name, between the host and the top-level domain is the domain.

The domain can be an organization name, such as "starnine"; a product ("webcollage"); or any other word, ("searchtools").

Domains can include several levels of naming, usually getting more specific from left to right. For example, the host name `www.ci.berkeley.ca.us` has these elements:

- host name ("www")
- domain ("ci.berkeley.ca": the City of Berkeley, California)
- top-level domain ("us").



For information on getting a domain name, see "Your Server's Host Name" on page 99.

Last Element: Top-Level Domain

Top-Level Domains (TLDs) are always the last element in a domain name.

In the United States, TLDs are divided by type of organization

- .com—businesses
- .edu—US four-year colleges and universities
- .gov—US government
- .mil—US military
- .net—network providers
- .org—non profit organizations and others

Hosts with interesting top-level domains include `rs.internic.net`, `www.nasa.gov`, `sims.berkeley.edu`, and `www.npr.org`.

Some US sites also use the two-letter state abbreviation followed by the “us” country code, like the City of Berkeley, above.

Most non-US sites use a two-letter country code as their top-level domain. Examples include `stairways.com.au`, `ibacom.es`, and `iph.fgov.be`. A full list of official codes is available at:

<http://www.bcpl.lib.md.us/~jspath/isocodes.html>

Your Server's Host Name

Together, a host name, domain name and top-level domain will identify your WebSTAR server to the Internet.

Your Domain Name and Top-Level Domain

If you are working within a larger organization, they probably already have a domain name. Therefore, the domain of your server will be the host name followed by the domain of the organization.

Registering a Domain Name

If you are independent, then you can register your own domain, and use it for your WebSTAR server. Your ISP should be able to help you register it. As of the time of this writing, the Domain Name Registry in the United States is run by Network Solutions, Inc. at:

<http://www.networksolutions.com/>

Your Host Name

If you control your own domain, you can choose any host name you like. Common practice is to make the host name for web servers “www”. Doing so gives information to people browsing the site, and



You can have more than one host name for a single WebSTAR server: see “Virtual Hosts: Hosting Multiple Web Sites” on page 193.

lets them type in the name even if they don't have a bookmark. The DNS system will automatically route requests to your server.

If you're in an organization, your computer may already have a host name. If you think you already have a host name, you can use the *IPNameTool* application from the AG Group, included on the WebSTAR CD. Enter your IP address and it will look up the name for you.

If you don't have a host name, or you want to change the name, you should arrange to have the Network Administrator help you name your server according to organization policies. They will also register it with their DNS server.

Serving Several Hosts

You can use the WebSTAR web server to respond to several host names, even in different domains, which can share the same IP address. In this case, you must arrange for the DNS records for each host name (as described in the next section), and use the WebSTAR Virtual Hosts panel to specify the names and IP addresses (if appropriate). For instructions, see "Virtual Hosts: Hosting Multiple Web Sites" on page 193.

DNS

To link the host names and the IP addresses, the Internet uses a system called the **Domain Name Service (DNS)** protocol. DNS servers keep databases of these name-address combinations and work together to keep the system up to date.

Your ISP or network administrator is probably running a DNS server. To enter your WebSTAR server into this system, you should request that your ISP or the network administrator make sure your server host name or names and IP address is in their DNS database. They will broadcast this information to other DNS servers across the Internet, and everyone will be able to find you shortly.

A Name Records

The A (Address) record is the vital link between the host name and the IP address. All Internet host machines must have an A name record somewhere in the DNS system.

The A name record contains the host name, class "IN" ("Internet"), the letter "A", and the IP address of the host machine.

domain.com	IN	A	192.0.1.1
------------	----	---	-----------

 While the host name is the name of your server, it must be included in the Domain Name system. Therefore, you'll have to work with your Network Administrator or ISP to register it.

 For technical information, see [RFC 1034](#). The most authoritative book on DNS is "DNS and Bind", published by O'Reilly.

 To distribute your server requests among machines (if your DNS server performs load sharing), you may direct one domain name to several IP addresses.

mail.domain.com	IN	A	192.0.1.2
www.domain.com	IN	A	192.0.1.1

In the example above, the `domain.com` and `www.domain.com` host names both point at the same IP address, while the `mail.domain.com` host name points at another address.



For HTTP (Web) and email serving, you must also create Host name entries in the WebSTAR Admin application. You do not have to do anything special for FTP services.

CNAME Records

The CNAME (Canonical Name) record is an alias, much like a Macintosh alias file: it points to another host name. The DNS administrator may use CNAME records to define virtual host names.

A CNAME record is just an alias, so don't try to add any more entries to that host name record, but put the other information in the A Name records instead. They are generally used in the case where you might be pointing to a host on another network that has an A record in another DNS system, for example, if your ftp server was actually located on a different network and some other DNS administrator was apt to change the A record for that host without notice.

The CNAME name record contains the host name which is the alias, class "IN" ("Internet"), "CNAME", and the real host name for the alias to point at. For example, this entry:

ftp.domain.com	IN	CNAME	www.domain.com.
----------------	----	-------	-----------------

directs all requests for the host name `ftp.domain.com` to the machine which hosts `www.domain.com`.

MX Records

MX (Mail Exchange) records specify whether the host is running an email server or messages for this host should go to another mail server machine. For more information, see "DNS Servers and Mail Hosts" on page 362.

Secondary DNS Services

If your DNS server goes offline for any reason, links to your site will fail and email will bounce. Therefore, the domain registries generally require you to register at least one alternate DNS server. You should make sure that the secondary servers are located on other networks (so local problems will not affect them) and have all current information. Your ISP or institutional DNS administrator can help you



Never put the CNAME on the right side of a DNS entry: always use the A (authoritative) name on the right.

to update this information. This is particularly important if you are running WebSTAR Mail.

Checking Your DNS Entries

To make sure that your DNS entries are correct, you should check them periodically.

There are two free online forms for checking DNS status. The British ISP Demon.net has a slightly different form at:

www.demon.net/external/ntools.html

And the Men & Mice company provides a form at

<http://us.mirror.menandmice.com/cgi-bin/DoDig>

Running Your Own DNS server

If you are independent or have a cooperative network administrator, you can run your own DNS server. This allows you to add Virtual Domains quickly, and to alias several IP Addresses to one domain name, for load balancing, mirroring and other purposes. There are several Mac OS DNS servers available, for information, see:

www.starnine.com/extendingwebstar.html

WebSTAR Server Suite includes a Plug-In to work with QuickDNS from Men & Mice, which provides local DNS services and server load balancing.

Port Numbers

The TCP/IP standard defines **port numbers** which allow one machine to serve several different kinds of data, such as HTTP, HTTPS, FTP, SMTP, POP and so on. The default services are specified in the range 1 to 1000.

WebSTAR Default Port Numbers

The WebSTAR Admin application and Plug-In also use ports to communicate for remote administration. The default number for each server is the port number of the server + 1000.

Web Server

- default port: 80
- administration default port: 1080 (default port + 1000)

You may notice attempts to use port 1080: this is also used by the network security protocol SOCKS, and is not necessarily an attempt to break into the WebSTAR Admin.



WebSTAR allows you to override the default Web request port numbers: see “HTTP Port” on page 135.

Secure (SSL) element of the Web Server

- default port: 443

FTP Server

- default ports: 20 and 21 (for commands and data, respectively).
- Browser FTP client defaults: port numbers 9000 through 12000. Browsers accessing the FTP server use the “PASV” option and these ports.

Mail Server

- SMTP port: 25
- POP client access port: 110
- IMAP client access port: 220
- LDAP client port: 389

Proxy Server

- default port: 8000

Firewalls and Server Ports



Firewalls are not required, but they definitely improve server security.

If you have a network security firewall in your company, your machines are probably limited to serving TCP requests from within your company. If you want to serve the Internet rather than an Intranet, you will probably have to ask your network administrator to open “holes” in the firewall for the appropriate ports on your WebSTAR server. Otherwise the firewall will refuse all URLs for your server from outside your company on those ports. WebSTAR Admin also communicates via TCP/IP. Therefore, to administer a WebSTAR server remotely, you must also have a hole in your firewall for the Admin application port (1080 by default).

IMPORTANT WEBSTAR FILES



All settings and User files have the WebSTAR file Creator code (wwwΩ) so they will never be served by WebSTAR.

The WebSTAR server application creates several important files. You should make sure to back these up regularly, and to copy them if you move your server to another machine. Many of these files can only be opened by WebSTAR, and have a Creator Code of “wwwΩ”. Others, such as the log files, are text files, and you can open them in a text editor, database import dialog or log analysis program.

The WebSTAR Log files correspond to the WebSTAR server monitor windows. They save a permanent record of all transactions on your Web, FTP, Mail and Proxy servers. Note that server log information is stored along with web server information in the *WebSTAR Web.log* file in the *logs* folder.

WebSTAR.Messages File

The WebSTAR Server logs all serious start-up problems it encounters to a special file called *WebSTAR.Messages*, which is always in the WebSTAR folder. Any line in this file that begins with the string “ERR:” contains a message describing a problem that caused WebSTAR to terminate.

This file is especially useful with the background-only version of the WebSTAR Server, which does not display a Status window. If you contact StarNine Technical Support, they may request that you open or send this file.

The *WebSTAR.Messages* file is **not** incremental: it is started anew every time you start the server. If you don’t look at the data before you relaunch the server, all the contents will be lost.

Web Server Files

Settings

The *WebSTAR Settings* file, always located in the WebSTAR folder, stores the WebSTAR serial number, custom server settings, and settings for the standard included WebSTAR Plug-Ins, including the Proxy Server Allow/Deny lists. As this file is very important, we recommend that you **archive it often** and save old versions.

If the *WebSTAR Settings* file gets damaged, the server may crash, you may be prompted to re-enter the serial number, or you may notice that your server’s configuration information has been lost. In that case, you should restore the previous backup of this file and re-enter any changes you have made.

Web Users File

The *WebSTAR Web Users* file stores user names and passwords for your web server (see “Web Users and Passwords” on page 168). The user entries are not synchronized to the *WebSTAR.Settings* file, so it may contain names for realms which no longer exist. This file is not stored in a human-readable format, and you cannot edit it. You should use WebSTAR Admin to export the list, edit the exported version, and import the changed list, as described in “Importing and Exporting Large Users Lists” on page 170.

It’s a good idea to back up this file often, in case something goes wrong on your hard drive or machine.



This file used to be known as *WebSTAR.pass*.



For information, see “Log Archiving” on page 122 and “Logging” on page 199.

Server and Web Log File

All WebSTAR initialization, error, and status messages, along with Web requests, are stored in the *WebSTAR Web.log* file, in the *logs* folder. If you want to perform log analysis on your web server, use this file.

If you enable the Log Archiver, which copies log files at specific intervals, web server log files will be stored in the *archived_logs* folder inside the *logs* folder.



For information on the FTP server, see “FTP Server Administration” on page 341.

FTP Server Files

FTP files are generally stored in the *Plug-Ins* folder, in the *WebSTAR FTP Data* folder.

FTP Settings File

This file contains the connection and server information.

FTP Users File

The *FTP Users* file stores the user names and passwords you've defined in your FTP server.

This file is not stored in a plain-text format, and you cannot edit it. You should use WebSTAR Admin to export the list, edit the exported version, and import the changed list, as described in “FTP Users Import & Export” on page 347.

WebSTAR FTP.log File

All FTP requests, responses and error messages are saved in this file. For more information, see “FTP Monitors & Logging” on page 349.

The *WebSTAR FTP.log file* is located in the *logs* folder.

Mail Server Files



For information, see “WebSTAR Mail Files” on page 357.

Most Mail server files are in the *Webstar Mail Data* folder in the *Plug-Ins* folder.

WebSTAR Mail.log File

Mail server transactions, including logons, logoffs, incoming and outgoing messages, LDAP requests and so on, are stored in this file. For information on setting the location and archiving schedule, see “Logging Options Settings” on page 403.

The *WebSTAR Mail.log file* is located in the *logs* folder.

Proxy Server Files

Proxy files are generally stored in the *Plug-Ins* folder, in the *WebSTAR Proxy Extensions* folder.

WebSTAR Proxy.log File

All Proxy requests, responses, status and error messages are saved in this file, located in the *logs* folder. For more information, see “Proxy Server Monitor & Logs” on page 421.



For information, see “WebSTAR Proxy Server” starting on page 411

SERVER TROUBLESHOOTING

How to Get Help

WebSTAR Support on the Web

The WebSTAR Support area contains the **FAQ** (Frequently Asked Questions List), Technical Notes, updated Troubleshooting, and additional online help about such topics as memory allocation and performance optimization. It can be found at:

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

WebSTAR-Talk Mailing list

The email discussion list, WebSTAR-Talk, provides an excellent resource for questions and discussions. In addition to StarNine support and engineering staff, other web administrators and third-party developers provide answers and advice.

Sign up for the WebSTAR-Talk list on the Web at:

<http://www.starnine.com/support/maillinglists/maillinglist.html>

Or send an email message with the word “subscribe” in the subject to:

<mailto:webstar-talk-request@starnine.com>

You can search the archives of this mailing list as well:

<http://search.starnine.com/talklists.html>

Email and US Mail Technical Support

StarNine's Support staff will answer email and mail in a timely manner. Email and mail support is free.

<mailto:support@starnine.com>

US Mail

StarNine Technologies, Inc.
ATTN: Support

2550 Ninth St. Suite 112
Berkeley, CA 94710 USA

Telephone and Fax Support

StarNine provides telephone support on weekdays between 8 am and 5 pm, Pacific Time. Telephone support is free for the first ninety (90) days after your purchase. Some charges may apply for additional telephone support.

phone: (510) 704-1272

fax: (510) 548-0393

WebSTAR Debug Plug-In

The WebSTAR Debug Plug-In is a troubleshooting tool that can help StarNine Support track down the causes of repeated server crashes. It will store information about your system, memory, server configuration and current applications, WebSTAR callbacks, internal data about the most recent functions called.

When the Debug Plug-In is installed, however, it will use some of the system resources, slowing down your server. You should only install it if you are having repeated crashes and someone at StarNine requests the information. Then, the next time your server crashes, you will find a file named *WebSTAR Debug.log* in your WebSTAR folder. When you launch WebSTAR again, the file will be renamed to include the date and time the server crashed, and the Debug Plug-In will create a new file for tracking any future problems.



Do **not** send the debug files to mailing lists. They are too long, and the information should be kept private for your security.

If you wish to read the contents of the file, open it in a good text editor such as BBEdit, but don't make any changes to the file if you intend to send it to StarNine.

If someone at StarNine has requested the information, you can email this file to them. To avoid sending the file as part of the message, stuff it before attaching it.

Installing and Enabling

WebSTAR Debug is not installed by default. You should launch the WebSTAR Server Suite Installer and select Custom Install, then WebSTAR Server Suite 4 > WebSTAR Plug-Ins > Extra Plug-In Modules > WebSTAR Debug. If you select the folder above the WebSTAR folder, and have not changed the folder name, the Installer will place the Plug-In in the *Plug-Ins* folder. Otherwise, it will make a new folder

containing a new *Plug-Ins* folder. In that case, drag the *WebSTAR Debug* file into your main *Plug-Ins* folder.

You must quit and restart the WebSTAR application to enable the WebSTAR Debug to start tracking the server's activities.

Removing and Disabling

To disable the Plug-In, remove it from your *Plug-Ins* folder. Then quit the WebSTAR application and restart it.

Debug Files

While WebSTAR is running, there will be a file named *WebSTAR Debug.log*. This file remains empty unless your server crashes. If that happens, data is written to the file.

If you relaunch your server, the file will be renamed to include the date and time, such as *WebSTAR Debug.19990507.122133*. This system retains old log files after restarts.

General Server Troubleshooting Guidelines

Please note that updated information for all troubleshooting is available at <http://www.starnine.com/support/>.

WebSTAR crashes, quits, reports “out of memory” errors, or has intermittent network problems.

- If WebSTAR crashes, it may be due to **conflicting software, hardware, or other application processes** on the server machine.
- Most crashes are caused by **a Plug-In or CGI**. If you have recently added a new Plug-In or CGI to your configuration and the server become less stable, you should first try removing the recently installed item(s). If that helps, be sure to check the web site of the publisher to make sure that you have the most recent version of the Plug-In or CGI, and to determine if there are known conflicts.

For more information, see “Plug-In Problems” on page 327.

- If Plug-Ins are not the culprit, try these steps:
 - **Run a disk repair utility and rebuild the desktop** file (with Extensions off). This will fix any resource problems that can cause the file system to report errors.
 - **Do not use a screen saver.**
 - Temporarily **disable any background applications or scripts** that are running on the server machine.
 - **Minimize extensions.** Install only the minimal or base Mac OS Extensions. If you continue to experience problems, disable third-party Extensions and Control Panels. The only extensions



See also “Web Server Troubleshooting” on page 327, “WebSTAR FTP Trouble-shooting” on page 355, “Mail Server Troubleshooting” on page 407 and “Proxy Server Trouble-shooting” on page 423.



If the server crashes more than once, install the WebSTAR Debug Plug-In (described above).



You may want to install Apple's MacsBug low-level debugger to log crashes and facilitate troubleshooting.



For best stability, set the RAM allocation according to the guidelines in “Server Application Issues” on page 87.

needed to run WebSTAR are Open Transport TCP/IP, and AppleScript.

- If you're **upgrading your system software**, we recommend following the Apple guidelines which suggest a clean install. If you experience server instability following an OS upgrade, it may be resolved by reformatting the hard drive, and reinstalling the system.

- **Bad RAM** can cause intermittent crashes or other inconsistent behavior. If you've recently installed additional RAM, try removing it, installing alternate RAM chips, or running WebSTAR on a different machine.

- **WebSTAR may have run out of memory.** The most common reason for this is an attempt to process too many concurrent connections. If you have increased the Maximum Connections setting, you should also increase the WebSTAR server application RAM allocation.

If you have followed the guidelines on RAM allocation, you should also check the documentation for any Plug-Ins you have installed as they may require additional memory.

- There may be a **problem with your TCP/IP settings** and memory fragmentation. See “Keep Open Transport Loaded” on page 31 for instructions on avoiding fragmentation
- A **bad Ethernet cable** can produce intermittent network errors. Try substituting a different cable.

Error message: -42 too many open files

Newer versions of the Mac OS use up more of the allowed files, so you may see this error. There are various ways you can reduce the load on the server:

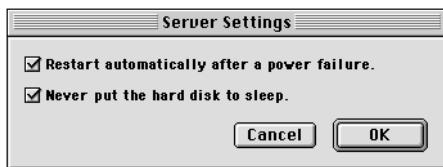
- Increase the size Data Cache (described on page 140) to load more files into memory rather than reading them from disk.
- Avoid using your WebSTAR server machine for other tasks.
- Close unused applications.
- Move some external functions to other servers, such as DNS servers or FileMaker databases.
- Run copies of WebSTAR on different machines, so the Web, FTP, Mail and Proxy servers can each handle specific requests. Contact sales@starnine.com for multiple-license pricing.

Server Fails To Respond

- On early Power Macintosh computers with built-in Ethernet (6100s-9500s), some server machine may **lose all networking communications (go “deaf”)** after large data transfers. This can be triggered by backup systems such as Retrospect, but is not caused by these programs.

The solutions are:

- upgrade to Mac OS 8.6 and the *Apple Enet* extension, version 2.1.2.
- use a third-party Ethernet card
- use Mac OS 8.1, remove the *Ethernet (Built-In)* extension and replace it with the *Apple Enet* extension, version 2.1.2.
- **Bad Ethernet drivers** can cause intermittent server “deafness”. Check Apple software updates or technical notes or consult with the manufacturer of your Ethernet card.
- **Open Transport problems** can also make your server fail to respond to any TCP connections. The only solution is to restart the server machine. Future versions of the Mac OS, after 8.6, may solve this problem.
- **The Mac OS Energy Saver** may have shut down your hard drive. Open the Energy Saver Control Panel, choose Server Settings from the Preferences menu, and check the boxes to automatically restart and never put the hard disk to sleep.



Error -120 while resolving alias path to log folder

- The server has lost track of one of the log folders. Use the Admin application to specify the correct location of your logs. If this fails, quit your WebSTAR Server Suite, move your logs out of the WebSTAR folder, and relaunch. New logs will be created in the locations specified by your settings in the Admin application.

Red “Memory Error” light appears in the Status window

- If you have recently added Plug-Ins or increased a cache, you may have used up all the server’s available memory. Look at the Status window displays on Memory (described on page 79) to see more information.
- If you are low on memory on the machine, you can remove Plug-Ins or decrease cache sizes.
- If you have more RAM available on the machine, allocate more to the server. Quit the WebSTAR application, select it, choose **Get Info** from the File menu. For Mac OS 8.5 and later, you should select **Memory** from the Show menu. Increase the number in the **Preferred Size** field, and close this window. Restart the WebSTAR server.
- If you have plenty of memory when you launch the server, but run out if you use the Directory Indexer Plug-In, you may be the victim of a corrupted resource fork. Try running Norton Utilities or

another hard drive diagnostic tool, and fix any files on your server with a bad resource fork.

Error: Log Archive FSSpec in the Web monitor or log

If you see this error, you have selected a disk other than the disk where the WebSTAR application is running as the location of your log archive folder. Copying log files to other disks can slow down the server considerably, so WebSTAR will only allow you to archive log files locally.

To fix this problem, open the WebSTAR Admin application, choose the Log Options panel for each server, and set the Log Archive location to a folder on the same hard drive as the WebSTAR folder. For instructions see “Log Archiving” starting on page 122.

This chapter provides information on using the WebSTAR Admin application. It covers how WebSTAR Admin connects to servers, and how to use the programs.

For information on individual servers in the suite, see “About Web Serving” starting on page 179; “WebSTAR FTP Server” starting on page 337; “WebSTAR Mail Server Overview” starting on page 357 and “WebSTAR Proxy Server” starting on page 411.

ABOUT THE WEBSTAR ADMIN APPLICATION



The WebSTAR Admin application is a Mac OS program which allows you to monitor and configure your WebSTAR server. As you change your server settings with the WebSTAR Admin application, it updates the *WebSTAR Settings* file on the server machine. Be sure to **back up the WebSTAR Settings file frequently**, so the data is preserved.

You can run the WebSTAR Admin application on the same machine as your server, or on any other local or remote PowerPC Mac with access to the server via an intranet or the Internet. That’s because it communicates with your WebSTAR server application using TCP/IP, just as web browsers and FTP clients contact your server.

WebSTAR Admin can simultaneously administer many different machines running WebSTAR servers. However, versions are not interchangeable: old versions of the Admin can’t control new versions of the server, and vice versa.

Connecting To A Server



If you have a firewall, you may have to ask your network administrator to let you access the WebSTAR administration port: see “Port Numbers” on page 102.

The WebSTAR Admin lets you connect to your WebSTAR server simply by entering the host name or IP address, port number, and password. You can even save this information in an Admin Connection file, and then use it to connect again.

The Connection dialog remembers the last ten servers you connected to, and displays them in a popup menu:

WebSTAR Admin connects only to the primary domain name and IP address: it ignores all secondary IP addresses and host names, even if you have enabled Virtual Hosts. You can do all administration for all hosts using this access.

You can see the monitor windows for Web, FTP, Mail and Proxy servers, and edit the server settings remotely. All your changes are cached, and will be sent to the server as soon as you press the **Save** button in the Settings window.

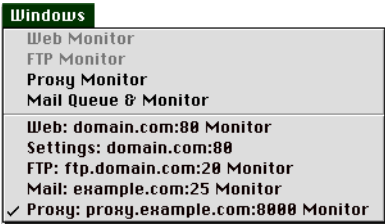
Connecting to Multiple Servers

You can open several connections to different servers, either on separate machines or on separate ports on the same machine (such as the SSL server).

If you have a connection to more than one server, only one is known as the **current server**, and all your commands will go to that server. The active monitor window defines the current server. As each monitor window displays the server name and port number in the title bar, you can always tell which server is currently selected.

The Windows menu also tells you which windows are available and which are already open.

 For more information on the monitor windows, see “Admin Monitor Windows” on page 116.



For your convenience, you can drag data and drop from one server setting window to another.

Admin Connection Documents

WebSTAR Admin can create **Admin Connection** files. These store the domain name or IP address and port number, so you don’t have to type them in every time, along with window positions. You can open them instead of retyping every time.

Disconnecting From a Server

There are two ways to disconnect your WebSTAR Admin application from a server.

Disconnecting by Closing Windows

You must have at least one monitor or settings windows for a server open to remain connected to that server. When you close all windows, you disconnect the Admin from that server.

Admin Timeout

The WebSTAR Admin will break its connection after one hour of inactivity. This reduces the chance that a forgotten administration session will be used by an unauthorized person, or permanently block one of the two allowed simultaneous Admin connections. WebSTAR Admin will bring up the Connection dialog and allow you to enter your password to reconnect.

WebSTAR Admin Security

The WebSTAR Admin encrypts all communication to the server, so no one else can read or send instructions. The encryption key is changed for each connection. This allows you to make changes from any Mac on the Internet, without worrying about security.

For security, access to the WebSTAR Admin application is password-protected. To set this password, you must have access to the WebSTAR Server Suite on the server machine. Do not use the same password as you use for the Browser Admin pages. Change the password at regular intervals, such as every month. For instructions on entering your administration password in the WebSTAR server, see “Admin Password” on page 49.



See Also: “Safe Passwords” on page 96.

The WebSTAR Admin Connection dialog can also remember your password. Only check the **Save Password** box if you are on a very secure computer, such as one in a locked room, that is not accessible to strangers.

ADMIN MONITOR WINDOWS

The WebSTAR Admin monitor windows contain much the same information as the server monitor windows. Each window title includes the server type (Web, FTP, Mail or Proxy), the host name or IP address (from the Connection dialog), and the port number.

The server monitor windows themselves contain a status pane and a log entry pane. Most of the information in these windows is the same as in the WebSTAR Status and Monitor Windows (described on page 77).

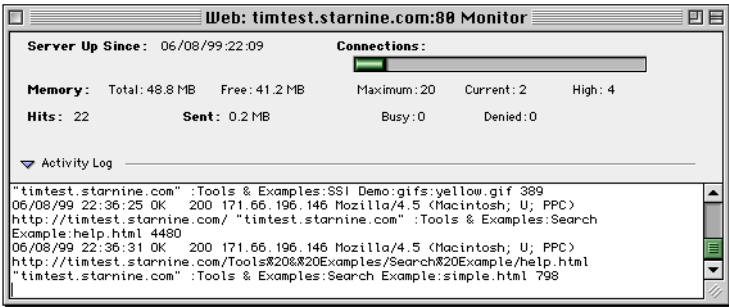
The Server Up Since number is updated while the Admin is connected: when the Admin is disconnected due to a timeout, that area says “Server Not Available”.

You can use the mouse to select text, then copy it to the Clipboard and paste to a text editor.

Admin Web Monitor

The WebSTAR Admin Web monitor window is somewhat different from the server Web monitor window. The Status pane is much like the Status Window Top Panel (described on page 78), although it does not have the histogram, LED, or “high-water marks” in the Connections and Memory bars.

 The monitor window is similar to that of the server: see “Web Server Monitoring” on page 81 and “Log Formats” on page 200 for details.



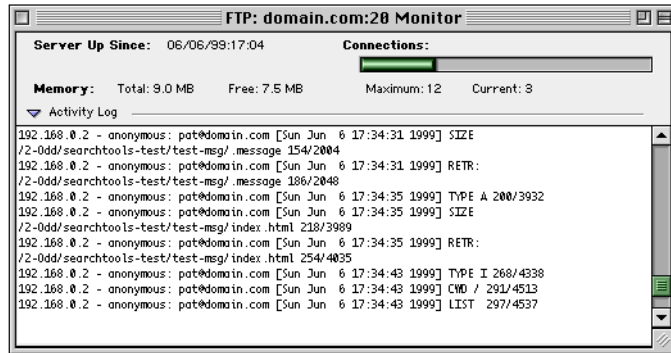
Admin FTP Monitor

The FTP monitor is much like that of the server. The status pane displays a Connections bar indicating the percentage of available connections now in use, the maximum possible connections and the current number of connections. The logging pane below it shows the



For more information, see “FTP Monitors & Logging” on page 349.

actions of the FTP server, including client logins, file transfers and so on.

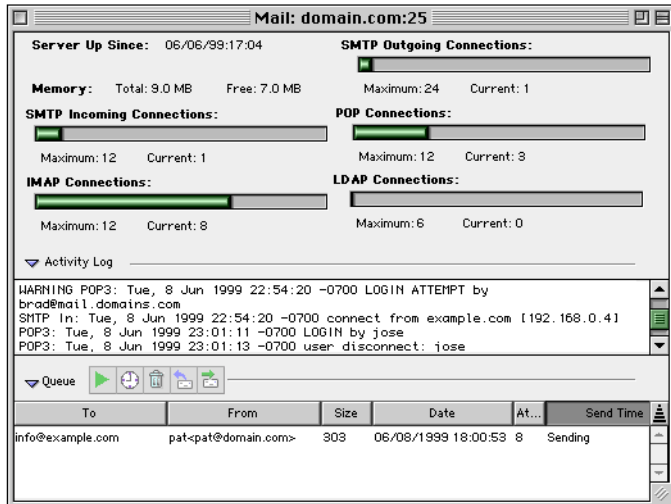


Admin Mail Monitor



For more information, see “Mail Monitors, Logs, and Reports” starting on page 399.

The Mail Monitor shows how many connections are currently in use, the log of the most recent mail transactions, and the items in the queue waiting to be sent.

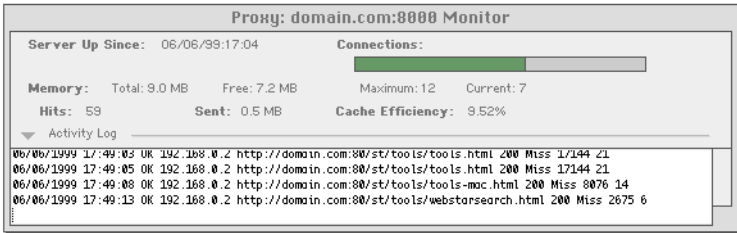


Admin Proxy Monitor

The Proxy monitor is much like that on the server. The status pane displays the number of bytes sent, the number of files matched in the cache, a bar indicating the percentage of connections used, the maximum number of connections and the current number of connections. Below it, the log pane shows the date, time, HTTP status,

requesting browser’s IP address, URL, Proxy Cache status (Hit, Miss or Pass), bytes transferred and time taken.

 For more information, see “Proxy Status Window & Log File” on page 421



WEBSTAR ADMIN MENUS

File Menu

New Connection

The New Connection dialog allows you to specify the host name (or IP Address), port number, and administration password of your WebSTAR server. If you should lose your connection to the server, you may have to re-connect using this dialog.

Open and Save

WebSTAR Admin can create **Admin Connection files**. These store the host name or IP address and port number, so you don’t have to type them in every time. When you choose Open, you can select one of these files and it will bring up the Connection dialog, with the information filled in. For security, you will always have to enter your password in this dialog.

Close and Quit

Closing all a server’s connection windows will close the connection to the server.

Quitting the Admin application will also close the connection to the server.

 There is also an option to quit the WebSTAR server application remotely: see “Quit WebSTAR” on page 119.

Edit Menu

Undo / Cut / Copy / Paste / Clear / Select All

Normal editing commands apply to the dialog text fields and log windows of the WebSTAR Admin application.

Server Settings

This option opens the Server Settings window for the active server, allowing you to specify settings for Web, FTP and Proxy servers. For more information, “Web Server Administration” starting on page 129, “FTP Server Administration” on page 341, “WebSTAR Mail Settings” on page 373, and “WebSTAR Proxy Server Settings” on page 415.

Options Menu

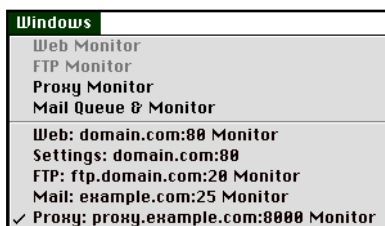
This menu always applies to the current server (the server in the active monitor window). They are permanent changes, saved in the *WebSTAR Settings* file. The commands on this menu duplicate those in the WebSTAR server Options Menu (described on page 85).

Quit WebSTAR

This will tell the active server to shut itself down, even if it's on a remote machine. It will not restart until a person launches it or, if you have arranged it, a script or other program launches it, so use this command with caution.

Windows Menu

This menu allows you to navigate among the Admin application's windows.



The active window is checked.

Available Windows

The four top menu items: Web Monitor, FTP Monitor, Proxy Monitor, and Mail Queue & Monitor refer to available windows for the current server (designated by the active window). If these items are gray and disabled, the windows are already open.

Open Windows

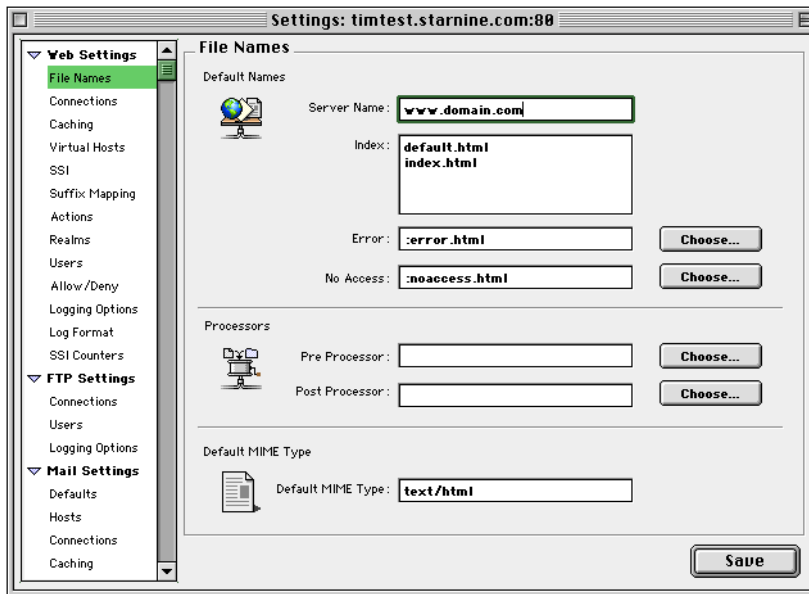
The lower part of the menu is a list of all open windows, including the server which that window is connected to.

WEBSTAR ADMIN SERVER SETTINGS

To open the settings window, connect to your server and choose **Server Settings** from the Edit menu.



To connect, see
“New Connection”
on page 118.



On the left, you'll see the Web, FTP, Mail and Proxy Settings, with disclosure triangles (like the Finder List view), and entries for the settings panels for each. If you are missing FTP, Mail, or Proxy, that Plug-In was not in the server's Plug-Ins folder when the server was launched.

The **Save** button at the lower right sends your changes to the WebSTAR server, which saves them in the *WebSTAR Settings* file.

If you close without saving, you'll get an opportunity to save changes to the server, or discard your changes.

Working With Admin Lists

Editing Entries

- To make a **new** entry, click the **New** button or press Command-Plus. This will allow you to fill in the fields for this entry. To insert an entry into an existing list, select the entry **before** the new entry, and then click “New”.

- To **edit** an entry, click on the line to select it. As you make changes in the edit fields, they will be reflected in the list. The changes aren't saved to the server until you click the **Save** button.
 - To **copy** an entry, select it and choose **Duplicate** from the Edit menu, or option-drag the entry.
 - To **move** an entry, select it and drag it with the mouse button down. A black bar will indicate where it will be inserted.
 - To **delete** an entry, select the line and click the **Delete** button.
- If you accidentally delete something and want to restore it, you can close the Settings window and click the **Don't Save** button.

Sorting Lists

You can sort the contents of many of the lists in the WebSTAR Admin: SSI Counters, FTP Users, Mail Hosts, and Mail Users & Accounts. To sort these lists, simply click on the title of the column containing the value you want to use for sorting. The data will be sorted from left to right using the standard Mac OS sorting toolkit, so numbers will go from 1 to 100 to 2 to 3 to 30 and so on.



These lists may not be stored in the sorted order, but you can control how you see them.

File Paths in WebSTAR Admin

There are several options in WebSTAR Admin that require you to specify a unique file. This **file path** lets the WebSTAR server locate the file properly. The Macintosh OS file path **delimiter** is a colon (":"), separating folder names. Paths to files end with the file name, while paths to folders end with a colon.

WebSTAR Admin file paths are not case-sensitive, and they can include spaces and Macintosh extended characters.

Absolute File Paths

File paths can be **absolute**, starting from the name of your hard disk. In that case, they do not start with a colon, because there is no parent folder:

```
Mac HD:WebSTAR 3.0:images:navbar.gif
WebServer:WebSTAR3.0:widgets:
FTP-HD:pub:human resources:
```

The FTP Server requires absolute file paths for the user root folders.



HTTP requests and URLs use slashes (/) as a delimiter, rather than colons.

Relative File Paths

Some server file paths can be **relative**, starting from your root folder. They always start with a colon, to indicate that they are subfolders, like these:

```
:images:navbar.gif
:default.html
:products:announcements:bluewidgets:version3:
```



Relative paths are usually used by the Web server.

Default Root Folder

The **default root folder** is the folder in which the active WebSTAR server application is stored. Virtual Hosts designate their own root folders, and paths for their files refer to that root: see “Virtual Host Root Folders and Default Files” on page 196.

LOG ARCHIVING

Log Archiving allows you to save separate log files covering specified periods of time, such as every day, every week on Thursday, or monthly. The log files are automatically created at the time you set, filled by the server, then closed, moved and the next one is created.

How Log Archiving Works

The automated archiving saves a copy of your log file at a specified interval, with the date and time in the file name. This keeps the log file from getting too big and makes it easy to locate a specific time period. By default, log archiving is **off**. You should enable it if your server is at all busy.

Log Archiving Process

When it archives a log, the WebSTAR server will temporarily suspend logging, transfer the log file to the specified location, then create a new log file in the *Logs* folder (or the location you specified in the Logging Options part of the panel).

The file will be named by the day and time that it is created. For example, a mail log archive made at 1 PM on February 6 is named *WebSTAR Mail 1999.02.06.13.log*.

The archived log file name specifies when the archived period **ended**, not the when the archive period **began**. While this is slightly



Make sure that you are copying logs to the same volume. It takes much longer to copy them to another volume than to move a file on the same volume.

confusing, it more accurately reflects the contents of the file, particularly if you switch from one schedule to another.

WebSTAR follows certain automated procedures when the scheduled log archiving time arrives. This allows the servers to continue handling requests while copying the log information and clearing the main log file.

- 1 The associated server (Web, FTP, Mail, Proxy) stops logging temporarily.
- 2 The Log Archiver moves the log file to the specified location and names it with the name of the server and the ending time (e.g. *WebSTAR 1999.06.01.14.log*).
- 3 It creates a new current log file so that logging can start fresh.
- 4 The Log Archiver notifies the associated server that it can start logging again.

Log Status Reporting

When the Log Archiver moves a log file, it reports it in the Web Monitor and Status window:



Log file analysis programs will ignore lines starting with !!.

```
!!LOG ARCHIVER: 05/04/1999 19:33:09 Log successfully archived for WebSTAR
Web server
```

If there's an error, it will report it as well.

When you start the WebSTAR application, the status of the archiving is displayed in the Status window and stored in the Web Log file, like this:

```
!!LOG ARCHIVER:Log archiving for WebSTAR FTP server is scheduled to run
hourly
!!LOG ARCHIVER:and will next occur on 06/01/1999 at 06:00 PM.
!!LOG ARCHIVER:Log archiving for WebSTAR Proxy server is disabled.
!!LOG ARCHIVER:Log archiving for WebSTAR Mail server is scheduled to run
hourly
!!LOG ARCHIVER:and will next occur on 06/01/1999 at 06:00 PM.
```

When you launch the WebSTAR application and the server was down during the time when the log was to be moved, you'll see a message like this:

```
!!LOG ARCHIVER:A scheduled WebSTAR Web server log archive operation was
missed.
!!LOG ARCHIVER:It has been re-scheduled to occur in 3 minutes.
```

```
!!LOG ARCHIVER:The WebSTAR Web server log will then be archived hourly, as configured.
```

```
!!LOG ARCHIVER:06/01/1999 17:06:47 Log successfully archived for WebSTAR Web server
```

Log Archiving Settings

Each server settings section of the WebSTAR Admin allows you to specify the log archive status, schedule and location.

The screenshot shows a window titled "Log Archiving". On the left is a folder icon. To its right are two radio buttons: "On" (selected) and "Off". Further right is the "Archiving Schedule:" label followed by four radio buttons: "Hourly", "Daily", "Weekly" (selected), and "Monthly". Below these are three input fields: "Hour of the day:" with a spinner box showing "0", "Days of the week:" with a dropdown menu showing "Sunday", and "Days of the month:" with a spinner box showing "0". At the bottom is the "Archive logs at:" label followed by a text box containing "logs:archived_logs:" and a "Choose..." button.

Archiving Schedule

There are several radio buttons for specifying the archive schedule to copy the mail log to an archive file:

- **Hourly** will make the copy every hour, on the hour
- **Daily** will make the copy once a day, at the specified hour.
- **Weekly** will make the copy once a week, at the specified hour and day of the week.
- **Monthly** will make the copy once a month, at the specified hour and day.

Hours of the day

This specifies the hour for archive copying in a 24-hour clock, so "17" is 5 PM. The hour can range from 1 (1 AM) to 24 (12 midnight).

The field is enabled except when the Hourly archiving is selected.

Days of the week

This popup menu lets you choose the day of the week for archive copying. It is only enabled when Weekly archiving is selected.

Days of the month

This field lets you specify the day of the month, from 1 to 31, on which to copy the log to the archive. It is enabled when you are archiving Monthly.

Archive logs at

This field lets you specify the folder to store archive log files. Press the **Choose** button, and choose the folder from the server disk or type a file path.

The default value is the *archived_logs* folder in the *Logs* folder in the WebSTAR folder. You can download the archived logs by FTP or view them as text files in your web browser. These can also be imported into FileMaker Pro or Excel, or analyzed with a third-party product such as Funnel Web.

The archived files will be named according to their server, date and time, except for the Web server log. For historical compatibility, it is just called "WebSTAR". Example log names are:

```
WebSTAR Mail 1999.02.06.13.log.
WebSTAR FTP 1999.02.06.14.log
WebSTAR 1999.02.06.15.log
WebSTAR Proxy 1999.02.06.16.log
```



Archiving on the same hard drive is much faster, because the server can move the file rather than copying it.

Be sure to store everything on the same hard drive as the server. Do **not** designate a remote volume, which may be inaccessible when needed.

Status Reports

The Log Archiver will provide periodic status reports in the Web server monitor window. For example:

```
!!LOG ARCHIVER:=====
!!LOG ARCHIVER:LOG ARCHIVER STATUS REPORT:
!!LOG ARCHIVER:No logs are currently being archived
!!LOG ARCHIVER:=====
```

BROWSER-BASED ADMIN

If don't have access to the WebSTAR Admin application, you can view your administration tasks from a browser. Note that the Browser Admin is not as secure as the Admin application: communications with the server are not encrypted. If you do use this method, be sure to change your password frequently.

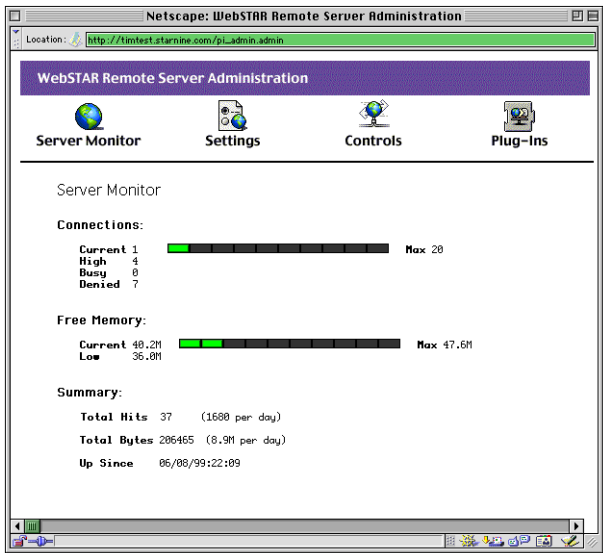
To use the Browser Admin pages, be sure that you have added an Allow entry or password for the ADMINISTRATION realm using the WebSTAR Admin application before trying the Browser Admin pages.

To access the administration pages, use the following procedure:

- 1 Launch the web browser of your choice.
- 2 Connect to the administration URL, which is your server's name followed by "pi_admin.admin", for example:
`http://www.domain.com/pi_admin.admin`
- 3 If you have not explicitly allowed your machine's host name, you'll see a User Name and Password dialog. Enter the name and password you have designated for the Administration realm.
- 4 You'll see the WebSTAR Remote Server Administration page. Use the buttons and links to navigate to the task you wish to accomplish.

 see "Setting the Browser Admin Password" on page 55.

 If you bookmark this URL, you won't have to type it in every time.



Server Monitor

The default page displays information like that in the Status Window Top Panel (described on page 78). This window updates according to the Status Report Delay (described on page 200): the default is every 15 seconds.

Settings

The Settings page contains links to pages for these web server settings:

- Suffix Mapping (described on page 154)
- Actions (described on page 161)
- Security Realms (described on page 164)
- Allow/Deny (described on page 172)
- Misc. Settings (see “Connections Settings” on page 134, “Caching” on page 139 and “File Names and Paths” on page 130)
- Log Formats (described on page 200)

Controls

The Controls page provides some of the options from the WebSTAR Server Menus (described on page 83).

Plug-Ins

The Plug-Ins page lists the WebSTAR server Plug-Ins. Some are only configurable through this page: they have a link that says **Click Here**. Others are not configurable and have a link that says **pre-set**. If you click on that link, you’ll see the server’s error page.



See “WebSTAR Plug-Ins” starting on page 235.

This chapter describes how to specify the Web server options, such as default files, number of connections, file info and data caches, virtual hosting setups, file mapping, security realms, user names and passwords. Web logging information is described in “Web Server Logging” starting on page 199, and for the SSI panels, see “SSI Administration & Security” on page 296. and “Editing Counters and Numeric Variables” on page 297.

For information on how web servers work and setting up your folders for web serving, see “About Web Serving” starting on page 179. For the other servers, see “WebSTAR FTP Settings” on page 341, “WebSTAR Mail Settings” on page 373, and WebSTAR Proxy Server Settings (described on page 415).

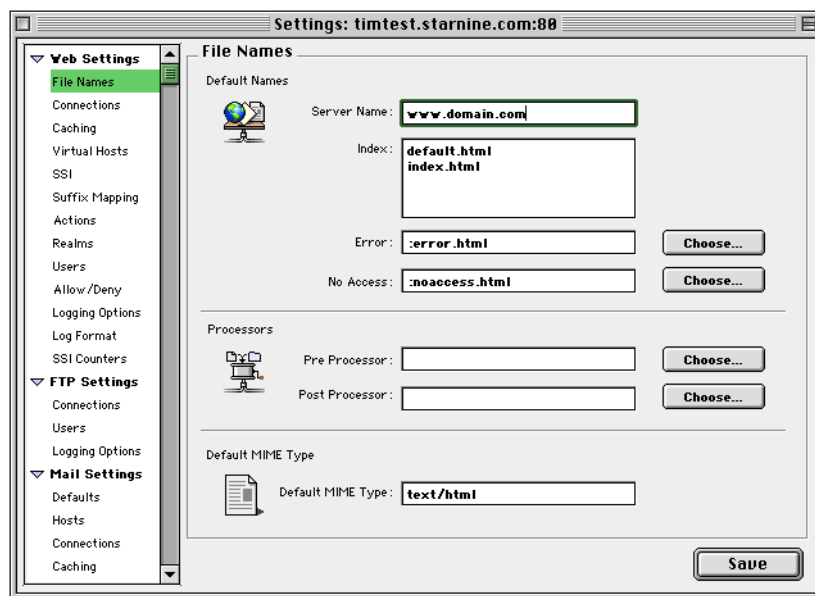
WEBSTAR ADMIN APPLICATION



WebSTAR stores the web admin data in the *WebSTAR Settings*, *WebSTAR Web Users* files. Be sure to back these up frequently.

You can use the WebSTAR Admin program to view your Web server activity and set all the web server options. For information on watching the Web server status, see “Admin Monitor Windows” on page 116.

Choose the panels from the Web Settings section at the left:



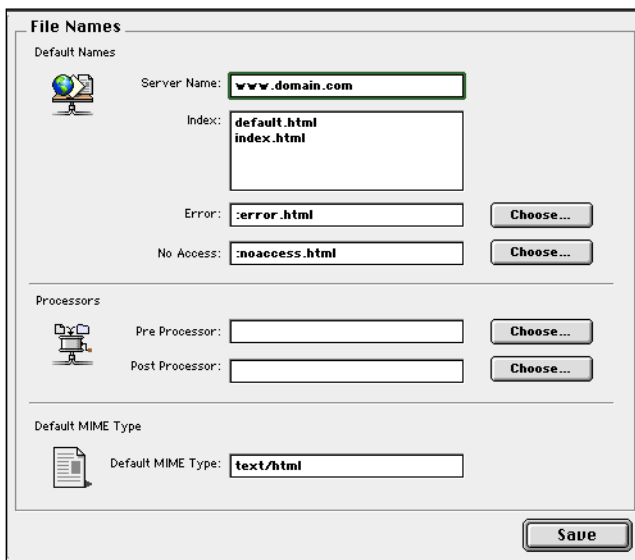
For instructions on launching and connecting to your server, see “About the WebSTAR Admin Application” on page 113.

You can also use the Browser Admin for status information and to set many options. For information and instructions, see “Browser-Based Admin” on page 126, and the sections below.

FILE NAMES AND PATHS

To access these settings, select the **File Names** item in the WebSTAR Admin application Settings window, or the **Settings / Misc. Settings** links in the WebSTAR Browser Admin pages.

 These settings apply to the default server: you can override the default files for Virtual Hosts: see “Virtual Host Options” on page 150



The screenshot shows the 'File Names' settings window. It has a title bar 'File Names' and a subtitle 'Default Names'. The window is divided into three sections: 'Default Names', 'Processors', and 'Default MIME Type'. In the 'Default Names' section, there are fields for 'Server Name' (containing 'www.domain.com'), 'Index' (containing 'default.html' and 'index.html'), 'Error' (containing '.error.html'), and 'No Access' (containing '.noaccess.html'). Each of these fields has a 'Choose...' button to its right. The 'Processors' section has fields for 'Pre Processor' and 'Post Processor', each with a 'Choose...' button. The 'Default MIME Type' section has a field for 'Default MIME Type' (containing 'text/html'). A 'Save' button is located at the bottom right of the window.

Default Names

WebSTAR has several standard default files and error files. To override these defaults, enter the name and file paths in this panel. For information on file paths, see “File Paths in WebSTAR Admin” on page 121.

Server Name

Your server host name is set by your host entry in the DNS server, as described in “Identifying Your Site: IP, Host Name and DNS” on page 96.

This Server Name field specifies the host name returned by WebSTAR in the redirect message and other server responses: it defines how the host refers to itself. You can just enter the host name in most cases.



Virtual Hosts can set the server name for each host.



You can only set multiple index file names if you have both the WebSTAR Data Cache and the WebSTAR Virtual Hosts Plug-Ins installed.



To override these file names for Virtual Hosts, see “Default File Name” on page 150.

If you want to have default files with more descriptive names in your subfolders, see “Redirection: Aliases and Redirect Files” on page 190.

WebSTAR will use this name to perform automatic redirection when it gets a URL to a folder name without a trailing slash.

Index File Name

The “Index” field allows you to specify the possible **default index file names** for all folders of this server. These are the names of the files WebSTAR looks for when a browser requests a folder: they are not paths to a specific files!

Each folder may contain a file with one of these names, and WebSTAR will recognize the name and return the contents when the browser requests a folder, for example:

```
http://www.domain.com/
```

```
http://www.example.com/party/blue/
```

To customize the contents of the default index files, use any HTML or text editor to create and change the text of the files with the default file names in the folders on your server.

You may want to add items to the Index file name list for several reasons:

- to use files on your web site designed for another system with default names different from the WebSTAR default of `default.html`. Examples of other common names include `index.html`, `index.htm`, and `default.htm`.
- to use a CGI script, Plug-In or other module to handle all default requests.

If you do choose to add to the Index file names, enter the new name in this field. Each of these names must be on a line by itself. The WebSTAR Web server will use the first index name that corresponds to an actual file in the folder. Remember that Virtual Host default file names, if set, override this functionality.

For Plug-Ins, if there is no corresponding file, the suffix is enough to send a message indicating that the user has requested the default file in this folder. The Plug-In must respond to this request, generate an HTML file, and send it back to WebSTAR to serve.

Error File Path

The WebSTAR Web server returns a special **Error file** when it receives a URL for a file that it can't find. The “Error” field allows you to specify the path to a specific Error file. There is only one Error file per host.

The default error file path is `:error.html`, meaning the *error.html* file in the WebSTAR root directory.

You can easily change the contents of this file, simply by editing it in any HTML or text editor, to show more useful information, such as URLs for the main areas on your server, or include SSI commands and have the page processed by the WebSTAR SSI Plug-In.

You can change the name of this file if you prefer a different name, or are using a CGI or Plug-In to handle errors. To use a different file, enter the new file path in this field. If you are using WebSTAR Admin, you can use the **Choose** button to select a file on the server, even if you're using a remote machine.

No Access File Path

A **No Access file** is the page displayed when a browser can't connect to the server, because it is refusing connections, or the client machine is denied access by the global allow/deny settings.

The No Access file can be an HTML file with helpful information about the site and how to get access. You can also specify a CGI or Plug-In, which might, for example, give different responses based on the address of the client browser.

The default No Access file path is `:noaccess.html`, meaning the *noaccess.html* file in the WebSTAR root directory.

To use a different file, enter the new file path in this field. If you are using WebSTAR Admin, you can use the **Choose** button to select a file on the server.

Processors

The Pre-processor and Post-processor fields allow you to specify Plug-Ins or CGIs to perform certain functions **before** the server processes a URL, or **after** the processing. These are server-wide and cannot be limited to specific Virtual Hosts. Third-party developers have created several of these CGIs and Plug-Ins. For more information, see:

<http://www.starnine.com/extendingwebstar.html>

Pre-Processor

Pre-processors can provide alternate security schemes, database routing, and more.

Only one pre-processor application can be called by WebSTAR, although that application can call others. WebSTAR launches the designated application and sends every URL and associated request



See also "File Paths in WebSTAR Admin" on page 121.



Note that any included graphics files in this page must be from a URL that doesn't have restricted access, or you'll get the error again!



See also: "Actions" on page 161.

for information it receives to the pre-processor application before continuing. Pre-processors perform their tasks and then allow WebSTAR to process the URL. In general, when WebSTAR gets data back, it will treat it like all other incoming URLs, and send it through the Suffix Mapping process. To make sure that your URLs are being handled properly, learn about your pre-processor and test it thoroughly.

To specify a pre-processor CGI application, enter the file path in this field (see “File Paths in WebSTAR Admin” on page 121). Or, to specify a Plug-In, set the file path to a file with the correct suffix for the Plug-In, and that Plug-In will get called in the pre-processor role.

Post -Processor

Post-processors can provide transaction logging, database storage, and other options based on the results of requests.

Only one post-processor application can be called by WebSTAR. WebSTAR retrieves the data requested by a URL, sends the file back to the browser, and closes the TCP connection. Only then does it send the file to the post-processor application. This application does not return any data to WebSTAR.

To specify a post-processor application, enter the file path in this field (see “File Paths in WebSTAR Admin” on page 121). Or, to specify a Plug-In, set the file path to a file with the correct suffix for the Plug-In, and that Plug-In will get called in the post-processor role.

Default MIME Type

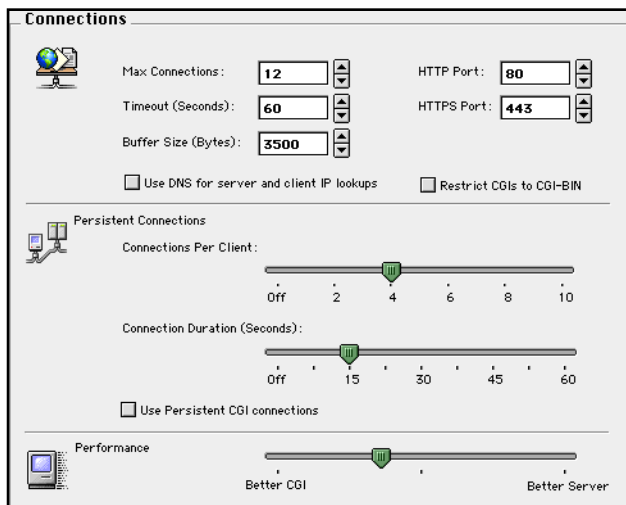
The **MIME Type** is included in the response sent from the web server to the browser, describing the kind of data it's sending. This information allows the browsers to use different parsers or helper applications to process the returned data intelligently. Suffix Mapping (described on page 154), specifies the MIME type for most files on your server.

The browser has its own MIME preferences list and uses it to determine how it should handle the data. It can display the text or graphic in the browser, launch a helper application, a browser Plug-In, save it to disk, and so on.

The Default MIME type, is used only when there is no Suffix Mapping entry, or it does not specify a type. The default type, text/html, tells browsers that the file is HTML text.

CONNECTIONS SETTINGS

To access these settings, select the Connections item in the WebSTAR Admin application or the **Settings > Misc. Settings** links in the WebSTAR Browser Admin pages.



The screenshot shows the 'Connections' settings window. It has a title bar 'Connections' and a globe icon. The settings are organized into sections: General, Persistent Connections, and Performance. The General section includes 'Max Connections' (12), 'Timeout (Seconds)' (60), 'Buffer Size (Bytes)' (3500), 'HTTP Port' (80), and 'HTTPS Port' (443). There are checkboxes for 'Use DNS for server and client IP lookups' and 'Restrict CGI's to CGI-BIN'. The Persistent Connections section includes a slider for 'Connections Per Client' (set to 4) and a slider for 'Connection Duration (Seconds)' (set to 15), with checkboxes for 'Use Persistent CGI connections'. The Performance section includes a slider for 'Performance' (set to a middle position between 'Better CGI' and 'Better Server').

Section	Parameter	Value
General	Max Connections	12
	Timeout (Seconds)	60
	Buffer Size (Bytes)	3500
	HTTP Port	80
	HTTPS Port	443
Persistent Connections	Connections Per Client	4
	Connection Duration (Seconds)	15
Performance	Use Persistent CGI connections	☐
	Performance	Better CGI / Better Server

i The HTTPS Port field only appears if you have SSL capacity: see "Installing SSL" on page 36.

Max Connections

This parameter specifies the maximum number of concurrent HTTP client connections to the WebSTAR web server. Many browsers request more than one element of a page, such as images, at the same time, to speed up their display. As soon as each file is entirely served, however, the browser disconnects itself. Therefore, the number of connections is not describing just the number of people trying to view your web site, but also the size and complexity of the web pages.

If a browser tries to access your site, and there are already too many connections, WebSTAR will send back a message indicating that the browser should try again in a few seconds. Many browsers automatically try again without displaying an error, but eventually, they may timeout and display a message indicating that the web site is busy. The Admin Web Monitor window shows you a Connections monitor, which can help you track whether you have enough connections allocated. If people complain that your sites are always busy, you should probably increase the number of Max Connections, if you have enough bandwidth.

i By default, Netscape browsers and Microsoft Internet Explorer are set to 4 simultaneous connections for each request.

i To further improve responsiveness, also increase the capacity of your network connection.

The faster your server machine and bandwidth, the more browsers you can serve without degrading performance. Conversely, the server can easily get swamped with connections if you have a limited bandwidth. Requests can come in faster than the server can transmit data to the clients

The basic rule of thumb is to watch the WebSTAR status window (the bar graphs) and adjust the Max Connections up or down, based on your server's load and performance under that load. Don't be afraid to restrict the number of connections if your server cannot handle the load (because either the computer or you have limited bandwidth). Doing so may actually help speed transfer rates, as the first requestors will finish and allow others to come in.

The default for Max Connections is **12**. The valid range for the Max Connections value is 4 to 500 (although you should leave some for other applications). After you change the number of connections, you must quit the WebSTAR application, update the memory allocation, and **restart** the server. The change will not take effect until you do so, although the monitor windows will reflect the new settings.



For every connection, increase the WebSTAR Memory Allocation by 100K: see "Server Administration Responsibilities" on page 87.

HTTP Port

This parameter specifies the port number WebSTAR listens to for all incoming HTTP requests. The default port is the standard Web server port: 80, but you can change this in special circumstances. Note that URLs will require the port number for ports other than 80, for example:

```
http://www.domain.com:9990/special.html
```



All Virtual Hosts use the same port: you can't have them listen on separate ports

For more information, see "Port Numbers" on page 102.

After you change a server's HTTP Port number, you must quit the WebSTAR application and **restart** it. The change will not take effect until you do so, even though the monitor windows may reflect the new port number.

The SSL portion of WebSTAR (which handles HTTPS requests) automatically listens on the standard HTTPS port number 443.

If you have multiple WebSTAR servers active on one computer, you will have to set each on a different port. For more information, see "Running Multiple Servers On The Same Machine" on page 92.

Timeout

This number determines the maximum amount of time (in seconds) that WebSTAR will wait before dropping an inactive connection. Timeouts can occur when a CGI application takes too long to execute or when a client doesn't respond to WebSTAR, implying that the connection has been dropped.

The default is **60** seconds, the minimum value is 15 seconds, and the maximum value is 120 seconds.

Buffer Size

This setting controls the size, in bytes, of the data blocks that WebSTAR uses when reading binary files from disk (such as HTML, GIF and JPEG images). WebSTAR reads from the disk and writes to Open Transport in chunks known as **buffers**, which are then passed to the client via the network connection. Adjusting this value will have little impact on server speed, although it may improve disk file access efficiency.

You can reset the buffer size based on the size of data you are serving. For example, if you have a lot of images of around 6K, you may want to increase your buffer to 7168 bytes (7K).

Browsers on slow connections may have trouble transferring large buffers, so you should experiment to find the best setting for your client mix.

The default **3500** bytes, the minimum size is 256 bytes and the maximum is 10240 bytes.



On fast network connections (T1 or greater), set the buffer size in multiples of the disk block size (512). On slower connections, set it in multiples of 1500 (the TCP/IP MTU size).

Use DNS for Server and Client Lookups

This checkbox specifies whether WebSTAR uses DNS to look up the host name of the IP address of each browser or other client that sends it a request to the server. If this box is checked, the host name rather than the IP address appears in the status monitor windows and the log file.

This DNS data is cached, so it doesn't have to look up the IP address every time. However, whenever WebSTAR has to make a DNS request to get the host name, the additional network activity can slow the system. If there's a problem, such as an IP address that doesn't have a host name, or a slow DNS server, it can slow down your WebSTAR server considerably. Many of the log file analysis programs will do a



See also: "DNS" on page 100 and "Log Formats" on page 200.

DNS lookup for you, at the time of analysis, so you don't have to give up analysis by host name. Therefore, for best speed, you can uncheck this option.

If you use host names or domain names in your Allow/Deny entries, you must have "Use DNS" checked.

The default is **Off** (do not use DNS).

Restrict CGIs to CGI-BIN

If this box is checked, all CGIs must be in the *cgi-bin* folder in the WebSTAR root folder. This makes your server safer: no one can upload a CGI to another folder and then run it.

Note that the CGIs must all be in the folder itself, not in a subfolder.

The default is **Off** (not to restrict CGIs).

Persistent Connections

The HTTP 1.1 standard allows a server to send several files to a browser during a single connection. This allows WebSTAR to serve an HTML file and several small images in one connection, instead of requiring the browser to set up a separate connection for each file being requested, and can be much faster. This is a feature of HTTP/1.1, and supports "HTTP 1.1 pipelining" which enables browser to send multiple GET requests in a single header.

Newer browsers automatically send a header element if they want to request a persistent connection for a page (or frame). When WebSTAR gets one of these elements in an HTTP request, it holds a connection open for that browser, to avoid the overhead of creating new connections for every transaction.

Persistent connections remain open for the Connection Duration. Therefore, they take up a connection even when the server is not actively sending a file. When you enable Persistent Connections, you'll notice that the status windows will report that the number of active connections is often increased by 25% to 50%. To avoid rejecting other requests with a server busy message, you should increase the number of connections allowed as well (see "Max Connections" on page 134).



See also: "Developing CGIs" on page 445.



Persistent connections are also known as "KeepAlive" connections in the Browser Admin.

Connections Per Client

The Persistent Connections field sets the maximum number of connections that the WebSTAR Web server will hold open to a client. The range is from 1 to 10 connections. The default value is **4** connections, because most browsers can only open up to four connections per frame.

A setting of 0 turns off Persistent Connections, which will slow down the apparent speed of your server.

Connection Duration

The Connection Duration field sets the number of seconds to keep idle client connections open. Idle connections are connections to browsers that are not currently requesting data. WebSTAR can retain those connections to avoid creating new connections if the client is likely to request data again. The range is from 1 to 60 seconds. A setting of 0 turns it off. If enabled, the recommended value is 15 seconds.

The default value is **15**.

Use Persistent CGI connections

The setting is for sites that are running only CGIs which support persistent CGI connections. Do not check this box unless **all** CGIs running on the server support persistent connections.

This feature is **unchecked** by default.

Performance

WebSTAR allows you to specify how many of its processing cycles should be used for the Server Suite itself, and how many for any running CGIs or other applications on your server. This allows you to tune your server depending on whether WebSTAR is running alone or other applications need more time.

- If you are running WebSTAR alone, or with Plug-In modules, you should set the slider towards **Better Server** on the right side
- If you have CGIs and you would like to speed up their processing, leave it at the default or move it to towards **Better CGI** on the left side.

By default, performance is set closer to Better CGI than to Better Server.



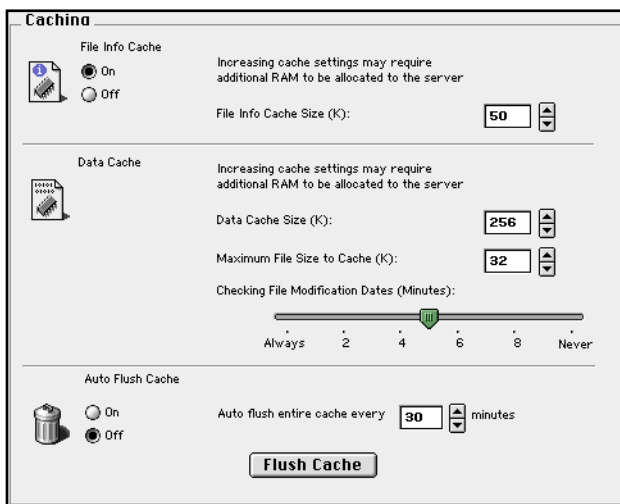
If you enable Persistent Connections, be sure to increase the Max Connections setting. For example, increase it from 12 to 24.



Both these caches are stored in WebSTAR's memory partition. Quitting WebSTAR will flush these caches.

CACHING

Caching is a method of storing data in memory (RAM) rather than reading it from the hard disk every time. WebSTAR includes caches for file information, and for the contents of the files that the server has sent (such as text, images, and sound).



File Info Cache

This cache stores information about files recently served: the file name and suffix, type, creator, size, and last modified date. Because this information is accessible in RAM, WebSTAR can perform Suffix Mapping lookups and other processing very quickly. In most cases, enabling this option will improve performance considerably.

It also uses this cache to track folder requests, where the URL does not include a slash at the end, like this:

`http://www.domain.com/widgets`

The server must check to see that there isn't a file named *widgets* before converting the URL to the folder format (*widgets/*) and then getting the index file. Storing this information in the file cache lets the Web server perform this step very quickly, which will improve performance on busy servers.

Note that this cache cannot tell when your files have been modified on the disk. You must flush it to make sure that the newest pages are

served: see “Updating Caches” on page 143 for more information. If you are making constant changes to your files, see “Auto Flush Cache” on page 143).

The **File Info Cache Size** is amount of RAM to use for this purpose, in kilobytes. The default setting for this field is **50 K**. Setting it smaller than the default setting results in virtually no performance gain, because the cache is continually being changed as new files are loaded into the few available slots. The maximum setting is the current amount of free memory displayed in the server's status window when file info caching is disabled. Increasing the application's memory partition increases this upper limit correspondingly.

A relatively small amount of data is stored for each file in the info cache, and there is some overhead in managing the cache itself. Therefore, if you are serving hundreds or even a few thousand files, you should probably set the File Info Cache at no more than 150 K.

Data Cache

Web server **data caching** stores copies of the contents of the files on your web site in memory (RAM) so that the server doesn't have to open each file to serve the data inside it. This is particularly useful for sites with many small graphics files (such as logos and navigation buttons) used throughout the site. Opening and reading files requires calls to the Mac file system and accessing the hard disk, so serving the contents of these files directly from the data cache will speed up access to your site considerably. In addition, the WebSTAR SSI Plug-In automatically caches its data in memory using the Data Cache, saving time and processing.

All files not explicitly handled by Plug-Ins are cached. This includes those with suffixes .html, .gif, .jpeg, and so on. SSI pages are also cached automatically. Unlike other web server caches, you do not have to designate the best files to cache: the Data Cache will do it for you.

The Data Cache is an intelligent cache, using a frequency-based algorithm to automatically adapt to changing server loads. The **Least Recently Used** system tracks when files are requested: when the Data Cache runs out of memory, the files requested recently are retained and the others removed.

As files change on the server disk, you want the Data Cache to serve the most recent version. However, checking the file before responding



To specify the File Info Cache size in the Browser Admin, use the “Misc. Settings” page.



The Data Cache is a WebSTAR Core Plug-In. If you remove it from the Plug-Ins folder, the Data Cache section of this panel will be disabled, and the server and WebSTAR SSI Plug-In will not cache data.



There is only one Data Cache per server: it works for all Virtual Hosts on the server.



Plug-In Developers, see “Calling WebSTAR Data Cache” on page 461.



The Data Cache is always enabled, and will be called whenever the Web server serves a file that is not handled by another Action (see “Suffix Mapping” on page 154).

to every request takes significant time, especially on busy servers. You can schedule how often the Data Cache should check to see if the file has been changed. See “Checking File Modification Date (Minutes)” on page 142.

Plug-Ins can use the WebSTAR Data Cache, and a number of third-party Plug-Ins do so, or have their own caching.

Data Cache Size

The **Maximum Data Cache Size** is the amount of RAM allocated for this purpose, in kilobytes. The default setting for this field is **256 K**. You can change the Maximum Data Cache size to any number between 32 K and the amount of memory allocated to the WebSTAR server. If you allocate more, be sure to **increase the memory allocation** of the WebSTAR server application by an equal amount (see “Server Administration Responsibilities” on page 87).

If you’re using the Browser Admin, use the Plug-Ins “WebSTAR Data Cache” page to set the Data Cache size.

Maximum File Size to Cache

You can control the Data Cache storage by defining how large a file can be cached. For example, if you have many 5 KB files and a few 200 KB files, it’s much more efficient to serve the smaller files from the Data Cache. Large files take less advantage of the data cache—WebSTAR overruns most network connections long before the file transmission is completed, so reading the file from disk does not slow the transfer rate.

If you have many large files, and your server has a lot of RAM, you can allocate more memory to the server, increase the Data Cache size, and increase the Maximum File size.

The default is **32K**, and the range is from 32 K to 10,000 K (10 MB).

Optimizing the Data Cache

Selecting the best cache size requires experimentation. A cache that is too small has no effect on performance, while a cache that is too large could waste memory. Use the Data Cache Information Window, described below, to help configure your data cache.

In addition, the data cache only avoids the overhead of disk access. You still have the network delays, even if you are on a T1 or a T3 internet connection. Data caching is most effective for small files used often in your web site.



If you are serving large files, you can also experiment with increasing the size of the system’s disk cache.

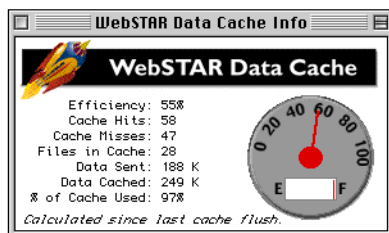
For testing, you may want to use a utility such as Pounder or Netsplat to simulate a high load on your site, as well as checking your site from several different locations. For testing tools, see the Extending WebSTAR pages on the StarNine site:

<http://www.starnine.com/extendingwebstar.html>

The Status windows and Browser Admin monitor page will show you the memory usage while you're testing. Be sure to wait while the data cache fills up during your experiments.

Data Cache Information Window

The Data Cache Information Window will appear when you choose **Data Cache** from the Plug-Ins menu in the WebSTAR server application.



After your server has been running for a while, refer to the WebSTAR Data Cache Info window. When the “Efficiency” and “% of Cache Used” numbers are high (over 75%) the Data Cache is working properly. These numbers are also displayed as the speedometer and fuel gauge.

If the cache usage is low, you may want to increase the Data Cache size. Make sure you also allocate more memory to the server. Keep testing and incrementing until you reach a balance.

Sometimes the Data Cache window will report a different amount of data sent than WebSTAR server status window, even though all suffixes are cached. Your Data Cache may be running out of RAM (it will say 100% efficiency). In addition, some items never appear in the Data Cache number, including CGI data, Error files, No Access files, and File-Not-Modified responses.

Checking File Modification Date (Minutes)

This slider specifies how often the Data Cache should check the server disk for the file modification date when it gets a client request for that file. It will only read the file from disk again if the date and time indicate that the file has changed.



Server performance is affected by the amount of bandwidth you have. If you have a large or busy site, you should consider getting a more bandwidth or mirroring your content at your ISP using a third-party Plug-in.

The default is to check when a request comes at least **5 minutes** after the last check. The allowed range is from Always (10-20 seconds) to Never (about 20 minutes).

Updating Caches

Because the Data Cache checks file modification dates, it will read your changes at most 20 minutes after you save the file to the server disk. However, if you are updating your site, you may want to see changes immediately. There are several ways to make sure you can see the changes.

Nocache HTTP request

You can use the **Super Reload** option, if your browser supports it. This will send a special nocache command as part of the request header, and the Data Cache will always check the file modification date. If it finds that the file on disk is newer than the cached data, it will open the file and read the data into the cache before serving it.

Flushing the Caches

The WebSTAR Web server can **flush the caches**, which means that it will clear the File Info Cache, the Data Cache, and the DNS cache, and send a message to third-party Plug-Ins to flush any caches they are keeping.

When you quit and restart WebSTAR, all caches are automatically flushed.

Manual Cache Flush

To flush the cache, you can use any of these commands:

- choose **Flush Cache** from the Options menu in the WebSTAR server
- choose **Flush Cache** from the Options menu in the WebSTAR Admin application
- press the **Flush Cache** button in the Caching panel of the WebSTAR Admin Settings window
- press the **Flush Cache Now** button on the Settings page in the Browser Admin pages

Auto Flush Cache

The WebSTAR Admin Web Settings Cache panel and Browser Admin Controls page allow you to set an interval for the system to automatically flush both the File Info Cache and the Data Cache. This is rarely necessary.



The caches are always flushed when you upload a file using the WebSTAR FTP Server (described on page 337).



When you view the WebSTAR server status window, you'll see an entry confirming that the cache was successfully flushed.

The default setting is to have Auto Flush Cache set **Off**. If you enable it, the default interval is **30** minutes.

VIRTUAL HOSTS

Virtual hosting allows you to serve several web sites, with different host names and even IP addresses, using the same WebSTAR server. Visitors to these sites will be routed by IP address, host name, and/or the browser Language setting to the correct Virtual Host, with its own default pages and web links.

Note that all hosts within WebSTAR share **all** other settings, including File Names, Caching, Suffix Mapping, CGIs and Plug-Ins, Security Realms, and Web Users and Passwords.

Before setting up your Virtual Hosts, you should do the following:

- 1 Read the section “Virtual Hosts: Hosting Multiple Web Sites” starting on page 193.
- 2 Work with your ISP or other DNS provider to register the domain names and direct them at your server (see “DNS” starting on page 100).
- 3 If you want to run IP Multihoming, make sure you have version 1.3 or later of Open Transport and obtain additional IP addresses from your service provider.
- 4 Create Virtual Host root folders and subfolders for each host on the server within the WebSTAR folder hierarchy.

Each Virtual Host can also have different Index file names, and Error and No Access files. If you want to restrict access to the host to certain machines or user names and passwords, make sure that the folder name is will not match any other folder or file name on the server, so that it can be used as a Realm Match String.

- 5 A few older browsers do not pass the HOST field in the HTTP header, so they cannot access Virtual Domains automatically. See “About Virtual Domains” on page 194 for information about making your virtual hosts accessible to these browsers.

Editing Virtual Hosts Entries

To create and edit Virtual Hosts Entries, you will need to specify the IP address, host name, or language, using the Virtual Hosts table in the WebSTAR Admin Settings Window. When WebSTAR receives an HTTP request, it will consult this table to figure out which host should get the request. Each host can have a separate root folder and folder hierarchy, as well as default index file name and so on.



See also: “Identifying Your Site: IP, Host Name and DNS” on page 96 and “Virtual Hosts: Hosting Multiple Web Sites” on page 193.

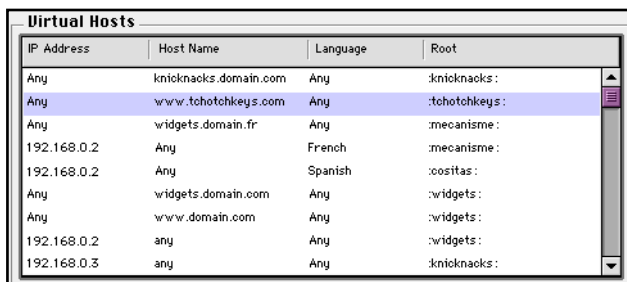


See also “Security Realms” on page 164.



You must edit the Virtual Hosts using the WebSTAR Admin application: there is no Browser Admin page.

To make entries, just click the **New** button and fill in the fields. You should follow the instructions below to arrange your Virtual Hosts routing entries in the correct order, and see “Working With Admin Lists” on page 120 for notes on creating, editing, moving, and deleting entries.



IP Address	Host Name	Language	Root
Any	knicknacks.domain.com	Any	:knicknacks:
Any	www.tohotchkeys.com	Any	:tohotchkeys:
Any	widgets.domain.fr	Any	:mecanisme:
192.168.0.2	Any	French	:mecanisme:
192.168.0.2	Any	Spanish	:cositas:
Any	widgets.domain.com	Any	:widgets:
Any	www.domain.com	Any	:widgets:
192.168.0.2	any	Any	:widgets:
192.168.0.3	any	Any	:knicknacks:

Special Routing Considerations

The first three columns in the routing table entry are IP address, host name, and language. Following the routing information is the **virtual host root folder**, the base folder for all HTML files for that host.

If the request matches **all** items with data in them for an entry, then the request is routed to that host. Be sure you follow the instructions below, or you may be surprised at the results.

- Fields marked “Any” will match any HTTP request. If the Host Name field is blank, it will match any request, even if the browser does not send a host name.
- Filled entry fields must match the request exactly. Capitalization doesn’t matter, but the **entire** string must match (no substring matches).

For example, if the Host Name matches the request but the IP Address does not match, the entry is not matched.

- Only the first exact matching entry in the routing table is used. Therefore, you should organize your requests with the most specific at the top, and the least specific (such as IP address only), at the bottom.
- If you use IP Multihoming, always make sure there is a default entry for each IP address. This should have “Any” Host Name and “Any” Language. This will catch all requests for that IP address that are not routed by the other entries.

If a request doesn’t match any entries in the table, it will use the **default host**: the IP address and host name of the machine, the

WebSTAR root folder, and the default names and files as defined in “File Names and Paths” on page 130.

Host Definition for Routing

The Host Definition fields allow you to specify the routing information, and the associated root folder, according to the instructions below.

IP Address

Any

Host Name:

www.tchotchkeys.com

Language:

Any

Root Folder:

:tchotchkeys:

Choose...

IP Address Routing

Hosting web sites on several IP addresses requires configuration using Open Transport 1.3 or later (described in “IP Multihoming: Special Configuration” on page 195). The IP Address popup menu reads the *IP Secondary Addresses* file in the Preferences folder of the current system disk, and allows you to specify the IP address for this host. If you have not set this up, you can’t route by IP address, and the popup menu will only have the entries “Any” and your main IP address.

Example IP Address Entries

IP ADDRESS	HOST NAME	LANGUAGE	ROOT FOLDER
192.168.0.2	Any	Any	:widgets:
192.168.0.3	Any	Any	:kkn:
192.168.0.4	Any	Any	:tch:

In simple cases, you can make a single entry for each IP address, and WebSTAR will route correctly. Just enter the IP address: **do not include the host name**. The browsers already know the host name, because they looked it up in the DNS entry for that IP address.

Virtual Domains (Host Name) Routing

If you are using Virtual Domains, you’re relying on the browser to send the host name in the header. In that case, the server will check the Host Name item in each entry until it finds a match. The **entire** host name must match, although the capitalization does not have to be the same. You do not need to include an IP Address for this routing. If you leave the Host Name field blank, it will be considered an “any” entry.

 Remember, the host name must be registered and the DNS entry enabled before the server will get requests for this host name.

 See also “Routing to Virtual Hosts” starting on page 193.

 You can have several Virtual Domains for each IP address, see “Combining IP Address, Host Name and Language Routing” on page 147 for instructions.



See also: “About Virtual Domains” on page 194.

Do not enter an IP address, just the host name. The browsers have already looked up the IP address.

Example Host Name Entries

IP ADDRESS	HOST NAME	LANGUAGE	ROOT FOLDER
Any	widgets.domain.com	Any	:widgets:
Any	knickknacks.domain.com	Any	:kkn:
Any	www.tchotchkeys.com	Any	:tch:
Any	Any	Any	:widgets:

If none of the entries matches the host name in the URL, or there is no header information, the web server will route the request to the default host. However, it's best to add an explicit default entry, so you keep track of these requests.

Language

You can route to different Virtual Hosts according to the language in the browser request header. This is set in the browser preferences by the user. Use the Language popup menu to select any of the standard browser languages. You can choose an overall language, such as Spanish, or a specific regional version, such as Mexican Spanish.



IP addresses and Host Names are not required for Language Routing.

Example Language Entries

IP ADDRESS	HOST NAME	LANGUAGE	ROOT FOLDER
Any	Any	French	:mecanisme:
Any	Any	Spanish	:cositas:
Any	Any	Any	:widgets:

If none of the entries matches the Language code in the URL, the web server will automatically route the request to the default host. Therefore, you should make an explicit entry, to remind yourself what will happen

Combining IP Address, Host Name and Language Routing

You can combine IP addresses, host names and/or language requirements in a single entry, for sophisticated routing to your Virtual Hosts. Remember that each URL header must match the entry **exactly**. The first exact match is the entry that will be used for routing that request. You should put the most specific entries first, and make sure you cover contingencies by putting general entries at the bottom. To move an entry to a better position, just select and drag the row.

Always test your Virtual Host Routing with a single element in each line before combining elements.

Complex Combined Example

In the following example, there are five different web sites, using the following elements:

- two IP addresses: 192.168.0.4 and 192.168.0.3.
- five host names between the two IP address:
 “widgets.domain.com”, “www.domain.com”, and
 “widgets.domain.fr” in 192.168.0.4 and
 “knickknacks.domain.com” and “www.tchotchkeys.com” in
 192.168.0.3.
- two specific languages supported: French and Spanish
- five Virtual Host Root Folders
 - *widgets* for widget information in English
 - *mecanisme* for widget information in French, using the
 widgets.domain.fr host.
 - *cositas* for widget information in Spanish, using the
 widgets.domain.com host.
 - *knickknacks* (knickknacks.domain.com, on 192.168.0.3)
 - *tchotchkeys* (www.tchotchkeys.com on 192.168.0.3)



In this example, we are hosting a site registered in France (.fr).

The routing table looks like this:

Example Combined Entries

IP ADDRESS	HOST NAME	LANGUAGE	ROOT FOLDER
Any	knickknacks.domain.com	Any	:kkn:
Any	www.tchotchkeys.com	Any	:tch:
Any	widgets.domain.fr	Any	:mecanisme:
192.168.0.4	Any	Spanish	:cositas:
192.168.0.4	Any	French	:mecanisme:
Any	widgets.domain.com	Any	:widgets:
Any	www.domain.com	Any	:widgets:
192.168.0.4	Any	Any	:widgets:
192.168.0.3	Any	Any	:kkn:



Remember, the hosts are evaluated from top to bottom, so make sure that the host names are above the IP address entries.

In the example above:

- All requests for knickknacks.domain.com are routed to the *kkn* folder.
- All requests for www.tchotchkeys.com are routed to the *tch* folder.

- All requests for `widgets.domain.fr` are routed to the *mecanisme* folder.
- Requests with a French language code and the widgets IP address are routed to the *mecanisme* folder, as though they came to the `widgets.domain.fr` host.
- Requests with a Spanish language code and the widgets IP address are routed to the *cositas* folder.
- All other requests for `widgets.domain.com` and `www.domain.com` are routed to the *widgets* folder.
- All other request for the 192.168.0.4 are routed to the *widgets* folder and the `www.domain.com` host.
- All other requests for 192.168.0.3 are routed to the *tch* folder and the `knickknacks.domain.com` host. To avoid confusion, the knickknacks default page should have a prominent link to the home page of `www.tchotchkeys.com`.

Virtual Host Routing Display

The WebSTAR Web server monitor window will display the routing information at startup and every time you make a change to those settings. The display looks like this, with asterisks (*) replacing the word “Any”:

```
WebSTAR Virtual Hosts
=====
* knickknacks.domain.com * -> :kkn:
* www.tchotchkeys.com * -> :tch:
* widgets.domain.fr * -> :mecanisme:
192.168.0.2 * fr -> :mecanisme:
192.168.0.2 * es -> :cositas:
* widgets.domain.com * -> :widgets:
* www.domain.com * -> :widgets:
192.168.0.2 * * -> :widgets:
192.168.0.3 * * -> :kkn:
```

Virtual Host Root Folders

Virtual Host Root Folder field specifies the folder designated as root for that host. The virtual hosts will work within this folder and its subfolders. This folder must be within the WebSTAR folder, for security. If the folder doesn't exist yet, you can create it on the server disk using the FTP server, if you have the correct permissions.

You can use the **Choose** button next to the Root Folder field in the Virtual Hosts panel. This will allow you to select the folder on your server disk. Or you can type the file path yourself.



See also “File Hierarchy and Virtual Hosting” on page 187.

For example, if your Virtual Host is using the *knickknacks* folder as its root folder, and it's in the WebSTAR folder, you could use either of these paths:

```
Web-HD:WebSTAR 3:kkn:  
:kkn:
```

The first is an absolute file path from the hard drive, the second is a relative file path from the WebSTAR root folder, but either of them will indicate the correct location of the Virtual Host root folder.

Virtual Host Options



Options	
Server: widgets.domain.fr	Error: :erreur.html Choose...
Index: index.html	No Access: :noaccess.html Choose...

Server

To correctly identify the Virtual Host, enter its name in the Server field. This is the name that will be used when the host builds full URLs for redirection and Plug-In use. It defines how the host will refer to itself. This is particularly important for IP address entries, language routing, and alternate host names, such as converting `domain.com` to `www.domain.com`.

Default File Name

For a given Virtual Host, you can override the default Index file names. If you leave this field blank, this Virtual Host will use all the Index file names you specified in the File Names and Paths panel field Index File Name (described on page 131).

Error and No Access Files

You can also specify different Error and No Access files for this Virtual Host. This allows you to give host-specific or language-specific error messages. For information on these settings, see “File Names and Paths” on page 130.

Virtual Hosts Settings File

The *WebSTAR Virtual Hosts Settings* file, in the *Plug-Ins* folder, stores the list of Virtual Hosts and their attributes. It is created after you enter the first Virtual Host using the WebSTAR Admin and save the information to the server. The WebSTAR Virtual Hosts Plug-In reads this file when



See also “File Names and Paths” on page 130.



Host names, even for Virtual Hosts, are also defined by the DNS entries for your IP addresses: see “DNS” on page 100 for details.



Back up this file so you do not have to re-enter the Virtual Hosts settings if something happens to your disk or server machine.

the server starts up: when you see the list in the Virtual Hosts panel in WebSTAR Admin, it comes from this file.

Format of the Virtual Hosts Settings File

The file has the eight fields, corresponding to the fields in the WebSTAR Admin panel, with tabs between them. To specify that a field should be “Any”, leave it blank, so there are two tabs together.

The fields are:

- IP Address
- domain name
- language code
- root folder path
- server name
- error file path
- default index file name
- no access file path
- entry ID number



The last character in the file should be a CR (Carriage Return) at the end of the last entry.

The first three are the routing information (see “Special Routing Considerations” on page 145). After that, the root folder path (see page 149), and options, as described in “Virtual Host Options” on page 150.

In this example Tab characters are replaced with dashes:

```
-knickknacks.domain.com--:kkn:-knickknacks.domain.com-:kkn:error.html--:kkin:noaccess.html-1
-www.tchotchkeys.com--:tch:-www.tchotchkeys.com-:tch:error.htm--:kkn:noaccess.htm-2
-widgets.domain.fr-:mecanisme:-widgets.domain.fr-:mecanisme:erreur.html-indix.html--3
192.168.0.2-fr-:mecanisme:-widgets.domain.fr-:mecanisme:erreur.html-indix.html--4
192.168.0.2-es-:cositas:-cositas.domain.com-:cositas:error.html--:cositas:noaccess.html-5
-widgets.domain.com--:widgets:-widgets.domain.com-:widgets:error.html--:widgets:noaccess.html-6
-www.domain.com--:widgets:-widgets.domain.com-:widgets:error.html--:widgets:noaccess.html-7
192.168.0.2--:widgets:-widgets.domain.com-:widgets:error.html--:widgets:noaccess.html-8
192.168.0.3--:kkn:-knickknacks.domain.com-:kkn:error.html--:kkin:noaccess.html-9
```



The WebSTAR Virtual Hosts Plug-In will only read this file when the server starts up. After editing the file, quit and restart the server.

Editing the Virtual Hosts Settings File

The file itself is a text file, and you can edit it if you are careful. **Be sure to back up the Virtual Hosts file before editing it.**

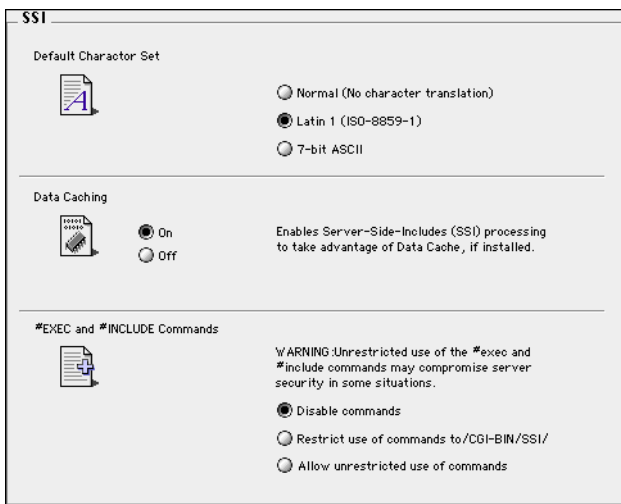
If you change this file, the WebSTAR Virtual Hosts Plug-In will read the new data when the server starts up. If the data is not entered in the correct format, it may ignore your virtual host settings. Always check the server status window on startup and use the Admin to verify your Virtual Host settings.

SSI

WebSTAR SSI provides a great deal of power and flexibility to your web site. You can use these commands to include header or footer files, to show dates and page access counters, to show and hide parts of web pages based on the date or the browser's IP address, to launch CGIs or call Plug-Ins, and more. For complete information, see “WebSTAR SSI” on page 275.

This panel allows you to set certain SSI options in the WebSTAR Admin application.

 In the Browser Admin, use the WebSTAR SSI Plug-In Page to set these options.



Default Character Set

When WebSTAR SSI processes HTML text that uses special characters (not in the simple HTML character set), WebSTAR SSI must encode them for transmission to browsers.

- Normal (no character translation)

Does no translation or encoding, so characters may not be represented correctly in the client browser. You should only select this option if your site is set up this way (for Kanji or other characters which should not be encoded again) and browsers are properly configured.

- Latin 1 (ISO - 8859 - 1)

Encodes according to the ISO specification. This should work correctly for most browsers and other clients. This is the default setting.

- 7-bit ASCII

Converts special characters by removing the “8th bit”.

Data Caching

WebSTAR SSI can take advantage of the WebSTAR Data Cache (described on page 140). This means that the data processed by the WebSTAR SSI, such as modification dates, text included from other files, and text created by CGIs, will be stored in the Data Cache for future use. This allows SSI to reuse data rather than regenerate it every time.

The default for SSI Data Caching is **On**. If you have dynamic data that should always be generated on-the-fly, set this option to **Off**.

#Exec and #Include Command Security

While WebSTAR SSI is extremely powerful, it has some security implications. The `#exec` and `#include` commands let include other files and run scripts, CGIs and applications. However, if you allow other people to upload files to your server, they could then use these commands to act without your knowledge. These security options help you restrict access and limit your vulnerability.



See also: “SSI Command List” on page 280.

■ Disable commands

Disallows `#exec` and `#include` commands—they are not processed, and an error is inserted into the HTML comment, so you can see it if you view the source.

This is the default setting.

■ Restrict use of commands to /CGI-BIN/SSI/

The WebSTAR SSI Plug-In will only allow these commands if the files to be executed are included are in the *cgi-bin* folder's *ssi* subfolder. As long as you limit access to that folder, no one can use these commands to change your site.

To avoid complicating your site organization, you can put the files in the normal folders, and place aliases to them in the *cgi-bin:ssi* folder.

■ Allow unrestricted use of commands

If you are the only person with upload access to your server, you may want to remove all restrictions and use the commands freely throughout the server. With this option checked, WebSTAR SSI can include the contents of files from anywhere on your hard drive, or on any mounted volume.

SUFFIX MAPPING

WebSTAR uses CGIs and Plug-Ins for file listing, database access, multimedia, Server-Side-Includes, and other dynamic interactions. To launch most CGIs and Plug-Ins, the WebSTAR Web server uses special URLs (as specified by those add-on programs). When one of these the URLs is received, the server will examine the file name element and send the request to the appropriate CGI or Plug-In.

Entries in the Suffix Mapping Table define what should happen, based on the file name suffix, file creator or file type code. This could be processing by a CGI or Plug-In, or serving the file without any modification on the server side.



Each URL can only go through one Action, although Plug-Ins and CGIs can call others for additional processing.

Suffixes, Type and Creator Codes

The **suffix** is the element of the file name after the last period, as in these examples:

- default **.html** is a normal HTML file.
- special **.bluewidget.html** is also a normal HTML file. The data before the last period is ignored in defining the suffix.
- bluewidget **.gif** is a GIF graphic file.
- red-widget **.jpeg** is a JPEG graphic file.
- letter **.txt** is a plain-text file which will be displayed without special formatting
- morning **.mov** is a QuickTime video to be played by a browser plug-in. For instructions on serving QuickTime, see <http://www.starnine.com/support/technotes/servingqtmovies.html>.
- widget **.song.midi** is a MIDI (music) file to be played
- guestbook **.cgi** requests a guestbook CGI application to process the URL

File Type and Creator Codes

Some files don't have special suffixes, or the suffix is not entered in the Actions. WebSTAR can also check files based on the **File Type and Creator Codes**. These are automatically generated by the application that creates a Mac file or converts it from another system. These codes control the icons on your desktop, and the automatic launching of the correct application when you double-click on a file.

To view these four-character codes, you need to use a resource editor, file code viewer such as the shareware FileTyper, or open Apple's Find

File, select type or creator from the popup menu, and drag an example file to the window, which will display the code. For an example, see “Handling a File With No Suffix” on page 156.

How Suffix Mapping Works

- 1 A browser sends a URL to WebSTAR.
products/shipping.shtml
- 2 If there's a suffix at the end of the file part of the URL, looks up that suffix. WebSTAR uses the Action in the first matching entry.
For example, .shtml maps to the “SSI” Action, by default.
- 3 If there is no suffix, or no match for the suffix, the web server reads the Type and Creator code for the file that was requested and looks that up in the Suffix Map.
 - If it finds a match on both fields, it uses the first matching entry in the Suffix Mapping Table.
 - Otherwise it looks for the first matching Type.
 - If it can't find the right type, it looks for the first matching Creator code.
- 4 If none of these match, the web server will use the defaults: Action = Binary and default MIME Type (usually TEXT/HTML).

Once the web server locates the correct entry, it either serves the file directly or sends the request to the Plug-In or CGI specified by the Action entry. For more information, see “Suffix Mapping Example: Using SSI for All HTML Files” on page 160.

Examples of Suffix Mapping

Handling a GIF File

Suppose our server receives this URL:

```
http://www.domain.com/logo.gif
```

The WebSTAR Web server looks up .gif in the Suffix Mapping Table. It finds only one entry with a suffix that matches, which has the Action of BINARY.

So the server locates the *logo.gif* file in the root folder, reads the data and returns it to the browser with the “image/gif” MIME type, and without any further processing. Most browsers will display images of this type directly in the browser window.

Handling an Image Map

If a server gets a URL like this (and has the WebSTAR Image Map Plug-In installed):



For information, see
“MIME Type” on
page 160

`http://www.domain.com/logo.map`

it first looks up `.map` in the Suffix Mapping Table, where it finds the first entry matching that suffix. Because the Action is `IMAGE_MAP`, the web server passes the appropriate data to the WebSTAR Image Map Plug-In, which processes the request and sends back a result. Then the server returns the resulting data to the browser with the MIME type `application/x-image-map`.

Handling a File With No Suffix

Here's an example without a suffix, to show how the Type and Creator code matching works. If this server got a request with this URL:

`http://www.domain.com/MyStuffedFile`

it would look into the Suffix Mapping Table. Because is no suffix, WebSTAR has to locate the file *MyStuffedFile*, and get the file Type and Creator codes. In this case, the web server will look in the Suffix Map for a file with a Creator of `"SITD"` and a File code of `"SIT!"`.

BINARY	SIT!	SITD	application/x-stuffit
--------	------	------	-----------------------

It finds one match (in our example), and returns the file with a special MIME type of `application/x-stuffit`. This tells the browser to use the helper application defined for this MIME type, which should launch Stuffit or Stuffit Expander and open this compressed file. Note that this entry will only match files created with Stuffit. To match all compressed files in this format, you could put an asterisk in the Creator field.

Editing Suffix Mapping Table Entries

The Suffix Mapping Table displays the WebSTAR Web server's current mapping, action and MIME type entries. You can rearrange and edit these entries, or add new entries as you add third-party Plug-Ins to WebSTAR. It's wise to write down a list of your suffix mapping changes, or take screenshots, in case you ever need to re-create them.

The pre-defined entries in the suffix mapping table, cover text, graphics, CGIs, encoding and compression, common application files, multimedia and Java. For descriptions, see "Suffix Mapping Defaults" on page 425.

Type and Creator Code fields which include a space as part of the four-letter code must be encoded when you enter them as part of the Suffix Map. For example, enter the code `'PDF '` as `PDF%20`.

 See also "WebSTAR Image Map" on page 253.

 Many third-party Plug-Ins automatically install Suffix Mapping entries in this table. Consult their documentation for details.

WebSTAR Admin Suffix Mapping Table

Choose the Suffix Mapping item in the WebSTAR Admin Settings window to open the Suffix Mapping Table. Each entry has a line in this table, and includes over 35 of the most common suffixes already. These defaults are listed in “Suffix Mapping Defaults” on page 425.

Ⓐ	Action	Suffix	Type	Creator	MIME Type
•	SEARCH	.SEARCH	*	*	application/x-search
•	SSI	.SSI	*	*	application/x-SSI
•	WEBINCLUDE	.WEBINCLUDE	*	*	application/x-webinclude
	BINARY	.GIF	GIFf	ogle	image/gif
	BINARY	.JPG	JPEG	ogle	image/jpeg
	BINARY	.JPEG	JPEG	ogle	image/jpeg
	BINARY	.PNG	PNGf	ogle	image/png
	SSI	.HTML	TEXT	R*ch	text/html
	BINARY	.HTM	TEXT	R*ch	text/html
	ACGI	.ACGI	APPL	*	text/html
	CGI	.CGI	APPL	*	text/html
	BINARY	.Hqx	TEXT	BnHq	application/mac-binhex40

Items: 71 Item Selected:



Changes in the Suffix Mapping Table are stored in the *WebSTAR Settings* file.



For more instructions, see “Working With Admin Lists” on page 120.

The entries for WebSTAR Plug-Ins are at the top of the list, marked as locked (•). You cannot change or delete these entries. You can change any other entry, and add your own.

To make a new Suffix Mapping entry, decide where you want it to be in the list. WebSTAR will use the first entry it can find (see “How Suffix Mapping Works” on page 155). Then select the entry **before** the new entry, and click the **New** button.

Browser Admin Suffix Mapping Table

The WebSTAR Browser Admin pages also allow you to work with the Suffix Mapping Table. Go to the Administration main page, and choose Settings > Suffix-Mappings.

To make a new Suffix Mapping entry, decide where you want it to be in the list. WebSTAR will use the first entry it can find (see “How Suffix Mapping Works” on page 155). Look at the Order Number for the entry **before** your preferred location, and type a new Order number after that number, but before the following number (for example, to add a new entry after .GIF but before .HTML, you’d enter the order number 1650. Follow the instructions below to fill the fields and choose the Action. Then click the **Add New Entry** Button.

To edit a Suffix Mapping entry, click on the **Select** radio button for that entry, and then click the **Edit Selection** button. When you’re done with your changes, click the **Replace Selection** button, and your changes will be saved.

To move an entry, type a new Order number in the Order field, and click the **Reorder** button. For example, to move .MIDI above .MOV, type 2150 in the .MIDI Order field and click **Reorder**.

To delete an entry, click on the **Select** radio button for that field and click the **Delete Selection** button.

Fields in the Suffix Mapping Table

The Suffix Mapping table has six fields. The Suffix, Type and Creator fields help WebSTAR identify a URL, the Action field defines how the URL should be handled, and the MIME Type field specifies the type of information being returned to the browser.



Locked

The locked column on the left includes a bullet (•) for those entries which cannot be edited, such as those used by Plug-Ins.

Action Popup Menu

The Action field tells the WebSTAR server what to do with this kind of URL. The Suffix Mapping interfaces include the available Actions in the popup menu. Several of them are extremely useful, while others are for internal use only.

- **BINARY**: Return the file contents using the BINARY transfer method, without changing anything. Only the data fork of Macintosh files is sent (not the resource fork). An HTML header with the MIME type is always added to the data. To return a file with no header information, use the RAW action, described below.

Use this BINARY action for files unless they require special processing.

- **TEXT**: Return the file contents using the TEXT transfer method, which converts line ends to 'CR/LF' for older browsers. This conversion will delay the response slightly.
- **CGI**: Load and execute the CGI application specified in the URL.

WebSTAR passes arguments to the application by using the “sdoc” Apple Event. The application is expected to generate a legal HTTP header and any response data and return it to the web server as a result of processing the Apple Event. This result will be transmitted to the browser without modification. For better performance, use the ACGI Action.

- **ACGI**: Load and execute the ACGI application specified in the URL.

WebSTAR passes arguments to the application by using the “Search Doc” Apple Event. The application is expected to generate a legal HTTP header and any response data and return it to the web server as a result of processing the Apple Event.

•	BINARY
	TEXT
	CGI
	ACGI
	RAW
	LASSO_PUBLISHER
	WVADAPTOR
	WEBINCLUDE
	SSI
	SEARCH
	MAIL
	SERVLET
	IMAGE_MAP
	FORMMAIL
	UPLOAD
	DIRECTORY
	CACHE
	BYTE_SERVER
	BINHEX
	ADMIN



For an example RAW file, see “Redirect Files” on page 191.

Unlike the **CGI** Action, ACGI applications can run asynchronously: the web server doesn’t have to wait for the results before proceeding.

- **RAW**: Return the file contents without changing anything or generating an HTTP header for the file. The RAW file should have their header inside the file. Only the data fork of Macintosh files is sent: the resource fork is not sent.

Useful Plug-In Actions

- **SSI**: Processes SSI commands within HTML documents (see “WebSTAR SSI” on page 275).
- **IMAGE_MAP**: return URLs based on the point on the image map that the person selected in the browser (see “WebSTAR Form Mail” on page 249).
- **BINHEX**: use WebSTAR Auto BinHex (described on page 238) for these files.

For Internal Use

Other actions are registered by WebSTAR Plug-Ins, and are used mainly by them. If a third-party Plug-In uses these Actions, it should instruct you what change to make in your Suffix Mapping Table.



For information about these Plug-Ins, see their sections in “WebSTAR Plug-Ins” starting on page 235.

- **ADMIN**: used by WebSTAR Admin
- **LESSO_PUBLISHER**: used by WebSTAR Lasso Publisher
- **WOADAPTOR**: used by WebSTAR WebObjects Adaptor
- **WEBINCLUDE**: used by the WebSTAR SSI WebInclude Plug-In
- **MAIL**: used by the WebSTAR Mail Server
- **SERVLET**: used by WebSTAR Java Servlet Runner
- **CACHE**: used by the WebSTAR Data Cache
- **BYTE-SERVER**: used by the WebSTAR Data Cache
- **FORMMAIL**: used by WebSTAR Form Mail
- **UPLOAD**: used by WebSTAR File Upload
- **DIRECTORY**: used by WebSTAR Directory Indexer

Adding Actions to the Menu

Some Plug-Ins add actions to the Actions list automatically. You can also define actions to be included on this menu, as described in “Actions” on page 161.

Match Fields: File Suffix, Type and Creator

The web server uses these fields to locate the correct entry in this table. For a description of this mapping process, see “How Suffix Mapping Works” on page 155.

To make a match field match anything, enter an asterisk (*). Blank fields will only match empty strings: a blank suffix field will match file URLs with no suffix at all.

To make a entry match all files created by a particular program, such as all files compressed by Stuffit, enter the Creator code (SITD) and an asterisk in the Type field. Likewise, to handle all files of a particular kind (such as QuickTime movies), you can enter an asterisk in the Creator field and the code in the Type field (in this case, MOOV).

Be sure to consider the order: WebSTAR uses the first suffix match, the first Type and Creator match, the first Type match and finally, the first Creator match.

MIME Type

The MIME Type appears in the form “general/specific”. These can be defined by the web community, like text/html or a vendor such as Apple, with video/quicktime. Your server can also send files to be opened by a specific application, when the MIME type is “application” and the program name. For example, you can specify application/pdf for Adobe Acrobat files or application/x-pn-realaudio for RealAudio files.

There's no definitive list of MIME types on the Web, but a useful listing is available at:

<http://www.isi.edu/in-notes/iana/assignments/media-types/media-types>

In addition, publishers of software that requires special MIME types may have describe them in their documentation or web site, or the information may be available through Usenet newsgroups or email discussion lists on the software. If the software includes a browser Plug-In, you can install it and then view the browser's application settings to discover the MIME type.

The WebSTAR Default MIME Type is text/html: you can reset this in the WebSTAR Admin File Names panel, as described in “Default MIME Type” on page 133.

Suffix Mapping Example: Using SSI for All HTML Files

Perhaps you'd like to include the modification date or other Server-Side Include feature in your pages, but you don't want to change the suffix from .html. You can use the Suffix Mapping Table to



All Mac files have a type and creator code, so if you use this feature, use asterisks and do not leave any field blank.



Some third-party CGIs and Plug-Ins use the MIME types for their own internal purposes as well. Check their documentation for information.



See also “WebSTAR SSI” on page 275.

instruct the web server to use the WebSTAR SSI Plug-In for all .html files.

The steps are:

- 1 In the WebSTAR Admin application, connect to the server, and open the Server Settings window, then select Suffix Mapping.
- 2 Select the entry for .HTML

BINARY	.HTML	TEXT	R*ch	text/html
--------	-------	------	------	-----------

- 3 Select the Action popup menu and choose SSI:

Action: SSI	Suffix: .HTML
Type: TEXT	Creator: R*ch
MIME Type: text/html	

The entry will update in the table.

- 4 Click Save to send the change back to your WebSTAR server.

From now on, all HTML files will be sent through SSI before they are returned to the browser. WebSTAR SSI will replace the SSI commands in the file with the appropriate data (such as the date the file was changed), and the browser will display these as standard text.

ACTIONS

To link CGIs and Plug-Ins to URLs, you may need to create an Action entry. Then you can select that new Action for the appropriate entries in the Suffix Mapping Table.

Many people use Actions to support operations where a single CGI or Plug-In can work with many data files. For example, on a site with several image maps, URL requests for any map file information is passed to the same CGI or Plug-In.

These Actions also allow you to hide implementation details from users. That is, the URL seen by users in a document isn't necessarily the URL that gets executed by the server.

Another use for user-defined Actions is to create new file types and define an Action to process them appropriately. For example, suppose you have .SQL files that contain SQL query statements. You would define an Action that would pass a query to an SQL database when an incoming URL request references a .SQL file.



See “Example: CGI Action” on page 163

User-defined Actions also allow you to swap out or change CGIs or plug-ins without having to change URLs in your documents. You simply edit the Action to point to a new script.

Editing Actions Entries

The Actions List lets you add, delete, or modify user-defined Actions. Actions with a mark in the lock column are defined by Plug-Ins and cannot be edited.

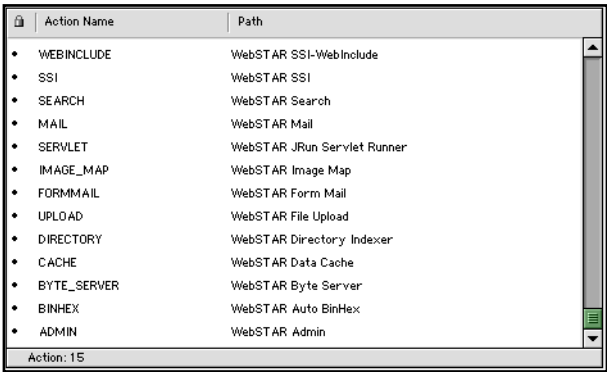
Defining an Action requires these two elements:

- **Action Name:** the name which will appear in the Suffix Mappings Action popup menu. The Action Name is not case-sensitive.
- **Application:** The path to the script or application file to be executed. These can be absolute (from the hard drive name or relative (starting with a colon and relative to the folder containing the WebSTAR application.

No spaces or Macintosh special characters may in the application path or Action name. If those characters appear in the application path or names, follow the instructions in “Web File and Folder Name Rules” on page 189 to encode them yourself.

WebSTAR Admin Actions List

Choose the Actions item in the WebSTAR Admin Settings window to open the Actions List. You’ll see a list like this:



Action Name	Path
• WEBINCLUDE	WebSTAR SSI-WebInclude
• SSI	WebSTAR SSI
• SEARCH	WebSTAR Search
• MAIL	WebSTAR Mail
• SERVLET	WebSTAR JRun Servlet Runner
• IMAGE_MAP	WebSTAR Image Map
• FORMMAIL	WebSTAR Form Mail
• UPLOAD	WebSTAR File Upload
• DIRECTORY	WebSTAR Directory Indexer
• CACHE	WebSTAR Data Cache
• BYTE_SERVER	WebSTAR Byte Server
• BINHEX	WebSTAR Auto BinHex
• ADMIN	WebSTAR Admin

Action: 15

Each default Action and WebSTAR Plug-In has a line in this list, and is marked as “locked” in the left column. You can change any other entry, or add your own Actions.

To make a new Action entry, decide where you want it to be in the list. WebSTAR will use this order in the Suffix Mapping Action Popup Menu

 Changes in the Actions List are stored in the *WebSTAR Settings* file.



see “Working With Admin Lists” on page 120.

(described on page 158). Then select the entry **before** the new entry, and click the **New** button. Follow the instructions above to fill in the fields.

Browser Admin Action List

The WebSTAR Browser Admin pages also allow you to work with the Actions List. Go to the Administration main page, and choose Settings > Actions.

To make a new Action entry, follow the instructions above to fill the fields. Then click the **Add New Entry** button.

To edit an Action entry, click on the **Select** radio button for that entry, and then click the **Edit Selection** button. When you’re done with your changes, click the **Replace Selection** button, and your changes will be saved.

To delete an entry, click on the **Select** radio button for that field and click the **Delete Selection** button.

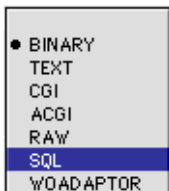
Using Actions

After you have defined an Action, you can use it in Suffix Mappings. When you add or change an Action, WebSTAR forces a reinterpretation of all Suffix Mappings. If it finds that a previously defined Action which was used by a mapping is now absent, that mapping is ignored (though it remains in the Settings file).

Example: ACGI Action

To use a (mythical) webstarSQL Plug-In to process all URLs searching a database, follow these steps:

- 1 Select the Actions panel and create a new Action entry.
- 2 Set the Action name to SQL and the path to the appropriate path to webstarSQL in the *Plug-Ins* folder, then press the **Save** button.



- 3 To associate the Action with all .SQL files, open the Suffix Mapping pane, and make a new Suffix Map entry.
- 4 Select the Action popup menu, and you’ll see “SQL” as a new option at the bottom. Select it.

- 5 Fill in the entry so that all URLs which end with .SQL use the SQL Action and the standard “text/html” MIME type.

SQL	.SQL	text/html
-----	------	-----------

From now on, all .SQL URLs will call the webstarSQL application for processing.

SECURITY REALMS

WebSTAR has options for limiting access to the web site, or to parts of the site. You do this by specifying a special word or phrase in the file or folder name, and defining that phrase as a WebSTAR **realm**. If that phrase is included in a URL, then you can hide the data from machines that do not have the correct host name, domain name or IP address. You can also allow others to see the data if they enter the correct user name and password. This is called **access control**.

WebSTAR also supports third-party CGI and Plug-In security solutions which are not affected by the limits of the server and provide additional functionality. For more information, see:

<http://www.starnine.com/extendingwebstar.html>



See also: “WebSTAR Security” on page 93.

For encrypted transmission of confidential information, see “SSL Web Security” starting on page 209.

About Realms

A **realm** is usually a folder on a local hard disk, and it includes all the files and folders within it. If a person visiting your site is allowed into a folder protected as a realm, they can see everything in that folder and all subfolders.

A word or string defines a realm, so you should consider it carefully. If it's a common word, you will not be able to use that word in any other file or folder name on your web site without invoking the security. If it's too long, it will make your URLs unwieldy.

You can't have “nested” realms—WebSTAR evaluates the entire URL and allows or denies access based on that. You can't allow someone to see a subfolder without allowing them access to the parent folder as well.



See “WebSTAR URL Security Processing” on page 183.

Realm Match Strings

Realms are defined by a unique word in the file path, usually a folder name, known as the **match string**.

If a URL can match more than one realm, WebSTAR will stop searching once it matches the first realm (based on the order in which they



Be sure that your match string is not used in any other file or folder names. All URLs are evaluated, so if that text is used in any other URL, the security processing will start up.

appear in the Realms list). If a Match String is entered twice, the second realm will never be used. A good solution is to make up a word or combine two words so that you make a code word which is only used for this purpose.

Example Realms

Suppose you want to configure your server with some files available to everyone, some files available to coworkers, and some files available to customers. You can do so by defining two realms such as:

- **Realm Name **WORK**, Match String **OURWORK**.** Folders and files in this realm may have URLs such as:

```
http://www.domain.com/ourwork/draft.html
http://www.domain.com/ourwork/new/test.html
http://www.domain.com/news/ourwork/
```

- **Realm Name **CUSTOMERS**, Match String **CSTMR**.** Folders and files in this realm may have URLs such as:

```
http://www.domain.com/cstmr/price_list.html
http://www.domain.com/news/cstmr/
```

Once the web server has found that a URL is in a realm and requires authentication, WebSTAR will check the lists in Allow/Deny (described on page 172) and Web Users and Passwords (described on page 168). For more information, see “Realms, Allow/Deny and User Names Work Together” on page 167.

Editing Realms Entries

A realm requires these two elements: the name and the match string. You should consider them both carefully, as you'll be using them often.



Make sure that your realm name is relatively short. User names and realm names together must be less than 30 characters long.

- **Realm Name:** a one-word name (you can use dashes or underscores to separate words). The Realm Name will be shown to users in the user name and password dialog presented by the browser, and will be used in the Admin for the Web Users and Passwords and Allow/Deny panels.

- **Match String:** the word or phrase that will be searched for in incoming URLs. It must appear in the names assigned to the actual folders and files that will be included in this realm.

You should try not to use spaces or Macintosh special characters in the Realm Match String. If a Match String must include special characters, follow the rules in “Macintosh Special Characters in File Names” on page 189 to encode them yourself.

WebSTAR stores your realm entries in the *WebSTAR Settings* file. There is no import/export function for realms, so you will have to create and edit the realm entries interactively.

To create or change realm entries, you'll need to use the Admin application or the Browser Admin page, described below.

Default Realms

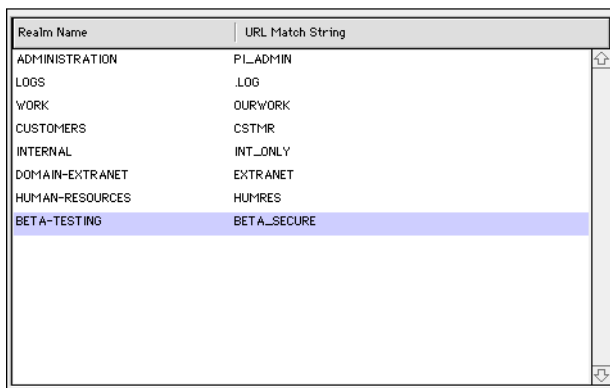
The default realms are **Administration**, which matches the `PI_ADMIN` string used by WebSTAR's Browser Admin pages; and **Logs** which protects your *WebSTAR.Log* file from unauthorized access. You can allow yourself access by creating Allow/Deny or Web Users and Passwords entries.

Realms Cannot Be Nested

As you design your realms, be sure that a folder that you designate as a realm does not contain any other folders that you'd like to control differently. Anyone with access to a subfolder must also have access to the parent folder, because WebSTAR will evaluate the entire URL.

WebSTAR Admin Realms List

Choose the Realms item in the WebSTAR Admin Settings window to open the Realm List. The only two entries when you start out are ADMINISTRATION and LOGS, but you can add many more.



Realm Name	URL Match String
ADMINISTRATION	PI_ADMIN
LOGS	.LOG
WORK	OURWORK
CUSTOMERS	CSTM
INTERNAL	INT_ONLY
DOMAIN-EXTRANET	EXTRANET
HUMAN-RESOURCES	HUMRES
BETA-TESTING	BETA_SECURE

To make a new realm entry, decide where you want it to be in the list. WebSTAR will stop at the first match of the folder hierarchy in the URL, so it's best to keep the names unique, rather than rely on partial matches. Then select the entry **before** the new entry, and click the **New** button. Follow the instructions above to fill in the fields.



For more instructions, see "Working With Admin Lists" on page 120.

Browser Admin Realms List

The WebSTAR Browser Admin pages also allow you to work with the Realms List. Go to the Administration main page, and choose Settings > Realms.

To make a new realm entry, follow the instructions above to fill the fields. Then click the **Add New Entry** button.

To edit an realm entry, click on the **Select** radio button for that entry, and then click the **Edit Selection** button. When you're done with your changes, click the **Replace Selection** button, and your changes will be saved.

To copy an entry, click on the **Select** radio button for that entry, and then click the **Edit Selection** button. When you're done with changes, click the **Add New Entry** button.

To delete an entry, click on the **Select** radio button for that field and click the **Delete Selection** button.

Realms, Allow/Deny and User Names Work Together

You can use a combination of Allow/Deny entries and User Name and Passwords to make your web server both secure and convenient.

- 1 Create a special realm for your secure data.
- 2 Create an Allow entry for that realm, with the domain name of your organization.
- 3 Create at least one User Name and Password entry for that realm.

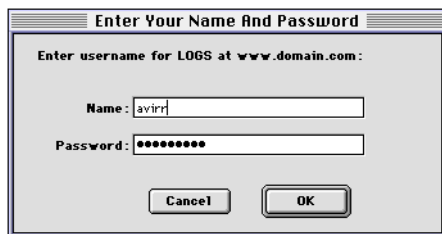
Now, anyone who's in your company with a machine whose name includes the domain name will be able to browser your site without problems. Those on the road and outside the organization can still have access by entering the User Name and Password. No one else can see the data.



See also "WebSTAR URL Security Processing" on page 183.

WEB USERS AND PASSWORDS

You can associate user names and passwords with realms. This means that when the browser sends a URL which includes the realm match string, the server tells the browser to display a dialog requiring the user to type in a user name and a password for access to that host or page.



- User names and realms provide **authentication**, they only allow authorized users who know the password access to certain data. For encrypted transmission of confidential information, see “SSL Web Security” starting on page 209.
- Note that many people can share a user name and password for a WebSTAR realm. You will be able to track transactions by their IP address or host name, if necessary.
- If a visitor doesn’t have the correct user name and password for that realm, they will get a chance to re-enter the data. If they choose **Cancel**, they will see the “Not Authorized” Error Message (described on page 183).
- Most browsers retain the user name and password (authentication), so the user only needs to enter it on the first access. This is convenient, but creates a small security problem: anyone who enters the password from a public computer, such as one at a library or cyber cafe, will be authenticated until the browser is restarted.



For more details, see “WebSTAR URL Security Processing” on page 183.

Editing User Entries

To create and edit Web User Name and Password entries, you must use the WebSTAR Admin application, as described below.

User Entry Editing Notes

- Before creating User entries, you must create the realm with its match string to the protected folder.
- Each user name within a realm must be unique. WebSTAR will only check one password per user name.



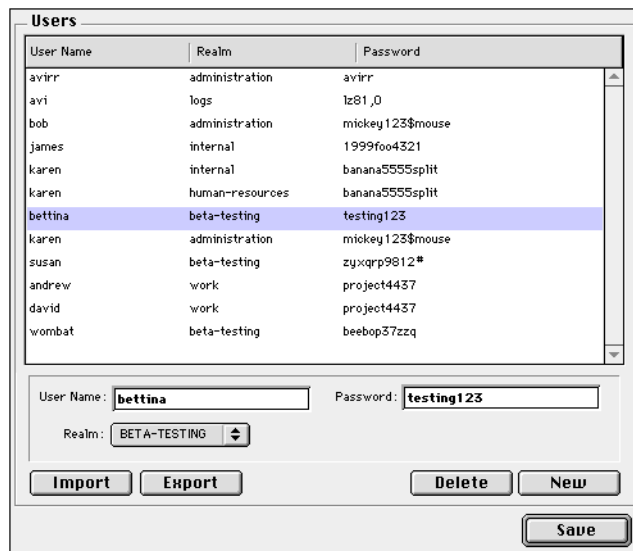
You can’t use the Browser Admin to create User entries.

- You can create several entries with the same user name for many realms. The password for that user name can be the same, or it can vary.
- The length of the user name and realm information together must be **less than 30 characters**.
- Do not use a bullet (•) or colon (:) in your user name or password. Those characters are used by the import/export file format.
- You can't have a blank password—you must at least have a single character (which can be a space) for the password.
- The password is limited to 64 characters.
- When you choose a password, make sure that it does not contain Macintosh-specific characters that cannot be typed from a PC-compatible Web client. You're safe with letters, numbers, underscore, (_), dash (-), and period.
- For better security, choose passwords carefully (see "Safe Passwords" on page 96). But note that passwords are not encrypted by the browsers, so for best security, use SSL as well.
- If you prefer, you can edit the Users list in a text editor or database and import it into WebSTAR: for instructions, see "Importing and Exporting Large Users Lists" on page 170.

WebSTAR Admin Users List

Choose the **Users** item in the WebSTAR Admin Settings window to open the Users List. You'll see a list like this, showing you all the Users and passwords in all the realms.

 Don't try to enter your user names in order: the server will store them internally in the best order for fast processing.



User Name	Realm	Password
avirr	administration	avirr
avi	logs	lz81_0
bob	administration	mickey123\$mouse
james	internal	1999foo4321
karen	internal	banana555split
karen	human-resources	banana555split
bettina	beta-testing	testing123
karen	administration	mickey123\$mouse
susan	beta-testing	zy:xqp9812*
andrew	work	project4437
david	work	project4437
wombat	beta-testing	beebop37zzq

User Name: Password:

Realm:

To make a user name entry, select entry before the new entry, and click the **New** button. Select the Realm from the popup menu, and fill in the User Name and Password fields. Names and passwords are not case sensitive.

The new user name will appear in the scrolling list, along with the realm to which it is assigned and the password.

User names are available immediately as soon as you add them; there is no need to stop or start the server. In addition, WebSTAR can continue to serve files while you are adding user name and password information.



For more instructions, see "Working With Admin Lists" on page 120.

Example Realm and User Entry

To assign a user name and password to a realm, follow these steps:

- 1 Create a folder in your WebSTAR folder named *mytest*, and make a little HTML file named *default.html*.
- 2 Open the WebSTAR Admin application and connect to your server, then choose **Server Settings** from the Options menu.
- 3 Choose **Realms** from the options list at the left and create a realm named *My_Test* with a Match String of *mytest*.
- 4 Choose **Users** from the Options list at the left.
- 5 Press the **New** button, to create a new User entry.
- 6 Select the realm in the Realm pop-up.
- 7 Type a user name and a password in the appropriate fields.
- 8 Press the **Save** button to save the results to the server.
- 9 Test that you are allowed to see the realm by opening a browser and trying the URL:

`http://www.domain.com/mytest/default.html`
(replace "www.domain.com" with your host name).
- 10 You should see a dialog requesting a user name and password for the *MY_TEST* area. Enter the name and password, and view your test default file.

Importing and Exporting Large Users Lists

You can edit thousands of Web User entries in the WebSTAR Admin application, but you may find it inconvenient: the list is not in alphabetical order, and cannot be sorted. If your connection to your server is slow, the transfer time may be quite long.

If your Web User list becomes unwieldy, we recommend that you store and update this data in another application, such as a database. WebSTAR includes Import/Export functions for the user names and passwords.

You can keep user names and passwords in a database, and make all changes in that database. For every change, you then export the list to a file on disk, and import it into WebSTAR. If you do this, be sure that you always make changes in the database, and do not make any changes using WebSTAR Admin, or your lists may become unsynchronized.

 Importing passwords will **replace** the existing password file: it does **not** append to it. Always copy your *WebSTAR Web Users* file and store it somewhere safe before importing new passwords.

To export, click the **Export** button in the WebSTAR Admin Users panel, and save the file to your disk.

To import, make sure that all your entries are in the file to be imported—you may want to export your existing users list, and combine it with the additional entries. You should always **back up** your *WebSTAR Web Users* file. Then click the **Import** button and choose the text file you have created, and it import the replacement users list.

Web Users Export File Format

The import/export format of this file consists of one user entry per line, followed by a Carriage Return. Each line has a user name, a bullet, the realm, a tab, then the password.

```
user name•realm <tab> password <CR>
user name•realm <tab> password <CR>
```

For example, a file might look like this:

```
Workers•OUR_WORK      TeamWork99
Widgets•CUSTOMERS     GetWidgets
Human Resources•HUMRES Be8Safe05
```

The last character in the file should be a CR (Carriage Return) at the end of the last entry. Make sure there aren't any extra Carriage Returns at the end of the file.

 The user name and realm together should be less than 30 characters.

ALLOW/DENY

WebSTAR can also limit access to your entire server or to selected realms according to a browser's host name, domain name or IP address. That way, you can allow in browsers residing on machines in your company, or outside contractors, but keep everyone else out.

Global Access Control

When you are creating Allow/Deny entries, you can choose the **Global** item from the Realm popup menu. While "Global" is not a realm, you can use it in arranging your Allow/Deny entries. It applies to the entire web server, and is not limited to any single realm.

Global access control is limited to Allow/Deny: you cannot create User name and password entries for denied machines.

If you make **any** Allow or Deny entries in the Global access section, all other machines will be denied. To allow all other machines, you must make an Allow * entry.

Realms Access Control

WebSTAR allows you to specify who can and can't see a specific security realm. As the name implies, an **Allow** entry for a realm means that browser requests for data in that realm will be accepted if they come from a machine with that domain name, host name or IP address. All requests from other machines will be allowed to enter a User Name and Password, and allowed to see the realm if they match one of your Web Users and Passwords entries.

A **Deny** entry for a realm means that all browser requests for data in that realm will be rejected if they come from a machine with that domain name, host name or IP address. If you enter **any** Allow or Deny entries for a realm, you must **specifically** Allow other machines to access that realm [you can use an asterisk (*) to Allow all other domain names].

Note that machines which use dialup Internet access do not have static host names or IP addresses, so you can't create Allow entries for them. You can set up Web Users and Passwords (described on page 168) to supplement the Allow/Deny entries. You can combine the two forms of access control to make the least intrusion, while still allowing access while co-workers are on the road, or from dialup connections at home.



A **domain name** refers to the whole company ("star-nine.com"). A **host name** ("me.domain.com") refers to a particular machine (even if it's not a server).



See also “WebSTAR URL Security Processing” on page 183.

For example, you could Allow the computers in your company to access the human resources information in the “HUMRES” realm. If machines on which interns work all have “intern” in the host name, you could Deny access to all machines in your domain starting with “intern”. For more examples, see “Allow/Deny Examples” on page 175.

When you start WebSTAR for the first time, there are no Allow or Deny entries.

Editing Allow/Deny Entries

When you create an Allow/Deny entry, you enter data about the browser machine’s IP address or host name, and designate either the **Global** section or the realm name.

About Address Matching

You can specify host names, domain names, subnets or IP addresses in the Address field. If you want to use names, make sure you’ve checked the box to Caching (described on page 139).

To find a machine’s IP address or host name, no matter where they are, have them access your site once. Then look at the WebSTAR Status Window or Log file. It will show you the IP address. If you have selected Use DNS, the transaction entry will also display the host name.

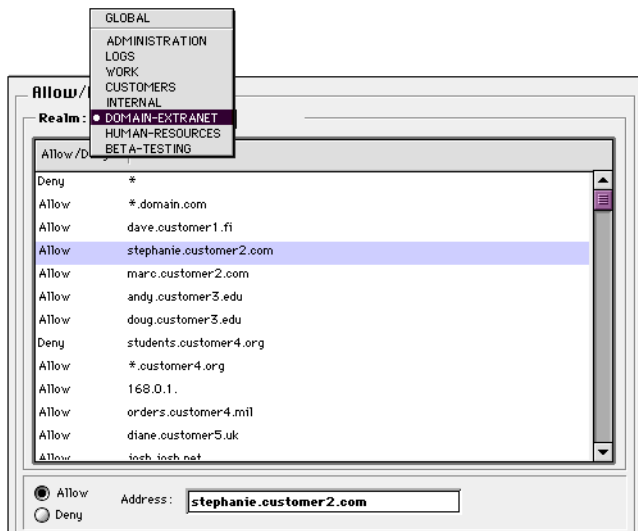


The Address can be any substring: it does not have to be complete host names or IP addresses. To match a specific domain name, IP address or subnet, use a trailing period (a period at the end of the Address field).

- 198.211.3
all machines which include these numbers in the site in all subnets that begin with the number 3.
- 198.211.33.
the trailing period makes the system only match the machines in the 33 subnet.
- 198.211.33.4.
refers to the single machine with that exact IP address (the trailing period means that machines ending in “40” would not be matched).
- starnine.com
all machines which include the text “starnine.com” anywhere in their host name.
- starnine.com.
the trailing period makes the system only match those machines which have “starnine.com” at the end of the host name.
- *
An asterisk by itself refers to all domains. This is usually used when you want to allow all but one or a few domains, as described in “Using Deny Entries” on page 176.

WebSTAR Admin Allow/Deny List

Choose the Allow/Deny item in the WebSTAR Admin Settings window to open the Allow/Deny List. The first time you open the panel, you'll see an empty list, with just the Administration and Logs realms in the popup menu. Once you add a number of entries, it will look like this:



The WebSTAR Admin Allow/Deny list is controlled by the Realm popup menu. The list for each realm will appear when you chose the realm from the menu.

To make a new Allow/Deny entry, decide where you want it to be in the list. In general, you don't have to worry about order, unless you are Denying a host name or subnet and Allowing others in the same domain or IP class. To specify the insertion row, select the entry **before** the new entry, and click the **New** button. Select the correct realm from the Realms popup menu, and follow the instructions above to fill in the Address field.

 See also: "About Address Matching" on page 173.

 For more instructions, see "Working With Admin Lists" on page 120.

Browser Admin Allow/Deny Editing

The WebSTAR Browser Admin pages also allow you to work with the Allow/Deny List. Go to the Administration main page, and choose Settings > Allow/Deny.

Warning: When you're editing Allow/Deny entries in the Browser Administration pages, be **sure** to select your realm in the popup menu, then **press the Change Realm button**. If you do not change



It's fairly easy to deny yourself access, so be sure that you always change the realm **before** you edit the entries.



For more on Address match strings, see "About Address Matching" on page 173.



See also "WebSTAR URL Security Processing" on page 183.

the realm explicitly, you will appear to edit a specific realm, but in fact you will be editing the "Global" access section.

To make a new Allow/Deny entry, decide where you want it to be in the list. In general, you don't have to worry about order, unless you are Denying a host name or subnet and Allowing others in the same domain or IP class. To specify the insertion row, enter an Order number so that the new Allow/Deny entry will be numerically placed within the list. Select the correct realm from the Realms popup menu, and change realms, then follow the instructions above for the Match String (Address) field, and press the **Add New Entry** button.

To edit an Allow/Deny entry, click on the **Select** radio button for that entry, and then press the **Edit Selection** button. You can rearrange the order by changing the number in the Order field. When you're done with your changes, press the **Replace Selection** button, and your changes will be saved.

To copy an entry, click on the **Select** radio button for that entry, and then click the **Edit Selection** button. When you're done with changes, press the **Add New Entry** button.

To delete an entry, click on the **Select** radio button for that field and press the **Delete Selection** button.

Allow/Deny Examples

These examples show how you can set up Allow and Deny access to specific folders, and limit access to those folders.

Allow One Machine

- 1 Create a folder in your WebSTAR folder named *mytest*, and make a little HTML file named *default.html*.
- 2 Open the WebSTAR Admin application and connect to your server, then choose **Server Settings** from the Options menu.
- 3 Choose realms from the options list at the left and create a realm named "My_Test" with a Match String of *mytest*. Be sure to click the **Save** button to send the information back to WebSTAR.
- 4 Open the Allow/Deny panel and click the **New** button.
- 5 Select **My_Test** from the Realms popup menu.
The **Allow** radio button is selected by default.
- 6 Enter your IP address into the Address field.
example: 192.168.33.1.

(replace this with the IP number of the machine you are using)

- 7 Press the **Save** button to send the changes back to the server.
- 8 Test that you are allowed to see the realm by opening a browser and trying the URL for the default file.
`http://www.domain.com/mytest/default.html`
(replace “www.domain.com” with your host name).
- 9 Test the security by trying to access the same URL from another machine. It should be denied.

Allow An Entire Site

- 1 Open the Allow/Deny panel and click the **New** button.
- 2 Select **My_Test** from the Realms popup menu.
- 3 Enter your domain name into the Match String field.
example: domain.com.
- 4 Click the **Save** button.
- 5 Test that you are allowed to see the realm by using the example above.
- 6 Test that you can see it from another machine in the same domain.
- 7 Ask a friend to try to access the URL from another domain. They should see a user name and password dialog, even if you have not entered a user for that realm. Check your log or web monitor pane to see the “PRIV” error entry.

Using Deny Entries

Deny entries are most useful to block out problem visitors, and to limit access for some machines within a site.

When you deny any site, WebSTAR’s default behavior is to deny all sites which don’t have a specific Allow entry. You can counteract this by specifying an Allow * entry.

Deny A Subnet

- 1 Open the Allow/Deny panel and create a new entry.
- 2 Select **My_Test** from the Realms popup menu.
- 3 Click on the Deny radio button.
- 4 Make the Match String deny the appropriate subnet:
example: 192.168.3.
This will allow everything except the specific subnet designated by the IP address.

- 5 Make another new entry, select **My_Test** and enter an asterisk (“*”) in the Address field. This allows everyone to access this realm, unless their IP address is matched above.
- 6 Choose the Users panel and make a new User and Password entry.
- 7 Set the User Name to “test” and the password to “test”.
- 8 Save the results to your WebSTAR server.
- 9 Test the results by trying to access the realm from a machine in this subnet.
- 10 You should see the User Name and Password dialog; enter “test” and “test”, and see if you can view the default page.
- 11 Make sure you can still access the realm from another machine in a different subnet without a password.

You can deny access to domains or specific host names as well, but don't forget to enter **Allow *** as the last entry, so that everyone else can get to the site.



See also “Web Server Administration” on page 129.

This chapter covers a number of important concepts necessary for the use and operation of your WebSTAR Web server, including background information on web serving and the basics of HTTP and HTTPS connections, URL requests and security processing, how best to setup your web folder hierarchy, and important information on using Virtual Hosts to serve multiple web sites.

WEB SERVING AND HTTP

This section describes how WebSTAR handles HTTP connections, including techniques for tracking user interaction; realm and web user security processing of URLs; procedure for serving a requested file or other data; and how WebSTAR responds to errors.

HTTP Connections



The WebSTAR Web server also supports the HTTPS (secure) protocol. It works like HTTP, but the data is encrypted before being transmitted. For more information, see “SSL Web Security” on page 209.

The ***HyperText Transfer Protocol (HTTP)*** defines how a Web server handles connections. Unlike some protocols, HTTP opens connections only for as long as needed to transfer the requested data. The connections are then closed immediately. Even “persistent” connections do not create a long-term link between the server and the client: as soon as the data is transferred, the connection is closed.

This method of handling connections has a few implications for the administrator of a Web server. First, there is no way for WebSTAR to keep track of where a connection leads. So, if a browser requests data from your server, there is no way for the WebSTAR Web server to track which links are followed within that data, because the connection is closed once the original data is returned.

Per-File Connections

In addition, each separate element in a page requires its own connection. For example, a page of text requires one connection to download. If that page contains a graphic, another connection is required. Therefore, connection information is not necessarily a reliable way of analyzing a server’s activity. For example, if you have a server with 5,000 connections a day serving a text document and you add a graphic to that document, your server will suddenly report serving 10,000 connections a day, simply because it’s serving an additional graphic each time.



see “Use DNS for Server and Client Lookups” on page 136.

By using the Persistent Connections feature of WebSTAR, the server can hold open a single connection and use it to transmit multiple files, thus reducing the overhead of setting up and closing connections.

Creating Client “Sessions”

As described above, HTTP closes connections as soon as the requested data is served. However, there are many good reasons why you would want to keep track of a person as they go through your site, and after they leave and come back. For example, you may want to suggest related pages, track online tests, show them what's new since the last time they looked at the site, or track the choices on a store.

There are a number of approaches to tracking viewers to your site:

- **cookies** are a standard solution. Most browsers can store these small amounts of information, which is sent back to the server when the browser accesses the site again. For more information, see:

<http://search.netscape.com/assist/security/faqs/cookies.html>

- **WebObjects** is Apple's high-end middleware solution that tracks browser interaction with the server and connects to large databases, and other WebObjects systems. For more information, see “WebSTAR WebObjects Adaptor” on page 272, and

<http://software.apple.com/webobjects/>

- **Database modules** can track by host name and IP number, allowing you to control what the visitor sees by where they have been before.
- **eCommerce modules** can include a “shopping basket” function, so shoppers can store their choices for later purchase. For more information, see:

<http://www.starnine.com/extendingwebstar.html>

Analyzing User Interaction

You can also track people viewing your site by viewing your log files (see “Web Server Logging” on page 199). For statistics and analysis, you may want to use a log analyzer. Many of them will let you learn how people travel within your site and which elements are the most effective. Many log analysis programs are available: see the Extending WebSTAR pages for links.

WebSTAR URL Processing

The Web browser (client) software is responsible for constructing the full URL for a document, which contains the server's hostname and possibly a path to the folder or file containing the desired data.

Once the WebSTAR Web server receives the URL and has routed it to the correct host, it has to find the data. Some URLs are for files, others for CGIs and Plug-Ins, but the process is very much the same.

For example, this is a full URL to an HTML document:

```
http://www.domain.com/widgets/bluewidget.html
```

The client machine looks up the domain in the DNS registry, and locates the IP address of your WebSTAR server machine.

Starting at the Root

By default, WebSTAR analyzes URLs relative to its own position on the disk. Therefore, the **WebSTAR root folder** for the WebSTAR web server is the folder in which the server application resides. A root URL is just the name of your host, which will bring up your default or index file in the root folder:

```
http://www.domain.com
```

If you are serving several hosts, the root folder for each of those hosts is the folder that you designate in the Virtual Hosts list. WebSTAR will respond to the URL relative to that folder for that virtual host, so it will bring up the index or default file in that folder.

How WebSTAR Handles a URL

When the WebSTAR server receives an incoming URL, it performs the steps described below.

- If you are using virtual hosts, it routes the URL to the correct site, depending on the IP address, domain name, and/or language (see “Routing to Virtual Hosts” on page 193). Otherwise, this step is skipped.
- If you have any Filter Plug-Ins installed, they perform their filter task on the request.
- If a Pre-Processor is installed, it will run next (see “Pre-Processor” on page 132).
- WebSTAR will also check for security controls on your server., as described in “WebSTAR URL Security Processing” on page 183.

From here on, the WebSTAR web server works on the **data path** elements of the URL. In this example:

```
http://www.domain.com/widgets/bluewidget.html
```

the data path elements are

```
widgets/bluewidget.html
```

The processing steps are:

- 1 WebSTAR converts the slashes in the URL to colons to obtain a Macintosh file path. In this case, it’s “widgets:bluewidget.html”.
- 2 The web server then converts any HTTP special characters from the two-digit hex numbers (such as “%20” for space) to Mac characters. For



For more information on virtual hosts, see below and “Routing to Virtual Hosts” on page 193.



See “Security Realms” on page 164.

more information, see “Macintosh Special Characters in File Names” on page 189.

It also replaces double colons (: :) with a single colon (:) to prevent clients from accessing parent directories in the Mac OS file system.

- 3 If the URL is for a folder (because it ends with a trailing slash), WebSTAR will automatically get the index file.
 - If there is a *.message* file in the folder and the Directory Index Plug-In is installed), the server will call the Plug-In to display a list of the files in that folder, and will skip the rest of the steps in this section.
 - Otherwise, it will serve the default file for that folder (as specified by the default index file setting, such as *default.html*). It will continue to the next step, using that file for future processing.
- 4 WebSTAR then looks up the file requested by the URL in the Suffix Mapping Table, using the file suffix or File Type and Creator (see “How Suffix Mapping Works” on page 155).
- 5 If the file is a redirect file or other RAW file, WebSTAR returns it without adding any header information (see “Redirect Files” on page 191).
- 6 If the Action is Binary, or Text, the WebSTAR web server returns the contents of the requested file to the browser, without changing it in any way. If it’s already in the Data Cache, the server can send it very quickly, without reading the file from the disk.
- 7 If the Suffix Mapping Action refers to a CGI or Plug-In, WebSTAR calls that module and sends it the URL. The CGI or Plug-In uses the URL to define the requested task: in most cases it will retrieve information, process the data and send the HTML page or data to WebSTAR, which will send it back to the client without any additional changes.
- 8 If no file is found, the URL matches a path to a folder, and it does not have the trailing slash, WebSTAR will return a redirect URL for that folder with the trailing slash, so the browser can resubmit the entry automatically for the index file. For example, this URL:

`http://www.domain.com/widgets`
will be converted to:

`http://www.domain.com/widgets/`
- 9 If none of these conditions are met, the request is an error. WebSTAR will return an error message for the host, as described in the next section.



If the URL points to an alias, WebSTAR will use the suffix of the alias: it will not use the suffix of the original file.



For more information, see “Suffix Mapping” starting on page 154.

Responding To Errors

If the requested data was not found, or the person requesting it was denied access to a security realm, WebSTAR will return one of the specified error messages.



If you are using Virtual Hosting, each host can have separate error message settings. See “Virtual Host Options” on page 150.

To designate a special error file or use a third-party CGI or Plug-In to respond to these errors, redirecting the browser to another file or giving a more useful error message, see “Default Names” on page 130.

Error.html: “File Not Found” Error Message

If a browser sends a URL for a file that does not exist, WebSTAR will send back a standard error message. The default behavior is to send the file *Error.html*, installed in the root folder, which has a “File Not Found” error message.

You can edit that file in your favorite HTML editor, to make it more useful to people accessing your site. For example, you can add a site map, a list of the most important links on your site, or a search form for your site—all tools to make it easier for your visitors to get back on track. You should also add the webmaster email address and consider providing a contact phone number as well.

Noaccess.html: “Access Denied” Error Message

You can use the Global option in the Allow/Deny interface to deny a browser access to the entire host, according to the browser machine’s host name, domain name or IP address. If you do so, and a browser from that domain attempts to access the server, they will get the No Access error page.

The default behavior is to send the file *NoAccess.html* from the root folder, with an “Access Denied” message. You can edit that file in your favorite HTML editor to explain how they can get access to the host, or replace the file entirely.

“Not Authorized” Error Message

When a browser tries to access a secure realm, but the user does not enter a valid user name and password, the web server will return the pre-set **Not Authorized** error message. You cannot edit this message in HTML.

WebSTAR URL Security Processing

When WebSTAR gets a URL, it must first make sure that the browser machine is allowed to access that particular data. Only once it has checked all security options will it go on to find and serve the data, as described below in “WebSTAR URL Processing” on page 180.

- 1 First, the WebSTAR server will check the global Allow/Deny settings for a match.



For information on using this security, see “Allow/Deny” on page 172.

If there are global Allow/Deny settings, and this host name or IP address is not granted access, WebSTAR rejects the request and returns the No Access response.

- 2 Otherwise, WebSTAR checks the Realms list for a match between the any part of the requested URL and the match strings.

If there is no match, skip to step 6.

- 3 WebSTAR checks to see if the browser has passed an **authenticated** username and password for this session (which means that a user has entered a correct user name and password from this host already).

If it has already been authenticated, it will not require the login for every secure page, so WebSTAR will skip to step 6.

- 4 Otherwise, check if there is an Allow or Deny entry for the realm.

If there is an Allow entry for the realm, skip to step 6.

- 5 If there is no Allow entry, or there is a Deny entry, respond to the browser requesting a User Name and Password.

- If they enter a correct User Name and Password, send that **authentication** information back to the browser, for future reference (it's used in step 3).
- If the user cannot enter the correct User Name and Password, reject the request and display the "Not Authorized" page.

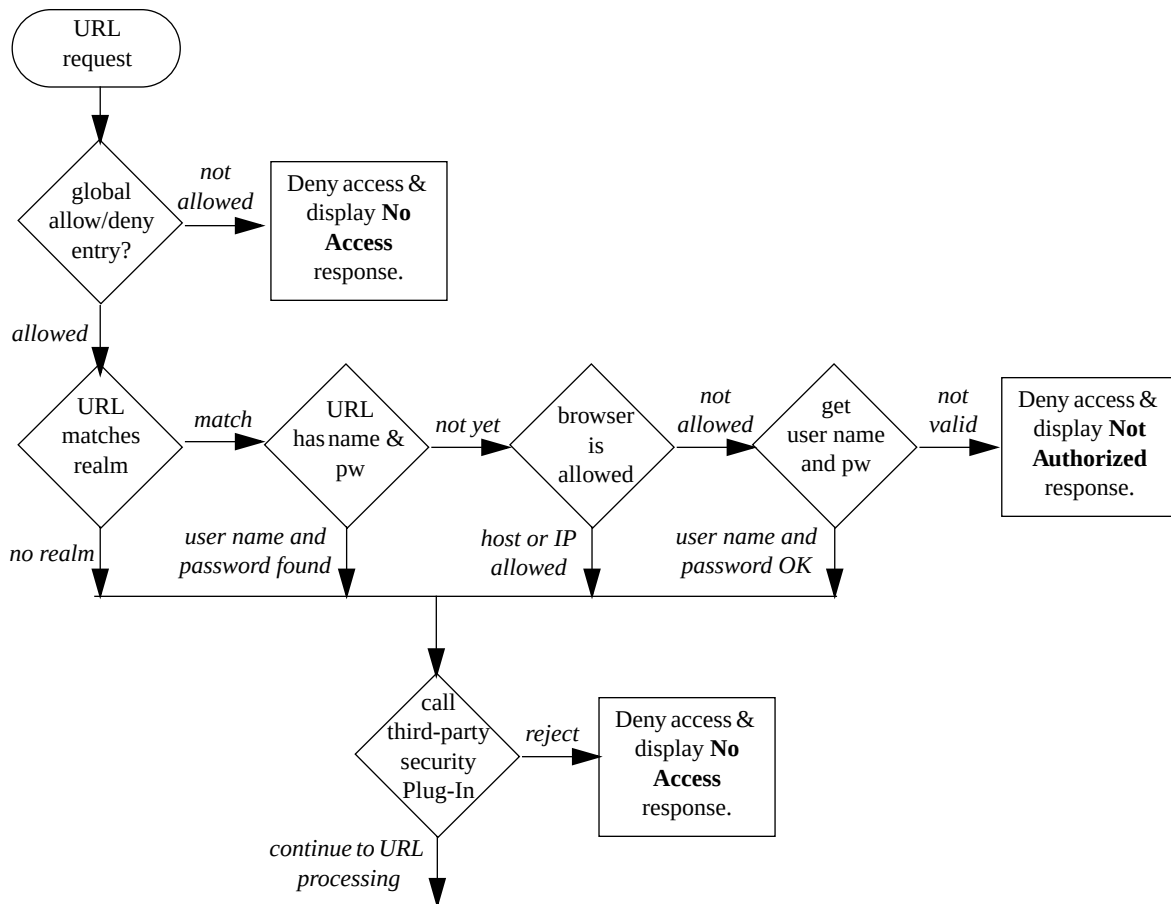
- 6 Call all security Plug-Ins. These third-party modules provide different forms of security and access control. Even if you do not use Realms, they will get a chance to perform security and access checking.

- 7 If all security Plug-Ins approve the request, the WebSTAR web server returns the file or data requested by the URL.



After a denial, the User Name and Password dialog will always appear in the browser, even if there is no User entry associated with a realm.

WebSTAR Security URL Processing



FOLDER HIERARCHY, FILE PATHS, AND NAMES

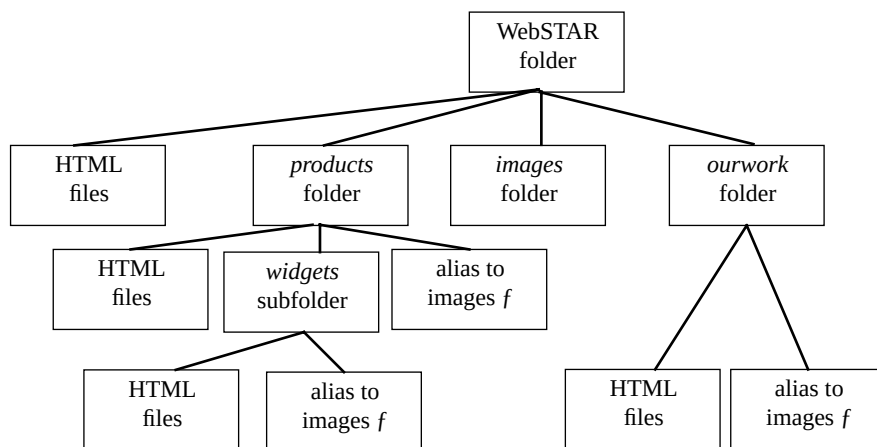
You can think of your website as a tree, with a main stem or root (the main WebSTAR folder) and branches (subfolders in that folder). We'll refer to these as the **WebSTAR root folder** and the **folder hierarchy**. You can use URLs to link to files all the way through the folder hierarchy, and to FTP folders as well.



WebSTAR uses standard Mac folders—they correspond to “directories” on other systems.

Example Hierarchy and File Paths

Our simple example, `www.domain.com`, has a *products* folder which includes a *widgets* subfolder, an *ourwork* folder (within a security realm), and an *FTP* folder including a *pub* folder set up for anonymous access and a *widgets* folder.



The **file path** is the description of how to find a file within the folder hierarchy. The **delimiter** is a slash (“/”), which surrounds a folder name.

In this case, you can have HTTP links, with their file paths, that would like this:

- `http://www.domain.com/`
display the default index page in the root folder of the web server.
- `http://www.domain.com/products/`
display the default index page in the *products* folder of the web server.
- `http://www.domain.com/widgets/bluewidget.html`
display a specific HTML page in the *widgets* subfolder.
- `http://www.domain.com/ourwork/images/picnic.gif`



See also: “Relative and Absolute Links” on page 188.

display an image file in the *images* folder (using an alias). If the “ourwork” string is a security realm match string, the server will check allow/deny entries and request a password if necessary.

File Hierarchy and Virtual Hosting

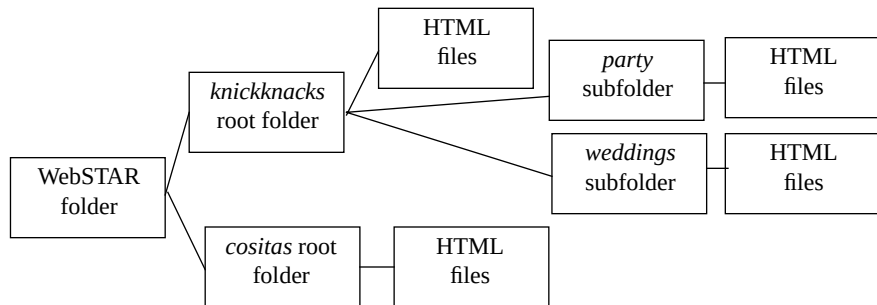


See also: “Special Virtual Domain Design Issues” on page 197.

If you have virtual hosting enabled, you set the **virtual host root folder** for each of your web site hosts. The folder hierarchy is the same, but instead of starting with the WebSTAR root folder, it starts with the folder that you have designated.

In the following simple example, the WebSTAR server has two virtual hosts: `www.knickknacks.com` (root folder is *knickknacks*) and the Spanish-language `cositas.domain.com` (root folder is *cositas*).

Virtual Hosts and Subfolders



These URLs do not refer to the WebSTAR folder, but to the root folder for that domain.

- `http://www.knickknacks.com/`
will display the default file in the *knickknacks* folder;
- `http://www.knickknacks.com/party/blue.html`
will display a specific page in the *party* subfolder
- `http://cositas.com/informaciones.html`
will display an information page in Spanish

Links to Subfolders and Parent Folders

To refer to a folder, you enter the name with slashes before and after the folder name. For example, this URL:

`http://www.domain.com/documentation/manual.html`

will tell WebSTAR to look inside the *Documentation* folder for a file called *manual.html* and serve it back to the browser.

To link to a page in a subfolder within your folder hierarchy, just use the name of the folder. For example, to show a page for your blue widget, make a folder called *widgets* in the WebSTAR folder, and a file named *bluewidget.html* in the *widgets* folder. To access this file, the URL would be:

```
http://www.domain.com/widgets/bluewidget.html
```

Remember, replace “www.domain.com” with your host name or IP address.

Default Files in Subfolders

When a URL for a folder arrives, WebSTAR will use the default file name that you've specified in the server or virtual host settings pane, as described in “Default Names” on page 130 and “Virtual Host Options” on page 150. This applies to all subfolders for each virtual host.

Relative and Absolute Links

You do not have to know HTML to run WebSTAR, but should understand how file paths and links work. This section helps you visualize the relationships between folders and HTML links.

When you make HTML links to files on your website, you can use **absolute paths** to link to files always starting from the root level. For example, a file in the *widgets* folder could refer to an image like this:

```
<A HREF="/images/bluehat.gif">
```

However, it's often easier for you to use **relative paths**, linking to files in **relation** to the HTML page which includes the link. The syntax of the relative addresses is standard UNIX: a slash (“/”) means a folder, and two periods (“..”) means a level up in the folder hierarchy.

Examples of Absolute and Relative Links

Here are some examples of both relative and absolute URL links, according to the example hierarchy above.

- `<A HREF="party/bluehat.gif">`

this **relative link** in a file in the *knickknacks* folder means “start at the location of this file, open the *party* folder and get the file *bluehat.gif*”.

- `<A HREF="greenknick.html">`

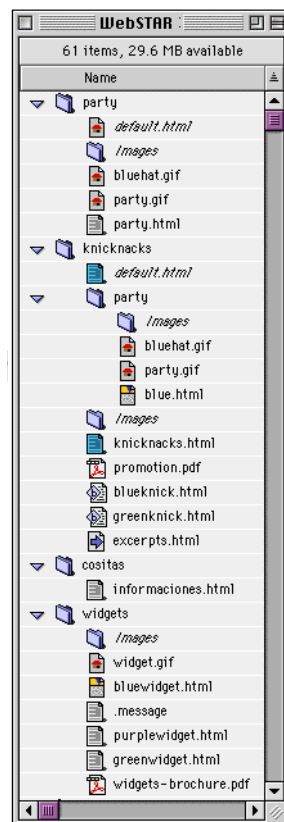
tells the browser to request a file called *greenknick.html* in the same folder as this HTML file (a **relative link**).

- `<A HREF="../greenknick.html">`

tells browser to go up one folder from this HTML file and request a file called *greenknick.html* from that folder (a **relative address**).



Directory indexing overrides the Default File display: see “WebSTAR Directory Indexer” starting on page 241.



■ `<A HREF="/knickknacks/greenknick.html">`

tells the browser to request the file *greenknick.html* from the *knickknacks* folder in the root folder, no matter where this HTML file is located (an **absolute address**).

■ `<A HREF="/knickknacks/party/bluehat.html">`

tells the browser to request a *bluehat.html* file inside a *party* folder in a *knickknacks* folder in the root folder (another **absolute address**).

Remember that you can't go above the root folder, even on virtual hosts. However, if you want a file in another virtual host on the same machine, you can link to it using the host name, for example:

`<A HREF="www.domain.com/widgets/widget.gif">`

Web File and Folder Name Rules

Although WebSTAR is running on your Mac, you still must work within the limits of the Internet and web serving conventions. Unfortunately, this may mean that you must rename or alias some of your files and folders.

For simplicity, you should use standard English letters and numbers in your file names. Hyphens ("‑"), periods (".") and dashes ("‑") are also fine, but spaces between words must be encoded (see below).

You should **never** include these characters in any file name:

- `/` (slash) is used by the HTTP and FTP standards as the **delimiter** between folders in a file path.
- `$` (dollar sign) and `?` (question mark) are reserved for CGI parameters by web servers.
- `<` and `>` (pointed brackets) are used in HTML and should not be in file names.

Macintosh Special Characters in File Names

Macintosh Extended characters (option-key characters) are useful and appropriate especially for languages other than English. However, file names in URLs cannot use these characters—the names are limited to the characters you see on the keyboard. Extended characters can cause additional problems. Some proxies and other caches may not be able to resolve URLs if they aren't exactly the same as the file name—they can't convert the encoded characters.

There are situations when you must use Extended ASCII characters in file names, because they are required for other languages or for scientific clarity. In that case, you must **encode** the links in HTML documents to these files using the standard Hex numbers for each



Macintosh Extended ASCII (or special characters) refer to those characters which you enter with the option key, like "â" and "£".

Hexadecimal (Hex) is the base-sixteen number system used by many computers. **ASCII** is the name for internal computer codes of letters and numbers.

special character. For example, “20” is the Hex number for space, and “26” is the number for ampersand (“&”). Thus, to link to a file named “my file”, you have to use “my%20file”, and for “cité f”, you must use “cit%8E%20%C4”.

Some Mac HTML editors will perform this encoding for you automatically when you select a file and link it. For Hex encoding information, see any Macintosh programming book, the BBEdit ASCII table, or an online list such as:

<http://developer.apple.com/techpubs/mac/Text/Text-516.html>

Redirection: Aliases and Redirect Files

Your web host directory structure does not have to match the actual file organization on your hard drive. For example, you may want to have descriptive default file names in each folder, store your images on another volume, move files without breaking links, or just make URLs simpler to type.

To have the WebSTAR web server **redirect** a URL from the apparent location to your preferred file, you have to create a file in the correct location and respond to the request appropriately. Standard Mac aliases and special WebSTAR Redirect files give you two simple ways to perform this redirection.

There are also third-party CGIs and Plug-Ins for more global processing: see the [Extending WebSTAR](#) page on the StarNine web site for information.

Folder and File Aliases

You can use aliases to link to a file in another folder. The browser will display the URL of the alias, not that of the original file. Aliases are good for creating several apparent URLs that actually refer to one original file, reducing the maintenance problems of keeping files synchronized. In addition, you can make URLs much shorter, by placing a link to the folder farther up in your folder hierarchy.

Aliases can also supply file suffixes without renaming the original files. WebSTAR uses the name of the alias for suffix mapping, and then translates the alias to find the original file's contents.

Be careful when using aliases: they require any relative links in HTML to be **relative to the alias location**, rather than the actual location in the folder hierarchy.



Aliases also allow you to double-click on the server machine and open the folder or file automatically.



Be careful with aliases to other volumes on your network: if the volume is not available, the warning alert box on the server will override everything, including your WebSTAR server, until someone clicks the **OK** button.

Aliases are particularly useful for storing images on a separate hard drive: create an images folder on the second drive, and make an alias to it in your root folder. All links to image files in the images folder will be directed to the original of the alias on the other drive.

Linking To Other Folders and Volumes

You can use aliases to folders and files that reside outside the WebSTAR folder, including those that reside on different volumes or mounted volumes on the network. As long as the alias resides within the WebSTAR folder, links to the file or folder will work correctly. However, you should make sure your files have relative links to other files and folders **within** the WebSTAR folder hierarchy—for security, WebSTAR will not serve files which are stored outside the hierarchy.

Redirect Files

WebSTAR also supports special **Redirect Files** (a special form of **RAW** files). These are text files which contain an HTTP **redirect** command, recognized by the browsers, followed by the URL for the browser to load. The WebSTAR web server checks for this information as soon as it locates the file. WebSTAR just returns the file, without processing, to the browser, and the browser then automatically requests the new URL. This happens very quickly, and is invisible to the person browsing, so all they see is the new URL in the Location field of the browser.



Redirect files are good for changing the visible URL as well as bringing up the desired file or folder.

Unlike aliases, they can't redirect to anything outside the site file hierarchy, such as files on other disks.

For example, suppose you move an entire branch of your file tree to another web server. You can redirect incoming requests to the default file for that folder simply by creating a Redirect file that contains a URL redirect header and new location. Replace the default file in that folder with the Redirect file, and browser requests will retrieve the redirect file, which sends them to the new host.

If you redirect to a folder, make sure to add the trailing slash that indicates a folder. Although the folder will be served, links to this redirect file are treated as links to a file, rather than a folder, and should not have the trailing slash.

Creating Redirect Files

To make Redirect files, use the *Make Redirect File* application in the *Tools & Examples* folder.

- 1 Make sure you have the URL for the **target file** (the file you want to redirect **to**),

- 2 Decide on the URL and file location for the new **redirect source file** (the URL to redirect **from**).
- 3 Open the *Make Redirect File* application, and enter the target URL in the edit field, then click OK.
- 4 You'll see a normal Save File dialog: give the Redirect file the new name and save it in the correct source folder.
- 5 Test your Redirect by opening a browser and entering the source URL (the location of the Redirect file). You should see the target file in the browser.

The WebSTAR web server log will show an entry for the Redirect file and then an entry for the target file if the target is on your server.

Internal Structure of Redirect Files

The easiest way to make Redirect files is to use the utility application, but you can also make them yourself. Redirect files are just text, but they have a Type code of "RAW!" and a creator code of "WWWΩ". These codes are required by WebSTAR to automate the redirection, but it makes it quite tricky to edit the files directly. You should either use a text editor that can open unknown file formats, such as BBEdit, or change the File Type code to TEXT. Be sure to change the codes back before you try to use the Redirect files, or it will not work properly.

There **must** be a "linefeed" character (encoded as ASCII 10 or Hex 0A) before both the second and third lines for compatibility with old browsers. In SimpleText, these will appear as boxes if you open an existing Redirect file: do not delete them. If your text editor allows you to save in DOS format, the linefeed characters will be added automatically.

The file should include the HTTP redirect statement like this:

```
HTTP/1.1 302 Found
Location: http://www.domain.com/widgets/blue.html
Server: WebSTAR 4
```

With your target file or folder URL replacing the example. This structure and data tells the browser:

- this URL has found a working HTTP 1.1 file
- it has found the requested URL
- the browser should use the URL in the Location line
- the server is WebSTAR

The browser will resubmit the request for the target URL right away.

VIRTUAL HOSTS: HOSTING MULTIPLE WEB SITES

WebSTAR allows your one server to host a number of different web sites through the use of **Virtual Hosts**. With Virtual Hosts, you can map multiple IP addresses, hosts (such as “special.domain.com”), domains (such as “www.example.com”), and languages, to different root folders within the WebSTAR folder. WebSTAR will respond to HTTP requests as though each site was on a separate machine.

There are several ways to implement virtual hosts within WebSTAR:

- **IP Multihoming** IP Multihoming allows a single machine to host web sites on more than one IP address. IP Multihoming on the Mac OS requires Open Transport 1.3 or greater and multiple IP addresses from your service provider.
- **Virtual Domains** lets you host more than one host name on a single IP address, using the “Host:” field passed in the header by most browsers.
- **Third-party CGIs and Plug-Ins** provide other options for virtual hosting, such as routing by host name or browser type, redirection based upon path name, and intelligent server load balancing. For details, see:

<http://www.starnine.com/extendingwebstar.html>

WebSTAR virtual hosts have different root folders and folder hierarchies, default file names, errors and no access files, but they share Caching, Suffix Mapping, CGIs and Plug-Ins, Security Realms, and more.

Routing to Virtual Hosts

When a URL comes to the server, WebSTAR routes differently based on IP address, Domain Name and the browser Language field (if any).

To set up this routing using the WebSTAR Admin application, see “Virtual Hosts” on page 144.

- Routing based upon IP addresses is done by checking which address received the request (in Open Transport TCP/IP), and then routing the URL request to the specified root folder, as defined in your Virtual Host list.
- Routing by Virtual Domain is done in WebSTAR by analyzing the “Host :” field passed by the browser in the HTTP header. WebSTAR then uses the contents of this field to route the URL request to the specified root folder, as defined in your Virtual Host list.



Virtual Hosting only applies to the WebSTAR Web Server. The FTP and Proxy servers can only use the default host name and IP address.



Third-party modules are not covered in this chapter.

- Routing of Virtual Host requests can also be done by analyzing the "Language:" field passed by the browser in the HTTP header. WebSTAR then uses the contents of this field to route the URL request to the specified root folder, as defined in your Virtual Host setup. Visitors can set the language preference in their browser, and it will send this in the header. This lets you set up different hosts for English, French and Japanese, for example, and automatically route visitors to your site to the correct virtual host.



For examples, see "Editing Virtual Hosts Entries" starting on page 144.

Configuring Virtual Hosts

To set up virtual hosts, you must decide whether to use IP Multihoming, Virtual Domains, or a third-party solution. Each method of implementing virtual hosting has its advantages and disadvantages, and you can experiment to find the best solution for your server.

About Virtual Domains

Virtual domains require only one IP address—no need to ask your ISP or network administrator for additional addresses. All you need to do is arrange for DNS services and, if you are setting up a new domain, register your additional names with your area's registry.

The World-Wide Web Consortium strongly recommends that web servers use virtual hosts, so as not to consume additional IP addresses simply for Web hosting. See section 19.5.1 of the HTTP standard at:

<http://www.w3c.org/Protocols/rfc2068/rfc2068>

Disadvantages include:

- you can't have a separate SSL security certificate, so you must direct all credit card acceptances and private data URLs to another server
- reliance on newer browsers and search engine robots which send the "Host:" field in the HTTP header.

About IP Multihoming

Advantages of this virtual hosting method include:

- can have SSL Certificates, for online stores and encrypting private data
- compatible with older browsers and search index robots
- uses standard IP address resolution
- routes requests slightly faster because the browser sends the IP address directly.

However, you'll need additional IP addresses, which are becoming scarce.



Once you've decided which method is best, you'll also need to create your hosts, make your root folders and set up the routing correctly.



For information on registration, see “Your Server’s Host Name” on page 99.



If you’re using Virtual Domains, see “Virtual Host Default Files” on page 197.

How To Set Up Virtual Hosts

- 1 Choose your virtual hosting method according to the information above.
- 2 If you want a new domain, you’ll need to register it with the Network Solutions or another domain registry.
- 3 Work with your DNS provider to enter your new host names in the DNS routing system.
- 4 If you’re using IP Multihoming, get an additional IP address and follow the instructions below.
- 5 Create new folders for each host, as described in “Virtual Host Root Folders and Default Files” on page 196.
- 6 Put unique default/index files in each virtual host root folder, and if you choose, Error and No Access files.
- 7 Use the WebSTAR Admin application to set up routing to each host and host defaults, as described in “Routing to Virtual Hosts” on page 193.
- 8 Test your routing to make sure that your hosts appear as you intend.

IP Multihoming: Special Configuration

IP Multihoming (which Apple refers to as “Single Link Multihoming”), was introduced in Mac OS 8.1.

When Open Transport activates TCP/IP, the **primary address** will be obtained from the TCP/IP Control Panel setting. Note that you must have “manual addressing” set in that panel. Open Transport then looks for the *IP Secondary Addresses* file in the *Preferences* folder to determine what other IP addresses the system is to support.

Enter IP Secondary Addresses

If you don’t already have one, WebSTAR’s Installer will automatically create an empty *IP Secondary Addresses* file in the *Preferences* folder. All you have to do is fill it in.

Each line of the IP Secondary Addresses file contains a secondary IP address to be used by the system, and an optional subnet mask, for the address. If there is no subnet mask entry, then a default subnet mask for the IP address class will be used.

To mark a secondary address, use the prefix “ip=”; for subnet mask use “sm=”, for the router address use “rt=”, for spacing use the space bar; and for comments, use a semicolon (“;”) at the beginning of the line.



Versions of the Mac OS after 8.6 are likely to have different interfaces to multiple IP addresses. See the Open Transport documentation for instructions.



You can leave the Subnet Mask and router address blank on all entries, or fill them in for all entries. However, you must be **consistent**.

For example:

; IP address	Subnet Mask	router addresses
;-----	-----	-----
ip=192.168.0.3	sm=255.255.255.0	rt=192.168.0.9
ip=192.168.0.4	sm=255.255.255.0	rt=192.168.0.9
ip=192.168.0.5	sm=255.255.255.0	rt=192.168.0.9

Reset Open Transport

Open the TCP/IP Control Panel, and make sure the default IP address is entered correctly. Restart the machine, so that it can use the new Open Transport configuration. If the IP address was previously used for another machine or another virtual hosting method, you may have to reset your router as well.

Testing Your Secondary Addresses

For testing, you can “ping” the new secondary IP address: if it is working correctly, your machine will answer. If you look up the host name, you can tell if the DNS entry is working, as well.

Once you have the system working, your secondary IP address will appear in the Virtual Hosts Routing table. To avoid common problems, make sure you have:

- Open Transport 1.3 or greater
- correct format IP Secondary Addresses file
- unique IP addresses, unused by other machines

Virtual Host Root Folders and Default Files

Each virtual host will have its own *virtual host root folder*. All URLs sent to that host relate to the virtual host root rather than the main WebSTAR root folder. Each host can also have individual default files.

Most of the WebSTAR settings are universal, including Suffix Mapping, Access Controls, and Logging options. Plug-Ins and CGIs are available to all virtual hosts, and the settings apply across hosts.

Setting Up Root Folders

To set up virtual host root folders, simply create a new folder somewhere within the WebSTAR folder on the server. You must have access to your Mac to do this, either directly, or through WebSTAR FTP, AppleShare, ARA or Timbuktu. All files in the virtual host will be inside of this folder.



Once you’re done with IP setup, continue to follow the instructions in “Configuring Virtual Hosts” on page 194.



See also “Links to Subfolders and Parent Folders” on page 187.

For ease of navigation, you should create the virtual host root folder in the WebSTAR folder, or in a special folder within the WebSTAR folder.

Virtual Host Default Files

Each of the virtual host root folders can contain different Error and No Access files, which is particularly useful for providing feedback in multiple languages. Each virtual host can also be set to have different default index file names (for example, *index.html* as well as *default.html*). The Virtual Hosts panel in the WebSTAR Admin application lets you specify these names in the Host Definition for Routing (described on page 146).

Special Virtual Domain Design Issues

When you use Virtual Domains (routing on host name rather than IP Address), the system relies on the browser sending the host name in the header. Older browsers (such as Netscape Navigator and Microsoft Internet Explorer versions 2 and older), do not send this information. Some web search index crawlers and spiders also do not send the header.

When a user with an older browser attempts to link to the virtual domain, the request will always go to the default host for that IP address. If you use Virtual Domains, design your default hosts' default pages so they be used to enter each Virtual Domain. You should also make sure that the default index file name, Error file, and No Access file settings will work in this case.



Although accessing a Virtual Domain through the default page is less convenient, it will still convey the HTML pages and other data correctly.

For internal links, be sure to use **relative** rather than absolute links in your HTML pages, using the double dot (. .) to move up a folder level, rather than always starting from the root. For example, use `http://../weddings/favors` rather than `http://weddings/favors`. As long as your links start from the current page rather than from the root folder, they will work properly (see “Relative and Absolute Links” on page 188).

WebSTAR Web server allows you to control the transaction information that you see in the monitor windows and save in the Log file. This chapter explains how you can specify the log file name, update interval, archiving information and the fields to display.

LOGGING

The Web Settings Logging panel in the WebSTAR Admin application includes a section for Logging Options. These options are also available within the Browser Admin pages.



Logging On and Off

When you click the Logging “Off” radio button, and press the Save button, the log file will no longer be updated. You must select the Logging On radio button and press Save to start logging again.

In the Browser Admin pages, choose the Controls page, then check or uncheck the “Suspend Logging” checkbox, and press Save.

The default is Logging **On**.

Log File Name

The default file name is : logs :WebSTAR Web . Log, specifying that the log file will be named *WebSTAR Web.log* and will be located in a *logs* folder in the WebSTAR root folder. A record of all client transactions is maintained in this file, in the format you set (see “Log Formats” on page 200). If the file does not exist, the WebSTAR server will create it.

The **Choose** button allows you to select a file on the server and append all future log information to that file. You cannot create a new log file this way, but you can select any file on your server as a log file, so be careful that you do not start appending log information to HTML or other files.

You can also set this file path in the Browser Admin pages: choose the **Settings > Misc. Settings** page and fill in the **Log File** field.



You can store the log files on any local disk using a file path. See “File Paths in WebSTAR Admin” on page 121. For automatic copying of the log on schedule, see “Log Archiving” starting on page 200.

Status Report Delay

This number, in seconds, is the interval used between updates of the Web monitor window on the server and browser and the Web, FTP and Proxy monitor windows in the WebSTAR Admin application.

This delay is used when there are more than five connections at a time. When there are fewer connections, the status messages are sent immediately. When the number is greater, the status messages are put into a memory storage buffer, which can hold up to 5 K of data. When a new status message comes in that will fill the buffer, or if the number of connections drops below five, all the messages are sent to the monitor windows.

The default status report delay is **15** seconds.

A low number will use more server time in displaying the status, a high number will reserve more of that time to serve data. On busy servers, you should consider increasing the Status Report delay to 20 or 30 seconds.

You can also set this number in the Browser Admin pages: choose the Settings > Misc. Settings page and fill in the “Log File” field.

Log Archiving

Log Archiving allows you to save separate log files covering specified periods of time, such as every day, every week on Thursday, or monthly. The log files are automatically created at the time you set, filled, and then closed when the next one is created.

For instructions, see “Log Archiving” on page 122.

LOG FORMATS

For each WebSTAR transaction, the server displays a line in the monitor window and saves an entry in the log file. The Log Format panel lets you specify what kind of information to include in these entries. You can choose between the WebSTAR Log Format, the Common Log Format (CLF) and Extended Log Format (ExLF). They allow you to save data in formats compatible with many third-party **log analysis programs**. These applications will read through your log file or multiple files, and create statistical reports on web site usage. For information on compatible log analyzers, see

<http://www.starnine.com/extendingwebstar.html>



It does not control the FTP and Proxy monitor windows in the WebSTAR server application.



You can change the WebSTAR Log Format and the Extended Log Format, but the Common Log Format is limited to standard tokens.



Don't forget to adjust your clock when Daylight Savings Time begins and ends. You can also use the Mac OS feature to do this automatically.

Log entries are composed of **tokens**—elementary pieces of data about a transaction, such as the date, time, result, and client host name. Each of these tokens is separated from the next by a Tab character. Each entry (all tokens for a single transaction) is on one line, separated from the next by a Carriage Return character. You can import these files into spreadsheet and database applications.

Beyond the standard formats, you can add additional data to your log, to give yourself more information to understand use of your site. Many log analyzers will ignore the additional tokens, but some will not: be prepared to remove the data if necessary. In addition, some fields may not have values for some browsers.

The DATE and TIME tokens use GMT (Greenwich Mean Time). This allows log analysis programs to compare logs from mirrored servers worldwide. If you need this functionality, be sure to set your Mac Date and Time control panel correctly, so WebSTAR can calculate the correct offset from GMT.

Initialization information, such as the list of the Plug-Ins installed and the Virtual Hosts, is not logged.

Host Name vs. IP Address

Some of the log tokens include the host name of the client or the server. These will only appear if you have selected the option to Caching (described on page 139). Otherwise, those log tokens will appear as dashes (“-”). Many log analysis programs can do batch host name lookups based on the IP address, which provides you with that information without slowing down your web server.

Format Display

Every time you change the log format, the new format token names will be displayed in the monitor window in the WebSTAR Admin application, and saved in the log file. For example, the default WebSTAR Web server log format appears like this:

```
...!!LOG_FORMAT DATE TIME RESULT STATUS HOSTNAME AGENT REFERER HOSTFIELD URL BYTES_SENT
```

Log analysis applications use this header to map to their internal databases, so changing formats may confuse the analysis. To avoid this, start a new log file when changing formats: choose **Suspend Logging** from the server or Admin Options menu, rename or move your log file, change formats, then choose **Start Logging** to begin saving data to the log file again.

Virtual Hosts and Log Information

Only one log is kept for each host served by the WebSTAR Web server: virtual domains do not have separate files. The file name tokens do include the entire file path, including the virtual host root folder names, and the HOSTNAME token displays the host name requested by the browser. Many log analysis applications are starting to log display statistic information for the entire server, which of course takes into consideration multiple sites. If you want separate log files, you will need to use a third-party logging application.

About Log Formats: WLF, CLF and ExLF

The three standard formats are WebSTAR Log Format (WLF), the Common Log Format (CLF) and Extended Log Format (ExLF). Entries in the log file are separated by tabs, and individual entries are terminated with a carriage return. This format is the standard text-only import format used by most spreadsheet applications, such as Excel, by database applications like FileMaker, and by log file analysis applications.

WebSTAR Log Format

The default value for the WebSTAR Log format (WLF) consists of the fields DATE TIME RESULT STATUS HOSTNAME AGENT REFERER HOSTFIELD URL BYTES_SENT. You can add, change or rearrange these fields. Many Mac-specific log analysis programs will handle these fields properly, although they may ignore other fields. WebSTAR Log format will make entries that look like this:

```
06/07/99 11:51:17 OK 200 171.66.196.146 Mozilla/4.5 (Macintosh; U; PPC) http://timtest.starnine.com/
"timtest.starnine.com" :documentation:graphics:starninelogo.white.gif 1133
06/07/99 11:51:17 OK 200 171.66.196.146 Mozilla/4.5 (Macintosh; U; PPC) http://timtest.starnine.com/
"timtest.starnine.com" :documentation:graphics:webstarserversuite.gif 5100
06/07/99 11:51:18 OK 200 171.66.196.146 Mozilla/4.5 (Macintosh; U; PPC) http://timtest.starnine.com/
"timtest.starnine.com" :documentation:graphics:starbackground.gif 55028
06/07/99 11:51:25 OK 200 171.66.196.146 Mozilla/4.5 (Macintosh; U; PPC) http://timtest.starnine.com/
"timtest.starnine.com" :Tools & Examples:toolsandexamples.html 2935 |
06/07/99 11:51:27 OK 200 171.66.196.146 Mozilla/4.5 (Macintosh; U; PPC)
```

 For information about these fields, see “Log Tokens Table” starting on page 205.

See “Configuring the Log Format” on page 207 for information about adding additional fields.

Common Log Format (CLF)

The Common Log Format is a standard used by most web servers that provides basic logging of the information necessary to do statistical analysis of server usage. Many analysis tools support this format. CLF uses standard fields that are not user-selectable. The standard information for this format is available at:

```
http://www.w3.org/Daemon/User/Config/Logging.html#
common-logfile-format
```

It produces entries that consist of the following tokens:

- host name or IP address of the client browser.
- the user name in the client browser (obsolete).
- the date and time of the request (in GMT -- Greenwich Mean Time).
- the request line exactly as it came from the client.
- The HTTP status code returned to the client.
- The length, in bytes, of the content of the document transferred.

```
!!LOG_FORMAT COMMON_LOG_FORMAT
171.66.196.146 - - [07/Jun/1999:13:52:51 -0700] "GET
/Tools%20%20Examples/File%20Upload/fileupload.html HTTP/1.0" 200 1089
171.66.196.146 - - [07/Jun/1999:13:52:54 -0700] "GET
/Tools%20%20Examples/Form%20Mail/formmail.html HTTP/1.0" 200 934
171.66.196.146 - - [07/Jun/1999:13:52:58 -0700] "GET /JRun/htdocs/index.html HTTP/1.0" 200
1909
171.66.196.146 - - [07/Jun/1999:13:53:50 -0700] "GET /JRun/htdocs/develop.gif HTTP/1.0"
```

Extended Log Format (ExLF)

There are no defaults for this format, but you can choose from any of the tokens available. This data is used by many cross-platform log analysis programs. For more information, see:

<http://www.w3.org/pub/WWW/TR/WD-logfile.html>

WebSTAR will display a header and the token names and store this information in the Log File. This allows log-file analysis programs to recognize and store the data correctly. The fields themselves are tab-delimited. Extended Log format files look like this:

```
#Version: 1.0#Software: WebSTAR/4.0#Start-Date: 06/07/99:12:23#Fields: DATE CS-STATUS
TIME CS-SIP CS-URL CS(HOST) CS(PREFERER) CS(USERS-AGENT)
1999-06-07 200 20:56:07 198.211.93.81:80 /JRun/htdocs/index.html "timtest.starnine.com"
"http://timtest.starnine.com/" "Mozilla/4.5 (Macintosh; U; PPC)"
!!LOG ARCHIVER: 06/07/1999 13:56:08 error -48 while renaming newly-archived WebSTAR FTP
server log
1999-06-07 200 20:56:11 198.211.93.81:80 /JRun/htdocs/docs/servlets/index.html
"timtest.starnine.com" "http://timtest.starnine.com/JRun/htdocs/index.html" "Mozilla/4.5
(Macintosh; U; PPC)"
1999-06-07 200 20:56:15 198.211.93.81:80 /JRun/htdocs/docs/servlets/samples.htm
"timtest.starnine.com" "http://timtest.starnine.com/JRun/htdocs/docs/servlets/index.html"
"Mozilla/4.5 (Macintosh; U; PPC)"
```

Log Format Tokens

WebSTAR allows you to customize your log data when using either WebSTAR or Extended log formats. Choose the tokens and the order that you prefer, as described in "Configuring the Log Format" on page 207.

CS Tokens

The tokens beginning with “CS” are “client to server”, where the information is mainly about the client.

“CS-” is used for information regarding the request itself, including the IP address, the client host name (if available), the HTTP request, and so on.

“CS()” tokens are used to designate data that is extracted from the HTTP header. Anything in the CS() parentheses will be the name of a header field.

For example, the client may send a `Host: www.domain.com` field in the header, so the `CS(HOST)` token will display `www.domain.com`. If you are using virtual hosts, the browser will send the host name of the Virtual Domain or that associated with the secondary IP address in the `CS(HOST)` token. This allows log analysis programs to track requests to the various hosts.

If data is missing, tokens with items in parentheses like `CS(METHOD)` are logged as an empty quoted string (“”) if they are empty or not present. All other tokens are logged as a single dash (“-”) if not present.

“DNS” tokens will be filled in and “IP” tokens will be a dash if you set Use DNS for Server and Client Lookups (described on page 136). Otherwise, the “IP” tokens will be filled in and the “DNS” tokens will be a dash.

Results Token

The `Results` token returns three codes: “OK”, “ERR” (error, usually if a file was not found) or “PRIV” (user was not allowed access to a realm). However, these are limited to what the WebSTAR server knows about. For example, you might have a bad URL that is pointing to a non-existent file, but if it is handled by a Plug-In WebSTAR regards this as OK, because it just hands off that URL to the Plug-In. By the time the plug-in knows that the file can't be found, it's too late to change the Results, which will be recorded as OK. This is why it's usually more accurate to record `SC-STATUS` instead.

Log Tokens Table

In this table, tokens which are included in the default WebSTAR Log format have a check in the “WLF” column, and tokens allowed in the Extended Log format have a checkmark in the “ExLF” column.

Log Tokens Table

TOKEN	VALUE	ExLF	WLF
AGENT	The identity of the browser software or other client example: Mozilla/4.04 (Macintosh; U; PPC)		
BYTES	The number of bytes transmitted (in Extended Log Format style). example: 2314	√	
BYTES_SENT	The number of bytes transmitted (in Common/WebSTAR Log Formats). example: 2314		√
C-DNS	Client (browser) host name., or a dash, if DNS lookups are not enabled. avi.starnine.com.	√	
C-IP	Client (browser) IP address, or a dash, if DNS lookups are enabled. 192.168.1.3.	√	
CONNECTION_ID	A number that is unique for each connection for this invocation of the server. 12		
CS(COOKIE)	The “cookie” information sent in this request Set-Cookie: CUSTOMER=WILE_E_COYOTE; path=/ expires=Wednesday, 09-Nov-99 23:12:40 GMT		
CS(HOST)	The host name requested by the browser. knickknacks.domain.com		
CS(METHOD)	The method of the request GET, POST, GET_CONDITIONAL		
CS(REFERER)	HTTP request’s “Referer” header field, sending the URL that referred to the current page. www.starnine.com/default.html		
CS(USER-AGENT)	HTTP request’s “User-Agent” header field. Mozilla/4.04 (Macintosh; U; PPC)		
CS-METHOD	The HTTP method GET or POST	√	

Log Tokens Table (Continued)

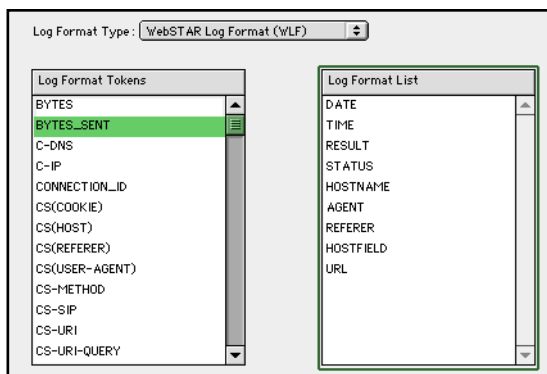
TOKEN	VALUE	ExLF	WLF
CS-SIP	The Server IP number and Port that the HTTP connection came in on 192.168.0.4:80	√	√
CS-STATUS	<i>Obsolete: use SC-STATUS</i>	√	
CS-URI	The URI path /default.html	√	
CS-URI-QUERY	Search argument portion of the HTTP request. first=last&last=first	√	
CS-URI-STEM	Path portion of the HTTP request. /status/stat.html	√	
DATE	The current date in the format month/day/year. 01/20/98	√	√
FROM	<i>(Obsolete)</i>		
HOSTFIELD	The host name requested by the browser. knickknacks.domain.com		√
HOSTNAME	The host name or IP address of the browser's computer. avi.starnine.com or 192.168.0.2		√
METHOD	The HTTP method, usually GET or POST.		
PATH_ARGS	The path arguments to the URL for a CGI (the text after a dollar sign). \$phantom.acgi		
REFERER	The name of the document referencing this URL www.starnine.com/default.html		
RESULT	Result code for this request (SC-STATUS and STATUS provide more details). OK, ERR!, or PRIV		√
SC-STATUS	Server response status (HTTP codes). 200, 404	√	
STATUS	Server response status (HTTP codes). 200, 404		√

Log Tokens Table (Continued)

TOKEN	VALUE	ExLF	WLF
SEARCH_ARGS	The search arguments to the URL (text after a question mark)		
TIME	The current time in the format: HH:MM:SS, as a 24 hour clock. This number appears in GMT (Greenwich Mean Time). 13:49:06	√	√
TIME_TAKEN	The time taken to complete the transmission in the format HH:MM:SS. 00:01:03		
TRANSFER_TIME	The number of seconds it takes for the process to complete. 1 to 2147483646.		
URL	The requested URL path in Mac OS file path format. :documentation:graphics:webstarserversuite.gif		√
USER	The User Name if there was a Web User entry for a realm. HumanResources		

Configuring the Log Format

You can specify the Log format in the WebSTAR Admin application or in the Browser Admin pages (Settings > Log Format). When you change from one format to another, make sure you Suspend Logging, and copy the current logfile. This is particularly important if you are using a log analysis application.



Log Format Type

Choose WebSTAR, Common or Extended Log format from the popup menu. If you're using the Browser admin, be sure to click the "Save Format Type" button.

Log Fields

You can use the default fields or customize your log fields (for WebSTAR and Extended Log Formats). WebSTAR will display the existing log format and allow you to add or remove tokens from the format.

In the WebSTAR Admin, the "Log Format List" on the right displays your current log tokens. The "Log Format Tokens" list on the left displays additional tokens, in alphabetical order. **Drag** a token from that list to the Log Format List to add this token to your log format. To remove a token from your list, drag it back to the Log Format Tokens list (don't worry about the order).

In the Browser Admin, the Log Format page displays 31 fields, each with a popup menu of the available log tokens. You can change each field to the format you prefer.

When you click the **Save** button, the server will display the header for the new format in the log file, and will use the new format for all transactions.



The obsolete CS-HOST and CS-IP are no longer available in this list.

SSL (Secure Sockets Layer) is an Internet protocol which specifies how to pass secure communications between your server and HTTP clients, such as browsers. This provides world-class security for your web site, allowing you to accept credit card numbers, serve medical records, human resources information, or other sensitive data without fear of interception.

ABOUT SSL SECURITY

WebSTAR Server Suite includes SSLv2 and SSLv3 as part of the server. This allows you to serve specific pages which are encrypted when sent to the browser, and any form responses, such as private personal data, are encrypted when they are sent back to the server. To invoke it, simply create URLs that uses the **https** (secure HTTP) protocol. For example, you can protect a credit card acceptance URL so that the information is automatically encrypted by the browser before it is sent.

Secure Sockets Layer (SSL) Protocol

WebSTAR SSL includes a full implementation of the **Secure Sockets Layer (SSL)** protocol, which provides server authentication, data encryption, and message integrity. These combine to keep the HTTP data truly secure as it travels across the Internet.

The Secure Sockets Layer Protocol, developed by Netscape, uses authentication and encryption technology developed by RSA Data Security Inc. For more information about the SSL protocol, see these URLs:

<http://www.netscape.com/eng/ssl3/draft302.txt>

<http://developer.netscape.com/misc/developer/conference/proceedings/cs2/index.html>

SSL is layered below application protocols such as HTTP and above TCP/IP. When SSL is implemented in both the client and the server software, all data is encrypted before it is transmitted.

WebSTAR Server Suite SSL supports SSL versions 2 and 3, and is based on the OpenSSL library.

Encryption Levels: US and International

The WebSTAR SSL server uses an ISO X.509 Certificate that is authenticated with **RSA public key cryptography** (encryption). With public-key cryptography, the server publishes a key and browsers contacting that server encrypt their messages using that public key.

Only the server can decrypt the messages, because only the server has the private key. For more information, see:

<http://www.rsa.com/rsalabs/newfaq/q3.html>

With public key cryptography, the longer the keys, the longer it would take to guess the keys and break the encryption. To break one message encrypted with RC4-40 (WebSTAR SSL's lowest level of encryption), a computer would have to attempt to decrypt the message with about 500 billion different keys. The effort of breaking the encryption of that one message would not apply to any other messages: they would have to be decrypted separately. The 56-bit and 128-bit keys are even more secure, and are used by banks and other institutions.

As of mid-1999, there are legal limits on export of this kind of cryptography from the United States. Therefore, WebSTAR is shipped in two versions: **US & Canada** with stronger encryption using longer keys, and **International** version with 40-bit encryption.

U.S. and Canada

The U.S. Domestic version of WebSTAR SSL implements the encryption described below, as well as the options included in the international version.

- RC4-128

The 128-bit version of the RC4 stream encryption algorithm provides very high-level encryption protection.

- 3DES

Triple DES, encrypted three times with three different DES keys. This is much more secure than DES and slightly less secure than RC4-128 (and much slower to process).

- DES

DES encryption is required by some United States government agencies. Allowing only a 56-bit key, DES provides less protection than RC4-128. It is also slower.

International

- RC4-40

The International version of SSL uses a 40-bit key size for the RC4 stream encryption algorithm. Although this version contains a lower level of encryption protection, RC4-40 is still a formidable cipher.

- DES-40

The International version of SSL uses the same algorithm as the DES encryption, and takes the same amount of time to process, with a 40-bit key.

- **MAC-only (no encryption)**

This provides message authentication only: it proves to the browser that the page was served by your server, but does not encrypt the HTML, so anyone monitoring your data stream could see the page.

Although the U.S. government prevents the export of RC4-128 and some versions of DES encryption software, that does not affect the ability of international sites to access a secure server. The server negotiates to the encryption level understood by the accessing browser.

How Browsers Access A Secure Server

Once you have installed and configured SSL in the WebSTAR Server Suite, clients can connect to the secure server using a URL that starts with `https`: instead of `http`:

For example the following URL will bring up a secure page (if you replace “domain.com” with your host, and have a file in this path).

```
https://www.domain.com/test/secure.html
```

Behind the scenes, the browsers automatically connects to the correct port (443), and perform a certificate negotiation. In this phase, the browser sends a message explaining what encryption ciphers it recognizes, and the server uses the strongest cipher it has available. If you have them all enabled, they are evaluated in this order:

- 1** RC4-128
- 2** 3DES
- 3** DES-56
- 4** RC4-40
- 5** DES-40
- 6** MAC (Authentication, no encryption)

Once it has found the strongest cipher they can both use, the server sends its certificate (proving who the owner is) and uses that to create the encryption key. This makes the secure connection.



The letter “s” at the end of the code “https” indicates that the connection will be secure.



You can turn these ciphers on and off in the SSL Security panel (see “Encryption Ciphers” on page 228), but you can’t change the order.

Then the browser encrypts data it sends to the server, such as credit card numbers, and decrypts data it gets from the server, such as medical data or bank records.

Browser Certificate Expiration Issues

Browser certificates expire periodically. Some older browsers have already passed their Thawte expiration date and many VeriSign certificates will expire at the end of 1999.

Browsers will report this apparent error to users. They can just tell the browser to accept the certificate, but they may contact you in confusion.

- To update browsers for Thawte server certificates, follow the instructions at:

<https://www.thawte.com/certs/server/rollover.html>

- To update browsers for VeriSign server certificates, contact VeriSign.

SSL and Multiple Domains

You can add an SSL certificate for each IP number on your server. This does not apply to virtual domains, which are created using the Header routing. In addition, the host name must be specified using an A Name entry in the DNS record: it must not be a CNAME alias.

However, the certificate authorities generally charge a significant amount of money per host certificate, per year. Therefore, a good solution is to obtain a domain name that, with a relevant host name, will seem appropriate to your clients and online users in the SSL URL. For example, you can get domain name like “seureserver.com”, then you could get a certificate for the host name “safe”, so your shoppers will see a URL like this:

<https://safe.seureserver.com/knickknacks/OrderForm.html>

Remember that the HTTPS URL will only be used for the few web pages where private data is collected or displayed for verification. It never has to be promoted, remembered or even displayed on a web page, since your SSL pages only need be accessed from a link on another web page.

Certificate Chains and Intermediate Certificates

Some large institutions have authorization power: they can sign internal certificates. Because they are between the Certificate Authority and the server certificate, they are called **intermediate certificates**.



For information, see “Virtual Hosts: Hosting Multiple Web Sites” on page 193

See also “DNS” on page 100.

If you get a certificate in this way, it's part of a **certificate chain**: It includes not only the "subject" certificate (for your host), but also the root certificates and intermediate certificate information.

For example, a Certificate Authority could sign a certificate for Domain.com that authorized them to sign web server certificates and personal/email certificates. Domain.com could then use that certificate to sign all of their internal SSL server certificates and certificates for their employees.

WebSTAR SSL supports these features, but intermediate certificates are very expensive.

Wildcard Certificates

Thawte allows you to generate wildcard certificates, (using an asterisk instead of the host name, as in: *.domain.com), with WebSTAR Server Suite 4. However many versions of Microsoft Internet Explorer will display an error message to the user when they connect to one of these certificates.

Therefore, you should only use wildcard certificates in circumstances where you are confident that most browsers will be version 4 and later, and you are prepared to reassure people with earlier browsers that their data is truly secure.

INSTALLING & CONFIGURING SSL

Before you enable SSL in your server, you should consider how it will interact with regular serving of unencrypted pages. In most cases it is not a good idea to use HTTPS for all of your pages. Because SSL encrypts each page before transmitting it, clients may notice that it is slower than the HTTP interchange. In addition, some older web browsers do not support encryption and will not be able to access documents served via the HTTPS protocol. Make sure you read and understand "SSL and Multiple Domains" on page 212 before proceeding.



For information, see "DNS" on page 100.

Steps to Secure Serving

To start serving your website securely, follow these overall steps:

- 1 Check your DNS records to be sure you know the authoritative host name and the exact IP address.
- 2 Generate a Private Key file for this host.

- 3 Generate a Certificate Request for this host.
- 4 Choose the Certificate Authority, and follow the directions below to buy a certificate. A certificate proves that you are authorized to use the business or institutional name.
- 5 Add your certificate and key information to the SSL entry for this host.
- 6 If you have private data areas, set up a security policy with Realms and passwords.
- 7 Test your secure uploads and private areas carefully.

To access your secure pages, you'll need a browser which supports SSL, such as Netscape Navigator or Internet Explorer. To run the browser on the same Macintosh as the server, you will need enough free RAM for the browser, and server performance will decrease while the browser is running.

Performing the Installation

The WebSTAR Server Suite Installer automatically includes SSL when you install from the CD. Due to export restrictions, download installers do not include SSL installations, although they will upgrade SSL servers.

For instructions on installing WebSTAR servers, see "Installation" starting on page 29.

Upgrading from Earlier Versions of SSL

If you are installing WebSTAR Server Suite 4 over an existing SSL configuration, be sure to use the Secure Server upgrade option (see "Upgrading SSL Versions of WebSTAR" on page 37).

The Installer does not move the *WebSTAR/SSL Settings* file to the *WebSTAR (old)* folder when upgrading. Instead, the first time the WebSTAR 4 server starts up, it extracts the Private Key password from this file and stores it in the new *WebSTAR Settings* file. After this extraction has taken place you are free to delete the old *WebSTAR/SSL Settings* file.

Your certificate will be converted the first time the new server is run. The old certificate will be renamed to *old Digital ID*. The new file will be named *Certificate*. The password is also converted.



You can store these files anywhere on your disk, but do not change their names after you have created them.



The older certificate format is only converted the first time WebSTAR 4 runs. See "Need to convert an old certificate" on page 232 for instructions on converting.

SSL Tools Folder

In the *Tools & Examples* folder, the *SSL Tools* folder contains two small applications for generating Private Keys and Certificate Signing Requests.

OBTAINING AND INSTALLING CERTIFICATES

To operate securely, SSL requires a **certificate** (sometimes called a **digital certificate** or **Digital ID**). A certificate is issued by a trusted third party known as the **Certificate Authority**. The Certificate Authorities covered in this manual are VeriSign, Inc. and Thawte Consulting.

For information on obtaining a test certificate, see page 225.

From a user's perspective, the certificate signifies that an independent party (VeriSign or Thawte) has verified that the information in the certificate accurately represents who it claims to represent, and that communications can be encrypted using the certificate's public/private key. This is similar to the Department of Motor Vehicles verifying that the picture on your driver's license corresponds to your name, birth date, and address. The certificate ensures that the user is actually communicating with your host domain name, not with an imposter who claims to be you.

Certificate Formats

WebSTAR Server Suite 4 is compatible with PKCS (the most common standard), Server Gated Cryptography and Netscape formatted certificates.

Certificate Authorities

As of mid-1999, the two most popular Certificate Authorities issuing certificates for WebSTAR SSL servers are VeriSign and Thawte. For information, we recommend that you visit both web sites.

- VeriSign <<http://www.verisign.com/>> (see "Using the VeriSign Certificate Authority" starting on page 218).
- Thawte <<http://www.thawte.com/>>, (see "Using the Thawte Certificate Authority" starting on page 220).



WebSTAR 4 with SSL will upgrade old certificates: see "Upgrading from Earlier Versions of SSL" on page 214.

Creating Certificate Signing Requests

The procedures for creating private keys and generating Certificate Signing Requests are the same for both VeriSign and Thawte.

- 1 Generate a Certificate Signing Request (CSR).
- 2 Submit the paperwork and CSR to the Certificate Authority, with payment.
- 3 Receive the certificate.
- 4 Install the certificate.
- 5 Store these vital materials in a safe place.

Generate a Key

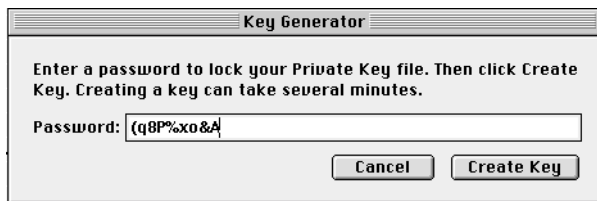
Use the *Key Generator* application in the *SSL Tools* folder to generate a file containing a private key for use with your secure server. Follow these steps:

- 1 Launch the *Key Generator* application (in the *Tools & Examples* folder, *SSL Tools* folder).
- 2 Enter a password to protect your key. You'll need it later to authorize WebSTAR SSL to use your public/private key pair. **Do not forget this password!** If you do, the private key cannot be recovered: there is no "back door" to this security.

Make sure that the password is at least 8 characters long, includes letters, numbers and punctuation, and is not a name or a word. For more suggestions on password security, see "Safe Passwords" on page 96.



Write the password down and store it in a secure place, such as a safety deposit box. If you lose the password, you will have to purchase a new certificate.



- 3 Click the **Create Key** button to generate your private key file.
- 4 Name the file something like "Private Key File" (the default), and save it in the root folder for the SSL host (the WebSTAR folder or the host folder if you have a secondary IP host as described in "SSL and Multiple Domains" on page 212).
- 5 When the key file is created, the Key Generator will beep and allow you to click **OK**, then it will quit.
- 6 Make sure that the key file is in your WebSTAR folder: if it's not there, move it into that folder now.



Your Certificate Signing Request may be rejected if the information is not properly formatted. Be sure to closely follow the conventions outlined in the instructions. If any of the information is improperly formatted, the Certificate Authority will ask you to correct it and send the request again.

Create the Certificate Signing Request

The Certificate Signing Request process requires that you supply an email address and certain identifying information, as described below.:

- 7 Launch the *CSR Utility* application (in the *Tools & Examples* folder, *SSL Tools* folder).

Certificate Request

This information describes your Distinguished Name. It must match the requested format or your Certificate request will have to be resubmitted. Review the manual for instructions.

Common Name:
(ex: www.starnine.com)

Organization:
(ex: StarNine Inc.)

Org. Unit:
(ex: Marketing)

City/Locality:
(ex: Berkeley)

State/Province: **Country:**
(ex: California - full name) (ex: US - 2 letter code)

E-mail Address:
(ex: WebMaster@starnine.com)

Phone Number:
(ex: 510 555-9601)

FAX Number:
(ex: 510 555-9601)

Key File:

Key File

- 8 Type the host name of your Web site in the "Common Name" field, for example:

www.domain.com

Make sure that the **Common Name** you specify will be the actual host name of your SSL server—it will be encoded into the signed Certificate and cannot be changed later without purchasing a new Certificate.

Furthermore, this host name should be the main "A name" entry for your machine on your DNS server. Your Certificate may have problems if you use an IP address or if the host name is a "CNAME" entry (DNS alias), for example. Contact your network administrator for guidance if necessary.

- 9 Type the name of your organization in the "Organization" field, for example:

Widgets Corporation

- 10 Type the name of the department or other organization unit in the "Org Unit" field, for example:

Support

- 11 Type the name of the city or town in which your organization is located in the "Locality" field, for example:



See also "DNS" on page 100.



You must something in the Org. Unit field, if only "store" or "security".

Berkeley

- 12** Type the name of the state or province in which the organization is located in the “State/Province” field, for example:

California

Do not abbreviate the state or province name: spell it out as shown above.

- 13** Type a two-letter code for the country in which you are located in the “Country Code” field, for example:

US

Do not spell out the country name: use a 2-letter code. The code for the United States is US. For Canada, the code is CA. For other codes, contact VeriSign at starnine-info@verisign.com.

- 14** Type the email address of the site's Webmaster or administrator in the “Email Address” field, for example:

webmaster@domain.com

- 15** In the “Phone Number” field, type a phone number where the Certificate Authority can reach you, and type your fax number in the “FAX Number” field.

- 16** Click **Choose** and select the Private Key file you created.

Once you select a private key file, the key file and the Certificate you will receive will be a **signed Certificate pair**, and cannot be separated.

- 17** Enter the password required to access your public/private key pair (the password you entered when generating the key pair, as described in “Generate a Key” on page 216).

- 18** Click the **Create** button to generate your encrypted Certificate request form.

- 19** The application creates a file named *Certificate Request* by default. You can use that name or rename it.

- 20** Quit the CSR Utility program.

Follow the instructions in “Using the VeriSign Certificate Authority” on page 218 or “Using the Thawte Certificate Authority” on page 220 to order your Certificate, then follow the instructions in “Installing Your Server Certificate” on page 226.

Using the VeriSign Certificate Authority

VeriSign calls their certificate a **Digital ID**. To be sure that your Digital ID Request is processed quickly, and that you are following the current procedures, we suggest that you check the instructions at:

<http://www.Verisign.com/starnine/>

The process includes these steps:



The Email Address, Phone Number, and FAX Number fields are not part of the Certificate. The Certificate Authority uses these fields to contact you if it finds a problem with the Certificate request.



If you lose the Private Key file and generate a new one, your Certificate will no longer match. You will have to send a request to the Certificate Authority for a new Certificate, which you may be charged for. For this reason, be sure to keep backup copies of your file in a secure location.



To avoid delays, submit all paper documents together.

- Enroll with VeriSign by clicking the **Begin** button on the introductory page, and filling out the form.
- Submit “Proof of Right to Use” paperwork to VeriSign with a service fee.
- Generate a public/private key for your site.
- Define a Distinguished Name (a unique identifier) for your site.
- Send an email message to VeriSign to apply for your Digital ID.

You can expect to receive an email message from VeriSign containing your Digital ID no sooner than three working days after VeriSign has received all the appropriate paper and email documents.

What Paperwork Does VeriSign need?

Submit a letter on your organization's letterhead identifying the Webmaster for your site, accompanied by “Proof of Right to Use” your organization's Distinguished Name.

Proof of Right to Use

“Proof of Right to Use” means proper documentation of your organization's identity. Choose one of the following types of documentation as appropriate for your type of organization:

- Business license (for local organizations)
- Partnership papers (for local or state-wide organizations)
- Articles of incorporation (for state-wide organizations)
- Notarized letter from office of the dean (for universities)
- Notarized letter from a properly authorized person (for government organizations).

Contacting VeriSign

After you have compiled the required documentation and completed the cover letter on letterhead, attach a means of payment and fax the entire package with the recipient name Digital ID Services to this fax number:

+1 (650) 961-7300

Payment Methods

You can use one of these payment methods:

- Credit card, with the card number, card expiration date, and the name of the card holder.
- Check
- A purchase order that includes the date, purchase order number, company name, amount, product, and authorization number.



Materials provided as “Proof of Right to Use” must be in English. If the original documents are not in English, then they must be translated by an official third party agency before being submitted to VeriSign. Requests including documents that require translation may result in a delay as VeriSign has them translated locally.

Acceptance of purchase orders is subject to approval by VeriSign. Be sure to fax a copy of your PO to VeriSign at the time of your order.

Sending Paper Copies

As soon as the fax is received, the process of obtaining your Digital ID can begin. However, you must also mail the originals of the entire package to this address:

VeriSign, Inc.
1390 Shorebird Way,
Mountain View, CA 94043

Corporate Offices: (650) 961-7500
Fax: (650) 961-7300
Customer Support Line: (650) 961-8820

Generate a Certificate Signing Request

Follow the instructions in “Creating Certificate Signing Requests” on page 216

Sending the Request to VeriSign

To apply for a Digital ID, follow these steps:

- 1 Use a text editor, such as SimpleText, to open the Certificate Request document.
- 2 Copy the entire contents of this document to a new email message. Do not alter the contents.
- 3 Send the message to this address:

`starnine-request-id@VeriSign.com`



Make sure that you do not get the older “PEM” format.

Receive the Certificate

VeriSign will send you the certificate, or instructions on how to find it online.

Install the Certificate

Follow the instructions in “Installing Your Server Certificate” on page 226.

Using the Thawte Certificate Authority

Thawte calls their certificate a **server certificate** (much like the VeriSign “Digital ID”). Thawte also provides Wildcard Certificates (described on page 213) and test certificates.

As their instructions may change, you may want to check their website to be sure that your certification request is processed quickly:

<http://www.thawte.com/>

The process includes these steps:

- Generate a Private Key file.
- Create a certificate signing request.
- Fill out Thawte's online certification request form.
- Send Thawte your documentation and payment.



To avoid delays, submit all paper documents together.

You can expect to receive an email message from Thawte containing a URL where you can pick up your server certificate approximately three working days after Thawte has received all the appropriate paper and email documents.

Thawte Compatibility

If you or any of your customers are using a browser created before August, 1996, you may see security errors. Go to

<https://www.thawte.com/servertest.crt>

and follow the instructions to install the Thawte root certificate.

What Paperwork Does Thawte Need?

Thawte requires that you submit a signed letter on your organization's letterhead identifying the Webmaster for your site, accompanied by "Proof of Your Right to Use the Certified Organization Name" and proof of the "Distinguished Name of Your Web Server".

Proof of Your Right to Use the Certified Organization Name

"Proof of your right to use the certified organization name" means proper documentation of your organization's identity.

Choose one of the following types of documentation as appropriate for your type of organization:

- Companies, corporations, partnerships or proprietorships

Thawte needs a copy of your company registration documents. Thawte will also accept a copy of your articles of incorporation, partnership declaration or income tax registration if it is stamped by the relevant authority.

- DBAs and Individuals

If you have a business name (DBA means "Doing Business As"), Thawte needs a copy of your DBA registration papers for local levies and taxes. Any official correspondence indicating your right to use the name given on your request will generally be sufficient.

- Government Departments



Materials provided as "Proof of Right to Use" may be in your local language, if Thawte has an International Representative in your country. Contact Thawte for more information.

Thawte requires an original signed letter from the Head of that department on the appropriate letterhead, along with contact information for his or her office and immediate superiors.

- **NGOs: Non-Government Organizations**

Thawte requires an original signed letter from the Chief Executive, Chairman or Managing Director of the NGO, on the appropriate letterhead.

- **Universities and University Departments**

Thawte requires an original signed letter from the Dean or Vice-Chancellor responsible for that department. Note that this must be on the appropriate letterhead, accompanied by contact information for the University concerned.

- **Special Interest Groups**

Special-interest groups are popping up all over the Internet: The Apache Group, Debian, Linux Groups and others. Thawte will issue such groups certificates, but requests that you contact them to discuss verification and authentication.

Distinguished Name of Your Web Server

The ***Distinguished Name*** of a web server certificate is, by convention, set to the domain name of the server upon which the certificate will be used. Your organization will have gone through a process of registration in order to register this domain name. Because Thawte will be issuing a certificate tied to a domain name they need to be sure that you have the right to use a domain.

The procedure that you followed depends upon your location. If your domain ends in “.COM” or “.SE”, you do not need to do anything.

For all other domains, you must include a letter with the following domain name registration information:

- 1 Which authority you registered through (InterNIC, etc.).
- 2 The name and contact information you gave as an administrative contact.
- 3 The name and contact information you gave as a technical contact.

Thawte uses this information to verify your right to use the domain name they are certifying. All you need to send Thawte is a printout of the domain registration application you made, or the “WHOIS” output for your domain.

Sending Information

Compile the required documentation and print your letter onto letterhead. Then attach payment and fax the entire package to the Thawte representative in your area. See Thawte's homepage at:

<http://www.thawte.com/>

for information about how to do this.

Payment Methods

You can use one of these payment methods:

- Company check (in local currency)
- Credit Card (Visa, MasterCard, Diners Club, American Express)
- Bank draft
- International ("SWIFT") Inter-bank Transfer
- Stronghold bundle
- Enterprise Account

Sending the request to Thawte

To apply for a server certificate, follow these steps:

- 1 Use a text editor, such as SimpleText, to open the *Certificate Request* document.
- 2 Copy the entire contents of this document to the Clipboard. Do not alter the contents.
- 3 Use a Web browser to navigate to Thawte's Server Certification Application form at:
<https://www.thawte.com/cgi/server/step1.exe>
- 4 Choose **Web Server** and continue.
- 5 Paste the Certificate Request text into the Certificate Signing Request (CSR) window as indicated.
- 6 On the pop-up menu for Web Server Software, choose **WebSTAR/SSL 4.0 and later**.
- 7 Indicate your payment method with the appropriate radio button.
- 8 Continue with the forms pages by clicking the **Next** button.
- 9 On page 2 of the Server Certificate Application, examine the information obtained from your CSR to make sure it's correct.
- 10 Use the company description pop-up menu to select an entry that most accurately describes your organization, or use the text box to enter a description of your own choosing.
- 11 Fill out the authorizing contact information as specified.
- 12 Fill out the Web server administrator information as specified.
- 13 Make sure you're able to comply with the Payment Procedure.
- 14 Continue with the forms pages by clicking the **Next** button.
- 15 Choose the currency type from the pop-up menu.



The email address you provide here is the email address where your notification is sent.

- 16** Provide the street address to which any correspondence to you must be sent. Provide an office fax number, if desired.
- 17** Choose the Thawte office closest to you, where you want to send your paper documentation and payment.
- 18** Click the **Submit Application** button.
The next page of the process contains a summary of your Server Certificate Application.
- 19** Print and save the Server Certificate Application Complete page.
Don't forget to send your paper documentation and payment to the address provided on the summary page.

Downloading Your Certificate

Shortly after clicking the **Submit Application** button, you'll receive an email message from Thawte acknowledging receipt of your application. Contained in the message is a URL specific to your application which, when browsed, displays a "Server Cert Request Status" page. You can use your Web browser to check the status of your application on this Web page.

When Thawte has verified your documentation, received payment and processed the other information it requires, you are sent another confirming email message and the Overall Status item on the Server Cert Request Status page will read, "ISSUED". At that time you can download and install the certificate.

Follow these steps:

- 20** Use your Web browser to connect to the URL in the email message.
- 21** Make sure the radio button for "Standard Format" is checked.
- 22** Scroll down so you can see and click the "Fetch Certificate" button to download your certificate.
The "getcert" page is displayed.
- 23** On this page you will see your returned certificate in an encoded form in a new web browser window. The text has a Begin and End statement like
-----BEGIN CERTIFICATE----- through -----END
CERTIFICATE----- (other certificates may say NETSCAPE CERTIFICATE
CHAIN, or PKCS7 CERTIFICATE CHAIN).
- 24** Save this as a text file in the WebSTAR folder, or the host folder if you have a secondary IP host as described in "SSL and Multiple Domains" on page 212.



Save a copy of the "getcert" file in a secure location.

Obtaining a Test Certificate

To obtain a test SSL certificate, you must first create a Certificate Signing Request, or CSR (see page 216).

When finished, open the CSR Request in SimpleText and copy the contents to the Clipboard.

Once you have created your CSR Request you next need to submit the CSR Request to Thawte or VeriSign.

Obtaining A Test Certificate From Thawte

- 1 In your browser, connect to
<<https://www.thawte.com/cgi/server/test.exe>>. If you have not already done so, download the test root certificate at
<<https://www.thawte.com/server/test.crt>>, which is also linked to from this page. Failure to download this root certificate may prevent your browser from accepting connections from any test certificate you create here.
- 2 Paste the CSR Request into the Certificate Signing Request text field.
- 3 Under Type of Certificate, select either Test SSL Cert or Test SGC 128-bit SSL Cert.
- 4 For the Certificate Format, choose either the "standard" format, the "Netscape cert chain" format, or the "PKCS#7 chain format".
- 5 From the Custom Certificate Options, you can optionally select "Generate a X.509v3 certificate" and/or "Use an intermediate key-signing cert".
- 6 Click the Generate Test Certificate button and save the resulting text to disk. Use a file name like "Certificate".

IMPORTANT: Do NOT save the file as "Digital ID".

- 7 Move the newly created certificate file into the WebSTAR Server Suite folder, storing it within the root of the appropriate host folder.

Obtaining A Test Certificate From VeriSign

- 1 In your browser, connect to
<<https://www.verisign.com/server/trial/index.html>>.
- 2 Complete the Free Trial Secure ID form, entering your First Name, Last Name, Company, E-Mail Address, Phone, Web Server and other various information. When asked to select Web Server select "Other" if WebSTAR 4 is not listed. Click Continue.
- 3 Read the Before You Start information and click Continue.
- 4 When prompted to generate a CSR Request click Continue if you have already completed this step as described above.

- 5 Paste the CSR Request into the Certificate Signing Request text field.
- 6 Enter additional Technical Contact Information, read the license agreement and click Accept.
- 7 Read the Install Test CA Root information and click Accept.
- 8 To complete the process VeriSign will email you a test certificate which that looks something like:

-----BEGIN CERTIFICATE-----

```
MIICNzCCAeECEE86maRLnPU0r2uYw/ogNEWQYJKoZIhvcNAQEEBQAwgaxFjAU
BgNVBAoTDVZlcm1TaWduLCBjbMxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20v
cmVub3NpdG9yeS90ZXN0Q1BTIEluY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUYw
RAYDVQQLZ1G6b3IgVmVyaVNPZ24gYXV0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIE5v
IGFzc3VyYW5jZXMGKEMPVlMxOTk3MB4XDTk5MDYxMDAwMDAwMFoXDTk5MDYyNDIz
NTk1OVowdDELMAkGA1UEBhMCVVMxEzARBgNVBAGTCkNhbGlmY3JuaWEeXETAPBgNV
BACUJlcm1lbG95MREwDwYDVQQKFAhTdGFyTm1uZTEPMA0GA1UEC3QGYXNmZHNm
MRkwFwYDVQQDFBFB3d3cuc3RhcM5pbmUuY29tMHwwDQYJKoZIhvcNAQEEBQADAwA
aAJhAMRPI5BAE+x3q94BIqI66TieIP0jBQVH1/frgipp+/257tGnbk1JmiCRhh0B
kn4sbYOLq2ag8H476r0twCfjNyNtfNnLI+DKcRZfkkNvON2F8pVR6EInBKvxZTte
EB80zQIDAQABMA0GCSqGSIb3DQEBBAUAA0EAmji0zPz4kNm6fu/b+DWewILRVlzs
mXHQNAspxQA1A8Bmtr9owmf1Drk118nash5gTDAb0ukTNJrll6sXQD475A==
```

-----END CERTIFICATE-----

- 9 Copy and paste the text into a new text file, saving it with a file name like "Certificate".

IMPORTANT: Do NOT save the file as "Digital ID".

- 10 Move the newly created certificate file into the WebSTAR Server Suite folder, storing it within the root of the appropriate host folder.

INSTALLING YOUR SERVER CERTIFICATE

- 1 Make sure that your web server has SSL capabilities. It should say "SSL" in the Status window on the server, and have an SSL Security item in the list of Settings in WebSTAR Admin.



See "Web Server Administration" starting on page 129 for details.



To install an SSL server, you may need to install WebSTAR from the distribution CD.

- 2 Make sure the Status window is open on the server machine.
- 3 In WebSTAR Admin, Settings window (on any machine), select **SSL Security**.



For information on setting up multiple IP addresses, see “Virtual Hosts” on page 144 and “SSL and Multiple Domains” on page 212.

- 4 The top area lists the IP addresses you have set using the IP Secondary Addresses file, as described in “IP Multihoming: Special Configuration” on page 195. The lower area sets your security options, including certificate and private key data. The checkboxes set your policy regarding incoming connections.

IP Address	Security	Certificate	Key File
192.168.0.2	SSL 2 & SSL 3	:store:ssl_certificate	:store:private_key
192.168.0.4	Off		

Items: 2

Security: SSL 2 & SSL 3

SSL Certificate File: :store:ssl_certificate **Choose...**

Private Key File: :store:private_key **Choose...**

Private Key Password:

Encryption Options

☒ MAC (No Encryption) ☒ RC4-40 ☒ DES-40

☒ 3DES ☒ RC4-128 ☒ DES-56

Each IP address uses a different certificate. You can have certificates for several of these addresses, but one IP address can only have a single certificate.

- 5 Select the item for the IP address which corresponds to the host name of the current Certificate.
- 6 On the Security popup menu, select **SSL 2 and SSL 3**.
- 7 Use the Certificate **Choose** button to select the certificate file you have saved in your host root folder described in “Generate a Key” on page 216.
- 8 Use the Private Key File **Choose** button to select the private key file saved in your host root folder, described in “Downloading Your Certificate” on page 224.
- 9 Type or paste your Private Key Password into the appropriate field.
- 10 Click the **Save** button.
- 11 Look at the server Status window. You should see a message confirming that the SSL certificate was accepted:

SSL context for 192.168.0.2:443 created.

Encryption Ciphers

The cipher checkboxes indicate which encryption algorithms you will support. The client can connect only if they support at least one of the cipher you enable, and they negotiate to find the best fit.

- Very high-security sites will just enable 3DES and RC4-128.
- Some U.S. government sites require DES only, so if you are in that situation, do not enable the RC4 options.
- If you decide that your server does not require DES as the primary method, consider whether to allow your server to negotiate DES (which is more computationally intensive), or to allow only RC4.
- Most sites that want to allow overseas users will need to turn on DES, DES-40 and RC4-40. RC4-40 is the only supported encryption method that can be exported from the United States to other countries.
- MAC is a little different, and should only be used if you need to allow users to connect to your SSL server in an unsecure mode. There are a few countries where authentication is allowed but encryption is not, and the MAC cipher is sometimes used by clients in these countries. The MAC cipher will send your certificate to the client and ensure the integrity of the data you send, but it won't encrypt the data.

When you have chosen your cipher settings, click **Save** again to send the information to the server.

USING SSL IN WEBSTAR

When you have installed the certificate, you should test your server to make sure it is encrypting communications properly. then you can start serving and accepting information with assurance that it is secure.

Testing Your Secure Server

To connect to WebSTAR SSL, follow these steps:

- 1 Launch your SSL-compatible browser (such as Netscape Navigator or Internet Explorer).
- 2 Create a test file named *secure.html* in a folder named *secure*.
- 3 Use HTTPS to open your page (using your host name):

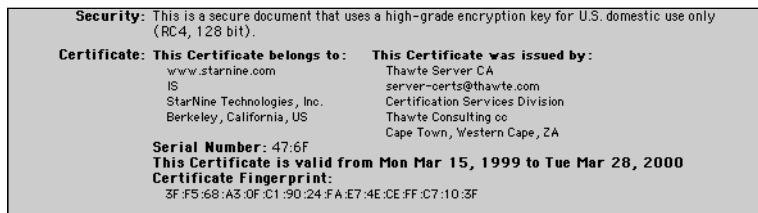
`https://www.domain.com/secure/secure.html`

The browser connects to the server and opens in secure mode. You can verify the security of a document by examining the security icon in the lower-left corner of the browser window.

In early versions of Netscape's browsers, the icon consists of a gold key on a blue background to show secure documents and a broken key on a gray background to show unsecure documents. In version 4 of Navigator and Communicator, it's a small padlock icon, open except for secure documents. Other browsers have similar icons to indicate security status.



To check security, you can use the Page Info command on the View menu. A window opens that includes this security information:



It shows the type of encryption protecting the document (see "Encryption Ciphers" on page 228) as well as Certificate information and the public part of the authentication key.



If you have trouble, see "SSL (Secure Socket Layer) Troubleshooting" on page 231.

Access Control

To preserve privacy, you should know who is accessing the information. Using WebSTAR's Realm-based access control with user names and passwords (see "Security Realms" starting on page 164), which will provide some of this accountability. Be sure that you use safe passwords and change them regularly, as well as using a log file analysis program to track all transactions.

You should also take extra security precautions with the machine serving private data.

- Limit or remove FTP access

You should never allow FTP access to the folders with the private data, or their parent folders. FTP passwords are sent in the clear, so anyone monitoring your data stream can see them.

- Install a server monitor application

A monitor, such as LogDoor from [Open Door Networks](#), lets you track whether outsiders are attempting to crack the security on your server, and can monitor more carefully if you are under attack.

- Consider a firewall

Macintosh servers are among the most secure, because they do not respond to remote commands or provide easy access to the data. However, if you store private data on your server, including credit card numbers, a firewall application or hardware will improve security. The firewall will allow only certain IP numbers to use specified protocols, which limits your vulnerability.

Additional Privacy Considerations

Serving private pages, such as medical records, personnel information, or financial data, is different from accepting credit cards. When you use SSL to accept a credit card, the browser encrypts the information before sending it to you. When you use SSL to display private information, the server encrypts it before sending it to the browser.

There are a number of ways to make sure you serve private pages via the secure HTTPS protocol:

- Run a second copy of WebSTAR Server Suite in a different folder on the same machine (using the same serial number).
- Run another copy of WebSTAR Server Suite on a secure machine (which requires a different serial number: contact StarNine Sales for a special pricing for this purpose).
- Use a third-party program, such as Welcome, to force certain URLs to be served by HTTPS.



To set the server to respond to HTTPS only, set the Web HTTP connections to 0: see "Max Connections" on page 134.

SSL Server Performance Issues

Serving and accepting encrypted data via HTTPS takes more time than serving plain text pages and even graphics.

The most processor-intensive portion of the SSL protocol is the key exchange, when the browser first connects to your server using the HTTPS protocol. WebSTAR Server Suite 4 implements the **resumable sessions**, which allow browsers to re-use previous key exchange information. The second and subsequent connections by a browser doesn't need the same expensive session setup as the first connection, so they are **much** faster. In addition, the persistent connections feature allows the server to keep the connection to the browser open until all elements of the page are sent, which is much faster than opening a new connection.

If you are concerned about speed, the RC4 cipher is twice as fast as DES, and 6 times faster than 3DES, while providing the same amount of encryption.



Most browsers released since 1997 support persistent connections and resumable sessions.

SSL (SECURE SOCKET LAYER) TROUBLESHOOTING

The only noticeable difference between the SSL server and the regular version, is that the SSL version encrypts all data it sends and decrypts all the encrypted data it receives. In practical terms this means that an identical page will take two to four times longer to serve from the SSL version.

Questions specific to the SSL version or issues relating to encryption, digital IDs and certificates are covered in this section.

WebSTAR quits immediately after launch.

- **If the Private Key file has been regenerated, it will no longer match with your Certificate.**

Make sure that the Private Key file is the same one that was used to generate the original Request for Certificate—if necessary, use Get Info under the File menu in the Finder to compare the creation dates on these files to see that they are the same. The Certificate and the Private Key file make up a pair, and must match; if they do not, browsers will be unable to access your WebSTAR SSL server.

- **The Certificate or Private Key files have been moved or renamed.**
Put them back and try again.

If you are still unable to launch WebSTAR after these steps, please contact StarNine technical support for further assistance.

Need to convert an old certificate

The old certificate file (WebSTAR/SSL 2 and 3 format) is only converted the first time WebSTAR 4 runs. It must be in a file named *Digital ID*.

- If you need to convert later, you can quit the server, remove the *WebSTAR Settings* file, and launch WebSTAR again: it will convert the certificate file at that point, and store the information in the *WebSTAR Settings* file.
- You can also fix it by hand:
 - Change the file TYPE code to TEXT to so that the file can be opened in BBEdit or another text editor.
 - Once the file is open, add this line at the beginning of the file:
-----BEGIN CERTIFICATE-----
and this line at the end of the file:
-----END CERTIFICATE-----
Do not include any spaces or tab characters on these lines.
- Save the file in the server folder.
- Quit the WebSTAR Server.
- Start WebSTAR again: it should recognize and accept this format.

URLs routed through third-party Plug-Ins don't work with HTTPS

Some third-party Plug-Ins may not support HTTPS and SSL connections. If you have difficulties, contact those developers directly.

When users click on a hypertext link to a secure page the connection is refused.

Connections to a secure server require the client software to communicate via the SSL (HTTPS) protocol. Older browsers do not support the SSL protocol. The most recent versions of most browsers do support SSL.

Users coming from networks which use a Proxy gateway cannot connect to my secure pages.

SSL does not work through many Proxy servers and firewalls. Consequently, you should provide both secure and unsecure versions if you want access to be available to everyone.

WebSTAR launches as usual, but browsers are unable to connect and the log contains messages that report "SSL Handshake failed"

This could indicate that the Certificate is corrupt. If you have a backup of the *Certificate* file, replace the one in the server's folder with the

backup. Otherwise, you can regenerate the Certificate from your *Certificate* file.

The “SSL Handshake failed” message could also indicate that the Certificate does not match the Public/Private key.

Browsers display an error message or security warning

- Certificate Authority is Expired
- Certificate issuer for this site is untrusted or unknown

When browser certificates expire, you will see these messages. For Thawte, that was July 28, 1998. For VeriSign, many certificates will expire at the end of 1999. You may have to help your customers or users change their browser certificates to recognize the new authorities.

To update browsers for Thawte server Certificates, follow the instructions at

<https://www.thawte.com/certs/server/rollover.html>

- Unable to establish a secure connection... (The identity certificate has expired)
- invalid site name
- An error occurred in the secure channel support

For all these errors, see the advice at

<https://www.thawte.com/support/server/browsers.html>

When people click a link on the SSL page to go back to the non-SSL page, the new page is still secure.

If you are serving SSL and non-SSL pages from the same folder and use relative references in your HTML, then links from your SSL page will use the HTTPS protocol instead of HTTP. Make sure that links in the HTML of your SSL pages specify “http” when you intend a non-SSL link.

When clients connect to a secure page they receive the message, “You have requested a secure document that contains insecure information. The insecure information will not be shown”

Netscape does not allow both secure and insecure documents to be displayed on the same page. The problem is likely that the HTML portion is being served by WebSTAR SSL (HTTPS) while navigation buttons or graphics are being served out by WebSTAR (http). Make sure that all referenced documents are also linked with “https”.

The **WebSTAR Plug-In** architecture allows WebSTAR to add power and flexibility through the use of Plug-In modules. WebSTAR includes a collection of Plug-Ins which perform additional tasks for your web server. They display listings of folder contents, handle server-side image maps, email form data, allow HTTP file uploads, serve byte-range data, search a site index, run server-side Java applications and link to Apple's WebObjects middleware.

WebSTAR also uses Plug-Ins for core features, such as administration, data caching and virtual host routing. For information on these features, see "Web Server Administration" on page 129.

In addition to the Plug-Ins that come with WebSTAR, there are many third-party developers writing Plug-Ins for WebSTAR. Almost anything you want to do with a server, from scheduling and calendars to surveys to database access to online stores, can be done with CGIs and Plug-Ins for WebSTAR. For information on third-party Plug-Ins, see:

<http://www.starnine.com/extendingwebstar.html>

This chapter does not cover third-party Plug-Ins.



If you're interested in writing your own Plug-Ins, see "Developing WebSTAR API Plug-Ins" starting on page 454.

ABOUT WEBSTAR PLUG-INS

All Plug-Ins apply to the entire WebSTAR server, including all web sites under virtual hosting. The WebSTAR *Plug-Ins* folder must be in the *WebSTAR* folder so that the server can find it.

When you launch WebSTAR, the Plug-In names, version numbers, and other informational notes are displayed in the Status window. In addition, the WebSTAR server's Plug-Ins menu will show you the installed Plug-Ins. If you select a Plug-In from that menu, it will display configuration information in the Status Window monitor pane. Some Plug-Ins display a status or information window on the server as well. When you install third-party Plug-Ins, they will also display startup information and appear on this menu.

Other copies of the WebSTAR application running on the same machine will have different Plug-Ins and Plug-In settings.

Plug-In Memory Issues

The "Preferred Size" for the WebSTAR application allocates enough memory to run all WebSTAR Plug-Ins at their default settings. However, the server shares memory with Plug-Ins, so you should watch the server status and increase memory if necessary. If you are

Plug-Ins

- WebSTAR Admin
- WebSTAR Auto BinHex
- WebSTAR Byte Server
- WebSTAR Data Cache
- WebSTAR Directory Indexer
- WebSTAR File Upload
- WebSTAR Form Mail
- WebSTAR FTP
- WebSTAR Image Map
- WebSTAR JRun Servlet Runner
- WebSTAR Lasso Publisher
- WebSTAR Log Archiver
- WebSTAR Mail
- WebSTAR Search
- WebSTAR SSI
- WebSTAR SSI-WebInclude
- WebSTAR Virtual Hosts
- WebSTAR WebObjects Adaptor

not using WebSTAR FTP, WebSTAR Mail or WebSTAR Proxy and remove the those Plug-Ins, you can reduce the memory allocation for the server by 250 K each.

To use some third-party Plug-Ins, you may need to increase the memory partition of the WebSTAR Server. For information, see “Server Application Issues” on page 87.

Installing and Removing Plug-Ins

A Plug-In is only recognized by WebSTAR when it is in the *Plug-Ins* folder in the WebSTAR root folder when the WebSTAR server starts up. If you put a new Plug-In file into the folder, it will not be used until you quit and restart the WebSTAR server.

Installing Plug-Ins

- 1 Quit the WebSTAR server application.
- 2 Run the WebSTAR Server Suite installer application, the Plug-In Installer, or drag the Plug-In file to the *Plug-Ins* folder in the WebSTAR folder.

Some third-party Plug-Ins should be installed in subfolders: be sure to follow the Plug-In's installation instructions carefully.
- 3 If the Plug-In's documentation says that it needs additional memory, increase the Preferred Size, as described in “Server Application Issues” on page 87.
- 4 Restart the WebSTAR server application.
- 5 Most Plug-Ins automatically define Actions and Suffix Mappings at server startup. If that is not the case, follow the instructions in the Plug-In documentation to use the WebSTAR Admin application or browser admin pages to configure the settings.

Removing Plug-Ins

- 1 If you've added custom entries in the Suffix Mapping Table or the Actions list for this Plug-In, remove them.

You may want to test your site for a while to make sure you aren't missing anything important.
- 2 Quit the WebSTAR server application.
- 3 Drag the Plug-In file out of the *Plug-Ins* folder located in the WebSTAR root folder.
- 4 If the server no longer requires additional RAM, you can reduce the Preferred Size for the WebSTAR application, as described in “Server Application Issues” on page 87.
- 5 Restart the WebSTAR server, and test your site again.



The WebSTAR *Plug-In* files are automatically put in the Plug-Ins folder when you run the WebSTAR Installer.



For information, see “Suffix Mapping” on page 154 and “Suffix Mapping Example: Using SSI for All HTML Files” on page 160.

WebSTAR Plug-In Settings

By default, the Plug-Ins included with WebSTAR do not require any special configuration.

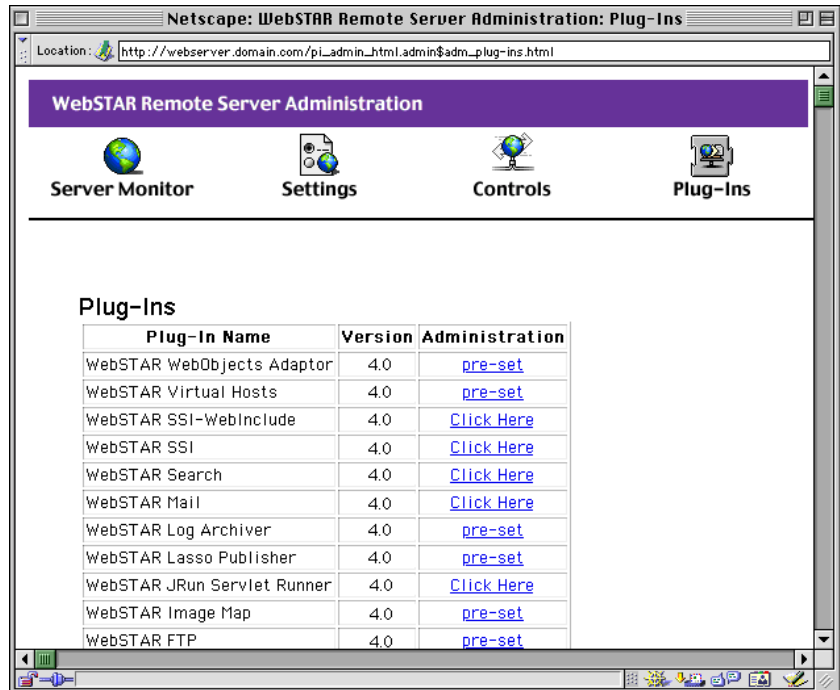
If you choose to adjust the settings, just open the WebSTAR Plug-In Administration pages through your web browser. You can access these pages from any browser on the Internet, and make changes to configure your Plug-Ins. You will probably need to enter a user name and password to view this page.

Open the Plug-In Administration Page using the “pi_admin.admin” URL, like this:

`http://www.domain.com/pi_admin_html.admin$admPlug-ins.html`

(replacing the name `www.domain.com` with your host name). Or you can go to the main `pi_admin.admin` page and click the Plug-Ins icon to see the list of WebSTAR Plug-Ins:

 For information on security and access, see “Browser-Based Admin” starting on page 126.



Some Plug-Ins, such as the WebSTAR Image Map, do not require any configuration. You just use them by creating files with the appropriate suffix.

If there are no options available for that Plug-In, or if the WebSTAR Admin application must be used to configure it (see “WebSTAR Admin Server Settings” on page 120), it will be marked as “pre-set” in the “Administration” column. Clicking on that link will take you to an error page.

Be sure to click on the **Save** button when you make changes in the Browser Administration pages—it’s very easy to enter the changes and then forget to save them. It’s also a good idea to test the changes right away, and make sure you’re happy with the results.

WEBSTAR AUTO BINHEX

Binhexing is a form of encoding that allows you to transfer Mac data files and applications (which include the Mac resource fork) via the Internet. The WebSTAR Auto BinHex Plug-In performs on-the-fly binhex-encoding of files and Macintosh applications. Most browsers have helpers installed to decode binhexed files automatically.

To trigger this behavior, simply append the `.hqx` suffix to the end of a URL for a file. For instance:

```
http://www.domain.com/products/widgetsinfo.sit.hqx
```

will encode the file *WidgetsInfo.sit* in the *products* folder and serve it to the browser. There will be some delay while the server processes the file. Then the browser will download it and decode it.

Using Auto BinHex

To enable auto binhexing for a folder, make sure there is a file named *.message* in the folder (the file can be empty). This will also allow you to view the contents of the folder, as described in “Enabling Directory Indexing: the “.message” File” on page 242.

When a URL for a file in this folder has the extension `.hqx`, and the file name does not include that extension, the WebSTAR Auto BinHex Plug-In will automatically encode the file before sending it back. If the file name ends in `.hqx`, it will be served without encoding.

Encoding can take several minutes if the file is large. When the file is finished encoding, it will start to download through the browser, and you’ll see an entry in the Web activity monitor window, and in the log file.

 For third-party Plug-In administration, see that Plug-In’s documentation.

 Remember, these settings and the Plug-Ins apply to all Virtual Hosts on your server.

 WebSTAR does **not** install the WebSTAR Auto BinHex Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

The WebSTAR Auto BinHex Plug-In will run anytime a browser sends a URL with `.hqx` at the end, as long as there’s a file named *.message* in the folder.

 If you dislike the delay in encoding, you can use a program such as Stuffit Deluxe, and encode your larger files manually.

Auto BinHex Settings

The WebSTAR Auto BinHex administration page allows you to specify which files to serve and whether to cache the encoded copies. To change settings on the WebSTAR Auto BinHex Plug-In, use your browser to open the administration page, and choose the Auto BinHex Plug-In at the URL like this:

```
http://www.domain.com/pi_admin.hqx
```

(replacing the name `www.domain.com` with your host name). You can update the settings in this page: don't forget to press the "Save" button at the bottom to save your changes to the server.



WebSTAR Auto BinHex will never allow files with a Creator Code that starts with "WWW" to be BinHexed and served, because these are control files and must be kept secure.



Plug-In Developers, see "Calling WebSTAR Auto BinHex" on page 460.

Security

The Auto BinHex security section allows you to either binhex and serve almost any kind of file, or to limit the files to those with specific suffixes, so as not to serve application files. The default is to "Allow any file".

If you choose to limit the suffixes to be served, the default suffixes are:

```
.sit .sea .cpt .bin
```

You can add more suffixes to this list by typing them in with a space before each. In this case, only files with one of these suffixes will be encoded and served.

Caching

The WebSTAR Auto BinHex default is to cache the encoded copy in a Temporary Items folder, which is flushed by the system if the cache gets too full, and at shutdown. You can configure the Plug-In to not cache, so it will always Binhex on the fly, which is appropriate for files that are constantly changing.

Binhexing Other Kinds Of Files

At server startup, the WebSTAR Auto BinHex Plug-In automatically adds an entry to the Suffix Mapping table to binhex files that end in the suffix `.HQX`. To automatically binhex file names using other suffixes, use the WebSTAR Admin to enter a new Suffix Mapping entry with an Action of "BINHEX", like this:

```
BINHEX .HQX * * application/binhex4.0
```

WEBSTAR BYTE SERVER

WebSTAR Byte Server is a WebSTAR Plug-In that supports **byte-range serving** of files according to the HTTP 1.1 specification. This allows WebSTAR to serve sections (i.e. “byte-ranges”) of very large files, rather than sending the entire file to the client application. Browsers and other clients that support this feature will become more common in the future.

Browser requests which contain an HTTP **Range:** request in the header will automatically be passed to the WebSTAR Byte Server for processing. Adobe Acrobat (PDF) is the most common format to take advantage of this option. You do not need to set up any suffix mapping; the Range: request in the HTTP header is enough to invoke this Plug-In.

You may need to configure your browser, file-viewer helper application and original files before you can successfully serve and view byte-range served files: see the Acrobat example below for instructions. The WebSTAR Byte Server does not require any configuration.

Example: Byte-Serving PDF files

The following describes how to use the WebSTAR Byte Server with Adobe Acrobat PDF files. Different configuration setups will be required for other file types.

- 1 Make sure you have the newest version of the free Acrobat Reader, which includes a PDFViewer Plug-In for browsers. Install it from the WebSTAR CD or download it from:

<http://www.adobe.com/prodindex/acrobat/readstep.html>

- 2 Use Adobe Acrobat version 3 or greater to generate a PDF file.
- 3 Make sure that you save the file in Adobe Acrobat Exchange with the “Optimize” option enabled, and that you use the .pdf suffix at the end of the file name.
- 4 Place the PDF file somewhere in your WebSTAR folder hierarchy.
- 5 Go to your browser machine and make sure you have Adobe Acrobat Reader, version 3 or later. Download and install it if necessary.
- 6 Launch the Acrobat Reader and **uncheck** the General Preference “Allow Background Download”
- 7 Save the Preferences and leave the Reader open.



WebSTAR installs the WebSTAR Byte Server Plug-In by default. If you need to change it, follow the instructions in “Installing and Removing Plug-Ins” on page 236. It does not require any additional RAM.

The WebSTAR Byte Server Plug-In is always enabled.



Some browsers, especially older browsers, may not take advantage of the byte serving and will download the entire file. There is nothing that you can do about that on the server.



The first time you select a PDF file, you may have to tell the browser where the Acrobat Reader application is located.

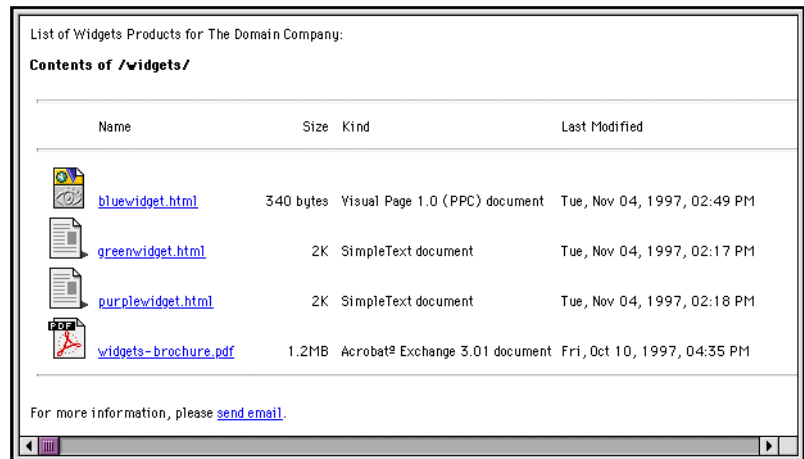
- 8 If you ran the Acrobat Reader Installer, it should have put the PDFViewer Plug-In in your browser's Plug-Ins folder. You may need to specify the PDFViewer Plug-In as the helper application for the Adobe Acrobat application/pdf MIME Type in your browser.
- 9 Launch the browser and connect to your server, then enter a URL requesting the PDF file.

As the PDF file loads, the browser will call the PDF Reader Plug-In (launching the Acrobat Reader application if necessary) and the Acrobat Plug-In page controls will become active in your web browser's window.

As you step forward through the document, the browser will request individual ranges of bytes from WebSTAR instead of the entire document. You'll see another request to the document in your log and monitor window, and if you have specified a BYTES_SENT log token, you'll see that only a small amount of data was sent.

WEBSTAR DIRECTORY INDEXER

To display a listing of files in a folder, via a browser, use the WebSTAR Directory Indexer Plug-In. All you have to do is put a special file name in the folder, and WebSTAR will display a list of files instead of a default page.



Using Directory Indexer

To tell WebSTAR to display the directory index listing (rather than a default index page) for a folder, put a file named *.message* into the

folder, as described below. When a browser requests that folder in a URL (that is, the URL ends with the folder name and a slash), for example:

```
http://www.domain.com/widgets/
```

the directory index listing for the *widgets* folder will be displayed.

The first 100 files in a folder will be displayed, alphabetically. If there are more files, the Directory Indexer will include a “More” button, which will display additional files. However, there may be a significant delay in displaying large numbers of files.

Enabling Directory Indexing: the “.message” File

You must create a *.message* file in each folder that will be display a listing. It's just a text file, named with a period followed by the word “message”:

```
.message
```

Do not add any text before the period.

The presence of this file is a signal to the WebSTAR Directory Indexer Plug-In to display the contents of that folder, overriding any default index file.

Display a Header: Text in the “.message” File

The *.message* file is used for two things. Its existence triggers the directory index listing, and the contents are displayed as a header to the listing.

The file contents can be a plain text string or HTML. It is processed by the WebSTAR SSI Plug-In (if installed) for character set encoding and other SSI processing. Although you can use HTML in this file, be careful with the encoding, as non-standard HTML can cause problems with the display. Note that the <TITLE> tag will be ignored.

Display a Footer: the “.footer” File

To display information at the bottom of the directory index listing, create a file called *.footer* (a period followed by the word “footer”). The contents of this file (HTML or text) are displayed at the bottom of the directory index listing, as shown on page 241.

Allow Upload: the “.upload” File

To allow people to upload files, you must have a file named *.upload* in the folder. Directory Indexer will display a form at the bottom of the listing. However, many older browsers do not support this feature.

 WebSTAR does **not** install the WebSTAR Directory Indexer Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

 The Directory Indexer will always run if there is a file named *.message* in a folder.

 Disk utilities, such as Norton, may alert you that you should fix files starting with a period. Do not allow them to “fix” these files, or these Plug-Ins will stop working.

For more information on uploading in the directory index listing, see “File Upload Option” on page 246 and “WebSTAR File Upload” on page 247.

Aliases and Security

The directory index listing will display aliases to files in other folders and mounted volumes. You can use this to allow people viewing your website to open or download pictures, text and HTML files, or any other file that you have access to from your server.



For more security features, see “WebSTAR Directory Indexer Administration” on page 244.

Before you add aliases to a folder with a *.message* file in it, review your security strategy, and think about who will have access to that file. It's often better to make a copy for the website, so you know exactly what the public will see.

Binhexing and Uploading

Visitors to your site can display or download the files by clicking on them in the browser. If you have installed WebSTAR Auto BinHex, it will encode the files with specified suffixes so that the file format can be transferred without losing important resource fork information. (see “WebSTAR Auto BinHex” on page 238).

If you have installed the WebSTAR File Upload Plug-In, and placed a *.upload* file in the folder, the browser will automatically display an Upload form at the bottom of the index listing enabling users to upload files to this folder (see below and “WebSTAR File Upload” on page 247).



Many browsers will display the Upload button but only some can actually upload the files.

Note that only newer browsers (such as Netscape version 3 or greater, Explorer version 4 or greater), will be able to upload the files. You may decide to use the WebSTAR FTP Server (described on page 337) for uploading instead.

Icon Caching

WebSTAR Directory Indexer creates a folder called *WebSTAR_Directory_Cache* in the WebSTAR root folder. This folder contains cached icon graphics, to speed display for all directory index listings.

Files created by applications not installed on this Macintosh may have an incorrect icon displayed. To force the correct icon to appear, copy the application onto the server briefly. If the icons are still not displayed correctly, try rebuilding the Desktop database (the Mac's list of application and file icons). To do this, restart your machine and hold

down the Command and Option keys through the Extension/Control Panel icons and until you see a dialog asking if you want to rebuild the Desktop, then click “OK”. Once the icon displays correctly, you can delete the application from your hard drive. The icon will remain until you rebuild the Desktop database again.

Default Index Pages vs. Directory Index Listings

The presence of a *.message* file and a folder URL (folder name and slash rather than file name) tells WebSTAR Directory Indexer to display the directory index listing.

- If you want to display a default index HTML file in a folder that contains a *.message* file, you **must** include the name of that default index file in the URL, for instance:
`http://www.domain.com/widgets/default.html`
- If a folder does not contain a *.message* file then there is no way to get a directory listing.



For information about adding more default page names, see “Index File Name” on page 131.

WebSTAR Directory Indexer Administration

To change settings on the WebSTAR Directory Indexer Plug-In, use your browser to open the administration page, and choose the Directory Indexer Plug-In at the URL like this:

```
http://www.domain.com/pi_admin.dir
```

(replacing the name *www.domain.com* with your host name). Use this page to configure the display, and don't forget to click the “Save” button to save your change to the server.

Files Beginning with a Period (.)

Files beginning with a period (like *.message*) are used to mark certain directories that are served in a special way. In most cases, the default option “Hide files beginning with a period (.)” is best: you don't want people downloading these files.

However, if you ever need to display these files, you can do so by selecting the “Show” option on this page.



Don't forget to save your changes by clicking the “Save” button at the bottom of the Administration page.

Links to Parent Directories

The WebSTAR Directory Index Plug-In can automatically display the path of this folder, from the site root folder, in the form of clickable links, like this:

```
Contents of /widgets/bluewidgets/info/forms/
```



The root folder for the host is always marked as “/”.

Each of these entries is a link to the default for that folder (either a directory index listing or a default index page).

The default is to generate these links. If you don’t want people to see the layout of your site, click the “Hide links to parent directories” radio button.

Large or Small Icons

Files are shown with their standard Mac icons. You can choose to display them as large or small icons, just like on the Mac desktop.

Date Format

The Directory Index shows the list of files with the date they were last changed. You can see this in one of two ways:

- Weekday, Month, Day, Year, Time format

Fri, Oct 24, 1997, 11:50 AM

- Month/Day/Year, Time format

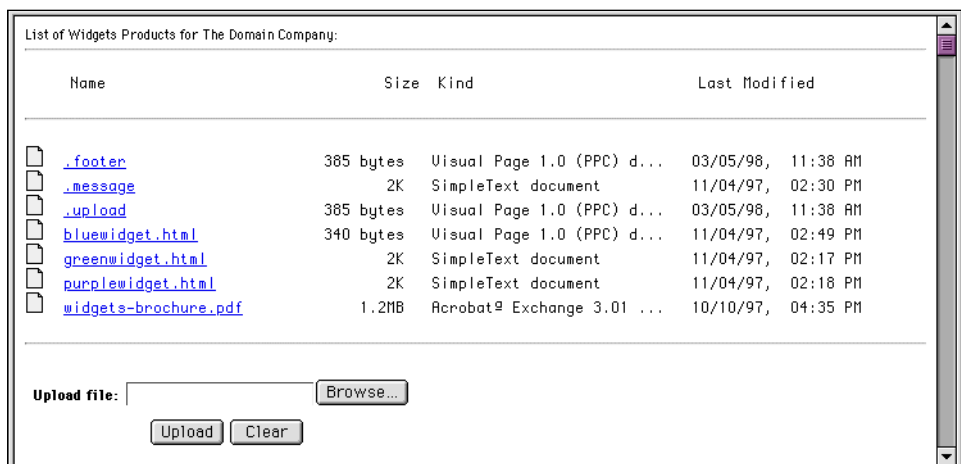
10/24/97, 11:50 AM

Use Tables

The screenshot in “WebSTAR Directory Indexer” on page 241 shows a display with tables. This allows the browser to line up the columns.

If you want to support browsers without tables, choose “Generate display without tables”. The directory index listing is not quite as easy to read, but it’s faster for displaying long listings.

Example with Small Icons, Short Date, No Tables, Upload, etc.



Binhex Options

These options control how the Directory Indexer works with the WebSTAR Auto BinHex Plug-In to encode files for transfer. For more information on binhexing, see “WebSTAR Auto BinHex” on page 238.

Don’t allow downloading of applications is the first default. This reduces the chance that you will accidentally allow someone else to copy a program from your server. If you are using the server to distribute applications you have written or otherwise have the rights to, you can change this setting to allow downloading.

BinHex only when sending applications is the second default. It will encode the application data so that the resource fork is retained. As with all Auto BinHexing, there may be a delay while the encoding is going on.

If you have document files which include resource forks, such as SimpleText (with graphics or formatting), HyperCard stacks, CodeWarrior projects and so on, you can change this setting to encode them as well.

File Upload Option

You can specify that people can upload files directly from their browsers to the folder they are viewing. This requires the WebSTAR File Upload Plug-In, as described in “WebSTAR File Upload” starting on page 247.

The page will display a file name prompt, an edit field to type the name, a “Browse” button to choose a file, and buttons to Upload or Clear the field. This will appear at the bottom of the directory index listing, before the text from the *.footer* file, as in the example above.

To enable this option for directory listings, select **Allow uploading of files** in the administration page. You will also have to put a file called *.upload* into any folder that can accept file uploads.

WEBSTAR FILE UPLOAD

You can let people upload files via their browser to your site, either within a directory index listing or by creating an HTML form to specify the file and start the upload.

If you're using it with WebSTAR Directory Indexer Plug-In, the File Upload option adds fields and buttons to the listing page automatically. For more information, see "WebSTAR Directory Indexer" on page 241).

HTTP Upload Compatibility

WebSTAR File Upload uses the HTTP Upload function of certain browsers. If you want to be compatible with other browsers, you can use the FTP Server, included with WebSTAR. For more information, see "WebSTAR FTP Server" starting on page 337.

Although many file systems allow very long file names, you can only upload files with names up to 29 characters long. If people try to upload files with longer names, you'll see a log error



WebSTAR does **not** install the WebSTAR File Uploader Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

The File Upload Plug-In will always allow uploading if there is a file named *.upload* in a folder, and an appropriate HTML form.

File Upload: Could not create upload file.

Using the WebSTAR File Upload Plug-In

To use the WebSTAR File Upload Plug-In, you must create a *.upload* file in each folder that will be display a listing. It's just a text file, named with a period followed by the word "upload":

.upload

Creating An Upload Form

Here is the form part of the *WebSTAR File Upload Example* in the *Examples* folder in the WebSTAR folder:

```
<FORM ENCTYPE="multipart/form-data" ACTION="/folder/x.upload" METHOD=POST>
Use the Browse button to select a file.<P>
File: <INPUT NAME="remotefile" TYPE="file"><P>
<INPUT TYPE="submit" VALUE="Send This File">
<INPUT TYPE="reset" VALUE="Reset">
</FORM>
```

The form Action is */folder/x.upload*: you should replace the */folder/part* with the path to your upload folder name. This tells the

browser to send an upload message to the server with the file you've selected or typed.

WebSTAR File Upload Administration

The WebSTAR File Upload Administration page allows you to specify whether people can upload files and replace other files with the same name.

To change settings on the WebSTAR File Upload Plug-In, use your browser to open the administration page, and choose the File Upload Plug-In at the URL like this:

```
http://www.domain.com/pi_admin.upload
```

(replacing the name `www.domain.com` with your host name). If you choose to change the option, be sure to **Save** the change.

The default is **Overwrite files having the same name**. If you choose **Don't overwrite files with the same name**, and someone tries to upload a duplicate file, they will see this error message:

This file already exists, overwrite permission was denied.



If you're using file uploads with WebSTAR Directory Indexer, make sure you enable the File Upload Option (described on page 246). It will look much like the example on page 245.

WEBSTAR FORM MAIL



This Plug-In was previously called WebSTAR QuickSend and used the form action “.quick-send”.

You can have web pages on your server send HTML form data by email, using the WebSTAR Form Mail Plug-In. This works on the server itself, and does not require the user's browser to be set up to use the “mailto:” tag. For example, you may want to have visitors send a message to the webmaster, ask a sales question or contact someone in your company. Be sure to configure your Form Mail Plug-In, especially the SMTP Host, according to the instructions below.

WebSTAR Form Mail is a very simple forms mailer, and can only have one recipient. For more complex form mail tools, see the lists of third-party extensions to WebSTAR at:

<http://www.starnine.com/extendingwebstar.html>



WebSTAR does **not** install the WebSTAR Form Mail Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

The Form Mail Plug-In is always enabled. It will only run if a form contains the Action x.form-mail.

Using WebSTAR Form Mail

WebSTAR Form Mail works with an **HTML form** to send the entered text via email. Make the FORM ACTION x.formmail and the METHOD post. Then add form fields with specific names for the message information, and let the sender fill in the data (or you can pre-enter it and hide the elements). When the visitor clicks the “Submit” button in their browser, the server will call the WebSTAR Form Mail Plug-In to transfer the message. To see how this works, see “WebSTAR Form Mail Examples” on page 250.

Form Fields

You must use these exact words as your form field tags to work with WebSTAR Form Mail:

- To
- From
- Subject
- Body

The “To” and “From” fields must be filled in: if they are not, WebSTAR Form Mail will display an error page requiring the person to enter them. You can enter the associated data beforehand, in visible or hidden fields, or have the person enter the data in their browser.

Sender Identification

For security and accountability, WebSTAR Form Mail includes the IP address of the browser machine. This address is recorded in an “X-Comment” field in the message header:



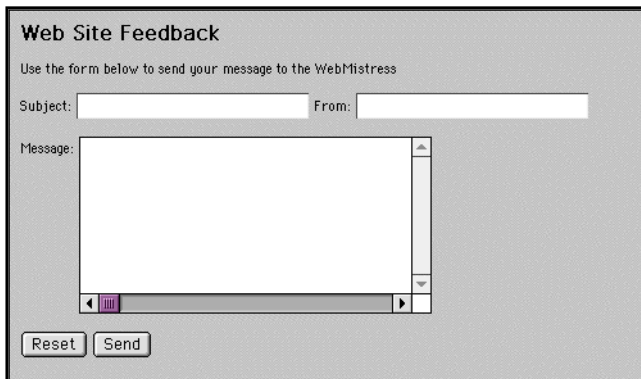
For additional fields, see “Additional Form Mail Options” starting on page 252.

X-Comment: (via WebSTAR) originating sender 198.211.93.29

Including this line prevents the WebSTAR Form Mail Plug-In from being used as an anonymous remailer: the originator is always identified.

WebSTAR Form Mail Examples

In this example, the form is set up to send a message to the webmaster. Therefore, the email, subject and message fields are visible, but the “To” field is hidden.



 To improve the layout of forms, use tables, as in the *form-mail.html* example.

```
<FORM ACTION="x.formmail" METHOD="POST"
ENCTYPE="application/x-www-form-urlencoded">
  <P>Subject: <INPUT TYPE="TEXT" NAME="Subject" SIZE="25">
  From: <INPUT TYPE="TEXT" NAME="From" SIZE="25"></P>
  <P>Message: <TEXTAREA NAME="Body" ROWS="7" COLS="35">
    </TEXTAREA></P>
  <P><INPUT TYPE="HIDDEN" NAME="To" SIZE="-1"
    VALUE="webform@domain.com">
  <INPUT TYPE="RESET" NAME="Reset" VALUE="Reset">
  <INPUT TYPE="SUBMIT" NAME="Submit" VALUE="Send"> </P>
</FORM>
```

- The first line starts the form, sets the Action to `x.formmail` and the other elements to standard form parameters. If you use an HTML editor, check the manual to see if they have a graphical user interface or if you have to hand-code this.
- The next line contains the Subject prompt and an input field named “Subject” which is 25 characters wide, and The prompt (From) and input field named “From” which is 25 characters wide.
- The prompt (Message) precedes an input text area named “Body” which is 35 characters wide and 7 lines high.

- The “To” field is required, so the next line contains the hidden field with the value pre-entered to `webform@domain.com`
- Standard Reset button will clear the form.
- The Submit button, labelled Send will tell the server to process the form according to the Form Action, in this case, Form Mail.
- End of form.

When the sender fills in the information in the browser and clicks the Send button, the WebSTAR Form Mail Plug-In will be called. It will format the message, call the SMTP host, and send the message. If you look in your log, you’ll see the `x.formmail` URL.

Table Form Example

The file named *formmail.html* in the *Form Mail* folder in the *Tools & Examples* folder displays a more elegant layout for the form, using table cells to line up the fields. It’s a very good example to customize to your own needs.

WebSTAR Form Mail Administration

To change settings on the WebSTAR Form Mail Plug-In, use your browser to open the administration page, and choose the WebSTAR Form Mail Plug-In at the URL like this:

`http://www.domain.com/pi_admin.formmail`

(replacing the name `www.domain.com` with your host name).

Mail Host

Enter the default mail (SMTP) host for WebSTAR Form Mail to use when sending mail. SMTP hosts take care of sending mail for POP/SMTP email programs, such as browser mail modules and client programs.

If you are using WebSTAR Mail, you can put your server name in this field. If you are using a different mail server, check with your mail administrator to be sure that this host will accept mail from your WebSTAR server: some hosts are restricted to certain accounts.

You can also override the default mail host in your web page forms: see “Mail Host” on page 252 for details.

Timeout in Seconds

The timeout value specifies the amount of time to wait for any response from the mail host. If WebSTAR Form Mail can’t get a response in this time, it will fail to send the message, and will display

this error in the browser (if you use “mail.domain.com” as your default host):

```
Host mail.domain.com did not respond to a
connection request.
```

If you have a slow mail server, you should increase the timeout value. The timeout range is 30 seconds (the default) to 3 minutes, configurable in 30 second increments.

Additional Form Mail Options

Mail Host

WebSTAR Form Mail must have an SMTP host to send the mail. You usually set this in the Admin page as described in “WebSTAR Form Mail Administration” on page 251.

To override the default SMTP host, put a hidden form field with a name of “Host” and a value filled in with a host name in the form block, as in:

```
<INPUT TYPE="HIDDEN" NAME="Host" VALUE="domain.com">
```

Specifying the mail host in the form will override the admin setting.

If no host has been configured and the HTML does not contain a form “Host” element, then WebSTAR Form Mail uses the host information from the “To:” field, and attempts to connect to that system.

Custom Return and Error Pages

You can have the Form Mail Plug-In return special pages based on the success or failure of a message.

The fields “Return-HTML” and “Error-HTML” must match exactly for this to work. In addition, the VALUE part of the field should contain a path to custom files, relative to the WebSTAR root folder. In these examples, the WebSTAR root folder contains a folder named *mailfiles*.

Custom Return File

If you want to display a special page when the mail is sent, add a hidden field to the form block in a WebSTAR Form Mail HTML form like this:



Be sure to save your changes—it’s very easy to forget. If you are getting unexpected results, check your settings again.



In general, it’s better to use one standard mail host than to use the host in the “To” field. You should configure the overall mail host information using WebSTAR Form Mail’s Administration options.

```
<INPUT TYPE=HIDDEN NAME="Return-HTML"
VALUE=":mailfiles:return.txt">
```

This file is displayed in the browser when the Form Mail Plug-In sends the message successfully.

Custom Error File

If you want to display a custom Error HTML file to the sender, add a hidden input type to the form block in a WebSTAR Form Mail form page:

```
<INPUT TYPE=HIDDEN NAME="Error-HTML"
VALUE=":mailfiles:qserror.txt">
```

This file is displayed in the browser when the email has an error and can't be sent. If the "To:" or "From:" field is missing, a standard WebSTAR Form Mail error page is displayed.

WEBSTAR IMAGE MAP



Newer browsers support **client-side image maps**, where the client (browser) finds the location. With WebSTAR Image Map, even older browsers can use your image maps.

Image maps let you specify **hot spots** in the graphics that you serve. This allows you to make maps and other graphical hyperlinks. You do this by mapping the coordinate location to the information that is created along with the image in the **map file** (many HTML editors allow you to create this map file automatically).

The WebSTAR web server, with the WebSTAR Image Map Plug-In, supports **server-side image maps**. WebSTAR Image Map supports these NCSA methods in the map file:

- circle
- poly
- rect
- point
- default

The Image Map Plug-In is compatible with NCSA format, but **not** with CERN format, so if you are using an HTML editor or an image-map generator, be sure that the preference is set to the NCSA format.

You do not need to do anything to administer the WebSTAR Image Map Plug-In. The server will automatically take care of this when it gets the URL ending in `.map`. If you would like to use other suffixes or files

without suffixes, you can make an entry in the Suffix Map Table and use “MAP” as the Action see “Suffix Mapping” on page 154).

Using the WebSTAR Image Map Plug-In

In your HTML pages, you will need to indicate that your graphic is a clickable map.

In this example, the “powered by WebSTAR” links to the StarNine website, and the Mac OS logo links to the Apple website.



The image file is named *poweredbywebstar.gif* and the map file is *poweredbywebstar.map*.

The map file is quite simple, since we just include two rectangles:

```
# Format: NCSA
default /
rect http://www.starnine.com/webstar/ 0,0 218,54
rect http://www.apple.com/ 218,0 272,54
```

- 1 The # is a comment saying that the map file uses the NCSA Image Map format.
- 2 All clicks on non-specified locations will go to the default page for this site.
- 3 Clicks in the rectangle defined by 0 at the left, 0 at the top, 218 at the right and 54 at the bottom will go to StarNine.
- 4 Clicks in the rectangle defined by left, top at 218,0 and right, bottom at 218,54 will go to Apple.

To use this image and map in an HTML page in the same folder, link the image to the map and make sure it has an ISMAP tag:

```
<A HREF="poweredby.map">
<IMG SRC="poweredby.gif" ISMAP></A>
```

Use your gif and map file names to create server-side image maps for your own graphics.

For more information on image maps, see the NCSA tutorial at:

i WebSTAR does **not** install the WebSTAR Image Map Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

The Image Map Plug-In is always enabled, and will be called any time you have a URL that ends in .map.

i To link to an image or map file in another folder, just use the file path.

<http://hoohoo.ncsa.uiuc.edu/docs/tutorials/imagemapping.html>

WEBSTAR JRUN SERVLET RUNNER

The WebSTAR JRun Servlet Runner allows you to use Java server-side applications known as **servlets**. Because servlets are platform-independent, you can use the growing number of free, shareware and commercial servlets without having to make any changes. Servlets can perform many tasks such as database access, text processing, and more.

For an explanation of how servlets can fit into your server design, see the JavaSoft white papers at:

<http://www.javasoft.com/marketing/collateral/servlets.html>

<http://www.javasoft.com/products/servlet/index.html>

System Requirements & Configuration

The WebSTAR JRun Servlet Runner requires at least 20 MB of installed RAM, and MRJ (Mac OS Runtime for Java) version 2.1.1 or greater. It supports version 2.1 of the Java Servlet API. You can test your installation by running one of the examples in the Apple Applet Runner.

The *JRun* folder must be in your WebSTAR root folder, and only the *WebSTAR JRun Servlet Runner* file belongs in the *Plug-Ins* folder.

Using WebSTAR JRun Servlet Runner

The WebSTAR JRun Servlet Runner works with Apple's MRJ to run servlets (server-side applications) written according to the JavaSoft specifications. It allows you to run Java-language software on the server rather than the client side, and does not require Java support in the browser.

Using a Java servlet is easy: WebSTAR will automatically direct all URLs with the string `/servlet/` before the name to the WebSTAR JRun Servlet Runner Plug-In. This is the standard way to call Java servlets on all platforms. The JRun Servlet Runner acts as a filter, changing the name so that it appears in your log file with a `.servlet` suffix. The WebSTAR suffix mapping then calls the JRun Servlet Runner, which uses MRJ to run the corresponding servlet in the *servlets* folder in the WebSTAR folder.



WebSTAR does **not** install the WebSTAR JRun Servlet Runner Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

The JRun Servlet Runner is always enabled, and will be called any time you have a URL that includes the string `/servlet/`. This is not the same as the *servlets* folder.

As long as the Servlet was written with the correct Java libraries, it will run on the server and return the results to the browser as HTML, GIF, or another web format.

There are some useful Servlet examples in the *Tools and Examples* folder. Use a URL like this:

```
http://www.domain.com/Tools%20&%20Examples/JRun/htdocs/
```

(replacing `www.domain.com` with your host name), to see the list of examples.

available Java Servlets, search the StarNine [Extending WebSTAR listings](#). For information about using JRun, JRun Pro and servlet development, contact Live Software at

```
http://www.livesoftware.com
```

Java Servlet Tips

- The URL must include the string “/servlet/” followed by the servlet name, like this:

```
http://www.domain.com/servlet/HelloWorld
```

The JRun Servlet Runner is case-sensitive, so the case of URL must match the servlet name **exactly**. A URL with “heLloworLd” would not match a servlet file named *HelloWorld*.

- The servlet must be in the *servlets* folder in the *JRun* folder in the WebSTAR root folder.

Java Servlet Development Information

For more information, see “Developing Java Servlets for WebSTAR” on page 464 and the examples in the *Tools & Examples* folder.

WEBSTAR POWERKEY PRO TICKLER

PowerKey Pro with the Server Restart Option from Sophisticated Circuits is a hardware power controller for Macs. You only need this Plug-In if you are using the PowerKey Pro hardware to monitor your server, detect system crashes and automatically restart the machine.

You can set up a PowerKey Event to track a timer, and restart the computer when it runs out. The WebSTAR PowerKey Pro Tickler sets the User Timer to 5 minutes at one-minute intervals. Once set, the User Timer starts counting down to zero. As long as WebSTAR is running, the Plug-In will continue to reset the User Timer, so it will never reach zero.



WebSTAR does **not** install the WebSTAR PowerKey Pro Tickler Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

If the User Timer ever actually reaches zero, it means that WebSTAR has stopped resetting it, usually due to a crash or freeze. PowerKey Pro will then execute the “When Timer Expires” Event. This will restart the system and restore WebSTAR to normal operation.

If you do not have PowerKey Pro installed, you will see error messages in the Status Window Web Monitor pane. Remove the *WebSTAR PowerKey Pro Tickler* file from the Plug-Ins folder and restart the server to avoid spurious restarts.



WebSTAR does **not** install the WebSTAR QuickDNS Load Balancer Plug-In by default. Use the WebSTAR Server Suite Installer to install it. It does not require any additional RAM.

See the QuickDNS Pro User Manual for additional configuration information.

WEBSTAR QUICKDNS LOAD BALANCER

QuickDNS Pro is a Mac OS DNS server from Men & Mice. WebSTAR QuickDNS Load Balancer works with QuickDNS Pro to provide DNS-level intelligent fault tolerance and load balancing for your WebSTAR Web and FTP servers.

Fault Tolerance

Intelligent fault tolerance is accomplished by running two or more WebSTAR Web or FTP servers with one or more QuickDNS Pro DNS servers on your site. When installed, WebSTAR QuickDNS Load Balancer periodically communicates with QuickDNS Pro. These transactions tell QuickDNS Pro that your WebSTAR server is online and able to handle requests. If the WebSTAR server goes offline, QuickDNS Pro automatically removes the server from its DNS records, only directing traffic to your other WebSTAR server(s). When the WebSTAR server comes back online the ping requests are once again received by the QuickDNS Pro server and the server is automatically added back to the DNS records.

Through this intelligent mechanism, the risk of hits going to non-responding servers is minimized, leading to maximum reliability of responses from your site.

Load Balancing

Intelligent load balancing is accomplished by running two or more WebSTAR Web or FTP servers with one or more QuickDNS Pro DNS servers on your site.

Load balancing yields maximum server performance by assigning optimum load to each server based upon its capacity, the current load level and the requested load level of the WebSTAR server. You can allocate the desired distribution of hits to your WebSTAR servers so

that each server handles the appropriate load at each time and provides fast and consistent responses from your site.

Load Balancing vs. Load Sharing

Distribution of load between servers is often accomplished through Load Sharing. However, Load Sharing is an inadequate approach because an equal number of hits are always allocated to each server, disregarding variations in capacity and current load. Servers begin handling too much or too little share of the load, resulting in inconsistent responses from your site.

On the other hand, Intelligent Load Balancing takes web server capacity and load into account, hence all the servers will get the appropriate load at each time and return fast and consistent responses.

For additional background information on these features, see:

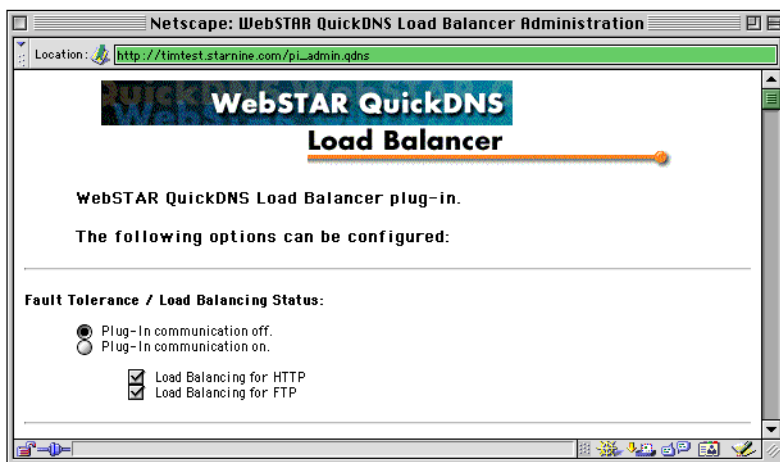
<http://www.starnine.com/quickdns/ftlb.html>

QuickDNS Configuration Page

To configure the load balancing and intelligent fault tolerance settings, open the Browser Admin page for this Plug-In by typing

http://www.domain.com/pi_admin.qdns

(replacing `www.domain.com` with your server name).



HTTP Configuration

Plug-In Communication On / Off

To send messages to the QuickDNS Pro Server, select the communication “on” radio button. To disable communications temporarily, select the “off” button. If you are not planning to use the Fault Tolerance or Load Balancing features any more, remove the file from the *Plug-Ins* folder.

HTTP/FTP Load Balancing

These checkboxes allow you to specify whether the Plug-In should send messages for HTTP (Web) load balancing, FTP load balancing, or both.

If you uncheck both boxes, the QuickDNS Plug-In will continue to provide Fault Tolerance services.

QuickDNS Pro Server(s)

This Plug-In will communicate with up to four QuickDNS Pro servers. Enter their host names in these fields.

IP Port Number

If you have changed the port number used by the QuickDNS Pro Server from the default **523**, enter the new number here.

Access Code

Enter the unique access code for this server from the QuickDNS Pro Admin record.

Fault Tolerance Preferences for HTTP

These settings control how the Web server communicates with the QuickDNS server, indicating that it can still accept connections.

Contact... setting specifies how often this server connects to the QuickDNS server.

Direct fewer hits... tells QuickDNS to send fewer requests to this server after a certain amount of time without a contact.

Remove from list... tells QuickDNS Pro how long to wait after the last contact before removing this DNS server from it's DNS entry.

Load Balancing Preferences for HTTP / FTP

There are separate preferences for HTTP and FTP, but they have the same effect.



See also: “WebSTAR FTP Server” starting on page 337.

Note that you must fill in the Web Server name field to match the name in the QuickDNS Pro Server.

Dynamic load... radio button allows QuickDNS to calculate the amount of load this server should get based upon the amount of load it reports, in comparison with the other servers in the load balancing setup.

Fixed load preference value lets you specify how heavily the server should be loaded, within the set of servers. The minimum value of 1 means very few connections, the maximum of 10 means it should get many connections. This is very useful when one of the machines in the load balancing array is slower than the rest.

WEBSTAR REBOUND! ASSIST

Rebound! is a product from Sophisticated Circuits that plugs into the ADB port and automatically restarts the Mac in the event of a crash. And with the Rebound! Assist Plug-in, it can also restart the WebSTAR application without rebooting the machine. You only need this Plug-in if you are using the Rebound! hardware.

When WebSTAR is running, the WebSTAR Rebound! Assist Plug-In sets the User Timer to 5 minutes at one-minute intervals. Once set, the User Timer starts counting down to zero. As long as WebSTAR is running, the Plug-In will continue to reset the User Timer, so it will never reach zero.

If the User Timer ever actually reaches zero, it means that WebSTAR has stopped resetting it, usually due to a crash or freeze. Rebound! will then send an ADB restart command, which forces your system to restart. Assuming you have an alias to the WebSTAR application in your *Startup Items* folder, the server will automatically launch and start responding to requests.

If you have installed the Plug-In but you do not have the Rebound! hardware, you will see error messages in the Status Window Web Monitor pane. Remove the file from the Plug-Ins folder and restart the server to avoid this error message.



WebSTAR does **not** install the WebSTAR Rebound! Assist Plug-In by default. Use the WebSTAR Server Suite Installer to custom install it. It does not require any additional RAM.



WebSTAR does **not** install the WebSTAR Search Plug-In by default. Use the WebSTAR Server Suite Installer to custom install it. It does not require any additional RAM.

The WebSTAR Search Plug-In is always enabled, and will always be called by URLs ending in `.search`.



for instructions, see “Installation” starting on page 264. For a search form example, see “Search Examples” on page 264



for instructions, see “Indexing and Index Files” on page 266.

WEBSTAR SEARCH

The WebSTAR Search Plug-In allows visitors to search the contents of the files on your site. WebSTAR Search indexes text files (including HTML) and PDF files, and provides an interface for very fast and powerful searching, including Boolean operators, relevance ranking, results formatting, and more. WebSTAR Search is based on Apple’s Find By Content toolkit used in Sherlock (formerly known as “Apple Internet Access Toolkit”, “AIAT” and “V-Twin”).

How the Searching Works

Before you can search, you must have an **index**: a file which stores data about the files to be searched in a special format. WebSTAR search uses this index, rather than opening each file and checking its data, for speed and flexibility. The example files include an example index, which indexes data in the *Test Collections* folder. You can create your own index of your own data—if you have very large data sets, you can even create multiple indexes.

Once you have an index, you can access it by using a **search form** (an HTML form with an Action link to the index file) for the search. When a visitor types the search terms and clicks the “Submit” button, the browser sends a form action request to the WebSTAR server. Because the form URL suffix is `.search`, WebSTAR sends this request to the WebSTAR Search Plug-In, which searches the index for the requested terms, and returns the results in a formatted page.

About Search Queries

With WebSTAR Search, you can enter the words in your **query** in any order. The search engine will compare them to the data in the index: it will find all files with at least one of the search terms. When it returns the results, WebSTAR Search will automatically rank them from most relevant to least relevant.

WebSTAR Search performs a **vector search**, where every indexed document is stored in the index as a point in a multi-dimensional space (a **vector**), and the dimensions correspond to terms found in the body of all documents. Normal queries are then interpreted as very short documents, and are also converted into a vector. The search engine then looks at the index for all document vectors within a certain distance of the query vector. Thus, the more that your query resembles the documents you are looking for, the better your results will be. That’s why natural language queries, such as questions or

descriptions, work so well with WebSTAR Search. For example, you could enter the query:

```
improve performance of web server
```

and get back results ranked according to how closely they resemble that query.

Adding Boolean Operators to Searches

In addition to the vector searching, you can add Boolean operators to your searches, if you prefer.

- **&** (ampersand) used between search terms is the Boolean AND operator. It indicates that both terms must be in a document. This is very useful for getting a more relevant set of results. For example, to search for documents that mention both “Sherlock” and “Apple”, enter `sher lock & apple`
- **|** (vertical bar or pipe character) used between search terms is the Boolean OR operator. It indicates that either term can be in a document, for example, to search for documents that either “AIAT” or “Sherlock”, enter `aiat | sher lock`
- **!** (exclamation point) used between search terms is the Boolean NOT operator. It indicates that only documents matching the terms before the it and not matching the term after it should be matched. Again, this removes irrelevant results. For example, to search for documents that mention “Sherlock” but not “Holmes”, enter `sher lock ! holmes`

Grouping

Another way to control the query is to explicitly **group** the terms—control the order of processing

For example, you may want to link the terms “Sherlock” and “Apple” and ignore “Holmes”. So you can use the grouping brackets “[” and “]” to specify how the search should be grouped:

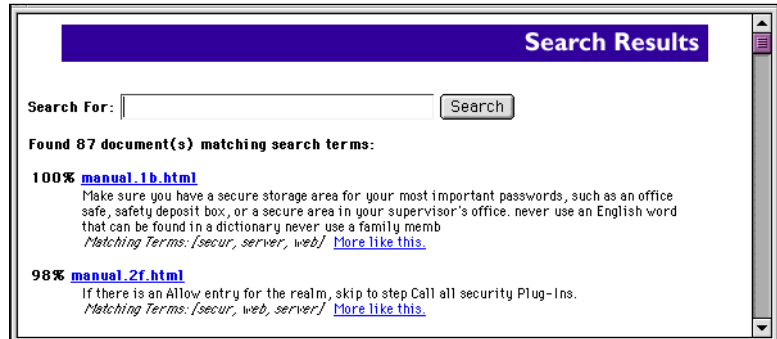
```
aiat | [[sherlock & apple] ! holmes]
```



The search engine uses special functions to improve word matching: see “Search Dictionaries” on page 269.

Search Results

WebSTAR search will automatically display formatted results of your search:



Note that the links for the results will take you to the beginning of the document containing the matched text. For an exact location, you must use the Find function of your browser.

Search Results Elements

- **Number Found:** displays the number of results which match. Note that if you do not specify a maximum number of results, WebSTAR Search will return no more than 10 matches.
- **Relevance Ranking:** the percentage number in the left column (100%, 58%, etc.) shows the how relevant the document is to your query. This number is calculated by the search engine.
- **File Link** the name of the matching document, with a link to the file itself. Acrobat files include the document title if there is one.
- **Summary:** For PDF documents which include Subject and Keyword fields, they are displayed here. For other files, the search engine computes the most important words and phrases from the document and displays them.
- **Matching Terms:** the query words which were matched in the document. If the word was converted by the Substitution Dictionary (for example “fallen” changed into “fall”), you’ll see the converted word here.
- **More like this:** WebSTAR Search and the search engine allow you to refine your search by using the document itself as a query string, to find similar documents. This works best for large collections of single-concept files.



See “Search Dictionaries” on page 269.

Customizing Results

The default setting will find only the 10 most relevant documents which have a relevance ranking of 50% or greater.

In the example, you'll see that the form includes options for the searcher to specify the relevance, along with the total number of results. In this case, WebSTAR Search will, by default, display 10 results per page and provide navigation links to go forward and backward, if there are more than 10 matches.

You can use the Search Parameters (described on page 271) in your forms and URLs to specify how many results, the relevance ranking, and how many to display per page. In addition, the section "Search Tags Using WebSTAR SSI" on page 270 describes how you can use SSI commands to display the results listings within your documents.

Search Result Resource

The default search result page is stored in a STR resource of the *WebSTAR Search* file. You can use ResEdit or Resorcerer to open that file and copy the HTML file in that file, edit it, and paste the changes back into the resource.

Before and after working on this file, make backup copies. You can also re-install the file using the Installer. When you update WebSTAR Search, the changed resource will not be transferred, so you'll need to copy it to the new file by hand.

Installation

When you choose WebSTAR Search from the Custom Install options, following items are installed in the *WebSTAR Plug-Ins* folder:

- *WebSTAR Search* (Plug-In)
- *WebSTAR Search Indexer* (application)
- *WebSTAR Search Data* (folder) containing the files described in "Search Dictionaries" on page 269.

WebSTAR Search automatically registers the ".search suffix". Make sure that all .search files are created by the WebSTAR Search Indexer application, and that they are always named with that suffix.

WebSTAR Search requires that the WebSTAR SSI Plug-In be installed.

Search Examples

The *Search Examples* folder in the *Tools & Examples* folder includes both simple and advanced example forms.

To try them out, follow these steps:

- 1 Launch the WebSTAR Search Indexer.
- 2 Click the **Create** button.
- 3 Leave the name of file *index.search*
- 4 Find the *Test Collection* folder in the *Tools & Examples* folder, *Search Example* subfolder.
- 5 Save the index.search file in that folder.
- 6 Use this folder as the root index search folder for this example.

Then open a browser window enter your host name and the path:

`/Tools%20%26%20Examples/Search%20Example/help.html`

When you do a search, you'll see a result list that looks like this:



WebSTAR Search Memory Issues

The Search Plug-In is very memory intensive. The exact amount of memory it requires depends upon the size of the index being searched, so large indexes may require more memory. To track

memory use, check the Status panel memory fields (described in “Memory” on page 79). Most of the required memory will be used during the first search performed, and will be retained by the Search Plug-In, rather than being released back to the WebSTAR server.

The performance of the WebSTAR Search plug-in will benefit from both increased memory in WebSTAR **and** a larger system disk cache (set in the Memory control panel).

Indexing and Index Files

WebSTAR Search uses **search index files**, which contain words from the designated files in a special format. The *Search Indexer* application (located in the *Plug-Ins* folder) builds, updates, and tests the index files.

Every index file is associated with a **search root folder** in the WebSTAR folder hierarchy. The Search Indexer will analyze and store data for all the text and PDF files within that folder and its subfolders in the index file. Indexing PDF files is a resource intensive process. Depending on the size of the PDF file, you may have to allocate as much as 20 MB or more to the Indexer. In addition, you should **not index encrypted PDF Documents**—make sure that all your documents are publicly-accessible.

Once you create an index, you should **update** it regularly. You can use the Search Indexer application, or have WebSTAR update your searches automatically (see “Search Plug-In Administration: Index Auto-Update” on page 271).

If you’re supporting several Virtual Hosts, you can have multiple index files on for your server, each containing separate data, starting from different root folders. That way, visitors searching for data from one web site will not accidentally get results from a different, unrelated site.

Search Index Security

Files created by WebSTAR, WebSTAR Admin, and WebSTAR Search (with Creator Codes of “wwwΩ”, “wwwx”, and “wsIx”) will not be indexed.

To avoid having a file indexed, move it out of the search root folder hierarchy, rearrange your folder hierarchy, or use an file resource editing application to change its Creator Code to “noIX”, which will indicate to the Search Indexer that this file should be skipped.

If you have security realms or confidential information in one of your indexes, name it carefully, and consider protecting it by using a



For instructions, see “Server Application Issues” on page 87.



WebSTAR Search Indexer **cannot** follow aliases: the original files must be in the search root folder or a subfolder.



Search Index Files cannot be moved: they must be generated on the disk and in the hierarchy in which they will be used.

security realm entry. That way, no one can search through it to find private data.

Creating A Search Index

To create a search index, decide which folder will be the **search root folder**. The Indexer will open and index all text and PDF files in this folder and its subfolders. For security, you should **not** make your WebSTAR root folder the search root. You should also index your secure realms separately from the public data. Limit your indexes to data folders, and merge them later if you want cross-folder searching.

i If you expect to use this application often, make an alias of it and put it in a convenient location.

- 1 Open the *Plug-Ins* folder and launch the Search Indexer application.



- 2 Click the **Create** button and set the name and folder for your search index. Note that all index names must end in the suffix `.search`, but you can customize the rest of the name. You can also choose **New** from the File menu to make a new index.
- 3 Once you have named the file, click **Save**.
- 4 Next, select the **search index root folder** for this index. Only files within this folder or a sub folder will be included in the index. In most cases, this will be a subfolder of the WebSTAR folder, especially if you're serving Virtual Hosts.

Be sure that there are no encrypted PDF documents in this folder hierarchy

- 5 The Search Indexer will open, analyze and index each text and PDF file within the root folder. It will not follow aliases to other files or folders. This may take several minutes, depending on the amount of data and the speed of the machine. It can operate, more slowly, in the background if you need to use the machine for other purposes.

If the indexer runs out of memory, just quit the indexer, increase its memory partition, launch it again, and **update** the index that was being built.

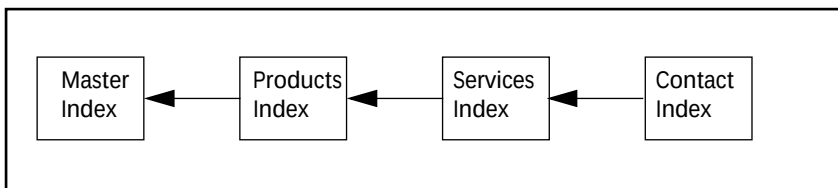
 See also "Web File and Folder Name Rules" on page 189.

- 6 Once done, you can choose the **Test** button to try out your index. Enter a query in the Test field and you'll see the same result as if you entered the data in a search form.

Once you have created your index, you can design search forms and links for your visitors: see “Web Tools For Searching” on page 269.

Merging Search Indexes

You can also use the Search Indexer application to merge index files together. You can use this to index only some subfolders of a site and search them as one:



To merge indexes:

- 1 Launch the Search Indexer
- 2 Choose **Open** to select and open the first index.
- 3 Click **Merge**, open the next index file, and wait while the application merges the second index file into the first.

Note that each index can only have **one** other index merged into it. Therefore, you must design an index chain of parent and child indexes, as shown above.

Updating Search Indexes

To keep your indexes synchronized with your files, you must update them periodically. Updating is much faster than indexing, because it just checks the root folder and subfolders, and adds new files, removes deleted file data, and re-indexes the data in files that have changed. Updating can run in the background without slowing down your server.

You can update a single index or a master index by using the Search Plug-In Administration: Index Auto-Update (described on page 271).

Otherwise, you'll have to update the indexes using the WebSTAR Search Indexer application or an AppleScript.

This example shows that you must include the exact path to the index file (you can copy it from the Indexer and paste it into your script):

```
tell application "WebSTAR Search Indexer"
    update "server HD:WebSTAR Server Suite:search:index.search"
end tell
```

Search Dictionaries

The Dictionaries installed in the *WebSTAR Search Data* folder, *Stopword Dictionary* and *Substitution Dictionary* provide lists used by the search engine in comparing queries with documents.



Dictionaries are optional, although very useful.

The Stopword Dictionary is just a list of words (one per line) that are never indexed or searched. These include single letters, HTML tags, and extremely common words such as “allow”, “is”, and “somewhere”. You can change this list and re-create your index to improve responsiveness and reduce inappropriate results.

The Substitution Dictionary helps the search engine match words and their various formats. For example, the past tense of “go” is “went”, but this would never be found in a direct comparison. This dictionary allows the index and search tools to make that kind of match.

The format of this dictionary is a list of words, one per line, where a substitution consists of a bullet, followed by a root word, followed by any number of words that should be reduced to that root.

```
•fall fell fallen
```

You can edit these files to change or remove entries, add more entries, and include text for languages other than English. Be sure to synchronize the index and the searching by re-creating your indexes if you change the dictionaries.

Web Tools For Searching

You can call WebSTAR Search in a number of ways: using HTML forms, search URL links, and WebSTAR SSI <Search> Tags.

Search Forms

To search an index, you must have an interface. The simplest interface is an HTML form. The easiest way to start making such a form is to copy the simple search form file from the *Tools & Examples : Search Examples* folder. For testing, just change the form action so that it refers to your index, for example:

```
ACTION="/widgets/widgets.search"
```

Once you have a form, you can open that page on your server and search your index.

The results of the search will be returned in the pre-defined page format. As you can see with the *advanced.html* form, WebSTAR Search will display 10 results per page, with page forward and back links, by default.

Search Form Error

If a visitor sees the message “The search parameters were not received, probably because you pressed Return instead of clicking on the submit button. Go back, and try clicking the button.”, it may also mean that there is no such index. To allow visitors to press the “Return” key in your form, move the “Submit” button out of the table. That way, all the browsers will do the right thing.

Search Links

You can set up URLs and links in pages that passes the query parameters in the search arguments section of the URL. For example, this URL:

```
http://www.domain.com/Tools%20%26%20Examples/Search%20Example/Test%20Collection/index.search?query=webstar
```

will search the example index for the word “webstar”, assuming you have created the index and you changed the host name from “www.domain.com” to your host name.

Likewise, the following link, in a file in the *Search Examples* folder, will search the Test Collections index for the query “web sever”:

```
<A HREF="http://Test%20Collection/index.search?query=web&20server">
```

Each link can also include parameters, as described below.

Search Tags Using WebSTAR SSI

WebSTAR Search works with WebSTAR SSI to give you more control over the search parameters and the location of the search result. You can set the query in an SSI variable and send that to WebSTAR Search, rather than having the user enter it.

You customize the search results page returned to the browser by creating your own SSI page that defines the desired format. Within this SSI page, a `<SEARCH . . .>` tag should be inserted at the point where the search results should be inserted. Note that the results are still formatted in the pre-defined layout.



Note that the space between “web” and “servers” is encoded (%20). You will have to make sure that all characters are encoded as part of the URL.



To be sure that your file will be processed by WebSTAR SSI, save it with the `.ssi` suffix.

For an example, see the *custom.html* and *custom.ssi* files in the Search Examples folder.

Search Parameters

The user may specify the several search parameters to the WebSTAR Search Plug-In. These parameters may be specified either via <INPUT> statements in an HTML form, as search arguments to a URL, or as tag parameters to the <SEARCH> tag handler.

Search Parameters List

PARAMETER	STATUS	USE
query	required	The question, description, or list of keywords that are to be matched against the documents in the index.
numdocs	optional default is 10	The maximum number of matching documents to return.
minscore	optional default is 50%	The minimum match score for documents that are to be displayed to the client. Scores range from 100% down to 0%, with 100% representing the best match.
To specify pagination of results		
firsthit	optional default is 1	Out of <numdocs> matching documents found by the plug-in, this parameter defines the first that is to be displayed to the client.
lasthit	optional default is 10	Out of <numdocs> matching documents found by the plug-in, this parameter defines the last that is to be displayed to the client.
For the <SEARCH> Tag only		
index	required	The path name to the index file to be used in the search. This path may be either a virtual path (e.g., /folder/index.search) or an absolute Mac pathname (e.g., Disk:WebSTAR Folder/folder/index.search).

Search Plug-In Administration: Index Auto-Update



See also "Updating Search Indexes" on page 268.

WebSTAR Search can automatically update the primary index and any merged indexes at specified intervals. This will take place in the background and should cause no problems to the server, unless you add many large files to a search folder hierarchy all at once. In that case, you should update using the Search Indexer application.

To enable automatic updating, follow these steps:

- 1 Use your web browser to locate the WebSTAR Plug-In Administration pages or use this URL (replacing “www.domain.com” with your host name):
`http://www.domain.com/pi_admin.search`
- 2 Type the Mac pathname to your primary index into the first text box. For information on the primary index, see “Merging Search Indexes” on page 268.
- 3 Click the checkbox to activate automatic updating of the primary index.
- 4 Type the number of hours (or days) between updates in the second text box.
- 5 Select the units (days or hours) for the update interval using the popup menu.
- 6 Click on the **Save** button.

WebSTAR Search will update the index based on the file modification date. For example, if the index file was modified at 11 AM on a Monday, and you set it update it every 7 days, it will always be updated at 11 am every Monday.

WEBSTAR WEBOBJECTS ADAPTOR

The WebSTAR WebObjects Adapter is used to connect a WebSTAR Web server to a WebObjects executable application. The WebObjects Adapter acts like a “traffic cop” routing requests to WebObjects executable applications running on other servers.

WebObjects can provide access to large databases, including legacy systems, mainframes and SQL interfaces, and it can do anything from general CGI processing to handling commerce transactions.

WebObjects executables are currently supported on the following systems: Solaris, Windows NT, HP-UX, and Mac OS X server. WebObjects executables cannot be run on a Mac OS 8.x server, although WebSTAR running on a Macintosh can provide the interface to browsers via the Web.

For information on WebObjects, see

<http://www.apple.com/webobjects/>

WebObjects Versions and Upgrading

WebSTAR WebObjects Adaptors come in two versions, to go with WebObjects 3 or 4. Be sure to install the WebSTAR WebObjects



WebSTAR does **not** install the WebSTAR WebObjects Adaptor Plug-Ins by default. Use the WebSTAR Server Suite Installer to custom install the version 3 or 4 Adaptor, depending on your needs. Neither version requires any additional RAM.

The WebObjects Adaptor Plug-In is always enabled when it is installed.

Adaptor that corresponds to the version of WebObjects you are running.

How the WebObjects Adaptor Works

At initialization time, the WebObjects Plug-In finds the configuration file (*WebObjects.conf*) in the Plug-Ins folder, and reads it into memory. This is the standard file used by all versions of WebObjects, and it must go in the Plug-Ins folder.

All WebObjects URLs will be passed to Web Objects. The requests include the following string:

```
/cgi-bin/WebObjects/
```

Any URL matching that string will be served as a WebObjects request.

A WebObjects **instance** is much like a DNS server's round-robin entry. It defines what goes where, meaning that the first request to a certain application can go to instance #1 and the second request can go to instance #2. This allows you to easily distribute the load to a particular WebObjects executables across several servers.

WebObjects Configuration

Entries in the WebObjects Configuration (*WebObjects.conf*) file look like this:

```
App1:1@W0Server1 2000 App1:2@W0Server2 2000 App2:5@W0Server1 2010
App3:6@W0Server3 2020
```

- “App1” is replaced with the name of the WebObjects executable application.
- The “:1” or “:2” is used to tell what instance of the application to use (see below).
- The “@” indicates that the application resides “at” the following server.
- “W0Server” is the name of the server, though it can also be an IP address.
- The “2000” and “2010” is the port number that the WebObjects executable is running on.

An example entry might look like:

```
taxform:1@tax.domain.com 2000
taxform:2@www.domain.com 2000
calc:5@test.domain.com 2010
```



WebSTAR installs the WebSTAR SSI Plug-In by default. It is a core Plug-In and you should **not** remove it. It does not require any additional RAM.

The WebSTAR SSI Plug-In is always enabled, and will always be called when the Action for a suffix is "SSI".



Plug-In Developers: see "Calling WebSTAR SSI" on page 463.

The WebSTAR **SSI (Server-Side Includes)** Plug-In allows you to use special commands in your HTML pages to display dynamic information to browsers and simplify the structure of your site. For example, you can display the current date and time, insert a standard header file into several different pages, show a counter displaying the number a times a certain page has been accessed, create a link to the referring page, execute CGIs and display the output, show or hide content based on a wide range of criteria, and more. All this, just by adding some SSI commands to your HTML pages.

WebSTAR SSI supports the standard NCSA SSI syntax used by many Unix servers. This is described at:

<http://hoohoo.ncsa.uiuc.edu/docs/tutorials/includes.html>

WebSTAR SSI extends the NCSA syntax and adds many other useful command. For a listing of command syntax, examples and reference, see "WebSTAR SSI Reference" starting on page 429.

You must use a file suffix to specify that the file will be processed by the WebSTAR SSI Plug-In. The default suffix for SSI files is .ssi, but you can configure WebSTAR to use another suffix, such as .shtml, or even .html to use SSI for all HTML files. For instructions, see "Suffix Mapping Example: Using SSI for All HTML Files" on page 160.

USING WEBSTAR SSI COMMANDS

The commands used by the WebSTAR SSI Plug-In take the form of HTML comments, which look like this:

```
<!-- this is a comment. -->
```

These comments do not show up in the browser, so a line like this:

```
Welcome to my site!<BR> <!-- Kilroy was here -->
```

will just appear in the browser as:

```
Welcome to my site!
```

Similarly, an SSI command is replaced with data or otherwise changed by WebSTAR SSI before being sent to the browser, so a line like this:

```
Today's date is <!--#echo var="date_local"-->
```

will appear in the browser as:

```
Today's date is 1997/12/25:01:01:57
```

WebSTAR SSI recognizes the `#echo` command and replaces it with the correct value before sending the page back to the browser. In this case, this command will always display the current local date and time whenever the page containing this line is requested by a browser.

SSI Command Structure

The general format for SSI commands is a command followed by a `tag="value"` pair, like this:

```
<!--#command tag="value"-->
```

and you must have at least one `tag="value"` pair in each command.

Examples include:

```
<!--#echo var="date_local"-->
```

which shows today's date,

```
<!--#include virtual="/header.txt"-->
```

which includes the contents of a file in the host root folder named "header.txt",

```
<!--#counter var="mycounter"-->
```

which increments a Counter Value (described on page 281).

- **command** tells WebSTAR SSI which action to take. For example, it can show or hide text, get file information, increment a counter, run a CGI, call a Plug-in Service, or include data from another file.
- **tag** specifies the kind of information that will follow.
- **value** points at the information specified by the tag. this could be the name of a counter, the date, or a file path.



You can also change the format of the date and time to something easier to read, by using the `#config` command: see "TimeFmt Tag" on page 293.



If you enter an unrecognized command, it's treated as an `#exec piservice` command. For more information, see "PIService Tag" on page 290.

Multiple Tags

Some SSI commands can include more than one tag, for example:

```
<!--#counter var="main_page_counter" display="true"-->
```

Here, the `#counter` command tells WebSTAR SSI to increment a counter variable, and the `var` tag tells it which counter ("main_page_counter"). Then the `display` tag tells it to set the display to "true", so this counter will appear in the page returned to the browser.

Special Characters in SSI Commands

Values used in `tag="value"` need to be surrounded by double-quote marks ("). WebSTAR SSI will automatically URL-encode anything within the double quotes, so you don't have to worry about spaces or Macintosh special characters. To use a value that has a double-quote as part of it, you can either use the URL encoding for it (Char les %22Rusty%22 Rahm) or double the quote (Char les ""Rusty"" Rham). The same applies to single-quotes (').

WebSTAR SSI is very flexible about spaces in commands: you can have as many as you like between the opening and closing comment marks and the actual command, though you must have at least one space before a tag. For example:

```
<!-- #command tag1 = "value1" tag2="value2" -->
```

is fine, while

```
<!-- #commandtag1 = "value1"tag2 = "value2" -->
```

is not, because there is no space before either of the two tags.

SSI Path Names: Virtual and File Paths

Several SSI commands, (the Include Command, FSize Command, FLastMod Command, and others), use paths to specific files on your hard drive. You can express these paths either using the tag **virtual** as paths using the URL-style paths or with the **file** tag using Macintosh paths.



SSI commands are not case sensitive: they treat upper and lowercase letters as being equivalent. This does not apply to field descriptors such as those for the TimeFmt Tag.

Virtual Paths

With the `virtual` tag, you can use paths like those in HTML links, with forward slashes ("/") to separate folder names. If the path begins with a slash, the **absolute** path will start at the host root folder, while if there is no slash at the beginning, the path is **relative** to the current file.

For example,

```
<!--#include virtual="/includes/navbar.inc"-->
```

will look for a file named *navbar.inc* inside a folder named *includes* in the host root folder. It is an absolute path.

The path in this command:

```
<!--#include virtual="includes/navbar.inc"-->
```

will look for a file named *navbar.inc* inside a folder named *includes* at the same level as the current file. It's a relative path.

If your page is served by a virtual host, the root (/) is at the top level of that host.

File Paths

With the `file` tag, you use Mac OS pathnames, where folder names are separated by colons (":").

File paths can **only** be absolute (they must start with the hard drive name). For example, this path:

```
<!--#include file="Mac HD:WebSTAR:includes:navbar.inc"-->
```

would include a file using the full path from the hard drive. You must include the entire path name when using file paths.

When you use file paths, you can serve data that is outside your WebSTAR folder hierarchy. Be careful when you do this, both for security and because it's harder to track and control files in other folders.

Aliases

WebSTAR SSI will resolve the alias, and attempt to load the data in the original file to which the alias points. It will treat the file as though it



Neither of these path formats allows you to use a Unix-style double period ('. .') to go up one folder.



The file path can have either standard Macintosh characters, or URL-style encoding (%20 for space, for example).

was in the alias location. However, if the original file cannot be found (perhaps because it's on an unmounted volume), your server will **not respond** until someone goes to the server machine and mounts that volume.

Error Handling

If for some reason WebSTAR SSI encounters an error while processing your SSI commands, it will replace the SSI command with an appropriate error message inside an HTML comment. If your commands are not working as expected, use "View Source" in your browser to see these error messages. If you see the original SSI command, your Suffix Mapping is probably set incorrectly; if you see an error message, there is likely a syntax error in the SSI command you were trying to use.

You can also replace these default error messages with your own using the `#config` command, described in "ErrMsg Tag" on page 293.

SSI Command Example

This example shows how to display today's date in the default format:

```
Today's date is <!--#echo var="date_local"-->
```

which looks like this in the browser:

```
Today's date is 1997/10/27:11:52:15
```

- `<!--` begins the comment
- `#` begins the SSI command
- `echo` is the SSI command meaning "display" (see below)
- `var` is the SSI **tag**, specifying that the value is a variable
- `"date_local"` is the **value** for the variable. In this case, it's an **SSI environmental variable**, always available for the date and time in your time zone.
- `-->` ends the comment

To make the date easier to read, you can add a time format configuration command on the previous line

```
<!--#config timefmt="%B %d, %Y"-->
Today's date is <!--#echo var="date_local"-->
```



See also: "SSI Command List" on page 280; for more information on environmental variables, see "SSI Environmental Variables" on page 431; to reformat dates, see "TimeFmt Tag" on page 293.

will change the date format, then display the current date in the new format:

```
Today's date is October 27, 1997
```

SSI COMMAND LIST

The valid SSI commands are listed below, with explanations of what they do and how to use them. For a handy reference to these commands and some of the values they use, as well as how they differ from the standard NCSA SSI syntax, see “WebSTAR SSI Reference” starting on page 429.

For examples of the SSI commands in action, see the *SSI Demo* in the *Tools & Examples* folder.

Echo Command

The `#echo` command displays a named value in your page. Examples of the available values include the name of the browser requesting the page, the current date, or the URL of the referring file. A typical `#echo` command might look like this:

```
<!--#echo var="http_user_agent"-->
```

which will display the name the current browser uses to identify itself in your page; it might look something like this.

```
Mozilla/4.03 (Macintosh; I; PPC, Nav)
```

Echo Tag: Var

The only tag for the `#echo` command is `var`, meaning “variable”. It can have multiple “`var`” tags, to display more than one variable in a single command.

Echo Environmental Variables

You can use it to display the wide range of environmental variables used in the NCSA SSI syntax. These include the file’s local path, URL, and last modified date; the date and time; browser’s IP address, and more. For example,



See also: “Additional SSI Features and Options” starting on page 298.



`#echo` extends the NCSA SSI syntax.



For a list of variables, see “SSI Environmental Variables” starting on page 431.



You can also display WebSTAR API parameters (otherwise used by Plug-Ins). For a list of these, see “WebSTAR API Parameter Definitions” on page 455.

```
<#echo var="last_modified"-->
```

will display the last modified date for the current HTML file. See “TimeFmt Tag” on page 293 for instructions on changing the time and date format.

Echo Special Variables

There are also a few special values that can be displayed with the #echo command:

Counter Value

The #echo command can display counter variables, such as page-access counters (see “Counter Command” on page 284). Once you have set up counters, you can display them on any page. For example, if you have set up a page-access counter named “main_page_counter”, you can use this command to display the current value:

```
<!--#echo var="main_page_counter"-->
```

Random Value

```
<!--#echo var="random"-->
```

will show the current random number. This is a number between 1 and 99, which is generated automatically the first time WebSTAR SSI encounters this variable on a page.

You can generate new random numbers on the same page and change the range of the random value: for more information, see “NewRandom Tag” on page 295.

Stored Variable Value

WebSTAR SSI lets you store data in variables for a page or more globally (see “Store Command” on page 291). For example, if you have created a variable called “soup-of-the-day”, you can display the contents of that variable with the command

```
<!--#echo var="soup-of-the-day"-->
```

Echo WebSTAR API Values

WebSTAR SSI has also been extended to display any of the parameters available to Plug-Ins. Therefore, you can use an `#echo` command such as

```
<!--#echo var="piCurrentFreeMemory"-->
```

to display the current free memory available to the server. Other options include the host name of the server, the list of currently installed Plug-Ins, the current number of connections, and more. These variables are described in “WebSTAR API Parameter Definitions” starting on page 455.

Include Command

The `#include` command inserts another file into the current page. This feature is extremely useful for displaying standard headers and footers in your pages, or any other elements that are common on multiple pages. Should you need to make changes, you only need to edit a single included file (instead of editing each separate page) to have the change reflected on every page that includes that file.

For example, to include a file named *header.txt* from the host root folder, you could use this command:

```
<!--#include virtual="/header.txt"-->
```

The `#include` command handles aliases automatically, so if you indicate the name of an alias, the file to which the alias points will be served.

See “SSI Path Names: Virtual and File Paths” on page 277 for information on file path formats.

Include Command Security

The `#include` command is powerful, but it can be misused. If your server allows many people to upload HTML files, someone might use this command to get access to files that should remain private. Therefore, this command is **disabled** by default.

The WebSTAR Admin and browser administration page “*pi_admin.ssi*” both contain options to enable the `#include` command, limited to the *ssi* folder in the *cgi-bin* folder; or to remove the limits entirely.

 `#include` extends the NCSA SSI syntax to use file path tags as well as virtual paths (see page 277).

 See also: “#Exec and #Include Command Security” on page 153.

If you choose to limit `#include` access to the *cgi-bin:ssi* folder, you can make aliases of files referred to in your SSI commands in that folder, and store the aliases with your HTML files. This system allows you to keep the logical organization of your site, and make simpler file paths. WebSTAR SSI will resolve aliases and allow you to include those files if the originals are in the safe folder.

FSize Command



`#fsize` extends the NCSA SSI syntax to use file path tags.

The `#fsize` command displays the size of a named file. For example,

```
<!--#fsize virtual="/disasters/report5.html"-->
```

will show the size of the *report5.html* file in the *disasters* folder in the host root folder.

FSize Tags: File and Virtual

The tags for this command are the path tags “file” and “virtual” as described in “SSI Path Names: Virtual and File Paths” on page 277.

By default, the file size is displayed in bytes, but this can be changed with the Config Command, using the SizeFmt Tag (described on page 294). For example, the commands:

```
<!--#config sizefmt="abbrev"-->
<!--#fsize virtual="wsman.pdf"-->
```

will display the file size of the *wsman.pdf* file in K (kilobytes) instead of bytes.

FLastMod Command



`#flastmod` extends the NCSA SSI syntax to use file path tags.

The `#flastmod` command displays the last modified date of a named file. For example:

```
<!--#flastmod virtual="/disasters/report5.html"-->
```

will show the last modified date of the *report5.html* file.

The tags for this command are the path tags file and virtual; see “SSI Path Names: Virtual and File Paths” on page 277 for an explanation of how they work.

By default the date format is set to look like this:

1997/12/25:01:01:57

You can change this format with the Config Command: for information, see “TimeFmt Tag” on page 293.

Counter Command

Use the `#counter` command with a counter variable to increment that variable each time the page containing that `#counter` command and variable is requested by a browser. For example, the command

```
<!--#counter var="juan's counter" display="true"-->
```

will create a new counter variable named “juan's counter” the first time a page containing the command is requested. Then it will add one to its value every time the page is requested after that. The display tag is set to “true”, so the command will also display the current value of the counter variable in the browser.

Counter variables are ***persistent variables***, stored in the *WebSTAR SSI Settings* file. You can view, edit or delete your counters on the browser administration page as described in “Editing Counters and Numeric Variables” on page 297. Browser access to pages stored in caches and proxy servers will not be counted except when the cache is refreshed.

You can display a page access counter, if you think your viewers would be interested, or hide it and just use it for your own internal statistics.

Advanced Counter Features

You can refer to the same counter variable on several pages, and the variable will be updated every time one of these pages is accessed.

This lets you use the `#counter` command to create a counter that keeps track of the number of times a group of pages has been accessed. You may want to keep an individual counter for each page as well, just by using another unique counter variable name.

You can use the same `#counter` command more than once on the same page, which will increment the counter variable by one for each separate command. Therefore, if you repeat the command three times on the same page, each repeated entry will display a number one higher than the previous entry, and the counter variable will increase by three every time that page is accessed.



To display the last modified date of the current HTML file (without requiring a path) see the example in “Echo Command” on page 280.



`#counter` is not part of the NCSA SSI syntax: it is a WebSTAR extension.

Counter Tags: Var and Display

The **var** tag is used to specify the name of the counter variable. When WebSTAR SSI encounters a `#counter` command, it will first look for an existing counter variable with this name, and will create a new variable if it does not find one. Each time the command is accessed, the named counter variable is incremented by one.



You can use several `var` tags in one `#counter` command to increment multiple counters.

Counter variable names can be up to 32 characters long, and can contain any characters you like, so you can be very descriptive, for example:

```
<!--#counter var="main_page_counter"-->
<!--#counter var="Counter for Marc & Luke's page"-->
```



Possible values for the `display` tag are "true", "on", or "yes" to display the current value, and "false", "off", or "no" to stop the value from being displayed.

The **display** tag is optional, and controls whether the current counter value is shown in the page or not. If you don't include a `display` tag entry, the counter value will appear automatically.

For example, the line:

```
Number of hits so far: <!--#counter var="big hits"-->
```

might look like this in the browser:

```
Number of hits so far: 814
```

However this line:

```
Number of hits so far: <!--#counter var="big hits" display="false"-->
```

will not display the current counter value because the `display` tag is set to `false`. The counter named "big hits" will still be incremented by one, but the number will be invisible.

```
Number of hits so far:
```

Hide and Show Commands



`#hide` and `#show` are not part of the NCSA SSI syntax: they are WebSTAR additions.

The `#hide` and `#show` commands allow you to turn on or off the display of sections of your HTML pages depending on certain circumstances. You can specify text to appear only for certain

browsers, hide page content from those outside specified IP addresses, display messages based on the current date, and more.

Anything after a `#hide` command will be hidden from the browser until WebSTAR SSI encounters a `#show` command further down the page that will allow the rest of the page to be displayed again.

Most `#hide` and `#show` commands are based on a **condition**—they are executed only if circumstances as defined by the operator tag are true.

For example, the following command will prevent the rest of the page from displaying if the browser's IP address contains "192.168.0":

```
<!--#hide variable="remote_addr" operator="contains" value="192.168.0"-->
```

For those IP addresses, the text after this command will be hidden unless there is a `#show` command further down in the page.

Combining #hide and #show commands

Since the `#hide` and `#show` commands turn the display off or on, you will usually have to combine several of these commands to get the behavior you want. For example:

```
<!--#hide-->
<!--#show operator="contains" value="192.168.0.2"-->
Hi Grandma! I'll be up for the holidays!<BR>
<!--#show-->
```

The first `#hide` command turns off the display completely. The `#show` command following it will then turn the display on only if the browser's IP address contains "192.168.0.2," and show the line of HTML below this command. The final `#show` command turns the display back on for all browsers. If this page is accessed from a computer with an IP address of 192.168.0.2, this section of the page will appear as:

```
Hi Grandma! I'll be up for the holidays!
```

This will be hidden from browsers coming from any other IP address; they will never know this part of your HTML page existed.

Hide and Show Tags: Variable, Operator and Value

The tags for the `#hide` and `#show` commands are `variable`, `operator`, and `value`.



For more information about conditions, see "operator (op)" on page 287.

Tags are optional for these commands. If the #hide and show tags are used without any tags, as in:

```
<!--#hide-->
```

```
<!--#show-->
```

anything following the command will always be hidden or shown.

The following tags can be combined to create your #hide and #show commands.

variable (var)

This tag can be used with any of the variables that the var tag for the #echo command has access to, including current random number, counter variables, and stored variables, SSI Environmental Variables and WebSTAR API Parameters. See “Echo Command” on page 280 for more information.

operator (op)

This tag defines the ***condition***. It specifies how you are comparing the variable named with the variable tag to the value named in the value tag. It is optional, and defaults to “=”, meaning that the values must match exactly.

Operators for Show and Hide Commands

OPERATOR TAG	MEANING
"contains" or "con"	variable contains the value string
"starts with" or "start"	variable starts with the value string
"ends with" or "end"	variable ends with the value string
"=" or "=="	variable equals the value string
"!=" or "<>"	variable does not equal the value string
"<"	variable is less than the value string (usually used for numbers)
"<=" or "<="	variable is less than or equal to the value string (usually used for numbers)
">"	variable is greater than the value string (usually used for numbers)
">=" or ">="	variable is greater than or equal to the value string (usually used for numbers)

value (val)

This tag is the value that you are comparing the variable named with the variable tag to; it is also optional and defaults to "" (an empty string).

Examples of #hide and #show

Show a message after a certain date:

```
<!--#hide -->
<!--#show var="date_local" op=">" value="1998/02" -->
<B>It is now after February, 1998</B>
<!--#show -->
<BR>
```

Show a message one time out of 100:

```
<!--#hide var="random" op=">=" value="1" -->
<B>You've won a free T-shirt!</B>
<!--#show -->
<BR>
```

More examples of the #hide and #show commands in action can be seen in the *SSI Demo* files installed with WebSTAR in the *Tools & Examples* folder.

Exec Command

The #exec command lets you call a CGI application or a WebSTAR API service routine registered by a Plug-In, and insert the results into your page.

For example, this command:

```
<!--#exec script="/cgi-bin/ssi/greeting.cgi"-->
```

which will run a CGI named *greeting.cgi* in the *ssi* folder inside the *cgi-bin* folder in the WebSTAR root folder. It might return a random welcome message out of a list of several greetings.

If there are any additional SSI commands in the result returned by the CGI or Plug-In, WebSTAR SSI will execute those as well. The final text will appear in the HTML page in place of the original command.

The #exec command handles aliases automatically, so if you indicate the name of an alias, the file to which the alias points will be served.

 #exec is implemented according to the NCSA SSI syntax, and adds some WebSTAR-specific tags.

Exec Command Security

The `#exec` command is powerful, but it can be misused. If your server allows many people to upload HTML files, they could use this command to run applications that are not public. Therefore, this command is **disabled** by default.



See also: “#Exec and #Include Command Security” on page 153.

The WebSTAR Admin and browser administration page “`pi_admin.ssi`” both contain options to enable the `#exec` command but limit it to the `ssi` folder in the `cgi-bin` folder, or to remove the limits entirely.

If you choose to limit `#exec` access to the `cgi-bin:ssi` folder, you can use aliases of files in there. This allows you to keep the logical organization of your site, and make simpler file paths. WebSTAR SSI will resolve aliases and allow you to include those files if the originals are in the safe folder.

Exec Tags: Script, CGI, PIService

There are three main tags used with the `#exec` command, ***script***, ***cgi***, and ***piservice***, which can also take other associated tags. Other optional tags extend this functionality.

Script Tag

The `script` tag is meant for use with stand-alone CGIs which are called directly (usually applications that have a `.cgi` or `.acgi` suffix), such as AppleScript CGIs. It specifies the file path to the CGI and can use Virtual Paths or File Paths.

CGI Tag

The `cgi` tag is meant for use with CGIs which rely on a Suffix Mapping to execute the actual CGI application, such as Frontier scripts (which usually have a `.fcgi` suffix) or Tango documents (which usually have a suffix of `.qry`). Instead of using the CGI name, the `cgi` tag specifies the path to a file or script name with the suffix used by the CGI, then looks up the correct Action in the Suffix Mapping Table and executes the appropriate CGI. This works as though WebSTAR had received a URL request for that file.

For example, the command:

```
<!--#exec cgi="/special/action.tpl"-->
```

will find the Suffix Mapping entry for `.tpl` then launch the WebCatalog CGI and pass the file path “`special/action.tpl`” as a

parameter. The WebCatalog CGI will process the information and return the results to WebSTAR SSI, which will insert the results into your HTML page in place of the original command.

Post Tag

Both script and cgi tags can use the optional post tag to pass information to the CGI. For example,

```
<!--#exec script="/cgi-bin/ssi/chocolate.cgi"
      post="20pounds"-->
```

will call a CGI named *chocolate.cgi*, pass it the value "20pounds", and return the resulting text.

PIService Tag

The piservice tag allows you to call a WebSTAR API service routine that is defined by another WebSTAR API Plug-In. An optional **param** tag can specify any parameters that need to be sent to the service routine. For example,

```
<!--#exec piservice="TextConverter"
      param="italic"-->
```

would look for a registered Plug-In service routine named "TextConverter", pass it a parameter of "italic", and insert the results into your HTML page.

In addition, WebSTAR SSI will expand all unknown commands to "#exec piservice=" so this command:

```
<!--#TextConverter="italic"-->
```

is converted to the piservice command above.

For information about Plug-In service routines, see the WebSTAR API SDK or your Plug-In's documentation.

Tag ="Value"

You can also use any named tag="value" pairs instead of the post or param tags. However, if any post or param tags are present, these tag="value" pairs will be ignored.

For example, this command:

 Plug-In Developers: you can register a Plug-In service routine with WebSTAR SSI: see "Calling WebSTAR SSI" on page 463.

```
<!--#exec cgi="destructo.xml" name="joe" return="true"-->
```

which will collect the values as "name=joe&return=true" and send them off, URL-encoded, in the post arguments parameter to the CGI that handles the "xml" suffix.

Store Command

The #store command permits you to store your own variables for later access by other SSI commands. The command looks like this:

```
<!--#store mammal="wombat" kind="shared"-->
```

which will create a new variable named "mammal" and set its value to "wombat".

Store Tags: Variable Names

The main tag for the #store command is a variable name, consisting of letters, numbers and/or underscores, of up to 33 characters, followed by the value for that tag. The following example will store this text in the variable famous_opening_lines:

```
<!--#store famous_opening_lines="Four score and seven years ago..."-->
```

You can also use the optional kind tag, which controls how long this variable is available. Possible values for the kind tag are

- local: makes the variable available only on the current page
- shared: will save the variable until WebSTAR is shut down
- persist: stores the variable in the *WebSTAR SSI Settings* file in the *Plug-Ins* folder, and makes it available to all SSI commands.

If no kind tag is specified, the default setting is "local".

If you give a persistent stored variable a numeric value, it will be displayed in the browser administration page along with the counter variables. See "Editing Counters and Numeric Variables" on page 297 for more information on editing these variables.

PostArg Command

The #postarg command lets you display named variables that have been sent to an SSI page from an HTML form.



#store is a WebSTAR SSI special command.



#postarg is a WebSTAR SSI special command.

For example, if you have a simple form like this:

```
<FORM METHOD = "POST" ACTION = "showme.ssi">  
  Name: <INPUT TYPE = "text" NAME = "your_name" SIZE = "20"><BR>  
  INPUT TYPE = "Submit" VALUE = "submit form">  
</FORM>
```

It will look like this in the browser:



You can create a page named “showme.ssi” and include the SSI command:

```
Hello, <!--#postarg var="your_name"-->!
```

If a person opens the first page and types “Mahalia” and clicks the Submit button in their browser, WebSTAR will use WebSTAR SSI to automatically display the “showme.ssi” page and the text:

```
Hello, Mahalia!
```

PostArg Tag: Var

The var tag specifies the name of the form variable to display. It should be the same as the value of the HTML form set by "NAME" for the input field you want to display. In the example above, it's “your_name”.

Config Command

The #config command controls the options and output format of several of the other SSI commands. For example, this command:

```
<!--#config sizefmt="abbrev"-->
```

will change the file size output unit to kilobytes instead of bytes. A #config command usually precedes another SSI command that depends on the format change. All #config changes are only applied to the current page.



#config is implemented according to the NCSA SSI syntax, and adds some WebSTAR-specific tags.

Config Tags

Errmsg Tag

WebSTAR SSI, when it encounters an error, automatically inserts an invisible error message as an HTML comment.

You can use the errmsg tag to override this and display a message. You may find this particularly useful during debugging.

If you use a command like this at the top of your pages:

```
<!--#config errmsg="WebSTAR SSI encountered
an error">-->
```

any errors will display the text “WebSTAR SSI encountered an error” in your page.

■ TimeFmt Tag

The timefmt tag lets you change the way that date and time is shown. The default format is

```
"%Y/%m/%d:%H:%M:%S"
```

which looks like this: "1997/12/25:01:01:57".

This coding, consisting of a percent sign (%) followed by a single letter code, is replaced by an element of the date or time. All other text and punctuation is retained. For example, %Y is always replaced by a four-digit year.

If you don't like the default format, you can use the timefmt tag to change it. For example, this command:

```
<!--#config timefmt="%A, %B %d, %Y"-->
<!--#echo var="date_local"-->
```

will change the date format, then display the current date in the new format:

```
Tuesday, March 08, 1998
```

You can also show or hide text using the new time and date format produced by the timefmt tag, as in this example:

```
<!--#config timefmt="%B"
```



For a complete list of time format codes, see “SSI Field Descriptors for TimeFmt” on page 433.

```
<!--#hide-->
<!--#show var="date_local" op="contains" val="Friday"-->
I'm glad it's Friday! <BR>
<!--#show-->
<!--#config timefmt="%Y/%m/%d:%H:%M:%S"-->
```

will change the date format so it gets the day of the week, then if the day of the week is Friday, uses the `#hide` and `#show` commands to show the line “I'm glad it's Friday!”, and finally sets the date format back to its default value.



See also: “operator (op)” on page 287.

SizeFmt Tag

The `sizefmt` tag controls how file sizes are displayed. It can only have two values, “bytes”, which displays the size in bytes (this is the default setting), and “abbrev”, which displays file size in kilobytes. For example,

```
<!--#config sizefmt="abbrev"-->
<!--#fsize virtual="mainpage.html"-->
```

will change the file size output format to kilobytes, then display the file size of the *mainpage.html* file in the new format, as “47 K”, instead of the old format, as “47152 bytes”.

CharSet Tag

The `charset` tag lets you to select a character set translation to perform on that page. Options are

- “normal”—no character translation at all; this setting should be used for multi-byte character sets, like Kanji.
- “latin 1 (ISO-8859-1)” —converts all special characters in the ISO Latin1 character set into the correct HTML escape sequences.
- “ascii”—converts characters to the 7-bit ASCII character set.

Therefore, the command

```
<!--#config charset="normal"-->
```

at the top of your page will turn character translation off for that page.

The default setting is set in the WebSTAR Admin or the browser administration page at “*pi_admin.ssi*”. For more information, see “Default Character Set” on page 152.

NewRandom Tag

SSI has a random variable, containing a number from 1 to 99, used by the #hide, #show and #echo commands. It is generated for every new page. The #config command using the newrandom tag lets you specify the range that the random number can be in, and generate a new random number. The command looks like this:

```
<!--#config newrandom="11"-->
```

which will generate a new random number whose value is between 1 and 10, inclusive.

The value used for the newrandom tag can be any integer between 2 and 10000, which WebSTAR SSI will use to generate a new random number between 1 and the value of newrandom minus 1 (inclusive). The newly generated random number will then be available as the "random" variable.

For example, these commands

```
<!--#echo var="random"--><BR>
<!--#config newrandom="5000"-->
<!--#echo var="random"--><BR>
```

will display the original random number, then change the random number to one between 1 and 4999, and display a new random number.

SSI Troubleshooting

If the SSI commands on your pages are not being processed at all, chances are something is wrong with your Suffix Mapping. The WebSTAR SSI Plug-In is probably never "seeing" the file, and thus never and getting a chance to act on the SSI commands contained in it. See "Suffix Mapping" on page 154 for more information.



Inclusive means that it could be 1, 10, or any number in-between.

SSI Administration & Security

There are a number of options you can set using WebSTAR Admin SSI (described on page 152).

SSI

Default Character Set

☐ Normal (No character translation)

☒ Latin 1 (ISO-8859-1)

☐ 7-bit ASCII

Data Caching

☒ On

☐ Off

Enables Server-Side-Includes (SSI) processing to take advantage of Data Cache, if installed.

#EXEC and #INCLUDE Commands

WARNING: Unrestricted use of the #exec and #include commands may compromise server security in some situations.

☒ Disable commands

☐ Restrict use of commands to /CGI-BIN/SSI/

☐ Allow unrestricted use of commands

To open the browser administration, use a URL like this:

`http://www.domain.com/pi_admin.ssi`

(replacing the name `www.domain.com` with your host name).

You can use the interface here to configure counters, choose the character encoding, and specify the level of security.



For information on the character set, see “Default Character Set” on page 152 and the Config command CharSet Tag (described on page 294).

SSI Security

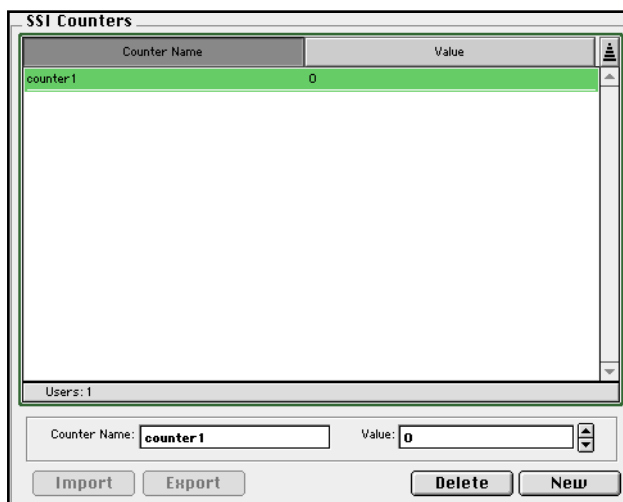
While WebSTAR SSI is extremely powerful, it has some security implications. The “include” and “exec” commands let you include other files and run other programs. However, if you allow other people to upload files to your server, they could then use these commands to act without your knowledge. These security options help you restrict access and limit your vulnerability. To understand your options, see “Exec Command Security” on page 289, “Include Command Security” on page 282 and the WebSTAR Admin section “SSI” starting on page 152.

Editing Counters and Numeric Variables

The WebSTAR SSI Plug-In allows you to create and save page-access counters and other variables (see “Counter Command” on page 284 and “Store Command” on page 291).

WebSTAR Admin SSI Counters

You can create and change values in the WebSTAR Admin SSI Counters panel:



This will update as your data changes from page views and so on.

Browser Admin SSI Panel

For numeric variables, you can also see and change the values on the Browser Administration page, “pi_admin.ssi”. For example, if you’ve accessed the *ssi_demo.ssi* file, you’ll see something like this on the Browser Admin page:

The existing COUNTER values are shown below:

counter1	0	☐ Delete
count1	1	☐ Delete
count2	3	☐ Delete

You can edit or delete these values, and the WebSTAR SSI Settings file will be updated when you click the Save button.

Counters and other variables can only accept numbers. If you enter spaces, letters or punctuation, your change will not be saved: the old number will reappear after you save the changes.

SSI and File Suffixes

To allow WebSTAR SSI to process the special SSI commands in your HTML pages, you must set up a Suffix Mapping in WebSTAR that tells the server to use the “SSI” Action for the files you choose.

The WebSTAR SSI Plug-In automatically registers an “SSI” Action and a Suffix Mapping for `.ssi` that uses this action, so that any file ending in `.ssi` will be handled by the WebSTAR SSI Plug-In. For information, see “Suffix Mapping Example: Using SSI for All HTML Files” on page 160, and “Actions” on page 161.

You can indicate that you want to use SSI commands in other files. For example, if you want to use SSI commands in all files ending in `.html` (a common suffix for pages which use server-side-includes), you can enter a Suffix Mapping that looks like this:

```
SSI .HTML * * text/html
```

This tells the WebSTAR Web server to call SSI for all entries ending in `.html`, for any type or creator code, and to return the MIME type “text/html”.

The WebSTAR SSI Plug-In takes advantage of WebSTAR Data Cache (if installed) and caches files. Thus SSI-processed files may actually be served out faster than uncached files served directly by the Web server.



See also: “Suffix Mapping Example: Using SSI for All HTML Files” on page 160.

Additional SSI Features and Options

- All values in command arguments (i.e., any quoted value) will be URL-decoded before being further processed by SSI.
- The number and size of command arguments in SSI commands is unlimited except where noted (the 32-character limit for variable names in the `#counter` command, for example).
- Values that contain double quotes should either double the double quote character, or use the URL encoding (`%22`), like

```
<!--#exec script="hi.cgi" post="Charles ""Rusty"" Rahm"-->
```

or

```
<!--#exec script="hi.cgi" post="Charles %22Rusty%22 Rahm"-->
```

- You may “nest” SSI commands inside command arguments by enclosing them in single quotes, like this:

```
<!--#counter var = '<!--#echo var="remote_address"-->' -->
```

which will first replace the #echo command with the client's IP address, then create or increment a counter variable with that IP address as the name. Commands in single quotes will be processed before the enclosing commands.

As with double quotes, any values that contain single quotes (') should either be doubled or should use the URL encoding (%27) instead of the single quote character.

- Any unrecognized command will be converted internally to an #exec service call, so a command like

```
<!--#zoink tag="value"-->
```

will be interpreted as

```
<!--#exec pIService="zoink" tag="value"-->
```

See “PIService Tag” on page 290 for more information.

WEBSTAR SSI-WEBINCLUDE

WebSTAR SSI-WebInclude is a WebSTAR Plug-In that adds functionality to the WebSTAR SSI Plug-In, allowing it to dynamically include parts of remote web pages into your web pages. WebInclude introduces two new HTML-like tags. The <WEBINCLUDE> tag retrieves HTML pages from a remote web site and merges them into the current SSI input stream. The <TAGEXTRACT> tag extracts specific images, tables, etc. from HTML text (usually HTML returned via <WEBINCLUDE>). Most relative URLs in the text returned by <WEBINCLUDE> are automatically converted into the correct full URLs.

WARNING: By installing the WebSTAR SSI-WebInclude Plug-In you may compromise the security of your Web server. Make sure you read and understand the security implications described below before installing this software.

WebInclude Security

Even if you never use it, installation of the WebSTAR SSI-WebInclude plug-in could compromise the security of your Web server, or other servers at your location. The problem is that all HTTP requests that are made by HTML files including the SSI-WebInclude tags are issued from **your** server, effectively masking the identity (i.e., the host name or IP address) of the person who is making the request. So servers that protect files from unauthorized access using a security mechanism,



WebSTAR does **not** install the WebSTAR SSI-WebInclude Plug-In by default. Use the WebSTAR Server Suite Installer to install it.

like WebSTAR's Allow/Deny, will see <WEBINCLUDE> requests coming from your server instead of the client's machine. If your server is allowed access, but the client is not, it is possible for the client to access confidential files via <WEBINCLUDE>.

Installation of WebInclude is **safe** whenever **either** of the following two conditions are met:

- 1 Only trusted people (such as the web site administrator) have the ability to add files to your web site.

If authors and other users can upload files to your site, they may use this feature to access other sites without permission.

- 2 Your Web server machine does not have unrestricted access to another Web server. If no other server is granting access to your server based on host name or IP address, then there is no way for someone else to abuse that access via the <WEBINCLUDE> command.

WebInclude is smart enough to ignore <WEBINCLUDE> commands that reference the same server (that is, when both client and server IP addresses are the same). The real danger is to other servers in the same domain, or other web sites being serviced by the same server (via virtual hosts), which allow other local machines access to their data. Thus, WebInclude may pose the greatest danger to your web site, when it installed on another server in your own domain!

To protect your web site against unauthorized use of WebInclude, you may need to use WebSTAR's Allow/Deny security to deny access to any local hosts (or IP addresses) that have no business sending HTTP requests to your web site.



The <TAGEXTRACT> command does not have cause any security problems.

Legal Issues

Do not use SSI-WebInclude data from other sites without asking permission: assume that all data is protected by copyright. Even within an institution, there may be implications in republishing data of which you are not aware. Many informational and even commercial sites will happily give you permission to include and republish their data, but you should always ask first. If you include data without permission, the original publishers may just deny you access to the site, or they may sue you for copyright infringement.

Installation

The WebSTAR Installer does not install the WebSTAR SSI-WebInclude plug-in by default. After you have read the security section above, you can install it easily:

- 1 Open the WebSTAR Server Suite Installer and choose Custom Install / Server Suite / Plug-Ins / Extra Plug-In modules / WebSTAR SSI-WebInclude.
- 2 If the WebSTAR SSI plug-in is not already installed in your Web server's Plug-Ins folder, choose Plug-Ins / Core Plug-Ins / WebSTAR SSI as well.
- 3 Select your current *WebSTAR Server Suite* folder.
- 4 Click the Install button and proceed.
- 5 Quit and restart the WebSTAR application.

Using WebSTAR SSI-WebInclude

WebSTAR SSI-WebInclude defines two new HTML-like tags that conform to the conventional syntax.

<WEBINCLUDE> goes to a server and gets a web page, just like a browser or other HTTP client. For example, the following HTML page grabs and re-servers the WebSTAR home page:

```
<HTML>
  <HEAD>
    <TITLE>WebSTAR SSI-WebInclude Example</TITLE>
  </HEAD>
  <BODY>
    <WEBINCLUDE
      URL="http://www.starnine.com/webstar/webstar.html">
    </BODY>
</HTML>
```

The <TAGINCLUDE> tag can extract specific text or images from the retrieved HTML and display it as part of your page. You define which parts of the HTML you want to include by using the TAG and WHICH attributes of the tag.

the following example extracts the third graphic image found on page <http://remote.host.com/somepage.html> and inserts it into the SSI input stream:

```
<TAGEXTRACT TAG="IMG" WHICH="3">
  <WEBINCLUDE URL="http://remote.host.com/somepage.html">
</TAGEXTRACT>
```

Relative URLs in `<IMG SRC="...">`, `<A HREF="...">`, and `<BODY BACKGROUND="...">` tags in the downloaded page are automatically converted to the correct full URLs (using the provided or default `baseurl` value). If the text retrieved by `webinclude` contains other relative URLs, you must precede the `webinclude` command with an HTML `<BASE HREF="...">` tag.

Syntax Notes

The WebSTAR SSI plug-in is very forgiving about the blank spaces in commands. In general, zero or more spaces may appear between any two symbols inside the comment markers; but at least one space must appear immediately before any tag name. All commands, tags, and values are case insensitive (i.e., there is no difference between upper and lower case). Although tags are limited to 32 characters, value sizes are bounded only by available memory.

If for any reason an WebSTAR SSI-WebInclude command generates an error, the appropriate error message is generated within an HTML comment and will appear at the original position of the command. For example:

```
<!--#WEBINCLUDE ERROR: Remote url not found. -->
```

Usually, the values associated with tags are constant strings, and are thus surrounded by double-quotes ("). To embed double-quotes within a quoted value, simply double all internal quote marks (e.g., "This (") is a double-quote"). Alternatively, you can URL encode the value (e.g., "This (%22) is a double-quote").

It is occasionally useful to associate a dynamic value with a tag. Because WebSTAR SSI-WebInclude merely augments the functionality of WebSTAR SSI, this can be done by surrounding SSI commands with single-quotes ('). For example:

```
<WEBINCLUDE URL='<!--#echo var = "piRefererKeyword"-->'
```

All single-quoted text is processed by SSI **before** being used as an argument to the specified SSI command (in this case, `config`). As with double-quotes, to embed a single-quote in a single-quoted value, either double the embedded double-quote marks (e.g., "don't") or URL encode the quoted value.



Although this plug-in extends the functionality of SSI, **do not** use the SSI command syntax (i.e., `<!--#command ... -->`)

SSI WebInclude Commands

webinclude

The webinclude command accepts four arguments, although only `url` is required.

url

The complete URL of the file to download. Relative URLs will result in an error.

baseurl

The initial portion of a URL to be inserted into all relative URLs. If this optional argument is omitted, it will be automatically derived from the `url`.

xtra_header

Extra header text to be inserted at the end of the HTTP request header. Remember to end each line with `%0D%0A` (i.e., `\r\n`). This argument is optional.

strip_header

A value denoting whether or not WebInclude should strip the HTTP response header from the downloaded page. Allowed values for this argument are:

`true`, `false`, `yes`, `no`, `0`, `1`.

This argument is optional. The default value is **true**.

tagextract

The tagextract command extracts specific pieces of HTML out of a larger body of HTML text. For example:

```
<TAGEXTRACT tag="img" which="3">
  <WEBINCLUDE url="http://www.domain.com/">
</TAGEXTRACT>
```

would extract the third image tag (e.g., `<IMG SRC="http://...">`) from the domain.com home page.

The tagextract command accepts four arguments:

tag

the name of the HTML tag to extract from the enclosed HTML.

The tag argument is required. Specific extraction code is provided for the following HTML tags: `IMG`, `BR`, `LI`, `META`.

In addition, any HTML tag that has both an open (e.g.,) and close (e.g.,), tag may also be extracted: TABLE, A, TITLE, OL, UL, P etc.

which

a number that specifies which tag of the specified type to extract. This argument is optional, and defaults to **1**.

start

used with a tag value of "search", see below.

end

used with a tag value of "search", see below.

Both the start and end tags are optional.

FLAY

This special tag strips the outermost open and close tags from the enclosed HTML text. For example:

```
<TAGEXTRACT tag="flay">
  <A HREF="http://www.domain.com/">This is an anchor.</A>
</TAGEXTRACT>
```

would strip the <A . . . > . . . tags, leaving only the text This is an anchor . displayed in the client's browser.

SEARCH

This tag allows you to extract substrings from a body of text. Two special arguments called **start** and **end** are strings which should surround the text you want to extract. For example:

```
<TAGEXTRACT tag="search" start="the " end=" system">
  This is a test of the emergency broadcast system.
</TAGEXTRACT>
```

would extract the string "emergency broadcast", but not the start and end text enclosing it. If you want that text, just tack it on before and after, as follows:

```
the <TAGEXTRACT tag="search" start="the " end=" system">
  This is a test of the emergency broadcast system.
</TAGEXTRACT> system
```

Both the start and end arguments are optional.

Nesting TAGEXTRACT Commands

Due to the vagaries of HTML parsing, you must not nest multiple tagextract commands within each other. However, because this is a very useful thing to do, the WebInclude Plug-In gets around this limitation by registering 10 distinct tagextract commands with SSI, named: "tagextract", "tagextract1", "tagextract2", ..., "tagextract9". Thus, you may nest different tagextract commands within each other, as long as they all have distinct numbers. For example, to extract the third image from the second row of the first table from a web page at "http://www.starnine.com/", the following command structure could be used:

```
<TAGEXTRACT tag="img" which="3">
  <TAGEXTRACT1 tag="tr" which="2">
    <TAGEXTRACT2 tag="table">
      <WEBINCLUDE url="http://www.starnine.com/">
    </TAGEXTRACT2>
  </TAGEXTRACT1>
</TAGEXTRACT>
```

Extracting Nested HTML Tags

The tagextract command properly handles nested HTML tags. For example, suppose an HTML page contains two tables, and that each of those tables contains several nested tables. Then the following commands:

```
<TAGEXTRACT1 tag="table" which="2">
  <TAGEXTRACT2 tag="flay">
    <TAGEXTRACT3 tag="table" which="2">
      <WEBINCLUDE url="http://www.domain.com/">
    </TAGEXTRACT3>
  </TAGEXTRACT2>
</TAGEXTRACT1>
```

would first retrieve the page specified in the webinclude command. The innermost tagextract command (i.e., TAGEXTRACT3) would find the first table, skip over it and all of its contents (including any nested tables), and then extract the second major table on the page. The middle tagextract command (i.e., TAGEXTRACT2) would then remove the <table>, </table> tags from the extracted text. The outermost tagextract commands (i.e., TAGEXTRACT1) would then find the second table in the extracted text.

EXTENDING WEBSTAR SSI

Tag Registry

Other Plug-Ins can now register with WebSTAR SSI to process HTML or custom tags.

For example, a Plug-In that converted text to uppercase might register with SSI to handle a custom `<UPPERCASE>` tag. When WebSTAR SSI encountered a set of `<UPPERCASE>` and `</UPPERCASE>` tags in a page, it would pass the text between these tags to this Plug-In for processing, then insert the results into the page before sending it off to the browser.

WebSTAR SSI Extensions

WebSTAR SSI can also support Plug-In modules. An example, “SSI-WebInclude” is distributed on the WebSTAR CD and available from the StarNine web site. It allows you to include parts of HTML pages in your SSI pages, using URLs. Therefore, you can dynamically load data from any web site into your HTML pages.



Plug-In Developers: for information on writing your own SSI Extensions, see “Calling WebSTAR SSI” on page 463.

WebSTAR lets you publish your databases to the Web, automatically! Just open your FileMaker Pro database or ODBC data source, and follow the instructions below to make your data web-accessible. You can show the world the items in your catalogs, accept survey entries, or make a private area where your employees can check inventory records.

WebSTAR Lasso Publisher is the WebSTAR Plug-In that allows you to pass information between a FileMaker Pro database or ODBC data source and web pages served by WebSTAR. For example, you can create an online guest book that visitors to your website may use by filling out a form. The information from that form can then be placed in a database by Lasso when the user clicks the Submit button. WebSTAR Lasso Publisher can also make it easy to browse that guest book by taking a search query on a web page and performing that search on the database, then returning the results in the form of another web page. For more powerful and flexible database access, you can use a third-party database integration CGI or Plug-In, such as Lasso Web Data Engine from Blue World Communications.

In addition to database connectivity, WebSTAR Lasso Publisher also provides a set of useful non-database related tags that allow you to perform tasks like automatically emailing the contents of a form. To see a list of these tags, see the LDML 3.5 Reference Database, which is in the *Lasso Tools* folder.



The specific examples in this chapter will refer only to FileMaker Pro databases.

INSTALLATION

Use the WebSTAR Server Suite 4 Installer and choose **Custom Install** to install WebSTAR Lasso Publisher for the first time. Later on, if you upgrade your server, the installer will also upgrade WebSTAR Lasso Publisher.

You can place aliases to your databases in the *Lasso Startup* Items folder to have them automatically opened when WebSTAR is launched, if the WebSTAR Lasso Publisher Plug-In is installed.



WebSTAR Lasso Publisher is not designed to run at the same time as other versions of Lasso. If you choose to install any other version of Lasso, remove all WebSTAR Lasso Publisher files before installing Lasso.

Files Installed

- **WebSTAR Lasso Publisher:** a Plug-In module file that must reside in the *Plug-Ins* folder. WebSTAR Lasso Publisher will not operate if it has been moved from the *Plug-Ins* folder.
- **WebSTAR Lasso Publisher Data Folder:** contains important files: do not remove.

- **LassoCommonCode** library.
- **LDML Reference Database:** a searchable list of Lasso Dynamic Markup Language tags including usage examples and explanations, in the *Documentation* folder.
- **FM Link:** is a tool for authoring LDML code. It allows you to author LDML tags and drag-and-drop them into your drag-and-drop aware HTML editor. It is in the *Lasso Instant Publishing* folder in the *Tools & Examples* folder.



See also: “LDML (Lasso Dynamic Markup Language)” on page 313.

HOW WEBSTAR LASSO PUBLISHER WORKS

WebSTAR Lasso Publisher sits between WebSTAR and your database acting as an interpreter, sometimes called “middleware”, between web pages and databases.

When WebSTAR Lasso Publisher is invoked the following process occurs:

- 1 Using data from a form or a URL, a web browser sends a request for information from a database or provides data to be added to the database.
- 2 WebSTAR receives this request and passes it to the WebSTAR Lasso Publisher Plug-In.
- 3 WebSTAR Lasso Publisher takes the request and connects with the database to perform the requested search or create the new record.
- 4 When the database has finished, Lasso gathers the results and formats them as HTML. This HTML is passed back to WebSTAR.
- 5 WebSTAR in turn takes the results and sends them to the browser where they are viewed as a web page.

While the above scenario is somewhat simplified and does not touch on the vast capabilities of WebSTAR Lasso Publisher, it should give you a basic sense of WebSTAR Lasso Publisher’s role as web page to database interpreter.

WebSTAR Lasso Publisher vs. Lasso Web Data Engine

WebSTAR Lasso Publisher’s features are a subset of Blue World Communications’ Lasso Web Data Engine. Certain functions available in the Lasso Web Data Engine are not available in WebSTAR Lasso Publisher. The most prominent restrictions are listed below:

- 1 While WebSTAR Lasso Publisher can be used to add new records to a database and browse existing records, database records cannot be edited.



For a complete list of the tags supported, open the LDML Reference Database and click the **Lasso Publisher** button.

- 2 Records cannot be deleted from a database using WebSTAR Lasso Publisher .
- 3 Solutions that utilize the Lasso Java Application Programming Interface will not work with WebSTAR Lasso Publisher.
- 4 WebSTAR's realm-based security features must be used to control access to databases published with WebSTAR Lasso Publisher. The advanced security features available with the Lasso Web Data Engine are not available when using WebSTAR Lasso Publisher.
- 5 WebSTAR Lasso Publisher will only access three FileMaker Pro databases or one ODBC data source at any given session.
- 6 WebSTAR Lasso Publisher will only return the first 50 records in a found set.
- 7 WebSTAR Lasso Publisher supports a subset of the tags in Lasso Dynamic Markup Language (LDML).

The above restrictions are not imposed on the Lasso Web Data Engine, which is available directly from Blue World Communications at <http://www.blueworld.com/> or StarNine's online store at <http://store.starnine.com/>.

What You Need to Know

The remainder of this chapter deals with the technical aspects of invoking WebSTAR Lasso Publisher from forms and using Lasso Dynamic Markup Language (LDML) tags to format results. Before attempting to use WebSTAR Lasso Publisher, you should have a working knowledge of HTML, particularly HTML forms, understanding of what a WebSTAR Plug-In is, and understand how web pages are served by WebSTAR. If you are unsure of your skills in these areas, you will probably save yourself some frustration by honing those skills first then coming back to this chapter when you feel more confident.

HTML Editor Requirements

Some HTML editing programs may not be ideal for creating documents with LDML. LDML uses square brackets '[']' rather than the angle brackets '<' >' used in HTML. If your HTML editor does not recognize LDML tags, it may encode the square brackets into character codes. While WebSTAR Lasso Publisher is able to interpret LDML tags even when the brackets have been encoded, it can make your documents difficult to edit.

If you're using a graphical HTML editor, you should use the included FM Link tool to author your tags and take advantage of LDML's "Alternative Syntax". When this option is selected, FM Link embeds substitution, process, container, and sub-container tags within <LDML=...> objects as follows:

```
<LDML tag="Lasso_tag_here">
```



In FM Link, the alternate syntax option can be toggled using the Drag menu or the command-Y key combination.

PREPARING A DATABASE FOR WEB PUBLISHING

Before you publish a FileMaker Pro database using WebSTAR Lasso Publisher, there are a few steps you should take to help ensure that your database will perform to your expectations.

Security

If possible, do not use FileMaker password protection: you can use the WebSTAR Realm security to limit access to the database from the Web. If you must have a password, make sure that the database opens with a default password that allows complete access to the database. WebSTAR Lasso Publisher cannot enter database passwords.

Likewise, don't use FileMaker's access restrictions, as they can interfere with the web publication.



If you need more security, the Lasso Web Data Engine provides many more security options.

Create a Layout

Make a layout specifically for web publishing. This layout should contain **only** the fields you wish to use on the web. Don't bother dressing up the layout with fancy graphics, colors or formatting; they won't show up on the web pages and could hinder performance.

Name your web publishing layout without spaces, punctuation or special symbols. A good name for this layout would be "Web" or "CGI"; avoid names like "Layout #2".

Open in Browse Mode

After you've created your layout, open database and display the layout you just created in Browse mode.

Using FileMaker Pro Server

If you wish to publish a database that is being served by FileMaker Pro Server, it is possible. Using a regular copy of FileMaker Pro installed on the same computer as WebSTAR, open the database as a guest of

FileMaker Pro Server. Under normal conditions, this approach will perform about as well as running the database directly on the web server computer.

TCP/IP Access

For best performance, access the FileMaker Pro Server database via TCP/IP. In this case, we strongly recommend that you password-protect your database(s), to prevent unauthorized access. Refer to your FileMaker Pro documentation for instructions on sharing databases via TCP/IP.

INSTANT WEB DATABASE PUBLISHING

Instant Web Database Publishing allows you to publish your databases on the web with just a few clicks. You don't have to write any HTML or LDML code at all. Just follow these steps to put your databases on the Web!

- 1 Open your FileMaker database.

If you don't want to use your own databases, open the CDs.fp3 database in the Lasso Tools folder.

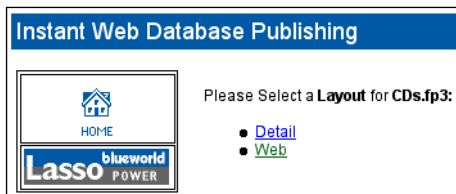
- 2 The instant web publishing documents are located in Tools and Examples folder in the WebSTAR folder. Using a web browser, open this URL:

`www.domain.com/Tools+&+Examples/Lasso+Instant+Publishing/`
(substituting your server host name for `www.domain.com`).

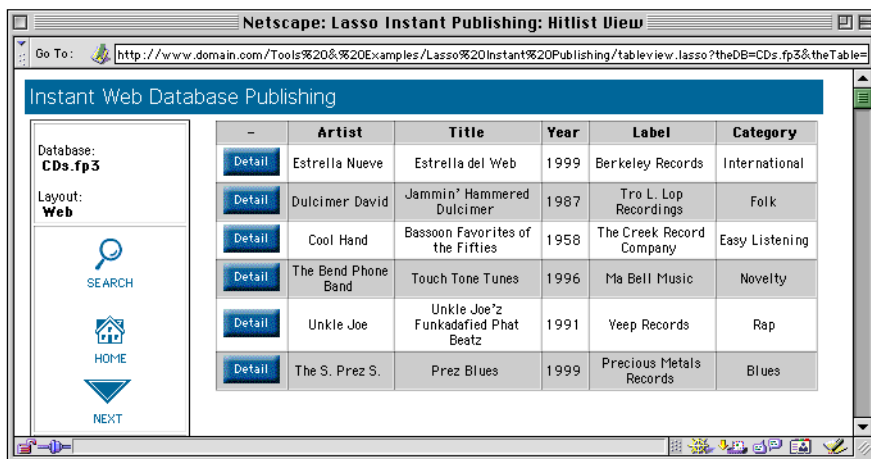
- 3 Click on the picture to start the publishing process.
- 4 Select the database you wish to access:



- 5 Select the layout you prepared in the previous section:



- 6 That's it! You're in business. The records are presented in a table format with each table row corresponding to one record.



You may now browse the records of this database, search for specific records, and add new records.

While this format is fine for internal publication of small databases with a few fields, you may need something more sophisticated. The following sections describe how to set up complex database search and information pages.

CUSTOM WEB DATABASE PUBLISHING

Custom web database publishing with WebSTAR Lasso Publisher gives you complete control of your database's web interface. You can create web pages that display information from your database, allow users to search the database, and allow users to create new database records. Using LDML tags in your HTML web pages, you have complete control over the look and functionality of your database's web interface, freeing you from the predetermined functions of Lasso Instant Web Database Publishing.



LDML is an entire “Markup” language, so this chapter will just provide an introduction.

LDML (Lasso Dynamic Markup Language)

LDML is a group of tags that, when embedded in your HTML documents, allow database information to be dynamically displayed. LDML tags can also send commands to WebSTAR Lasso Publisher to do things like creating new database records using information entered into a form on a web page.

WebSTAR Lasso Publisher includes the *LDML 3.5 Reference Database*, which contains every LDML tag with a description of each one and many usage examples. You'll find it extremely helpful to have this database open to refer to while you're developing your Lasso solutions. The WebSTAR installer automatically installs the *LDML 3.5 Reference Database* into the *Documentation* folder.

Action Tags

An **action** tag sends an instruction to the database requesting that a certain action be taken. Things like adding a record and searching are actions. In LDML, actions are preceded by a - (dash). In this example:

```
<input type="Submit" name="-Add" value="Add Record">
```

the -Add action takes the form of a Submit button that directs the database to add a new record using the data in that form.

Command Tags

Command tags contain parameters for an associated action. For example, the -Add tag above is useless if you haven't told Lasso which database the record should be added to. So somewhere in the same form as our -Add example above should be a command like this:

```
<input type="Hidden" name="-Database" value="CDs.fp3">
```

Using the -Database command tag, Lasso now knows which database the new record should be added to.

Substitution Tags

Substitution tags act as place holders in your documents where information from a database is filled in. The most common substitution tag you'll encounter is the [Field] tag. In a Lasso format file, the tag [Field: 'Artist'] is replaced with the actual data from

the database field named “Artist” in the database, when the page is sent to the web browser.

Container Tags

Container tags are pairs of tags in the traditional HTML `<tag> . . . </tag>` style. LDML container tags, however, use square brackets. One example is `[If] . . . [/If]` where conditional statements can be used to show different results in different situations.

LDML Syntax Notes

Like any language, LDML has some specific syntax rules that must be adhered to. Action and command tags are always preceded by a - (dash.) Substitution and Container tags appear inside square brackets. Values that appear inside a tag must be inside single quotes. These are just three of the most commonly encountered syntax rules. For a complete list, open the *LDML 3.5 Reference Database* and click on the **Tag Info** button.

FM Link

Use FM Link to avoid typographical errors in your LDML code. When layout and field names appear in LDML, they must **exactly** match their database spellings. If you use FM Link when writing LDML tags, you avoid spelling and syntax errors. Because FM Link communicates directly with your database to obtain layout and field names, you can be confident that your LDML tags are error free.

CREATING A SEARCH FORM

Now that you have an overview of what LDML is, we’re going to step through the creation of a form that will search the included *CDs.fp3* database.

Required Tags for a Search

When creating a web page that can be used to search your web enabled database, you must use certain action and command tags. Our example database will be the *CDs.fp3* database that can be found in the *Tools & Examples* folder.

Search Example

Below is an example form with the minimum tags required for performing a search. Each line of the form is discussed in detail.

```
<form method="post" action="action.lasso">
  <input type="hidden" name="-Database" value="CDs.fp3">
  <input type="hidden" name="-Layout" value="Web">
  <input type="hidden" name="-Response" value="hitlist.html">
    Artist: <input type="text" name="Artist"><br>
    Title: <input type="text" name="Title"><br>
  <input type="submit" name="-Search" value="Search">
</form>
```

Line 1:

```
<form method="post" action="action.lasso">
```

This is a standard HTML form tag. The important part for this discussion is the action attribute, `action="action.lasso"`. When you installed WebSTAR Lasso Publisher, it automatically installed Action and Suffix Map entries within WebSTAR to redirect "action.lasso" forms and URLs to Lasso.

Line 2:

```
<input type="hidden" name="-Database" value="CDs.fp3">
```

This command tag tells Lasso that the information contained in this form is intended for the *CDs.fp3* database.

Line 3:

```
<input type="hidden" name="-Layout" value="Web">
```

Similar to the above command tag, you must tell Lasso which database layout to access.

Line 4:

```
<input type="hidden" name="-Response" value="hitlist.html">
```

This command specifies which page is to be returned when the search is completed. If the file is in the same folder as the form page you're working on, you only need to enter the file name. If the file is in any other folder, you'll need to use standard HTML paths (see "Example Hierarchy and File Paths" on page 186).



For *hitlist.html*, see "Displaying Search Results" on page 318.

Lines 5 and 6:

```
Artist: <input type="text" name="Artist">
Title: <input type="text" name="Title">
```

These are standard text input fields. It is important to put the **exact** name of the field you wish to search on in the name attribute.

Line 7:

```
<input type="submit" name="-Search" value="Search">
```

Now that you've told Lasso which database and layout to use, what page to return with the results, and which fields to search on, the -Search action tells Lasso to perform the find. Whatever text you place in the value attribute will become the Submit button's text.

Line 8:

```
</form>
```

Standard HTML, this tag closes the form.

Other Important Tags

Before deploying a search page, there are some tags that should be included in your form even though they are not strictly necessary.

-AnyError

The -AnyError tag tells Lasso which page to return in the event of an error. In a form, it looks like this:

```
<input type="hidden" name="-AnyError" value="error.html">
```

When Lasso encounters an error, it returns the error.html document instead of the document specified in the -Response command.

-NoResultsError

Sometimes a user will perform a search that yields no matches in the database. Lasso allows you to return a special page when these circumstances occur.

```
<input type="hidden" name="-NoResultsError" value="noresults.html">
```

In the above example, when a search has no results, Lasso returns the *noresults.html* document. You can put a search form, along with useful hints and tips on this page.



If they are on the same page, -AnyError always takes precedence over -NoResultsError.

-MaxRecords

This command specifies how many records will be displayed on the response page. For example, if your search results in 30 matches, you may want to show the matches ten at a time. Setting the -MaxRecords to 10 tells Lasso you only want to see your results ten at a time.

Users of your site may appreciate the ability to choose their own value for this feature. Below is the HTML you would use to give them a pop-up list.

```
<p>Show me
<select name="-MaxRecords">
<option value=5>5
<option value=10>10
<option value=15>15
<option value=20>20
</select>
results per page.</p>
```

Search Operators

Operators (sometimes called **Boolean Operators**) are commands for searching. You can specify how search terms should be interpreted by FileMaker on the back end, to define which records from the database match the search.

For example, say you've typed Bass into the Artist field of the search form and Hits into the Title field. If you are doing a logical AND search, the database will only return records that contain **both** Bass in the Artist field **and** Hits in the Title field. If you do a logical OR search, the database will return every record with **either** Bass in the Artist field **or** Hits in the Title field.

Because our *CDs.fp3* database has one record each for "Bass Man Floyd, *Rock Bottom Hits*" and "The Vallejo Lifestyle, *Super Hits of the 70s*" the AND search would only return the "Bass Man Floyd" record, while the OR search would return both of them, because they both have the word "HITS" in the title.

-LogicalOperator

In Lasso, the command to tell the server what you want is -LogicalOperator, which can have a value of and or or. In the example code below, it is controlled by a set of radio buttons:

```
<input type="radio" name="-LogicalOperator" value="and">And
<input type="radio" name="-LogicalOperator" value="or">Or<br>
```



DISPLAYING SEARCH RESULTS

Search results (also known as *hits*) are those records which match the search terms and operators. Once FileMaker does the search, you need a way to send the data from the matched records back to the browser and show them to the user. You do this by setting up a page in HTML which stores placeholders for the data from the database, and shows it when the search is complete.

When you first created a search form, one of the required tags was -Response where the page containing the results of a search was specified. In the example above, this page is called "hitList.html".

Listing the Matched Record Data

There are two important Lasso tags for formatting the results of searches and showing the data in the results page.

The [Field] Tag

The [Field] tag is a substitution tag, a place holder where data from a particular field is inserted. The name of the field you wish to display must be specified.

```
[Field: 'Category']
```

When Lasso processes a page with the tag above, the data in the Category field of the current record will be inserted in place of the tag. It's OK if your field names have spaces, as the WebSTAR Lasso Publisher Plug-In will replace the field name with the text from the field before sending it to the browser.

 The [Field] tag cannot be used by itself to display images stored in FileMaker Pro container fields. For more information about displaying images from a container field, please refer to the [Image] tag in the *LDML 3.5 Reference Database*.

The [Records]...[/Records] Container

This `hitlist.html` page displays a list of records that match the terms searched on using the search form. Because some searches will result in one or two matching records, while others may have dozens, we need a way to specify what information we want to be displayed for each matching record and let Lasso handle displaying the actual data. The `[Records]...[/Records]` container is used to achieve this. Take a look at this example:

```
<p>
Your search found the following matches:<br>
  [Records]
    [Field: 'Artist']: [Field: 'Title']<br>
  [/Records]
</p>
```

Lasso will repeat everything between `[Records]` and `[/Records]` once for each found record. As you can see, the page lists the artist name, a colon, and the title.

Your search resulted in the following matches:

Estrella Nueve: Estrella del Web
 Dulcimer David: Jammin' Hammered Dulcimer
 Cool Hand: Bassoon Favorites of the Fifties
 The Bend Phone Band: Touch Tone Tunes
 Unkle Joe: Unkle Joe's Funkadafied Phat Beatz

Navigating the Found Set

The next step is to set up links to navigate through hit lists too long to display on one page.

One of the parameters that a search form specifies is the maximum number of records to be displayed on a results page. This is done through the previously discussed `-MaxRecords` tag. But what happens if `-MaxRecords` is set to 10 and your search results in 25 matches? There must be a way to navigate past the first ten to see the next ten hits and the next five after that. LDML has a set of tags for this purpose.

[FoundCount]

Lasso substitutes the number of records in the found set for the [FoundCount] substitution tag. Regardless of how many records are currently displayed, the [FoundCount] value will always equal the found set of records in your database.

[Shown_First],[Shown_Last],[Shown_Count]

All three tags are substitution tags. [Shown_First] displays the record number of the first record displayed in a [Records]...[/Records] list. [Shown_Last] displays the record number of the last record displayed in a [Records]...[/Records] list. [Shown_Count] displays the total number of records displayed in a [Records]...[/Records] list.

Using the four tags introduced above, you can display useful navigational information to the user such as in this example:

```
<p>
Displaying records [Shown_First] through [Shown_Last] out of [Found_Count]
total found. ([Shown_Count] records displayed.)
</p>
```

[Shown_NextGroup]...[/ShownNextGroup], [Shown_PrevGroup]...[/ShownPrevGroup]

These two container tags will create a link to the next or previous set of matches. Any text or images you place between the opening and closing tags will be linked. When there are no previous matches to link to (such as on the first page of hits) Lasso will not display anything. Likewise, on the last page of hits, Lasso will not display anything in the [Shown_NextGroup] container. Here is some example code:

```
<p>
[Shown_PrevGroup]See Previous Page[/ShownPrevGroup]
 
[Shown_NextGroup]See Next Page[/ShownNextGroup]
</p>
```

Showing Details

Often, when presented with a list of matching records from a search, you'll want to see more details for an item on the list. The hitlist.html page (from the example on page 315) only displays the Artist and Title fields. For the user to see all the fields associated with

that record in the layout, you can create a `detail.html` page with `[Field]` substitution tags for all the fields on the layout.

[Link_Detail]

Using the `[Link_Detail]` substitution tag, Lasso can automatically link each record in the hitlist to the `detail.html` page. You must include `Layout` and `Response` attributes in the `Link_Detail` tag.

```
<p>
Your search found the following matches:<br>
  [Records]
  <A HREF="[Link_Detail: Layout='Web', Response='detail.html']">
  [Field: 'Artist']</A>:
  [Field: 'Title']<br>
  [/Records]
</p>
```

In the example above, the first name is a link to a page called `detail.html` where more information from each record can be viewed.

Displaying records 6 through 10 out of 12 total found. (5 records displayed.)

Your search resulted in the following matches:

[The S. Prez S.](#): Prez Blues
[The Vallejo Lifestyle](#): Super Hits of the 70s
[Bass Man Floyd](#): Rock Bottom Hits
[Jay Jay G.](#): Sounds of the Siren
[Shelob](#): Make Mine a Martini

[Previous Matches](#) [Next Matches](#)

Creating a Detail Page

To show the details of a record, you simply create a regular HTML document inserting `[Field]` substitution tags wherever you want data from a field to show up. Before WebSTAR serves your page, the WebSTAR Lasso Plug-In will fill in the appropriate data from your database in place of the `[Field]` tags.

Keep in mind the proper syntax for field tags: [Field: 'field name here']. The text "field name here" should be replaced with the name of your database field, surrounded by plain single quotes. Spaces and spelling count here, so be precise when entering your field names.

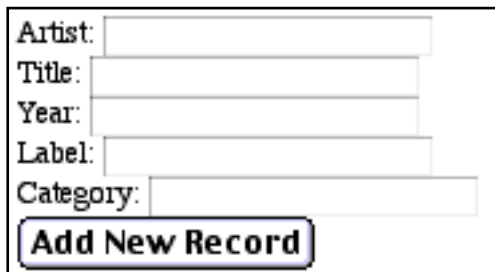
CREATING A FORM TO ADD RECORDS

You can use WebSTAR Lasso Publisher to allow users to add new records to your web-enabled databases. When creating such a form, you must use certain action and command tags. Our example database will be the *CDs.fp3* database that can be found in the Tools & Examples folder.

Add Record Example

Below is an example form with the minimum tags required for adding records. Each line of the form is discussed in detail.

```
<form method="post" action="action.lasso">
  <input type="hidden" name="-Database" value="CDs.fp3">
  <input type="hidden" name="-Layout" value="Web">
  <input type="hidden" name="-Response" value="added.html">
    Artist: <input type="text" name="Artist"><br>
    Title: <input type="text" name="Title"><br>
    Year: <input type="text" name="Year"><br>
    Label: <input type="text" name="Label"><br>
    Category: <input type="text" name="Category"><br>
  <input type="submit" name="-Add" value="Add New Record">
</form>
```



Line 1:

```
<form method="post" action="action.lasso">
```

As with any other form, the action attribute tells the web server how to handle the form. The "action.lasso" value ensures that WebSTAR will pass the form off to Lasso.



WebSTAR Lasso Publisher allows you to add records to your database, but not edit existing records. For that functionality, you need the Lasso Web Data Engine from BlueWorld.

Line 2:

```
<input type="hidden" name="-Database" value="CDs.fp3">
```

This command tag tells Lasso that the information contained in this form is intended for the *CDs.fp3* database.

Line 3:

```
<input type="hidden" name="-Layout" value="Web">
```

Similar to the above command tag, you must tell Lasso which database layout to access.

Line 4:

```
<input type="hidden" name="-Response" value="added.html">
```

This command specifies which page is to be returned after the new record has been added. You may specify a path to the file to be returned, however if the file resides in the same directory as the form page we're working on now, you only need to enter the file name.

Note that the response page does not require any Lasso tags on it. When you create that page, you can simply display a message telling the user their information has been entered into the database.

Lines 5 through 9:

```
Artist: <input type="text" name="Artist">
Title: <input type="text" name="Title">...
```

These are standard text input fields where the user enters the information that will comprise the new record. It is important to put the **exact** name of the field in the name attribute.

Line 10:

```
<input type="submit" name="-Add" value="Add New Record">
```

Now that you've told Lasso which database and layout to use, what page to return with the results, and what information is to be included, the -Add action tells Lasso to go ahead and make the new record. The value attribute becomes the button's text.

Line 11:

```
</form>
```

Standard HTML, this tag closes the form.

Other Important Tags

While not strictly required, the -AddError and -Required tags are very useful when adding database records.

-AddError

The AddError tag tells Lasso which file to display when there has been an error during an attempt to add a new record.

```
<input type="hidden" name="-AddError" value="adderror.html">
```

The error page that is returned does not need to have any LDML tags in it. It can simply be a regular HTML document containing a message that an error has occurred.

-Required and -ReqFieldMissingError

The -Required command is used to prevent a field from being submitted empty. To use it, place the command in a hidden field directly before the field you wish to require.

The -ReqFieldMissingError tag tells Lasso which file to display when a required field has been left blank.

Consider this example:

```
<p>
<input type="hidden" name="-ReqFieldMissingError"
value="reqfielderror.html">
Artist: <input type="text" name="Artist"><BR>
<input type="hidden" name="-Required">
Title:<input type="text" name="Title">
</p>
```

A user of the above form may leave the Artist field blank. However, if they leave the Title field blank, Lasso will return the *reqfielderror.html* page.

The error page that is returned does not need to have any LDML tags in it. It can simply be a regular HTML document containing a message that a required field has been left blank.

WEBSTAR LASSO PUBLISHER TROUBLESHOOTING

Errors can be caused by a variety of problems that may pertain to the database, configuration of WebSTAR, incorrect installation of WebSTAR Lasso Publisher, LDML coding errors, etc.

Installation

When you launch WebSTAR, WebSTAR Lasso Publisher and its various modules display their initialization status in the status window. When

WebSTAR Lasso Publisher is correctly installed and loaded, you should see the following lines displayed at startup:

```
WebSTAR Lasso Publisher: Loading Tag Modules
    Loaded " Lasso_Tags.mod" module successfully.
    Loaded "DB_Info_Tags.mod" module successfully.
WebSTAR Lasso Publisher: 6/5/1999 5:42:01 PM New Lasso Tag Parser is ON.
    Loaded "NewParser_On.mod" module successfully.
WebSTAR Lasso Publisher: Loading DataSource Modules
    Loaded "FM_DataSource.mod" module successfully.
    Loaded "Send_Mail_DataSource.mod" module successfully.
```

If you don't see these messages, check to see if another version of Lasso is installed. If not, try reinstalling the WebSTAR Lasso Publisher using the WebSTAR Server Suite Installer.

Debugging Errors

When Lasso encounters a problem it will return the error page you specified with the `-AnyError`, `-NoResultsError`, or `-AddError` tags.

To pinpoint what is causing the problem you're experiencing, place the substitution tag `[Error_CurrentError]` on your error page. Lasso will insert the specific error name in place of the tag when the error page is displayed. Armed with that information, you can efficiently target your troubleshooting efforts.

GOING FURTHER

Advanced Topics

WebSTAR Lasso Publisher is capable of much more than this introductory chapter is able to cover. Using LDML, you can display data from related databases, display pop-up menus automatically populated with the contents of a FileMaker Pro value list, and use conditional statements to intelligently tailor the information that gets displayed to the user based on a variety of conditions. The best place for learning about advanced LDML tags is in the *LDML 3.5 Reference Database*.

The LDML 3.5 Reference Database

Included with WebSTAR Lasso Publisher is a copy of the LDML 3.5 Reference Database. This is a searchable list of every tag in the Lasso Dynamic Markup Language. Clicking the **Lasso Publisher** button on

the main screen will present a list of all the LDML tags that you can use with WebSTAR Lasso Publisher.

Each tag is described in detail with a usage example and cross-referenced where appropriate. You'll find it extremely useful to keep this database handy as you develop your Lasso-based solutions.

Online Help

Blue World has a full support area on their web site and the Lasso-Talk email discussion group is a community of Lasso developers assisting one another with questions and participating in conversations about the Lasso family of products. You may join the list or search the list archives if you have a question about Lasso or can't solve a problem. Visit Blue World's website at

<http://www.blueworld.com/lasso/>

Purchasing the Lasso Web Data Engine

If you find WebSTAR Lasso Publisher to be a useful addition to your website and would like to expand beyond the limitations it imposes, we invite you to step up to the Lasso Web Data Engine. This full version of Lasso does not impose the 3 database, 50 record restrictions, nor any of the other restrictions of WebSTAR Lasso Publisher. And, because it uses the same LDML tags, your existing pages will work without changes.

You can buy the Lasso Web Data Engine directly from Blue World Communications at <http://www.blueworld.com/> or StarNine's online store at <http://store.starnine.com/>.



The LDML 3.5 Reference Database lists every LDML tag, not just those supported by WebSTAR Lasso Publisher. Appendix C lists only WebSTAR Lasso Publisher supported LDML tags.



See also “How to Get Help” on page 106, “WebSTAR Debug Plug-In” on page 107 and “General Server Troubleshooting Guidelines” on page 108.



See “Index File Name” on page 131 and “Editing Suffix Mapping Table Entries” on page 156.



See “WebSTAR Plug-Ins” starting on page 235. For maximum performance and compatibility the core Plug-Ins (WebSTAR Admin, WebSTAR Byte Server, WebSTAR Data Cache, WebSTAR Log Archiver, WebSTAR SSI, WebSTAR Virtual Hosts) should always be installed.

This chapter helps you locate and fix problems with web serving.

Please note that updated information for all troubleshooting is available at <http://www.starnine.com/support/>.

WebSTAR crashes at its first attempt to serve a page

- **Bad Ethernet card.** Some older PCI-based Ethernet cards may not work correctly under Open Transport and may cause WebSTAR to crash upon receipt of the first connection. Contact the manufacturer to see if a driver or hardware update is available.
- **Poorly written Plug-Ins and CGIs** may cause the server to crash. This is especially true of Plug-Ins and CGIs that run as a Router, Filter or Preprocessor.

To determine if a Plug-In is at fault, launch the WebSTAR server with no Plug-Ins installed. If the server responds successfully to a request, try adding them back one at a time until the conflicting Plug-In is found. The WebSTAR server must be restarted each time you add a Plug-In back into the configuration. In severe cases, you may need to restart the server machine as well.

If you are using a CGI to handle the default Index File Name files, it may be causing the problem. In that case, change to a simple text file for testing.

If you have a CGI assigned to handle a particular suffix in the Suffix Mapping Table, test it by changing the Action to “BINARY”. If the CGI is at fault, it will no longer be called.

If you can reproduce the crash, you should install the WebSTAR Debug Plug-In (described on page 107). When the module causes the server to crash again, the WebSTAR Debug Log should contain useful information for StarNine. Send an email address explaining the problem, and the WebSTAR Debug Log, to support@starnine.com. Then be sure to remove the WebSTAR Debug Plug-In, as it makes the server substantially slower.

The Browser Admin URL returns “document contains no data”

- **Make sure that the WebSTAR Admin Plug-In and the WebSTAR Admin Data folder are correctly installed in the *Plug-Ins* folder.** For information, see “Installation” starting on page 29.
- **You don’t have the WebSTAR SSI Plug-In installed.** The browser-based administration pages require WebSTAR SSI (described on page 275).

Plug-In Problems

WebSTAR comes with various useful Plug-ins. In addition, Plug-In developers have created many third-party Plug-Ins to provide additional modules to WebSTAR.

If you have trouble with Plug-Ins, follow these steps:

- To activate **newly installed Plug-Ins**, you must quit WebSTAR and relaunch it.
- To confirm that files you wish to have processed by a Plug-In have the **correct suffix**, check the Suffix Mapping (described on page 154).
- Some Plug-Ins require additional RAM to be allocated to the server and **may not function without sufficient memory**. Consult relevant documentation.
- If a Plug-In has previously functioned correctly and is now failing to work, try **reinstalling the Plug-In**.

Plug-Ins load as part of the server at launch and are more likely to cause crashes than CGIs. If you can substitute a CGI for any of your installed Plug-Ins, it may help in determining which specific Plug-In is problematic.

There are often **3-way conflicts**. Try running without any Plug-Ins or CGIs, then add them back in one by one (quitting and relaunching WebSTAR each time), until a culprit is discovered. Then try that Plug-In or CGI alone, to determine if it is problematic by itself or only in combination with others.

If **you've written your own CGI or Plug-In**, you may need to do some more debugging.

WebSTAR Plug-Ins

- **Auto BinHex isn't working.** For files to be auto-binhexed, they must be in a folder that contains a text file named ".message". Also, make sure that the URL to the file ends with ".hqx". Additionally, this Plug-In can be configured to limit auto-binhexing to files with specified suffixes, so check whether or not the desired file has an allowed suffix.
- **WebSTAR Byte Server does not appear to work when serving Acrobat PDF files.**
 - Follow the instructions for optimizing the Acrobat files and setting up the browser in "Example: Byte-Serving PDF files" on page 240.
 - HTTP "Range:" header requests will only be processed when the WebSTAR Byte Server Plug-In is installed.
- **Directory Indexer listings are not being displayed.**

In order for the directory index listing to be displayed for a particular folder, the folder must contain a text file named ".message".
- **WebSTAR File Upload isn't working.**
 - For file uploading to be allowed, the folder must contain a text file named ".upload".
 - Check the browser version: only some browsers support uploading via HTTP and HTTPS.



See "WebSTAR Auto BinHex" on page 238.



See "WebSTAR Byte Server" on page 240.



See "WebSTAR Directory Indexer" on page 241.



See "WebSTAR File Upload" on page 247.



See “WebSTAR Image Map” on page 253.



See “WebSTAR Form Mail” on page 249.



See “WebSTAR SSI” on page 275.

- If you are using an upload form, make sure that it has the correct folder path.
- Make sure that the file names are 29 characters or shorter. When they are longer, the browser error says that the request failed, and the log contains an entry “File Upload: Count not create upload file”.
- The Plug-In may be configured to disallow overwriting of existing files.

■ **Image Map isn't working.**

The image map must be in NCSA format, and the suffix must be “.map”. To test the Plug-in, try the image map files in the *Tools and Examples* folder.

■ **Form Mail form is not working** or the mail is not going through

- The Form Mail Plug-In only supports simple forms with 4 fields: To, From, Subject and Body. If your form is more complex, you will need to write your own CGI or use one of the 3rd party forms-to-files or forms-to-email products.
- you may have an incorrect form “action” or “method.”
- check the SMTP host information.
- the form must have both the To or From fields.
- the time-out value may be too short relative to the speed of your mail server.

Try the Form Mail example from the *Tools & Examples* folder to see if you have the Plug-In installed correctly. You can also use this as a model for your own Form Mail form.

■ **SSI isn't working.**

- Always view the source of the processed page to see what has been generated.
- Check syntax carefully.
- Be sure that your page has the correct suffix so that it will be processed by SSI. The default suffix is .ssi.
- When testing, remember that the file must be served through WebSTAR and SSI in order for the commands to be processed, opening it locally in a browser won't work.
- Try the SSI example from the *Tools & Examples* folder to see if you have the Plug-In installed correctly. You can also use this as a model for your own SSI commands.

Third-Party Plug-ins

- If you suspect a third-party Plug-In is causing trouble, take it out of the *Plug-Ins* folder and restart your server. The file must be out of the folder entirely, not stored in a subfolder within the *Plug-Ins* folder. If the symptoms go away, it was probably that Plug-In; contact the developer for support.

Web pages aren't being served correctly

- If the **pages serve correctly when you are using a browser on the same machine**, that indicates that WebSTAR is serving pages correctly. The problem may be with the TCP or browser settings on the client machine, your LAN, router, DNS or connection to the internet. Below are some suggestions for things to try to determine where the problem lies.

- Determine if the server machine can be seen over your AppleTalk network.
- On an internal network, the TCP/IP settings for all machines need to have the same setting for the "Connect via" field.
- Confirm that ethernet cables are installed.
- Determine if the server machine can see out to the Internet from a browser.
- Determine if the client machine can access other web sites.
- If you have changed the IP number on the server, this might necessitate reconfiguring and/or restarting your router.
- If you're not sure about your IP Address or host name, see "Identifying Your Site: IP, Host Name and DNS" starting on page 96.
- Try "pinging" the server using an application like MacTCPWatcher.
- Trace the packets using a tool for this purpose.

- **It works when I use my IP number, but not when I use my domain name.** That indicates that there is a problem with DNS.

Confirm registration of your domain with InterNIC, or the local DNS authority for your geographic region. Confirm your Domain-Name-Service from your upstream internet service provider or if you run in-house DNS, check the settings and confer with your network administrator.

- **My home page isn't being served**—I keep getting the WebSTAR default page instead.

Make sure that you have replaced *default.html* with your preferred home page. If you're using a different name, make sure you have the new file in the WebSTAR root folder, and have set WebSTAR to see the correct name.

- **Some default pages are not served:** pages named "default.html" work fine but those named "index.html" can't be found.
 - Check using the WebSTAR Admin Web Settings, File Names panel to make sure that you set the Default Names (described on page 130).
 - Make sure that *WebSTAR Data Cache Plug-In* and *WebSTAR Virtual Host Plug-In* are in the *Plug-Ins* folder. They are both necessary to allow multiple default page names.



To check or change the default index file names, see "Index File Name" on page 131.



You can set the Data Cache (described on page 140) to always check the file modification date while you are making changes.

- Request for particular pages return **“Document contains no data”**. This is usually because the file has a suffix which has an action that will be processed by a CGI or Plug-In, and the CGI or Plug-In is not configured or installed correctly.
- There may be material included in the page, such as Java or video images, which the client browser version doesn't support.
- **Check your HTML very carefully.** There are a number of utilities available for this. You can find some listed on the Extending WebSTAR pages at <http://www.starnine.com/extendingwebstar.html>.
- If the **page is being cut off midway through:**
 - There may be a problem with the file itself. Make sure there are no unmatched quotes or closing HTML tags. If you are using BBEdit, open the file and select ‘Zap “Gremlins”’ from the Edit menu.
 - If the page is not being processed by a Plug-In or CGI, and it has a different suffix (not .html or .txt), try setting the suffix entry to BINARY.
- **If you just modified the page**, make sure you have **flushed the cache** in WebSTAR after saving the modified file (Command-F in either the WebSTAR server or Admin applications). You might also want to clear the browser's cache or do a forced reload.
- **Misplaced links** are a common problem with WYSIWYG web page editors or if you've moved the site or reorganized folders. You may need to open the file in a text editor and change the links yourself. Some HTML editors let you specify a “root” folder as part of their preferences—if so, choose the WebSTAR folder.
- **My audio/video/Excel/etc., files are not serving correctly.** Any files which are not the standard types served by HTTP servers—HTML, GIF, JPEG—will usually require configuration on both the server and browser end.
 - For testing purposes, substitute a plain HTML file and see if it serves correctly.

If even a plain file does not serve correctly, carefully check the path to the file in your HTML.

If a plain HTML file serves correctly, check to see that there is a Suffix Mapping entry for the specific file type you are trying to serve.

If you can successfully serve the file from WebSTAR, and can correctly view/hear/open it with your own browser, it is more likely that the browser of the user who is reporting problems needs configuration, rather than the server.
- Requested pages return **“file not found” messages**. The usual cause for this is that the path specified in the HTML link to this file is

incorrect. Place the file directly in the root WebSTAR folder—then in your browser, open the location

```
http://www.domain.com/the-file-you-want-served
```

(replacing `www.domain.com` with your host name): does it work? If so, move the file to the location where you want it, and check your HTML to see that the path to the file includes all folders in the path.

If the file doesn't serve correctly upon a direct request while it is located in the root WebSTAR folder, you may have a more serious hard drive or file system problem. You should run a disk utility and rebuild the Desktop file.

■ Some **HTML files are truncated**.

- WebSTAR has no file size limit, but some CGIs or Plug-Ins may. If you have a special Action for that file's suffix, try serving the file with an action of BINARY. If that works, consult the publisher of the CGI or Plug-In to determine the limitations of the product.
- Some HTML files may have a NULL character (ASCII 0) in the text. This is an "end of file" character for many servers and clients: use BBEdit's Zap Gremlin's commands or otherwise make sure you have no control characters in the files.
- If you're getting **broken files**—flush the cache, Command-F in either the WebSTAR server or Admin applications.
- You have **Java files containing "\$"** in the filename, WebSTAR cannot serve those files. A "\$" as part of a URL is interpreted as something to be processed by a CGI or Plug-In. See "WebSTAR JRun Servlet Runner" on page 255 for more information on how to get your Java working.



See "Editing Suffix Mapping Table Entries" on page 156.



See "Web File and Folder Name Rules" on page 189.

Images served from WebSTAR are broken or cut off in the browser

- The **image files themselves may be corrupted**. Try opening the files locally in the browser, or in a graphics application, to make sure that they display properly.
- If you have specified an **exact size in your HTML**, make sure that the actual dimensions for the image file correspond to the size given in HTML code.
- If possible, **reduce the image file size**. Many images can be set to a web-compatible palette, compressed or otherwise shrunk. This allows visitors on slow connections to view the files properly.
- The **browser may not have enough memory** allocated to it, or it may have **corrupted cache** files. Try increasing the amount of RAM allocated to the browser, clear the cache or move the browser's cache folder to the Trash and restart the browser.
- **WebSTAR may not have enough connections** assigned for sending out data.

A page that contains text, 8 graphics and 1 background image will require WebSTAR to open 10 different connections if persistent connections is not



See “Connections” on page 88 and “Max Connections” on page 134.



See “Use DNS for Server and Client Lookups” on page 136.

enabled. The WebSTAR Web server is shipped with a default setting of 12 Max Connections. If your site is set for this default and two clients connect at the same time, one or both of the clients may get broken image icons. You'll need to increase the number of connections, and the memory allocation for WebSTAR as well.

- **Do the images load properly if the person clicks reload in the browser?** If so, it is probably due to the number of persistent connections (keep-alive) or slow PPP or modem connection on the browser side.

For each Persistent Connection (keep-alive) you allow, you should increase the Maximum Connections setting, and WebSTAR's memory allocation by two to three times. The server maintains a particular browser's connection for a longer period of time, meaning that additional browser requests may not encounter enough open connections on your server to get everything on the page at the first try.

- If you've modified the file but **not flushed the cache**, the server may not send the entire file. You can set the Data Cache (described on page 140) to always check the file modification date while you are making changes.
- There may be **hard disk or file system problems** preventing WebSTAR from sending out the complete file. You can check to see if WebSTAR is serving out the complete file by comparing the size of the file against the number of bytes being sent out.
 - Make sure you are set to log the BYTES_SENT field. Compare the actual number of bytes sent to the byte size of the graphic listed in the Get Info dialog box under the File menu in the Finder. (Keep in mind that only the data fork of a file is served out, so you may need to get information on the file with an application like ResEdit if the file has a custom icon or other data stored in the resource fork).
 - If the byte count matches, WebSTAR is serving out the entire file and the problem is likely a client related issue.
 - If the numbers are different, there is a problem with the Macintosh file system. To correct this, rebuild the Desktop file. Once the desktop has been rebuilt, restart the server. If this does not resolve the problem, try running a hard drive diagnostic utility such as Disk First Aid or Norton Disk Doctor.

People report that their browser crashes when they view certain pages

- Some **sound files, animated gifs or Java scripts** may cause some browsers, or browser versions to crash.
- You may have **image files that are actually larger** than the size specified in the HTML.

- It may be a **browser Plug-In** causing the problem. When you include files on your site that require Plug-Ins or helpers on the client side, it is helpful to provide information about which version(s) work best and, if possible, a link for downloading the appropriate Plug-In.

The WebSTAR status window is displaying lots of strange error messages

- If you have “**verbose messages**” enabled, turn it off. Most of those messages are of interest only for debugging during CGI or Plug-In development.
- After turning off verbose messaging, if you’re still getting error messages which are not explained on StarNine’s support web pages at <http://www.starnine.com/support/>, contact StarNine technical support.

After moving WebSTAR to a new machine, Java doesn’t work anymore.

To move your WebSTAR server and site to a new machine, all you have to do is copy the WebSTAR folder and all its contents. WebSTAR keeps all its files, such as settings, log, etc., in its own folder. This is what makes it possible to run more than one copy on a single machine with each copy having different settings.

If you have placed aliases within the WebSTAR folder which reference files or folders outside the WebSTAR folder or if you have used SSI included files which are referenced by explicit path, you will have to reconfigure those on the new machine as well.



Make sure you have Apple’s MRJ (Mac OS Runtime for Java) version 2.1.1 or later.

Browsers are getting “broken pipes” messages

- This message comes up when the browser-to-server connection has broken, rather than being disconnected in the correct way. There are many reasons this can happen, for example, the browser could be on a machine that has lost its Internet connection.
- WebSTAR Web server version 4 has a special header that works around some versions of this problem: make sure you are using the most recent version.
- If it’s happening often, and to different browser machines, check on the list at

<http://www.starnine.com/extendingwebstar.html>

for tools that enable you to watch the connection and monitor packets being sent. This can help determine where things are getting lost in the path from browser to server and back to the browser.

Virtual Hosts requests are not being routed properly

- You must register the domain names and work with your DNS service provider to make sure that requests for your hosts are being directed to your browser.



For details, see “Virtual Hosts” starting on page 144.

- The **browser's request must match the Virtual Hosts entry exactly** in order for the request to be routed to the correct folder. For example, if the entry has all the fields filled in:

```
192.1.1.1 www.domain.com English :widget:
```

the browser must connect to the IP address "192.1.1.1" **and** pass to the server a Host : field of "www.domain.com" **and** include the English language field, in order for the request to get routed to the correct root folder.

If you only have one host for this IP address, it's better to just use the IP Address field, like this:

```
192.1.1.1 Any Any :widget:
```

This entry routes all browser requests for the IP address "192.1.1.1" to the folder *domain* located inside the WebSTAR folder.

- **Virtual Host entries are order dependent.** For example, if you wanted to route browser requests to a specific folder based upon the language specified in the browser, the specific Virtual Host entry for that language should be listed before the more generic entry. The proper order to make this works would be:

```
192.1.1.1 Any French :mechanisme:
```

```
192.1.1.1 Any Any :widget:
```

- Make sure you've set your **Virtual Host files** to the correct names and file paths. For information on these settings, see "Virtual Host Options" on page 150.
- The **"Server Name" field** is the name that the server uses when sending redirects when a user has connected to the server but has failed to append a trailing "/". Always set it to the host name for that virtual host.

Problems configuring Open Transport to support multiple IP addresses

For information, see "IP Multihoming: Special Configuration" on page 195.

- You must be **running Open Transport 1.3** or later in order to use IP multihoming.
- You will need to **restart the machine** after entering additional IP addresses or making changes to the *IP Secondary Addresses* file.
- If **subnet mask and router address information** is entered for one IP address in the *IP Secondary Addresses* file, then subnet mask and router information must be entered for all secondary IP addresses. If all subnet mask and router information is excluded from the file, Open Transport will use the defaults entered into the TCP/IP Control Panel. Try removing that information and rebooting.

This section explains how the WebSTAR FTP server works, how to configure the server, and how to understand the information in the monitor window and the FTP log file.

ABOUT THE WEBSTAR FTP SERVER



Uploading: to transfer Files from a client machine to the FTP server.

Downloading: Transfer files from the server to the client.



For step-by-step instructions for getting started, see “Connect To Your FTP Server” on page 57.

FTP (File Transfer Protocol) is a widespread and fast way of moving files from one computer to another. It allows clients to both **upload** and **download** files. Many browsers include FTP support, and stand-alone FTP client applications are also available.

WebSTAR FTP provides controlled access to your server folders using this protocol. You can create users who have to log in with a name and password, and specify which folder (and subfolders) they can view, and so on.

In addition, you can create a public FTP area. According to the FTP conventions, anyone can download data from this area by logging in with the name “anonymous”. For information, see “Anonymous FTP” on page 347.

FTP and Cache Flushing

The WebSTAR FTP server does not take advantage of the Web server's File Info Cache and the Data Cache: it accesses the disk directly.

However, when a user uploads a file using WebSTAR FTP, the server sends a message to flush the caches. This automatically flushes the File Info Cache and the Data Cache, and sends a message to third-party Plug-Ins to flush their caches as well.

FTP Security

WebSTAR FTP provides a great deal of flexibility in choosing what folders are visible to FTP users, but this can compromise your server security if you are not careful. In addition, FTP passwords are not protected so anyone monitoring your data stream might be able to extract them and have access to your server folders.

Folder Security

With WebSTAR FTP, you can give users access to any folder on any mounted drive. This is a powerful feature, but should be used with caution. Each FTP user can access all the subfolders within their root folder, but they cannot see any other folders on the disk. You can specify the maximum amount of data that can be inside that folder,

which gives you reassurance that uploads will not take all the space on your hard drive.

FTP root folders can be in the WebSTAR folder, in another folder on the hard drive, in a separate partition or on another hard drive. This allows you to take best advantage of your available disk space, but can cause major security risks, so think carefully before you designate the root folder.

In addition to local files and folders, WebSTAR FTP will attempt to follow aliases to other files and folders. Be sure that you know what aliases you include in FTP folders.

In general, you should allow FTP access to carefully specified folders, which contain limited amounts of material, and which do not include private or confidential data.

File Security

WebSTAR FTP will not display or allow the transfer of WebSTAR control files (files with a Creator Code starting with “WWW”). These include WebSTAR application and Plug-In files.

FTP users can also download applications, so you can distribute programs you have written or otherwise have the rights to. Make sure that you and any users with FTP upload privileges do not distribute commercial software.

Password Security

FTP passwords are always sent as plain text. This is a security problem: if someone is monitoring your data stream, or that of one of your users, they can see the password clearly. They could then use the password to use your server for their own purposes, such as, passing pirated software or hacking your web site. The limits on FTP folder size can only help to a certain extent. To avoid this, limit user access to certain very specific folders.

If you use FTP to update your web site, try to use a “staging” folder for storing changes, and then transfer the changes to the main folder using another protocol. If you must use FTP to access your main server folder, change your password often.

Monitoring FTP Use

All FTP requests and responses are logged. You can watch your FTP server usage in the WebSTAR Admin Monitor window, and check your



If an FTP client attempts to open a folder with an alias to an unmounted network volume, the WebSTAR server machine will attempt to mount it. If a volume password is required, or the volume is unavailable, this may stop or slow your server until someone dismisses the alert on the WebSTAR server machine.



If an FTP client attempts to get a resource-only file without using MacBinary, WebSTAR FTP will send back an error. The solution is to put the FTP client into MacBinary mode.

For server settings, see “Use MacBinary for .bin files” on page 342.

server logs for any unauthorized transfers regularly. For more information, see “FTP Monitors & Logging” starting on page 349.

FTP Data Types Supported

The WebSTAR FTP Server supports the following FTP data types:

- **ASCII** for text files (default type)
- **BINARY** for graphics and other binary file types (this will transfer the data fork of Mac files but not the resource fork)
- **MacBinary** for applications and other files that require the resource fork. Mac FTP clients can be configured to request the this data type. WebSTAR FTP will automatically use MacBinary if the file name ends in the suffix “.bin”.

FTP and Multiple Hosts

You can have the FTP server respond to requests for multiple hosts on the one server. FTP servers don’t have to match the domain with any particular file (unlike Web servers), and WebSTAR FTP doesn’t use the Web server’s Virtual Hosts settings.

To respond to FTP requests for your other host and domain names, work with your ISP or network administrator to add an alias record (“CNAME”) in the hosts’s DNS record.

For example, you can add a CNAME alias from `ftp.domain.com` to `www.domain.com`. FTP requests for the second domain name will be automatically routed to your WebSTAR FTP server.

FTP Load Balancing

If you run several servers, you may want to distribute FTP requests among them. WebSTAR FTP Server and the QuickDNS Load Balancer Plug-In allow QuickDNS Pro from Men and Mice to track the FTP server load and distribute requests to the least used server.

FTP URLs in HTML

With most web browsers, it’s very easy to link to FTP, using the URL “ftp://”. For example, to see the WebSTAR Update directory, use this URL:

```
ftp://ftp.starnine.com/pub/updates/webstar/
```

In this case, the folder has anonymous access, so it will display immediately.



For more information, see “DNS” on page 100.



See also: “WebSTAR QuickDNS Load Balancer” on page 257.

You can also create a link to a file, rather than a folder, and it will start downloading right away. Just put the file name as part of the URL, like this:

```
ftp://ftp.starnine.com/pub/updates/webstar/readme
```

For private folders, the browser will display a login dialog, and you'll have to enter a user name and password. Then the browser will display the folder listing or start downloading a file.

You can also use FTP URLs with a user name and password included. To do this, include the user name, a colon, the password, and an at sign ("@") before the host name:

```
ftp://HumanResources:hM3z9S@www.domain.com/humres/news.html
```

Most FTP clients can take this apart and send the correct URL and login information to the server. Be sure to test this before publishing such URLs, and limit the data in these folders carefully.

You should use only letters, numbers and standard punctuation in the folder and file names. **Do not use the / (slash) or : (colon) characters in file names.** If you must use other characters, such as spaces, in file names, you'll have to encode the URLs, as described in "Macintosh Special Characters in File Names" on page 189.

FTP STANDARDS AND CONVENTIONS

WebSTAR FTP is written according to the FTP standards. It supports all common ports, all standard commands, and some optional commands.

FTP Specification

The official FTP specification is at:

```
ftp://nic.merit.edu/documents/rfc/rfc0959.txt
```

FTP Ports

FTP clients usually use two ports: port 20 for the Data Connection, and port 21 for the Control Connection. Browsers that act as FTP clients using the "PASV" command may use any port in the 9000 to 12000 range, and WebSTAR FTP will handle the requests properly.



See also: "FTP Users: Access Control" on page 344.



See also: "Firewalls and Server Ports" on page 103.

This chapter explains how to configure the WebSTAR FTP server.

WebSTAR FTP is always enabled, as long as the WebSTAR FTP Plug-In is in the *Plug-Ins* folder. Use the WebSTAR Admin application to configure the FTP server, as well as set up user names and passwords (described in “FTP Users: Access Control” on page 344).

WEBSTAR FTP SETTINGS

Open the WebSTAR Admin application, select Server Settings command from the Edit menu, and choose the FTP Connections panel.



For step-by-step instructions for getting started, see “Connect To Your FTP Server” on page 57.



WebSTAR FTP requires 32K of RAM for each connection you assign it. If you increase the default, be **sure** to increase the RAM as described in “Server Application Issues” on page 87.

Max Connections

This is the number of users that can be using FTP service simultaneously. The default number of connections is **12**, and the maximum is 500.

Timeout

WebSTAR FTP must automatically close connections to FTP clients. Unlike HTTP clients (web browsers), FTP clients log in and retain a connection. However, many users do not bother to log out or close their FTP session, so the server must close it for them, after they stop communicating (no client will be closed while it is active). The timeout value defines the inactivity interval.

The default timeout interval is **300** seconds, and the range is from 30 to 999 seconds.

Reported Server Name

When an FTP client connects to a server, it asks what kind of server it is. Unfortunately some FTP clients display, format or return results differently depending on what type of server they are talking to.

Setting the server to **UNIX WebSTAR FTP** with the **“Append “.bin” suffix to file names”** turned on should be the most compatible as it will cause both Mac and Windows browsers to display information correctly and allow for downloading of files in MacBinary format.

Other options, included for Mac-only Intranets, are **Mac OS WebSTAR FTP** and **Mac OS Peter's Server**.



Some older versions of Navigator don't handle FTP properly for Mac unless the server identifies itself as “Peter's Server”.

Use MacBinary for .bin files

MacBinary is a Mac-specific extension to the FTP standard to transfer both the data and the resource forks of Macintosh files. Many files, especially applications, contain important information in this resource fork, so Mac FTP clients support MacBinary, as do most Mac browsers, since Netscape 4 and Internet Explorer 3.

If this option is checked, the WebSTAR FTP server will assume that all files with the suffix “.bin” are MacBinary, and will use this data type to transfer the files.

Unfortunately, the Restart command, used by FTP clients to resume downloads if they are interrupted, is not compatible with MacBinary files, because all the file information is at the beginning of the file.



If you upload a file using FTP from a Mac, it should automatically be transferred as MacBinary.

Displaying Files with Resource Forks

The WebSTAR FTP server will not display the names of files with resources forks unless you have one of the following checkboxes selected.

Append “.bin” suffix to file names

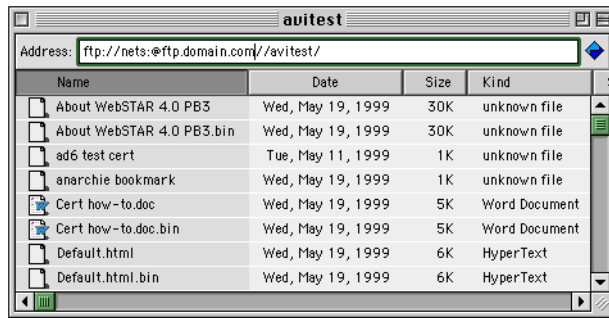
Checking this box will automatically put the text “.bin” after file names of files with resource forks, when the FTP server sends the listing to the FTP client. You can see the file names with the suffix, and the client will then transfer and decode them properly.

Display actual file names

Checking this box will display files with resource forks without adding a “.bin” suffix. However, some FTP clients may not transfer the resource forks correctly, because they don't recognize the format.

Both Display Options Selected

If you check both boxes, you'll show two copies of each file with a resource fork, one with “.bin” and one without.



Default Type & Creator Codes For Upload

Type and Creator codes control the Mac desktop icons for files, and which application opens a file when you double-click that file.

When someone uploads a file using WebSTAR FTP, the server looks up that file's suffix in the Suffix Mapping table. If it finds a match, and there is a Type and/or Creator code entered, WebSTAR FTP will assign them to that file. The default Suffix Mappings have Type and Creator codes, and you can add them for files created by other applications: see "Editing Suffix Mapping Table Entries" on page 156.

i Check the documentation for the application to learn its Type and Creator Codes, or drag one of its files to the Find File window with those fields visible.

If no Type or Creator can be found for the suffix, WebSTAR FTP saves the file with the default Type and Creator code set in this panel. If you have a favorite HTML editor, for example, you can have WebSTAR FTP assign the creator code for that program to all ASCII text files you upload.

If you upload using the FTP server and the MacBinary format, your Mac files will retain their resource forks, including Type and Creator codes.

ASCII

These codes will be used when you upload using the ASCII (plain text) data type.

- **Type**—the four-character code for the kind of file. HTML files are always of Type “TEXT”, and that is the default for this setting.
- **Creator**—the four-character code for the preferred application to open this file. The default is “ttxx” (Apple’s SimpleText application).

Binary

These codes will be assigned when you upload using the Binary data type (anything but text).

- **Type**—the four-character code for the kind of file. The default is Type “TEXT”.
- **Creator**—the four-character code for the preferred application to open this file. The default is “ttxx” (Apple’s SimpleText application).

Connection Messages

Some FTP clients, especially text-based clients on Unix machines, will display a message when you login and logout, and when you open each folder. WebSTAR FTP allows you to designate text files which store these messages and will display them at the appropriate times.

- **Log-On Message**—path to the text file containing the welcome message. Type the file path from the server root folder or click the **Choose** button to select it.
- **Log-Off Message**—path to the text file containing the goodbye message. Type the file path from the server root folder or click the **Choose** button to select it.
- **Folder Message**—this is a file name, like the Web server index file name field. Enter the name here (such as “. readme”). If you put a text file of that name in a folder, WebSTAR FTP will send that file to the client whenever they open that folder. Some FTP clients will display it to the user, others will ignore it.

FTP USERS: ACCESS CONTROL

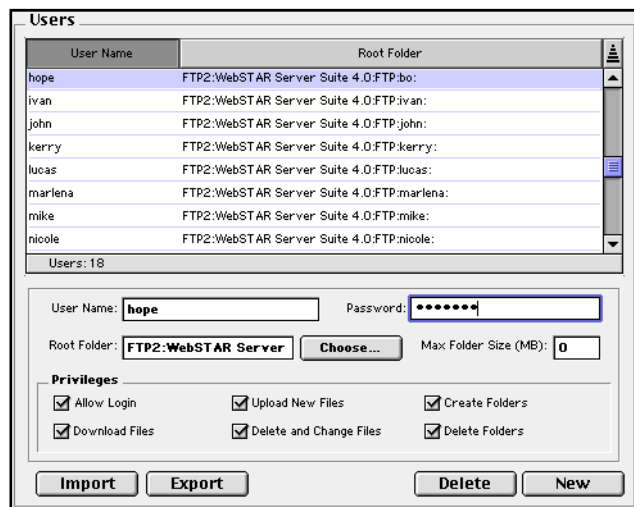
WebSTAR FTP allows you to specify individual users, and for each user, a user name, password, root folder, and file access privileges. This information is stored in *WebSTAR FTP Users* file in the *WebSTAR FTP Data* folder in the *Plug-Ins* folder. Be sure to keep frequent backup copies of this file, in case you have any problems with your file, drive or server machine.

You should only have one FTP user entry per name, because when a client attempts to log in, the server will use the first name which matches exactly.

Making an FTP User Entry

Before you make a new FTP User entry, you should decide which folder will be the root folder for this user. If it doesn't exist, you'll have to create it, either at the server Mac or by logging in via FTP and using the FTP client's command to make a new folder (also called a "directory").

To edit the FTP Users list, open the WebSTAR Admin application, select "Server Settings" from the Edit menu, and choose the "FTP Users" panel.



User Name and Password

- **User Name**—the name the user enters in the FTP client, or in the login dialog. It can be up to 31 characters long, and can include spaces.
- **Password**—the password associated with this user name. This can also be up to 31 characters long. For security suggestions, see "Safe Passwords" on page 96.

Note that FTP users may log in from any computer. Therefore, it's a good idea for names and passwords to use standard ASCII characters, rather than Mac extended characters.



See also "FTP Security" on page 337.

For public access without password protection, see "Anonymous FTP" on page 347.

FTP Root Folder File Path

The **FTP Root Folder** is the user's base FTP folder. It can be anywhere on your server's hard disks, so be sure that you don't accidentally allow others to access personal or sensitive data. Note that a user can open all subfolders in this folder, but not any folders enclosing this folder.

The FTP server requires a **complete file path** from the Mac hard drive name to the desired folder. The **Choose** button allows you to use a Mac interface to specify the folder on the server machine, and creates the file path for you. This string can be up to 255 characters.

These example paths start from the same drive as the WebSTAR application, and the root folder is within the WebSTAR folder:

```
ServerHD:WebSTAR:users:ericz:
ServerHD:WebSTAR:widgets:marketing:
```

Here are some example paths starting from a separate volume, such as a second hard drive:

```
pub:
FTP:HD:ericz:
FTP:a:avirr:
```



It's best to avoid spaces or Mac Extended characters in the folder and file names. If you must use them, you'll have to encode them in any FTP URLs, as described in "Macintosh Special Characters in File Names" on page 189.

Max Folder Size

To control your server's disk space, you can limit the size of the users's folders (their root folder and all enclosed folders).

When a user tries to upload a file to a folder that is too full, they will get a message that they have exceeded the storage limit. WebSTAR FTP will allow users to upload additional files, even large ones, until they reach that limit.

The default value, **0**, means that there is no limit. The allowed range is from 1 MB to 999 MB and you can set the limit individually for each user.

Privileges

You can use these items to allow limited access to some users and more control to others.

- **Allow Login**—uncheck this item to temporarily disable this user's access.



Clients cannot delete folders if there are any files in them. Some FTP clients will do a recursive delete, removing the contents of the child folders and then the parent folders.

- **Download Files**—allow this user to copy files from the server to their local disk.
- **Upload New Files**—allow this user to copy files from their local disk to the server, in their root folder.
- **Delete and Change Files**—allow this user to delete files in their root folder, or replace a file with another of the same name.
- **Create Folders**—allow this user to make new subfolders in their root folder on the server.
- **Delete Folders**—allow this user to delete subfolders from the server. They cannot delete their root folder.

FTP Users Import & Export

If you have many FTP Users, you may want to edit their access information in a database or text file, rather than in WebSTAR Admin. These buttons let you import and export the user entries to a tab-delimited text file. The format is:

- username
- password
- root folder path
- privileges codes, corresponding to the checkboxes in the FTP Users panel (in any order)
 - **a**—allow login
 - **r**—download files
 - **c**—upload files
 - **w**—delete & change files
 - **f**—create folders
 - **x**—delete folders
- maximum folder size

For example, the following entries allow some users to change files and others simply to view them.

anonymous	*	FTP-HD:pub:	ar	0
knickknacks	z8ck2	Web-HD:WebSTAR 3.0:knickknacks	arcf	500
widgets	2wid6	Web-HD:WebSTAR 3.0:widgets:	arcfw	0

Anonymous FTP

The Internet custom is to allow public FTP access to a server via a special **anonymous** user: the FTP client enters “anonymous” for their user name. In many cases, the client automatically sends the user’s

email address as the password. The WebSTAR FTP server supports an anonymous user account.

When a client logs in, the FTP monitor and log file shows you the client software name, and password, if any:

```
FTP: Anonymous user (user@domain.com) logged in
```



Anonymous access requires special attention to security issues: see “FTP Security” on page 337.

To make a public-access folder for your FTP server:

- 1** Select the location of the FTP root folder carefully, preferably on a separate disk or partition.
- 2** Name your FTP root folder. A common name for these folders is “pub”, short for “publications”.
- 3** Put an example file in the anonymous root folder, for testing.
- 4** Make an FTP User entry with the name “anonymous”, and the public-access folder as the root folder.
 - If you leave the password field empty, anonymous users are not required to send a password to the server.
 - If you put anything in the password field, anonymous users must send something, such as their email address, in the password field. You can use an asterisk (“*”) in this field to remind yourself that any word will match.
- 5** Set the FTP Privileges. You may not want anonymous users creating folders or even uploading files.
- 6** Save the entry to your server.
- 7** Log into your FTP server’s “pub” folder from any FTP client using their “anonymous” setting, to make sure that you can access the correct folder.



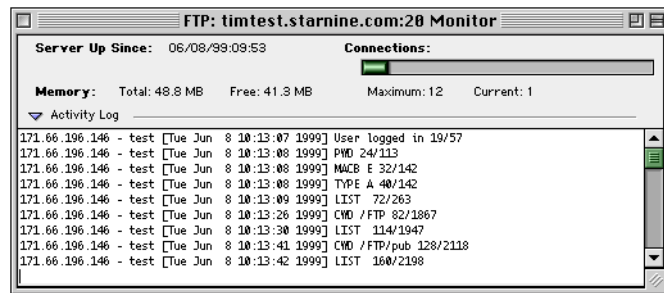
Even if you require some text, it’s not a real password: you cannot require a specific password on an anonymous account.

WebSTAR FTP allows you to monitor the FTP status in real time, save a log file of FTP activity, and automatically archive that log file at hourly, daily, weekly, or monthly intervals.

FTP MONITOR WINDOWS

WebSTAR FTP has its own monitor windows on the server and in the WebSTAR Admin application. This information is saved in the *WebSTAR FTP.log* file, described in “FTP Logging Information”.

In addition, the FTP Monitor window on the server machine will show you the maximum number of connections allowed, according to your Max Connections (described on page 341), and the current number of connections.



FTP LOGGING INFORMATION

The FTP logging and monitoring information contains entries for each request that an FTP client sends, and the server response information.

FTP Log Elements

- **IP Address:** the IP address of the FTP client
- **User Name:** the login name of the account
- **Date and Time:** the date and local time of the server
- **Activity or Command:** the interaction with the FTP client (see below)
- **Time/Transfer:** the time taken to respond to the command in ticks (1/60 of a second) and the number of bytes sent or received.
- **Received/Sent:** The amount of data received by the server from the client, and the amount of data sent by the server to the client (this includes both data and control connections).

FTP Activities

WebSTAR FTP will log many activities including commands from the client, user interaction and problems.

Logins

Every successful FTP connection from a client, with the FTP User name.

```
192.168.0.2 - anonymous: user@domain.com [Tue Apr 27 12:37:32 1999]
Anonymous user logged in 50/72
192.168.0.2 - HumanResources [Tue Apr 27 12:12:26 1999] User logged in
20/57
```

Logouts

Every explicit log out command and every timed-out connection, with the FTP User name.

```
192.168.0.2 - HumanResources [Tue Apr 27 12:40:02 1999] User logged out
20/57
192.168.0.2 - anonymous: user@domain.com [Tue Apr 27 12:38:04 1999] User
timed out 104/2619
```

Uploads

Every file uploaded to the server, with the absolute path of the new file on the server disk.

```
192.168.0.2 - HumanResources [Tue Apr 27 12:14:14 1999] STOR:
/FTP-HD/pub/human resources/FAQs/employment FAQ 254/2887
```

Downloads

Every file downloaded from the server, with the path of the file.

```
192.168.0.2 - HumanResources[Tue Apr 27 12:43:44 1999] RETR:
/FTP-HD/pub/human resources/HR tips3 356/3757
```

Problems

System errors and attempts by clients to do things they are not allowed to do, such as send a command that is not supported, try to open a folder they aren't allowed to see, or login with the wrong user name or password:

```
192.168.0.2 - avi [Tue Apr 27 12:45:46 1999] Login failed, unknown user
'lucia'. 18/80.
```

192.168.0.4 - widgets [Tue Apr 27 12:47:32 1999] Login failed, bad password. 22/80
 192.168.0.6 -tchotchkeys [Tue Apr 27 12:48:37 1999] Login failed, bad folder. 32/80
 192.168.0.8 -knickknacks [Tue Apr 27 12:49:39 1999] Login failed, login not allowed. 32/80.

FTP Commands

WebSTAR FTP supports all of the commands required by the RFC 959 specification, and many of the optional commands. These are all displayed in the FTP Monitor and Log file.

WebSTAR FTP Commands

COMMAND	MEANING
ABOR	abort file transfer or FTP command
APPE	upload a file to the server (if a file of the same name already exists, append the new data to that file)
CWD	change working directory
CDUP	change directory to parent
DELE	delete a file
HELP	help
LIST	list files in the current directory
MODE	change mode
MKD	make directory
MACB	use the MacBinary data type—a Mac extension to the standard
NLST	list of files in the current directory, with additional information
NOOP	no-op (no operation: nothing happened)
PASS	password
PORT	specify the data port
PASV	passive - listen for connection (often used by web browser FTP clients)
PWD	get name of current directory
QUIT	log out of the FTP server
REIN	re-initialize the user
REST	resume FTP file transfers (not MacBinary)
RETR	retrieve a file from the server, aka “download”
RMD	remove directory

WebSTAR FTP Commands

COMMAND	MEANING
RNFR	rename with both write and read permission
RNTO	rename with just write permission
STRU	change file structure mode
STOR	store a file on the server, aka “upload”
SYST	get the name of the FTP server OS
SIZE	get the size of a file—a non-standard command used by Anarchie
TYPE	specify the data type
USER	send the user name

FTP LOG FILES

The FTP Logging Options panel in the WebSTAR Admin application includes a section for controlling the basic logging functionality.

Logging Options



Logging On and Off

When you click the Logging “Off” radio button, and press the Save button, the log file will no longer be updated. You must select the Logging On radio button and press Save to start logging again.

The default is Logging **On**.

Log File Name

The default file name is : logs :WebSTAR FTP . Log, specifying that the log file will be named *WebSTAR FTP.log* and will be located in a *logs* folder in the WebSTAR root folder. A record of all FTP transactions is maintained in this file. If the file does not exist, the WebSTAR FTP server will create it.

The **Choose** button allows you to select a file on the server and append all future log information to that file. You cannot create a new log file this way, but you can select any file on your server as a log file, so be careful that you do not start appending log information to HTML or other files.

Log Archiving

Log Archiving allows you to save separate log files covering specified periods of time, such as every day, every week on Thursday, or monthly. The log files are automatically created at the time you set, filled, and then closed when the next one is created.

For instructions, see “Log Archiving” on page 122.



See also “How to Get Help” on page 106, “WebSTAR Debug Plug-In” on page 107 and “General Server Troubleshooting Guidelines” on page 108.

This chapter helps you locate and fix problems with the WebSTAR FTP server.

FTP Server Troubleshooting

If you see errors on startup, in monitors, logs or users report problems, use this list of common problems to locate and fix your FTP server.

The WebSTAR FTP Server Startup Errors

Error “FTP port already in use, server not running”.

- If you have **another FTP server running** on the same machine, the first one launched will be listening on port 21 for control transmission, and if WebSTAR is launched second, the FTP Plug-In won't be able to listen on that port. You can't change this port number.

Error “startlistener failed (-3247)”.

- You may have a second copy of WebSTAR running on the same machine. While the Web server can listen on multiple ports, the FTP server cannot. You should remove the FTP Plug-In from the *Plug-Ins* folder of the alternate server.

Error in initialization: “The FTP Plug-in could not open the “WebSTAR FTP Users” file”.

The *WebSTAR FTP Users* file was not found in the *WebSTAR FTP Data* folder in the *Plug-Ins* folder.

- If you have not yet created any FTP users entries, don't worry, WebSTAR FTP will create the file for you.
- If you do have FTP user entries, quit the server, locate the file or a backup, make sure it's in the right folder and restart WebSTAR. Otherwise, you'll have to re-enter all the FTP user entries.

Error “could not get ftp* configuration resource”

- The folder *WebSTAR FTP Data* is probably missing from the *Plug-Ins* folder. Make a new folder of that name or re-install the WebSTAR FTP server, and the server will work properly.

Error “WebSTAR FTP: Could not determine IP address of server”

- The DNS server is not responding properly: it may be down or otherwise inaccessible. WebSTAR FTP is trying to do a DNS lookup of it's own IP address, and the lookup is failing for some reason.
- First, try using a web browser or FTP client to check another server. If your DNS server is down, you will get an error.

- If that works, make sure you have entered a server name in the Admin Web Settings panel File Names and Paths (described on page 130).
- If the FTP server still doesn't work, check your TCP/IP control panel and work with your DNS administrator to check your DNS records.

Errors and Error Codes

- **Bad Folder** entry in the Log means that the folder has a slash (/) somewhere in the path. Check your hard drive and enclosing folders for this character, and remove it.
- **Write Stream Error -5** means that the client has closed the connection. This is informational only, does not indicate a problem with the server or the client, and does not require any action by an administrator.
- **Error -17** means that the request failed. This usually occurs when the server requests that the client close the connection and the client has already closed the connection. In most cases, it does not indicate any problem or require any action.
- **Error -550** (Write Permission Denied): this user account does not have the "Upload New Files" option checked, and the user tried to upload a file.
- **Error -552** (Exceeded storage limit): the user account has reached the folder size limit and the user has tried to upload additional files.



See "FTP Users: Access Control" on page 344 to change these settings.

Client Errors

Server does not respond to requests outside company

If your FTP server is behind a **firewall**, the network administrator will need to ensure that ports are available for access. Another option would be to configure the specific IP address for the server machine to be outside the firewall.



See "Firewalls and Server Ports" on page 103.

Folders Not Visible in FTP Client

- Try changing the server response: see "Reported Server Name" on page 342.

Can't Download WebSTAR Files

- WebSTAR checks the Mac OS Creator Code before allowing users to download files. As a security feature, any files created by WebSTAR, with the Creator Code `wwwΩ`, will not be transferred. This prevents accidental or malicious downloading of server settings files.

WebSTAR Server Suite 4 includes a powerful mail server, providing Internet-standard SMTP mail services and allowing users to retrieve their messages via the POP and IMAP standards. It also provides Web browser email access, limited LDAP directory services, and tools to prevent unsolicited 'spam' email.

Key features include:

- Internet-standard email server protocol (SMTP)
- Internet-standard client protocols (POP and IMAP)
- Web-based email access — a simple web page allows users to log in, read and send messages using a web browser.
- Directory services — lists user names and email addresses via the Internet-standard LDAP protocol.
- Multiple Hosts — works with your DNS server to receive and send mail from many different host and domain names.

ABOUT THE WEBSTAR MAIL SERVER

The WebSTAR Mail server plug-in is installed automatically when you install WebSTAR Server Suite 4.

WebSTAR Mail Files

WebSTAR will only run the mail server if the plug-in file *WebSTAR Mail* is in the *Plug-Ins* folder when the server application starts up.

WebSTAR Mail Data Files

The *WebSTAR Mail Data* folder stores the mail server information files and folders:

- *WebSTAR Mail Users* file stores all the user and account information, including pending client messages and IMAP messages stored on the server. If you remove the file from this folder, the server will not be able to find it and will create a new empty file and start to fill it in. **This file is extremely important and you should back it up frequently (see page 370).**
- *WebSTAR Mail Settings* file is for emergency repairs. See "Mail Server Troubleshooting" on page 407 for solutions to mail server file problems.
- *Attachments* folder stores incoming attachments and IMAP enclosure files saved on the server. These files will have code names like e0EE6B29B.
- *WebSTAR Mail Users Backup.1* and *.2* files are not installed, but they are created automatically by the server.



Having a unified file for storage of mail user data makes it easy to perform backups, audits, integrity checking, and automated recovery of mail user data in case of problems.

- *Transaction Log* files store all of the changes made to a backup snapshot of the user/message database, used to restore changes if there are any problems.
- *SMTP Outgoing Index* and *SMTP Outgoing Data* files store outgoing messages until the receiving SMTP servers can be located and accepts those messages. Outgoing messages are displayed in the Mail monitor window: see “Mail Monitor & Queue Window” on page 399 for details.
- *Temporary Mail* file is used internally to handle messages which overflow the Mail disk cache.



To keep this information safe, see “Backing Up and Restoring Email Files” on page 370.

ABOUT INTERNET EMAIL

Email servers are the intermediaries that help you send messages to other people. **Client** programs read and write those messages: examples include Eudora, EMailer, Netscape Messenger, and Microsoft Outlook. The WebSTAR Mail server supports SMTP, so it can communicate with other servers that support the same Internet standard, such as Sendmail on Unix, Microsoft Exchange on Windows NT, and Eudora Internet Mail Server (EIMS) on the Mac.

SMTP

WebSTAR Mail is a standard **SMTP** (Simple Mail Transfer Protocol) server. This means that it participates as a peer of all other Internet SMTP mail servers, sending messages via the most direct route available to the recipients' mail servers, and receiving messages from other servers. SMTP servers do not “log in” to retrieve messages, they simply wait for messages to come to them.

To send a message using the WebSTAR Mail server, a user creates it in their email client, which transfers the message to the server. WebSTAR Mail then looks up the IP address of the recipient's mail host and sends the message to that server. In some cases, other servers are authorized to accept and forward email messages—this is all directed by DNS and routing configurations.

Assuming all is well, the message and any attachments are sent right away. If the receiving server is temporarily unavailable, the sending server will **queue** (store) it and try again later. If there is another problem, such as a mistake in the email address, the receiving server may **bounce** (reject) the message. WebSTAR Mail will then pass that bounced message back to the original sender.



For technical details on SMTP, see RFC 822. For enclosure processing, see RFCs 1652 and 2045-2049.



WebSTAR Mail supports POP version 3 For technical details, see RFCs 1939 and 2195.

POP

POP stands for “Post Office Protocol”, which allows email client programs (also known as **POP clients**) to log in and download messages from the mail server. The user then reads the messages and replies, and the email program uses the SMTP protocol to send the messages back out through the server.

Many POP clients allow users to specify if the messages should be retained on the server or deleted right away. The only reason to retain messages is if the user is accessing the mail account from more than one place and wants to read their email at all their computers. IMAP (described below) is a better solution for this problem than POP.

All WebSTAR Mail accounts are accessible via POP clients. You can set the message size limit, forwarding, total storage, and APOP security options. See “POP Connections” on page 381 and “Users & Accounts Settings” on page 391 for more details.

Standard POP passwords are not encrypted. This means that anyone who is between the client and the server can intercept the login command and capture the password. They could then use that password to send messages from accounts on your server, without anyone’s knowledge. This can be used for unwanted email, threats and other undesirable activity. For this reason, we recommend using APOP whenever possible (see below).

POP Compatibility

The following are examples of POP compatible mail clients:

SOFTWARE	VERSIONS
Eudora Pro and Eudora Lite from Qualcomm (Mac and Windows)	2.0 and greater
Microsoft Internet Mail and News (Mac and Windows)	3.0 and greater
Microsoft Outlook and Outlook Express (Mac and Windows)	3.0 and greater
Netscape Messenger (Mac and Windows)	3.0 and greater



For technical details about APOP, see RFC1734.

APOP

WebSTAR Mail supports **APOP**—Authenticated Post Office Protocol—which uses a secret passphrase system to identify each

client for security. However, some older email programs do not support APOP, so you can set this option for each individual account.

IMAP

IMAP—the Internet Mail Access Protocol—allows users to read their mail on the server and only download messages and attachments to a local machine when appropriate. Its main advantage is that the user can see all the message headers at a glance, and open only those which are interesting. This saves significant download time, especially if users often forward or delete messages without reading them.

IMAP demands on the server disk can be significant, as messages are often left on the server, rather than stored on many client machines.

WebSTAR Mail supports IMAP clients with settings for message size limit, forwarding, and total storage limits. In addition, you can specify for each account whether IMAP clients can create, rename or delete mailboxes on the server.

IMAP Compatibility

WebSTAR Mail supports IMAP version 4 revision 1. The following are examples of IMAP compatible mail clients:

SOFTWARE	VERSIONS
Eudora Pro from Qualcomm (Mac and Windows)	4.2 and greater
Microsoft Outlook and Outlook Express (Mac and Windows)	3.0 and greater
Netscape Messenger, and Communicator Mail Module (Mac and Windows)	3.0 and greater

Web Mail

WebSTAR Mail is also accessible from any browser, so your users can read mail from shared computers, while travelling, and so on. For more information, see “Email Access from Web Browsers” on page 363

LDAP

LDAP (Lightweight Directory Access Protocol) allows people to look up names and email addresses in your company listings. This is particularly useful for Intranets and distributed corporations, so users

 For information on IMAP, see the IMAP Connection at www.imap.org. For technical details, see RFC 1203 and 2060.

 For information on LDAP, see www.umich.edu/~dirsvcs/ldap/index.html. For technical details, see RFC 2251.

 Some firewalls may restrict access to your LDAP server on port 389. You may need to talk to your Network Administrator or ISP about opening a hole in the firewall if you want access from outside.

can find addresses for other employees quickly and efficiently. It is like a company phonebook for email addresses.

Using the LDAP Server

Users may have to add your WebSTAR Mail LDAP server to their list of directory servers. They don't need to worry about logging in or root servers. All they need to do is enter the name of the WebSTAR Mail server host into the Directory field, and they will be able to search for all the user names and email addresses local to that server (including groups and forwarding addresses).

Directory Listing Security

You should restrict access to your LDAP server, so that only people in your organization can find these addresses. Otherwise, they could easily be harvested by spammers. For restrictions, see "Protect Your User Directory" on page 62 and "Restricting Access to LDAP" on page 388.

LDAP Compatibility

LDAP is an Internet Standard and all LDAP clients should be able to see the WebSTAR LDAP server. The following are examples of LDAP compatible mail clients:

SOFTWARE	VERSIONS
Eudora Pro from Qualcomm for Mac and Windows	4.2 and greater
Microsoft Outlook and Outlook Express for Mac and Windows	3.0 and greater
Netscape Messenger for Mac and Windows.	3.0 and greater

DNS SERVERS AND MAIL HOSTS

To connect to WebSTAR Mail, your server must be properly identified in the Domain Name System (DNS). This requires more than a host name DNS record: you must also indicate that you can handle email.

Mail Exchange Records

The MX (Mail Exchange) record for your server points to hosts that can accept mail for that domain. For example, domain.com's DNS entry could include an MX record that directs all messages to a host named mail.domain.com.

MX records include the domain name, the code "IN" (Internet Data Class), the priority , and the host which will accept the messages.

If you have a single host, you do not have to set up an MX record (although you should be sure that your DNS administrator has not directed mail elsewhere). If you do choose to create an MX record, just repeat the host name:

```
example.com.  IN  MX  10  example.com.
```

If you have a separate mail server machine, point at that host name. In this example, all mail to domain.com will be handled by the host named mail.domain.com:

```
domain.com.  IN  MX  10  mail.domain.com.
```

Handling Mail for Multiple Host Names

For each host that you serve, you need to do two things:

- Create an MX record in each DNS entry, telling other servers that this server can handle email messages locally. If you do not run your own DNS server, work with your ISP or institutional DNS administrator to add this information.
- In the following example, email messages for domain.com will all be handled by mail.domain.com, and messages for example.com will be handled by the same host, example.com.

```
mail.domain.com  A      192.168.0.2
mail.domain.com. MX  10  mail.domain.com.
domain.com.      A      192.168.0.4
domain.com.      MX  10  mail.domain.com.
```

 For more information, see "DNS" on page 100.

 For technical information on MX Records, see RFC 974.

 Make sure that the name on the right side is an A (authoritative name), not a CNAME (alias).

 See "Checking Your DNS Entries" on page 102, and keep very good records of your DNS data.

```
example.com.      A      192.168.0.5
example.com.      MX     10  example.com.
```



For instructions, see
“Mail Hosts” on
page 375.

- Create a host entry in WebSTAR Admin, so that WebSTAR Mail knows that it should handle messages for this host.

EMAIL ACCESS FROM WEB BROWSERS

In addition to the traditional email clients, WebSTAR Mail provides an interface for users to read their mail via web browsers. While users can accept and download attachment files, they cannot upload and send attachments.

To use the web browser mail interface, have your users login to your mail server with a page URL that includes a `.mail` suffix, for example:

```
http://www.domain.com/web.mail
```

(replacing `www.domain.com` with your server's host name)

The WebSTAR Web Server will recognize the `.mail` suffix and bring up the web mail login page.

Log In

You'll see a very simple login page. Enter your email address and the password, and click **Login**. Some browsers, such as Microsoft Internet Explorer allow you to press the Return key to submit your name, while others such as Netscape's browser, require the Tab key.

Message List

As soon as you log in, you can see the list of messages, read and delete messages, download attachments, and write new messages.



The browser mail interface is compatible with all standard browsers. It does not use any advanced features such as DHTML..



If your email address is unique on the server, you can just enter the name part without the host or domain name.

Writing Messages

To create a message, click on the **Send Email** link in the message listing page. You'll see the message form.

The screenshot shows a Netscape browser window titled "Netscape: elaine@timtest.starnine.com - Send E-mail Message". The address bar contains the URL "http://timtest.starnine.com/web.mail?252@3.52qfjQWuM5Z*4@". The main content area displays the "Send E-mail Message" form. The form includes the following fields: "From: elaine@timtest.starnine.com", "To:", "Subject:", "Cc:", and "Bcc:". Below these fields is a large, empty text area for the message body. At the bottom left of the form area is a "Send Message" button. The browser's status bar at the bottom shows various icons.

i To go back to the message list without sending anything, just use the Back button or menu item in your browser.

Message Form Headers

This form has several fields for message headers, and a body field to enter your message.

- **From:** already includes your email address
- **To:** the email address of the main recipient(s)
- **Subject:** the subject of the message
- **Cc:** other recipients
- **Bcc:** invisible recipients, not displayed to any other recipients

Message Body

Type the body of your message in the scrolling text field. It can handle about 32,000 characters and uses the font you specify in your browser's monospaced font preference.

i For people on the same mail host, you can just type the first part of the address: you don't have to type the host name.

You can't upload any attachments or enclosures when you send messages using browser-based mail. You must use a POP or IMAP client to send enclosures.

Sending Messages

When you're finished with your message you can click the **Send Message** button. This will send the message to the server and take you back to the message list page.

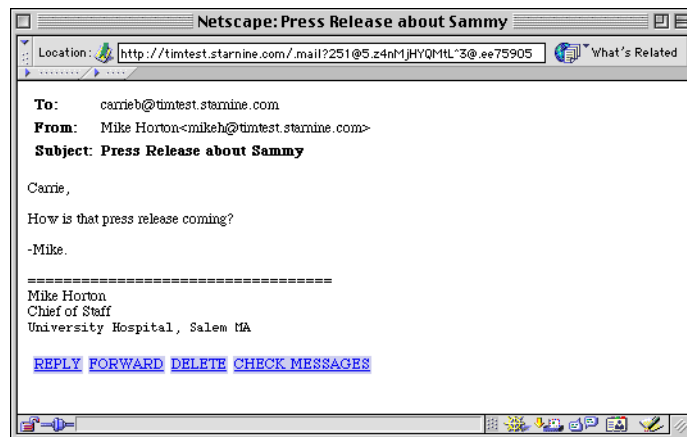
Viewing Messages

Click the **Check Messages** link to bring up the listing of messages, or refresh it to be sure you see all incoming messages, just like when you log in. To reply, forward or delete messages, click on the message to view it, then click on one of the command links in the message page.

After reading messages, the links will be marked as viewed, using the browser preference setting.

Acting on Messages

To read a message, click on the date, sender or subject in the listing page. You'll see the message header, with the main recipient (indicating mailing lists, for example), the sender, and the subject, followed by the body of the message.



If there are any enclosures, they are listed after the text of the message. When you click on the enclosure link, the browser will automatically start to download the file. In some cases, it will bring up

a dialog allowing you to specify where on your local system to save the enclosed file.

All messages are retained until you delete them or download them to an email application that uses the POP protocol, which will delete them unless you override that option.

Reply

When you click the **Reply** link, you'll see a Message Form Headers (described on page 364). The **To** field is filled in with the sender's address, and the **Subject** field has their subject. The original message is already entered into that field.

The body area contains the original message, with message quote marks (>) on the left side. When you type your new text into the field, start the line without the message quote, to show that it's your reply and not the original words.

Netscape: carrieb@timest.starnine.com - Reply to E-mail Message

Location: <http://timest.starnine.com/mail?253@5.z4n1jHYQM1L4@.ee75905> What's Related

Reply to E-mail Message

From: carrieb@timest.starnine.com

To: Mike Horton<mikeh@timest.starnine.com>

Subject: Re: Press Release about Sammy

Cc:

Bcc:

>Carrie,
>
>How is that press release coming?
>
>--Mike.

Nearly done---just need a final proof and I'll be ready with plenty of time to spare before the briefing this afternoon.

Carrie
=====

Carrie Brady
Public Relations Director
University Hospital, Salem MA

Send Message Send And Delete Original

When you're finished with your message, you can click the **Send Message** button, or **Send And Delete Original**. This will send the message to the server and take you back to the message list page.

Forward

Clicking the Forward link is much like Reply. The Message Form Headers has the subject and body fields filled in, but the To field is blank, so you can enter a new recipient's email address.

When you're finished with your message, click the **Send Message** button or **Send And Delete Original**. This will send the message to the server and take you back to the message list page.

Delete

To delete a message, you must view it and click the **Delete** button. There is no confirmation, and no way to get a message back if you change your mind, so be careful when you delete messages.

MAIL ADMINISTRATOR RESPONSIBILITIES

Once you have installed a mail server, you have to manage email accounts actively, and users may require substantial technical support. You will also need to be very careful to keep the server up and running—many people rely on their email servers even more than their web sites.

Mail Server Account Management

You will have to create and maintain accounts, explain the differences between accounts and email addresses, reset passwords when users forget them, help with login and email client problems, and so on. For more information on this, see “Account Tips and Examples” on page 397.

We recommend that you inform your users that their email is not private, that you can see the senders and recipients in the log, and that you can change their password and log into their account at any time. Make sure they understand your rules, especially if you do not allow private messages to be sent via a company server.

In more serious situations, email users on your host may be sending spam or threats. In those cases, your Terms of Service agreement (if you are an ISP) or company policy on email use should clarify what behavior you will and will not accept.

Reading the Postmaster Messages

You must have and read a “Postmaster” account that accepts mail to the postmaster address at all email hosts. This account will get



For background, see “Server Administration Responsibilities” on page 87, and RFC1173: Responsibilities of Host and Network Mangers.



See also: “Dealing With Spam (Unsolicited Email)” on page 370.

messages from other mail administrators, other mail servers which have received messages with problems in the headers, confused people looking for someone in your company, and so on.

You must read these messages frequently, at least five times a week, as some of them will be urgent and require immediate attention. For example, if one of your users is sending unsolicited messages or their system has been infected by an email attachment virus, and someone sends a message to this account, they will expect you to act right away. If you are unable to read messages to this account, because you are on vacation or otherwise inaccessible, be **sure** to arrange for someone else to read the messages in the Postmaster account.

Server Error Reports

When incoming mail is not accepted due to insufficient disk space, or when automatic backups fail for any reason, the Mail server will send a message to the Postmaster account. That's another reason to make sure you check mail for this account frequently.

Unknown Accounts

When messages come to the server for accounts that do not exist in the specified host, they will be forwarded to the account that you have specified to accept mail for unknown accounts for that host. This can be the Postmaster address, or another address. These messages will be a mix of legitimate messages sent by mistake, spam and other junk.

In any case, be sure that someone reads and handles these messages, either by answering them, returning them to the sender, forwarding to the appropriate person, or deleting them (if they are spam or other unwanted messages).

Tracking Mail Server Usage

As a mail administrator, you must track the activity of your server. If you have a busy server and many users, you should check the server often and make sure that messages are moving properly, that you have enough disk space, and so on. For servers with few accounts, you can just check once a day or even less often.

Monitoring Connections

You should use the WebSTAR Admin Mail Monitor to track your mail server activity. If your server is very busy, you may see the Connections bars fill up. In that case, you should use the Mail Connections (described on page 377) to add more connections to your most



You can forward postmaster mail to another email address. For details on configuring a forwarding address, see "Forward To" on page 393.



See "Unknown Address" on page 376.



See “Server Administration Responsibilities” on page 87.



For information and examples, see “Reporting” on page 404



To set this period, see “Hold Undeliverable Mail” on page 378.



To set limits on how much space a user can have see “Mail Storage” on page 373.

overloaded protocols. You should also quit the server and allocate more RAM to WebSTAR, unless you have a lot of free memory.

Reading Reports

Mail server reports show you how many messages and how much data is flowing through your server. You can see how many SMTP messages come in and go out of your mail hosts, and activity of each individual user on your server. You can get Mail server reports daily, weekly or monthly (see “Setting the Report Schedule” on page 405). This tells you if a particular host or account is extremely busy: then you may want to mandate reduced use of the server, increase WebSTAR’s memory allocation, or move a mail host to another server.

Managing Your Mail Queue

When you look at the mail queue, you’ll see all the messages that could not be sent because the receiving SMTP server was not responding. Messages will stay in the queue until the receiving server appears or the undeliverable mail period passes, in which case, the server returns the message to the sender.

Checking the Disk Space

Tracking disk space is very important. Email can fill up a disk very quickly with messages and attachments, especially if you have many IMAP accounts and allow users to store messages and files on the server. Servers can also fill up when users go on vacation, suddenly start sending large graphics or binary files, or subscribe to active mailing lists, adding many entries to the mail log files.

All messages are saved in the *WebSTAR Mail Users* file, and the attachments are in the *Attachments* folder. The server always keeps two backup copies, and requires swap space to make a new backup before deleting the old one. For example, if your current *WebSTAR Mail Users* file takes up 25 MB, your next backups will also take that much room, and you need at least 25 MB free space on the disk for the copy process.

You should check the server disk space regularly, to make sure there is free space. Track the rate of disk space usage to make sure you check it often enough.

For example, if you have a server with 10 users and 500 MB of free space, if you notice that the disk is filling up at the rate of 5 MB per week, you can check disk space weekly. On the other hand, if you have 100 users, 500 MB of free space, and the disk is filling up at 50 MB per

week, you may want to check the space daily (and implement a storage limit for some or all users).

Checking Logs

Mail logs provide detailed information about logins, incoming and outgoing messages, connection errors, and forgotten passwords. You can use these logs to identify patterns of problems such as routing errors or attempts to break into accounts by guessing passwords. In addition, you can inspect the log to decide if one of your users is sending messages to many recipients at once, which may be considered spam.



For information see “Activity Log” on page 400.

Backing Up and Restoring Email Files

The most important file to back up is *WebSTAR Mail Users*. It stores the messages as well as the user information.

WebSTAR automatically keeps two backup copies: *WebSTAR Mail Users Backup.1* and *WebSTAR Mail Users Backup.2*. It will automatically delete the older backup after successfully making a new copy.

If something happens to the *WebSTAR Mail Users* file, the server will automatically recreate it, with all the previous email messages and account information. It does this by comparing the *Backup* files and the *Transaction Log* and rebuilding the users file based upon that data.

It's always a good idea to keep external backups of your email files. You should be prepared for a hard drive crash, a server machine failure or a physical disaster such as a fire in the building. Be sure that you store backups offsite frequently, so that you can re-create your mail system in an emergency.

Dealing With Spam (Unsolicited Email)

Unsolicited messages, whether for business, political or other purposes, is a serious problem on the Internet. This email, known as **spam**, wastes the time and money of the recipients, especially those who must pay for their Internet connection by the minute or second. Therefore, all mail administrators should keep their servers from participating in spam mailings. In addition, if your server sends out spam, it may be **blacklisted**—registered as a spammer by a spam-checking service—and all messages from your server will be rejected by other mail servers who use that service.

There are three ways your server might become involved in spam mailings.

1 Another server is using yours to send spam.

If you allow your server to be a **relay** server (to forward messages from other servers without restriction), your server will probably be used without your consent to send spam.

To avoid this, always check the Require Prior Client Login box in the Mail Setting panel Mail Connections (described on page 377). This will require users to check mail before sending messages, proving that they are in fact legitimate users.

2 One of your mail users is sending spam.

Your users may be convinced that sending unsolicited email is acceptable, and start sending spam. You can check this in your log file to see whether this account has sent many messages to large numbers of recipients. In that case, you may need to invoke your Terms of Service agreement and remove the account from your server. Again, you should do this before your server is blacklisted.

3 Your users receive large amounts of spam.

A few pieces of unwanted email should not be cause for alarm, but some users get on lists and start getting dozens of spam messages a week or even every day. In that case, you can use Mail Allow/Deny (described on page 387) to reject messages from the host names or IP addresses of the most blatant spammers.

In addition, services such as spamcop.net will help you track down and remove spam accounts.

This chapter explains how to use the Defaults, Hosts, Connections, Caching, and Routing panels to set Mail server preferences in the WebSTAR Admin application.

For information on administering email accounts, see “Users & Accounts Settings” on page 391; for reporting and logging, see “Mail Monitors, Logs, and Reports” on page 399.

MAIL DEFAULTS

This panel provides general settings for the WebSTAR Mail server.

Mail Storage

Storage

You can limit the amount of disk space for each Mail server user account. You may set the **Limit Storage Per User** field to any amount from 1 MB to 9999 MBs. If you retain the **No Limit** default, you risk filling up your hard disk, so you should consider this option carefully.

Messages

You can also limit the number of messages retained for each user account. This includes IMAP messages in server mailboxes, POP messages that have not yet been read or those that have been read



You can override the storage and message limits individuals in Users & Accounts Settings (described on page 391).

but retained on the server. The number of messages can range from 1 MB to 99999 . The default is **No Limit**.

Alternate DNS Server

Your WebSTAR Mail server uses the Domain Name System (DNS) to locate domains and send messages. By default, WebSTAR uses the DNS server entries in the machine's TCP/IP Control Panel. However, if your DNS servers are slow to respond, email may pile up.

To specify a particular DNS server for mail server lookups, type the IP address or DNS host name, like this: `dns.domain.com`.

Most servers will not need an alternate DNS server, and the default for this is an empty field.

Web-Based Email

The WebSTAR Mail server allows users to read and send email using forms in web browser pages, like this:



You can enable or disable that feature with this checkbox. The default is **enabled**, so if you do not want your users to access their mail through this form, you must check the box and click the **Save** button.



For information, see "Email Access from Web Browsers" starting on page 363.

Backup Scheduling

Email messages are very valuable to your users, so you should be particularly careful in making sure that you have archive copies of the message storage file.

The default on the backup menu is **Weekly**, but you can use the popup menu to select **Daily** or **None**. You can also set the exact time of day: the default is 4:00 AM. If you choose **Weekly**, you can also set



For instructions on backup, see "Backing Up and Restoring Email Files" on page 370.

the day of the week using the popup menu that below the time field: the default is **Sunday**.

If you select **None**, be sure that you have another way to back up the messages, such as an automated archive system, or you risk losing your entire mail system if the server fails.

MAIL HOSTS

This panel allows you to send and receive email for more than one email host or domain name. For example, you could accept messages for your main domain address, for example joe@domain.com, for a specific host in that domain: cj@hq.domain.com, for another domain entirely: mike@knickknacks.com, or for another host in another domain: david@products.tchotchkeys.com.

SMTP hosts are somewhat different from the Web server hosts. Mail hosts rely on both CNAME and MX (mail exchange) records in the DNS server: for more information, see “DNS Servers and Mail Hosts” on page 362.

Your DNS records must be set up correctly before you will receive mail on your local server.

For each email host, you can specify separate information.

The screenshot shows a window titled "Hosts" with a table of email hosts. The table has four columns: Host Name, Unknown Address, Copy To, and Redirect To. The rows are as follows:

Host Name	Unknown Address	Copy To	Redirect To
domain.com			mail.domain.com
example.com	unknown@example....		
knickknacks.com	postmaster@domain... monitor@knickknack...		
mail.domain.com	postmaster@domain...		
tchotchkeys.com	mail-handler@tchoto...		

Below the table, there are input fields for the selected host (knickknacks.com):

Host Name: Unknown Address:

Copy To: Redirect To:

At the bottom, there are buttons for "Import", "Export", "Delete", and "New".

Host Name

This is the name of the Internet host or domain as it will be in the incoming email messages (the part after the @). If you only have one host name in one domain, just click the **New** button to enter it here. For multiple mail hosts, enter each one in this list.

If you do not enter a name in this list, WebSTAR Mail will not accept mail for the host. You must enter a host name for each email host and domain name which will receive mail on this server.

Unknown Address

Your WebSTAR Mail server will receive some messages for addresses that do not exist at this mail host. This happens for several reasons:

- typing mistakes by the sender
- attempts to send legitimate mail by guessing email addresses
- messages to addresses have been deleted because the account is removed
- replies to messages masquerading under an address from your server (usually from spammers)
- unsolicited mail attempting to guess account names on your server.

When the mail server receives messages for accounts that don't exist, it will send them on to the email address you enter in this field. This address can be on this mail server or any other server.

This feature is optional, and WebSTAR Mail will automatically return an error to the sender if you do not fill in the field.

Copy To

If you need to monitor all incoming messages on your server, for legal or security reasons, you can do so. Enter the email address, on this mail server or any other, in the **Copy To** field and a copy of all messages will be sent to that address.

Redirect To

If you need to redirect all email addresses for a host to another host or a specific email address. You may want to use this as a backup to the MX records in your DNS record when you have a particular host taking care of your mail.

For example, you could make a host entry for `knickknacks.com` and redirect all messages to `domain.com`, or to `knickknacks@domain.com`.



Someone will have to read these messages, forward the misdirected ones and delete the spam. Make sure that you allocate time for this task.



If you are monitoring messages, we recommend that you **inform your mail users** that they should not send or receive private messages via this server.



Be sure that the server on the other end knows what to do with these messages: you do not want to get into a mail loop!

Before continuing, send a test email to an address on this host name. It should be sent on to the equivalent address on the redirect host, or the specific email address if that's what you entered in the field.

When you use this, the server does no local processing, so it does not use the **Unknown Address** or **Copy To** fields.

MAIL CONNECTIONS

This panel lets you control every external connection that the WebSTAR Mail server makes.

About Connections

Email **Connections** are interactions between a server and another server or a client, via TCP/IP. For example, when a POP mail account logs in to download email, that's a connection.

The Mac OS Open Transport system allows a total of 500 connections per machine. WebSTAR Server Suite uses 94 in its default configuration, so it's a good idea to keep a running total and make sure you stay under 500 connections.

To tune your server, start with the default configuration and watch the monitor to see if you need to increase the connections for any particular service. Note that increasing connections will not compensate for problems in network connection bandwidth and latency.

Connections may be restricted by available RAM, processor speed, other applications and CGIs, capacity of the network connection, and so on. The online WebSTAR Tech Note will give you updated suggestions for the most current techniques to optimize your server:

<http://www.starnine.com/support/technotes/wsperformance.html>

Mail Server Auto-Restart

To accept the connections settings, the Mail server must be restarted. WebSTAR Mail automatically restarts itself when you make changes and click the **Save** button—you do not have to quit and restart the WebSTAR application.

You'll see that the log window reflects the fact that the IMAP, POP and SMTP servers all restart themselves.

```
Tue, 1 Jun 1999 12:26:31 -0700 ** Restart IMAP
Tue, 1 Jun 1999 12:26:31 -0700 ** Restart POP
```

Tue, 1 Jun 1999 12:26:32 -0700 ** Restart SMTP incoming
Tue, 1 Jun 1999 12:26:32 -0700 ** Restart SMTP outgoing

This process usually takes one to two seconds, but during that time, **all incoming and outgoing connections are terminated.**

Connections

SMTP Connections

Outgoing Connections:

12

Incoming Connections:

12

Hold Undeliverable Mail (hours):

4

☒ Enable 8-bit message format

Incoming Timeout (Minutes):

10

Incoming Size Limit (MB):

0

Relay Restrictions & Spam Prevention

☒ Enable SMTP Forwarding

☐ Enable VRFY

☐ Enable EXPN

☒ Require prior client login within

160

minutes.

IMAP Connections

Maximum Connections:

12

Timeout (Minutes):

30

Post Size Limit (MB):

0

POP Connections

Maximum Connections:

12

Timeout (Minutes):

10

☐ Require APOP authentication

LDAP Connections

Maximum Connections:

6

Timeout (Minutes):

30

SMTP Connections

WebSTAR Mail uses the SMTP protocol to send and receive messages from other Internet mail servers.

Outgoing Connections

This is the number of simultaneous connections to other SMTP servers, while attempting to send mail. The number of connections can range from 0 (which will disable outgoing mail services) to 500, and the default is **12** connections.

If you have an active server and notice that your outgoing mail queue is getting large, you can increase this number. If you allocate more connections, be sure to increase the WebSTAR memory partition by an additional 10K of RAM per connection.

Hold Undeliverable Mail

When WebSTAR Mail server tries to send messages to other SMTP servers, they may be temporarily unavailable due to network or server problems. The SMTP protocol allows servers to try connecting over

 For more information, see “SMTP” on page 358.

and over again, and the WebSTAR Mail server tries every five minutes. This field lets you specify how long to keep trying.

If the server cannot be found during the specified time, it returns the message with an “undeliverable” error. The mail log will contain an error as well.

The default is **4** hours and the length of time can range from 0 to 999 hours. Many Internet mail servers use three days (72 hours) as their hold time.

Incoming Connections

The number of connections for incoming messages from other SMTP servers can range from 0 (no messages accepted) to 500, and the default is **12** connections.

If you allocate more connections, be sure to increase the WebSTAR memory partition by an additional 10K of RAM per connection.

Timeout

Email messages come into the WebSTAR Mail server in packets, rather than the entire message coming at once. Therefore, the server must wait for all the packets for each message before storing it locally. If the network is busy, incoming data may take a while to get to the server. The timeout value specifies how long the server should wait before considering that the message has been lost in transit.

The range is from 0 to 999999 minutes and the default value is **10** minutes.

Maximum Message Size

You can limit the size of incoming messages, including attachments. Very large messages can slow down the server and fill up the hard disk. The default is **0** (no limit) and the maximum size allowed is 999 MB.

Enable 8-bit message format

Older email servers only recognize English letters and basic punctuation: these are known as **7-bit ASCII** characters. If they see other letters in the Roman character set, such as **ø** and diacriticals like **é** and **ü** (these use another bit, so they are called **8-bit** or **high-ASCII** characters) older servers get confused. In addition, attachment files in binary format, including MacBinary, may also include 8-bit characters.



For more information, see “SMTP Connections” on page 378.



If someone tries to send a message that is too large, the WebSTAR Mail server replies that it was too long (error 552) and displays a message in the monitor and log.

The WebSTAR Mail server will automatically handle these high-ASCII characters, so the default for this setting is **enabled**.

If your server often connects with others which cannot handle these characters, uncheck this box and the server will take care of converting them into 7-bit characters.

Relay Restrictions and Spam Prevention

WebSTAR Mail provides several options to avoid having your server used by spammers to send their messages. Before changing any of these, be sure you understand the implications.

Enable SMTP Forwarding

This option allows email clients, including those of your users, to send mail messages via your server. It is **enabled** by default.

When forwarding is enabled, you should set the option below to require the clients to log in before sending mail. Otherwise, you are providing an **open relay**—a conduit by which spammers may send unrequested email using your identity. The only case in which you might want to relay without requiring a login is if you are within a corporate intranet, and are not accessible to spammers.

Require Prior Client Login

To make sure that the only people sending messages via your server are your users, you can require them to check their mail within a certain time period before allowing them to send mail via this server.

The time period can range from 0 to 999 minutes, and the default is **160** minutes.

Enable SMTP VRFY Command

This command is used by email clients to verify a user name with the server. Given a string, the server responds with a positive reply code if it knows of the user or with a negative reply code if it does not. This allows email clients to notify users that an address does not exist on a server, rather than waiting for a reply from the postmaster.

By default, VRFY is **disabled**.

Enable EXPN

EXPN command accepts a mailing list name and returns the list address. It is important for diagnosing inadvertent mail loops.

By default, EXPN is **disabled**.



See also “Dealing With Spam (Unsolicited Email)” on page 370.



Web mail is not affected by this restriction: if you want to stop all outgoing messages, set the SMTP Outgoing Connections (described on page 378), to 0.



Some spammers may attempt to use these commands to harvest addresses on your server. That is why the features are disabled.

IMAP Connections

When an IMAP mail client logs in, they create a connection. They will hold that connection until they log out or the timeout value is reached.

Maximum Connections

The number of connections can range from 0 to 500 and the default is **12** connections.

If you allocate more connections, be sure to increase the WebSTAR memory partition by an additional 10K of RAM per connection.

Timeout

WebSTAR Mail server will automatically close the connection when a client is idle (not asking for or sending messages). This opens a space for other clients to connect.

Some IMAP email programs will automatically disconnect after all contacts, and then re-connect after a specified period of time, to check for new messages. Reconnecting involves a delay, so your users might prefer to stay connected as long as possible.

The timeout can range from 30 to 999 minutes and the default value is **30** minutes.

Post Size Limit

You can limit the size of data transferred from IMAP local folders to the server. This avoids a situation where a huge attachment might fill up your available disk space. The default is **0** MB (no limit), and you can set it up to 999 MB.

POP Connections

When an email client application logs in to download messages using the POP protocol, it creates a POP connection. You can adjust the settings for best performance in your particular situation.

Maximum Connections

The number of connections can range from 0 (will ignore all POP login requests) to 500, and the default is **12** connections.

If you allocate more connections, be sure to increase the WebSTAR memory partition by an additional 10K of RAM per connection.



For more information, see "Mail Connections" on page 377.

Timeout

POP mail clients log in and download mail, then users read the messages on their local systems. Each of these accesses creates a connection. When the POP client doesn't request any new messages for a certain period of time, the server closes the connection, to allow other POP clients to connect.

The range can be from 0 (no timeout, not recommended) to 999 minutes and the default is **10** minutes.

Require APOP Authentication

APOP adds a great deal of security to POP client passwords: for details, see "APOP" on page 359.

This feature is **disabled** by default.

LDAP Connections

The LDAP server allows clients to look up email addresses on your server: it's like a corporate or school directory.

Maximum Connections

The number of connections can range from 0 to 500 and the default is **6** connections.

If you allocate more connections, be sure to increase the WebSTAR memory partition by an additional 10K of RAM per connection.

Timeout

LDAP clients may hold a connection open: in that case, the server will automatically close it after this amount of time.

The default is **30** minutes, and the amount of time can range from 30 to 999 minutes.

MAIL CACHING

WebSTAR Mail uses temporary storage in memory and on disk to improve access to data. This allows the server to respond quickly when users retrieve or send their messages.

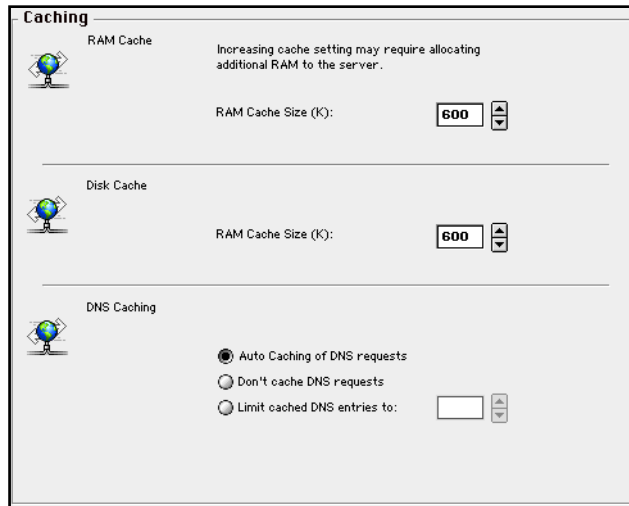


While a client has a connection open to a POP account, the mailbox is "locked" for incoming mail and anyone else trying to access that account.



You can override the this setting for individuals in the Users & Accounts panel, see "Require APOP" on page 394.

You can adjust the settings if you have a lightly used mail server and want to free some memory, or heavy traffic and want to make the server more responsive.



RAM Cache

This setting specifies how much of the WebSTAR server's memory allocation will be used for the mail server internal lists such as which messages have been read, messages in a mailbox, whether the session is locked or not, and so on. This cache automatically purges old information as it needs the room.

i The Mail monitor window will indicate how much memory is available. Keep an eye on this window to learn if you need to allocate more memory.

The default is **600 K**, and the values can range from 600K to 9999K. If you have a large number of concurrent users, which is most likely when they are using IMAP or Web Mail, increasing this cache size will improve performance.

If you increase the cache, be sure to increase the WebSTAR server application memory partition the same amount.

Disk Cache

The disk cache stores transactions for the mail database. The actual message content and user directory are permanently stored on the disk, so the cache is used to load these into memory as needed.

The default is **600 K**, and the values can range from 600 to 9999K.

Increase this if you are running a very busy server with many simultaneous connections.

DNS Caching

Every time the a mail server sends a message or checks a login, it has to convert the host name to an IP address using a Domain Name Server and MX records. Looking up the same host names over and over can be very inefficient, so the WebSTAR Mail server can store the IP addresses.



For more information, see “DNS” on page 100

- **Auto Caching of DNS requests** (the default) lets WebSTAR Mail server use it's internal caching algorithm and remove entries when it fills up the available memory. DNS entries in this cache are refreshed every 12 hours as well.
- **Minimal DNS Caching** flushes DNS entries every five minutes. You may want to use this for mail servers with little traffic, or if your DNS server is being updated, and you want to make sure you get the new addresses.
- **Limit cached DNS entries to:** limits DNS caching to a certain number of records. The range is from 0 to 999 DNS entries, and there is no default.

MAIL ROUTING

Routing allows you to override the default SMTP system of sending messages. You may need create routing entries if you:

- use a **relay host**: a mail server that will look up addresses and send outgoing mail along to its destination. You might do this to reduce the load on the server, or because you are behind a firewall and cannot send messages directly.
- send many messages to a particular country, and you have access to mail server there which is more efficient at sending messages in that area.
- send many messages to remote or international mail servers that do not respond quickly and may need a long timeout value.
- have a server that is not always connected to the Internet.
- need to change settings for a specific mail host, such as timeout or ETRN.

All messages to hosts and domains which do not have entries in this routing table will use the normal DNS and SMTP system.



In most cases, you do not need to set up any additional routing.



If you want an SMTP server to relay messages, contact the mail administrator and make arrangements before creating a routing entry.

Editing the Routing Entries

Use the WebSTAR Admin Mail Settings Routing page to edit the routing entries.

Domain	Route
domain.com	mail.example.edu

Action: 1

Domain: Route:

Timeout (Seconds): Retry Interval (Minutes):

Expire After (Hours): ☐ Enable SMTP ETRN Command

Routing Wildcards

You can use a wildcard (*) for part of the host name or IP addresses, or the following regular expression items:

- * matches 0 or more characters.
- ? matches any single character
- [...] matches any single character in the set
- [^...] matches any single character not in the set
-] can be the first character in the set
- x-y is the range of characters from x to y
- x is a specific character
- - can be used as a specific character at the start or end of the list of characters and ranges
- \ matches the following character, disregarding special characters

Examples:

```
*.domain.com
mail[123].example.org
post[a-z].domain.za
mail?*.example.com
```



The first matching entry will be used for routing.

Domain

Enter the domain name, host name, or IP address for this entry. All messages going to matching hosts will be processed according to the settings in this entry.

Route

The host and domain name of the destination SMTP server, or one which will relay messages from your server to their destinations.

Routing Options

Timeout (Seconds)

This field specifies how long to wait for the relay server to respond before dropping the connection and trying again later. This may happen when the network between you and the relay server is overloaded, the relay server goes down, or there is another problem.

The default is **0**, meaning that this entry should use the value from the SMTP Connections Timeout (described on page 379), and the range is from 0 to 100 seconds.

Retry Interval (Minutes)

This field specifies how often to try contacting the destination or relay server.

The default is **0**, meaning the default internal value of four hours (240 minutes), and the range is from 0 to 999 minutes.

Expire After (Hours)

This field specifies how long to keep trying to contact the relay server before returning the message to the sender.

The default is **0**, meaning that the value from the SMTP Connections Hold Undeliverable Mail (described on page 378) and the range is from 0 to 100.

Enable SMTP ETRN Command

If your computer is only intermittently connected to the Internet (or another TCP/IP network), you can still run a mail server. You must work with the network administrator or ISP to make sure that their mail server can hold your incoming messages for you when you are not connected, and respond to the ETRN command when WebSTAR Mail has reconnected and is ready to receive these messages. Not all ISPs will provide these services. If so, that server will be your remote host,

storing incoming messages until your server connects. WebSTAR Mail server will also store (queue) the outgoing messages and send them whenever your machine connects to the TCP/IP network.

MAIL ALLOW/DENY

The WebSTAR Mail server allows you to specify exactly who can access the mail services and who cannot. This increases your security, reduces your vulnerability to hackers, and protects your server from spammers who may want to use it to send mail or gather email addresses.

As the name implies, an **Allow** entry for a realm means that the Mail server will accept connections if they come from a machine with that domain name, host name or IP address.

A **Deny** entry means the Mail server will reject connections if they come from a machine with that domain name, host name or IP address.

Allow/Deny Services

Restricting Access to SMTP Incoming

You can reject messages from certain email servers which you know send spam messages to users on your server. For example, if a mail server named mail.spam.example.com has sent several unwanted messages, you could create a Deny entry for that server, and your WebSTAR Mail server will reject all messages from that server.

Use this option rarely and wisely: spammers tend to move around and hijack servers, so you could reject legitimate messages from customers or colleagues.

Restricting Access to POP

You can specify that only certain hosts, domain names or IP address ranges can log into your WebSTAR Mail server using the POP protocol. For example, you could limit access to the machines in your institution's domain. However, this means that your users cannot read their mail from home or while travelling if they use a commercial ISP.

Restricting Access to IMAP

You may also choose to allow only specific hosts, domains or IP addresses can use the IMAP protocol to access the server. Again, it can make users who want to access their messages from home or on the road quite unhappy.



Machines which use dialup Internet access via ISPs do not have static host names or IP addresses, so you can't create Allow entries for them.



To accept messages from all other Internet mail servers, be sure to add an Allow * entry at the end of this list.

Restricting Access to LDAP

In most cases you should Deny access to the LDAP server to everyone outside of your domain. While it would be nice to allow customers or friends to look up email addresses for your users, that access could also be used for **address harvesting** (spammers gathering addresses for future messages). You might also want to limit access to IMAP accounts to certain domains or IP addresses.

Editing Allow/Deny Entries

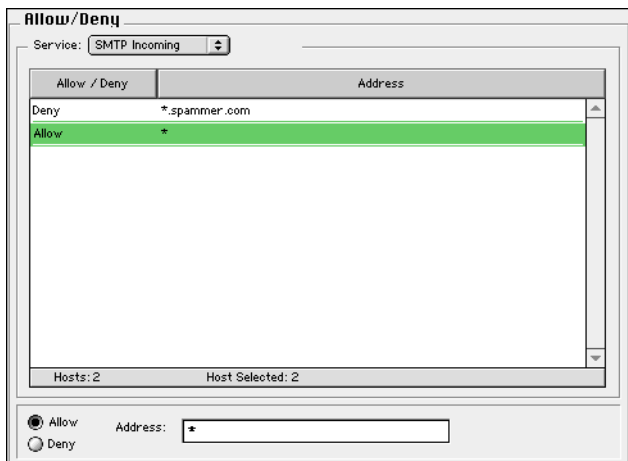
By default, all lists are empty, which means that they allow access to all hosts. This is like adding an entry that says Allow * (where the star is a wildcard meaning to match every machine). You can create entries for specific hosts, domains or IP addresses.



For details of wildcards and domain names and IP addresses see “About Address Matching” on page 389.

Creating an Allow/Deny Entry

- 1 Open the WebSTAR Admin application File Settings window.
- 2 Choose the Mail Settings Allow/Deny panel.



- 3 Designate the Service (SMTP Incoming, POP, IMAP or LDAP) in the popup menu at the upper left of the panel.
- 4 Select the row before you want the new entry, the **New** button to create a new entry. The new row will be inserted above the row you selected.

If you already have some entries, think about the order of processing in the list: the server stops at the first matching entry, so go from the most specific to the most general.

- 5 Choose the **Allow** or **Deny** radio button at the left.



To avoid confusion, always create an explicit **Allow *** or **Deny *** entry at the end of your list, so you can tell what will happen to other hosts.

- 6 Enter the host name or IP address of the machine you want to deny or allow access to (see below for details).
- 7 The last row specifies how to handle all other hosts. If it is Deny, all other hosts will be denied; if it's Allow, all others will be allowed.
- 8 Click the **Save** button to send the setting back to the server.

Server Update

To handle these changes, the SMTP, POP, IMAP and LDAP servers will automatically restart themselves. You'll see a message to that effect in the server log.

About Address Matching

You can specify host names, domain names or IP addresses in the Address field.

If you want to use host or domain names, make sure you've checked the box to Use DNS for Server and Client Lookups (described on page 136).

You can use the wildcard (*) to take the place of part of any text, such as the host name. For example, you can deny SMTP Incoming access to a specific mail server which has been sending unwanted messages:

Deny *.spam.example.com

or allow IMAP access to all "tech" machines in your organization, using the wildcard as part of a simple string:

Allow tech*.domain.org

You could also allow LDAP access to a specific IP address subnet

Allow 192.168.19*

Don't forget to add an **Allow *** (or **Deny ***) row at the end of the list, so you'll remember what happens to the other machines.



For other mail settings, see "Mail Users & Accounts" starting on page 391 and "Mail Monitors, Logs, and Reports" starting on page 399.

To allow people to send and receive email messages, you must create accounts with user names on your WebSTAR Mail server. Each person can use their account to log in, download their messages to a POP mail reader, or read them on the server using IMAP or the Web Mail interface, and send messages to other email addresses.

With WebSTAR Mail, you can set up multiple domains, hosts and user accounts, and you have a great of flexibility in automatically forwarding mail from one host or account to another.

This chapter explains the options in the WebSTAR Admin Mail Settings Users & Accounts panel, and provides some advice on setting up and administering your mail server.

USERS & ACCOUNTS SETTINGS

Use this panel in the WebSTAR Admin Mail Settings section to create and administer email accounts. Each user name is a unique log-in name associated with an email address, and is used when the mail client gets POP or IMAP messages.

The account list at the top shows each account and their settings. This list will be updated when you click the **Save** button to send the new information to the server.

Users & Accounts

Account ID	E-mail	Storage	APOP	Messages
jim	jim@timestest.starnine.com	0	false	0
jjones	jjones@timestest.starnine.com	0	false	0
joakim	joakim@timestest.starnine.com	0	false	0
joe	joe@example.org	0	false	0
john1	john1@timestest.starnine.com	0	false	0
johnbtest	johnbtest@timestest.starnine....	0	false	0
jsanborn	jsanborn@timestest.starnine....	0	false	0
jvhelpu	jvhelpu@timestest.starnine.com	0	false	0

Accounts 185

Account ID: Password:

E-mail Name: Host: Message Limit:

Forward To: Storage Limit (K): ☐ Require APOP

IMAP Privileges

☐ Create Mailboxes ☐ Delete Mailboxes ☐ Rename Mailboxes

Account ID

The Account ID is the unique user name for each account on this mail server: it is **not** the same as the email address. When a user sets up

their email client, there is always a field for user or account name, so they can log in.

As with email addresses, you cannot use any spaces or diacritical characters in the account name. You should also avoid punctuation, although you can use plus (+) if necessary.

Password

This is the password for the user to log into the server. For security, follow the standard password rules (for more information, see “Safe Passwords” on page 96). **If no password is entered, the user will not be able to log in to the account.**

E-Mail

This is the public email address which will send and receive Internet email messages, so it's in the form name@host.tld (name, @, then the mail server host name, domain and top-level domain type). It can be the same as the user name or different.

Unique Email Addresses

You can only have one email address with the same name on the same mail server host. If you have one mail server host name, you must create unique names for each user. For example, there can only be one “david@starnine.com”, even if five Davids work for the company at the same time, so each one must include a differentiating factor, such as a last name.

If you have several email hosts, you can have the same email name on each one, because the host names are different. You can have four email addresses which are simply “joe” as long as they are on different hosts and have unique user names:

- joe@knicknacks.com (user name: joe)
- joe@tchotchkeies.com (user name: joejoe)
- joe@mail.domain.com (user name: watanabe)
- joe@africa.domain.com (user name: joe2)

Host

This popup menu lets you choose which mail host name goes with this email address. All the host and domain names you have entered in Mail Hosts (described on page 375) will be available here.



Users cannot change this password remotely, so make sure that your passwords are long enough to be safe but short enough to be memorable.



For tips on how to organize email addresses in your company, see “Account Tips and Examples” on page 397.

The default is **any**, meaning that this is account should get email coming to any of the mail hosts defined in this WebSTAR Mail server. For example, the Postmaster account can use this feature to get messages sent to the Postmaster account of all hosts on this mail server.

Message Limit

This field allows you to override the message limit in Mail Defaults (described on page 373) for this particular user. The default for this is **0** (which means “use the default value”), and the range is from 0 to 999999.

Forward To

You can create accounts that simply forward messages on to another email account, without allowing login access. For example, if a person changes their name, they may want to change their primary email address, while still getting messages sent to their old address.

The forward-to field must include a full email address, such as `stephanie@domain.com`.

When the message is forwarded, it is not retained in this account, so if you log in, there will be no mail for this account. The log entry shows the forward information, but not the original account, so a message forwarded to another server would look like this:

```
SMTP In: Wed, 9 Jun 1999 20:49:57 -0700 connect from 192.168.0.4
SMTP In: Wed, 9 Jun 1999 20:49:57 -0700 (Received mail from:
tina@timtest.starnine.com to: myisha@domain.com)
SMTP Out: Wed, 9 Jun 1999 20:49:57 -0700 ID=1 SMTP relay. Outgoing message
queued To: myisha@example.org From: tina@timtest.starnine.com
SMTP In: Wed, 9 Jun 1999 20:49:58 -0700 disconnect from
timtest.starnine.com [192.168.0.4]
```



A forwarding account is like an alias: it just forwards and does not allow a user to log in and read mail.



These forwarded messages are not changed in any way. Unlike messages from mail clients, these messages do not have quote indicators such as brackets (>) on the left side.

Forwarding To Groups

The **Forward To** address can be a set of email addresses or refer to a disk file with email addresses. This allows you to make the address into a distribution list.

Type Addresses

To enter the addresses in this field, just type them one after another, with commas between them:

```
scott@domain.com, pat@domain.com, elaine@mail.example.com
```

You can only type 255 characters in this field, and the field itself is very small, so a text file of addresses is better in most cases (see below).

Addresses From a File

You can also use a text file to set up address lists. This file must be in the *WebSTAR Mail Data* folder (in the *Plug-Ins* folder). To specify a file name, type a colon and the file name, like this:

```
:teachergroup.txt
```

The file must be a plain text file with addresses with commas between them, or one email address on each line:

```
scott@domain.com  
joe@example.com  
elaine@mail.example.com
```

Storage Limit

This field allows you to override the message limit in Mail Defaults (described on page 373) for this particular user.

The default for this is **0** (which means “use the default value”). The range is from 0 , and the range is from 0 to 999999.

Require APOP

This field lets you override the setting for authentication for POP client login for this particular user. See “Require APOP Authentication” on page 382 for details.

IMAP Privileges

The Internet Mail Access Protocol (IMAP) allows users to read their mail on the server, rather than downloading it and reading it on their personal computer. The default location for IMAP mail is in a standard “Inbox”. These options specify whether users can create other mailboxes, so they can manage their mail on the server more effectively.



To take advantage of the IMAP features, users must have an IMAP-capable email client.

Create Mailboxes

Allows this user to create additional mailboxes on the server using their IMAP client application.

When users can create mailboxes on the server, they tend to leave messages there, which can fill up your server very quickly. Be sure to watch your server disk space to make sure you have room for your Mail Data file, and a swap file for backups.

Delete Mailboxes

Allows this user to delete their server mailboxes using their IMAP client application.

Rename Mailboxes

Allows this user to rename their server mailboxes using their IMAP client application.

IMPORT AND EXPORT

For moving from one mail server to another, WebSTAR Mail allows you to import user information and messages and export them to a standard format.

WebSTAR Mail Export Formats

WebSTAR Mail has a simple tagged format for importing and exporting mail user settings and messages. It has tags and attributes, and can be read by SGML or XML processors.

This example shows an outgoing message from the Queue, with user and message data.

```
<user unique=000000BF mailbox="test@domain.com" alias="test"
passwordc="a8cr1S" apop="a8cr1S" isSysop=0 emailStorage=0 emailMessages=0
requireApop=0 mailboxCreate=0 mailboxDestroy=0 mailboxRename=0
forwardTo="">
<email to="test@domain.com">
Return-Path: &lt;elaine@example.com&gt;
Received: from mail.example.com. by www.domain.com. [192.168.0.7]; Mon, 24
May 1999 17:39:59 -0700
From: testing webstar &lt;elaine@example.com&gt;
To: test@domain.com
Subject: test
Message-ID: &lt;v04205227b36fa19e4d14@[192.168.0.7]&gt;
Date: Mon, 24 May 1999 17:39:59 -0700
MIME-Version: 1.0
Content-Type: text/plain; charset="ISO-8859-1"
```



Be careful with these export files -- they contain user passwords. You should store them only in secure locations, such as computers which do not serve any data.

Content-Transfer-Encoding: 8bit
</email>

Mail Export User Information

The <user> tag stores the User Setting attributes as described in “Users & Accounts Settings” starting on page 391:

- unique: the unique ID
- mailbox: the email address
- alias: the user name
- passwordc: the password
- apop: the APOP password
- isSysop: whether this is the Postmaster account
- emailStorage: limits on the size of the server mailboxes
- emailMessages: limit on the number of messages on the server
- requireAPOP: whether APOP is required for POP login
- mailboxCreate: whether IMAP clients can create mailboxes
- mailboxDestroy: whether IMAP clients can delete mailboxes
- mailboxRename: whether IMAP clients can rename mailboxes
- forwardTo: forwarding address for alias accounts.



A value of 0 in the storage, messages and APOP fields means that the user account conforms to the default settings for this server.

Mail Export Message Part

The <email> tag has one attribute, which stores the email address of the recipient, the body stores the body of the mail message, including message headers, and enclosures, which are stored with encoding, such as base64,. All quotes and brackets (<>) are converted to their HTML equivalents, such as "e ;.

Import User Mailboxes

WebSTAR Mail allows you to import user mailboxes, containing all current messages, from EIMS (Eudora Internet Mail Server) or AIMS (Apple Internet Mail Server).

- 1 If the old mail server is running, shut it down and quit the application.
- 2 Make sure you have the correct Host entries in the WebSTAR Admin, Mail Settings Hosts panel.
- 3 Launch the *Mailbox Extraction Tool* (in the *Tools & Examples* folder).
- 4 Select **Choose Mail Folder** from the File menu.
- 5 Select a folder or mailbox file from the old server's folder, and click **Choose**.



The old server folder is probably in the *Mail* folder in the *System* folder.

- 6 Give the export file any name (or use the default *Mailbox Extraction.sgmI*) and click **Save**.
- 7 Launch WebSTAR Admin on the same machine, choose the Mail Settings Users & Accounts panel, and click the **Import** button.
- 8 Now you can select the export file, and WebSTAR Mail will create new user accounts and import the old mail into each user's account, just as it was on the old server.

Exporting Mail Users and Messages

You can export mail user information, and even messages on the server, into text files for local storage.

To export the user and message information, open the WebSTAR Admin, choose Mail Settings, Users and Accounts, and click the **Export** button at the lower left.

Options are:

- **Selected User and Mail:** includes the user name, password, and other information, as well as the mail messages stored on the server, in the WebSTAR Mail Export Formats.
- **All Users and Mail:** user settings and server messages for all users in the WebSTAR Mail Export Formats
- **User List Tab Delimited:** user list with a header line at the beginning and a row for each entry with user name, password, and other information, separated by tab characters into columns.
- **Export User List SGML Format:** user list in the WebSTAR Mail Export Formats, without messages.
- **Outgoing Mail Queue:** messages from the Queue, in the WebSTAR Mail Export Formats, with the user information, message and any enclosure.

By default, the file is named *Mail Users*, but you can and should change the name to reflect the contents and date.

ACCOUNT TIPS AND EXAMPLES

Postmaster Account

You must have and read a "Postmaster" account that accepts mail to the postmaster address at all email hosts. This account will get messages from other mail administrators, other mail servers which have received messages with problems in the headers, confused people looking for someone in your company, and so on.



For details of the format see "WebSTAR Mail Export Formats" on page 395.



Be careful with these files -- they contain passwords and should be secured at all times.

You must read these messages frequently, at least five times a week, as some of them will be urgent and require immediate attention.

Characters Allowed in Names Addresses

User names and mail addresses formats are limited: you should only use unaccented Roman characters, numbers, and a few punctuation marks (usually plus, period, hyphen and underscore “_”). Do not use spaces in names or email addresses.

Creating Address Conventions

When you set up email addresses for your mail host(s), you should use a basic naming pattern, with variations and exceptions as appropriate. That helps people both inside and outside your organization to guess an email address, when they need to get in touch with someone and don't have access to your LDAP server.

There are a number of patterns you may choose to set up user names in your mail hosts:

- lastname.firstname (for example, steward.scott@domain.com).
- firstname_lastname (scott.steward@domain.com)
- lastname-first initial (steward-s@domain.com)
- firstinitial lastname (ssteward@domain.com)

You can mix and match the order and the punctuation as you please.

Allowing Exceptions

Some people who have been active on the Internet for many years have created a **net identity** with their email address. They may prefer to use that email address rather than following your conventions.

In that case, you can make multiple entries for that person, and forward all messages from the conventional names to the preferred account. For instructions, see “Forward To” on page 393.



For additional information, see “Reading the Postmaster Messages” on page 367.

To set up a Postmaster account, see “Creating a Mail User Account” on page 59.

MAIL MONITOR & QUEUE WINDOW

The screenshot displays the Mail Server Control Panel with the following sections:

- Header:** Mail: mailserver.domain.com:25
- Server Up Since:** 04/15/99:21:15
- Memory:** Total: 9.0 MB Free: 7.7 MB
- SMTP Outgoing Connections:** Maximum: 12 Current: 0
- SMTP Incoming Connections:** Maximum: 12 Current: 0
- POP Connections:** Maximum: 12 Current: 1
- IMAP Connections:** Maximum: 12 Current: 0
- LDAP Connections:** Maximum: 6 Current: 0
- Activity Log:**
 - INAP: Tue, 8 Jun 1999 13:45:41 -0700 LOGIN by david@timtest.starnine.com
 - INAP: Tue, 8 Jun 1999 13:45:41 -0700 user disconnect: david@timtest.starnine.com
 - INAP: Tue, 8 Jun 1999 13:45:41 -0700 LOGIN by postmaster
 - INAP: Tue, 8 Jun 1999 13:45:42 -0700 user disconnect: postmaster
- Queue:** Includes icons for play, stop, refresh, and mail.
- Table:**

To	From	Size	Date	Atte	Send time	or

The current number of connections for outgoing email. This may fill up if your users are sending copies of messages to several hosts.

SMTP Incoming

The number of connections for incoming email from other network servers.

POP

The number of connections opened by users retrieving their messages using POP clients.

IMAP

The number of connections opened by users reading messages using IMAP clients. IMAP users tend to hold their connections longer, as they often read and reply to messages directly from the server.

LDAP

The number of connections opened by LDAP clients.

Activity Log

This panel adds entries when users log in to read mail, send mail, when incoming mail is received, when the WebSTAR Admin sends changes to the server, and so on.

■ Restarting servers

```
05-May-99 12:38:56 ** Restart IMAP
05-May-99 12:38:56 ** Restart POP3
05-May-99 12:38:56 ** Restart SMTP incoming
05-May-99 12:38:56 ** Restart SMTP outgoing
```

■ Receiving via SMTP (insmtp)

- Connection: connect from mail.starnine.com.
- Reception: (Received mail from: <webstar-talk%40starnine.com> to: jose%40domain.com)
- Disconnection: disconnect from mail.starnine.com. This clears the SMTP Incoming Connection and you'll see the change in the gauge above.

■ Sending via SMTP (outsmtp)

- Queuing: SMTP relay Outgoing message queued To: webstar-talk@starnine.com From: mahalia@domain.com
- Sending: Sent e-mail To: info@starnine.com From: <andy@domain.com>

- Error: Mail delivery error () To: info@example.com
From: doug@domain.com
- Purging (manually deleting mail from the queue): terror WCTL message. Message purged by sysop To: avirr@domain.com From: jose<jose@domain.com>.
- Unknown address: 08-Jun-99 12:07:24 ID=5 SMTP relay. Could not deliver mail within 1 hour(s)
To: noway@starnine.com From: doug@timtest.starnine.com
- IMAP (imap)
 - connect from IP address of SMTP server
 - Received mail from and to email address
 - status warning LOGIN ATTEMPT (bad password)
- POP (pop3)
 - log into account: LOGIN by DavidK
 - user disconnect
 - status warning: LOGIN ATTEMPT (bad password)

Queue

This panel shows outgoing messages that have not yet been sent due to congestion, network problems or servers not found. [tbd: need new picture]

Queue					
To	From	Size	Date	Atte...	Send Time
andy-m@domain.com	les<leslie@domain.com>	328	05/05/1999 15:32:...	5	05/05/1999 16:09:11
leslie@domain.com	Tina<tina@example.com>	320	05/05/1999 15:24:...	5	05/05/1999 16:09:11
alaine@domain.com	Andy<andy-m@domain.com>	301	05/05/1999 15:46:...	5	05/05/1999 16:11:25

Each queue entry is a message to a specific email address. If you send a message to ten people, there will be ten entries in the Queue. These items are removed as soon as the message is transferred to the recipient's SMTP server, and that process can be extremely fast when the connections and servers are responsive.

Queue Items

Queue items include the following columns. Click on the title to sort the queue by the values in that column.

- **To** - recipient's email address
- **From** - the sender's email address
- **Size** - the size of the message, in bytes



Multiply the size by 1024 to get the size in **K** (kilobytes).

- **Date** - the date and time the message was originally sent
- **Attempts** - the number of times the server has tried to send the message
- **Send Time** - the last time the server attempted to send the message
- **Message Group** - an ID number for a message going to multiple recipients. Each copy of this message has the same ID, so you can see whether the message has gone through to the SMTP server.

In this list, you can select individual messages and act on them, using the buttons.

Queue Item Buttons

Clicking on the buttons acts on the selected items. You can stop, delay, delete, return or forward messages.



- The red **Stop** button will stop trying to send the message. The icon will switch to a green arrow: when you click that, it will start sending again.
- The **clock** button will bring up a delay dialog: you can set the day and time to start sending the message again.
- The **trash can** button will delete the message (you will have to confirm that you want to delete it).
- The **back arrow** button will return the message to the sender. You'll have a chance to confirm that.
- The **forward arrow** icon will let you send the message to another address for checking. You'll see a dialog for the address, and you can enter your address or that of another administrator.

 Hold down the Shift key to select several items at once.

 You can also Option-click to delete items directly.

LOGGING OPTIONS SETTINGS

The mail server can save logs and store archive copies of the log hourly, daily, weekly, or monthly.



Logging Options

By default, the mail server saves all transactions in a log file on disk. If you have mail problems, this log information will help you track down and fix them.

Logging is on by default: you can disable it by selecting the **Off** radio button.

The default file name is *WebSTAR Mail.log* and it is stored in the *logs* folder, inside the WebSTAR root folder. You can change the file name in the **Log File Name** field, or use the **Choose** button to select a log file and location.

TCP Logging

Checking this box enables a verbose log that tracks all TCP activity to and from the mail server. It is used for debugging only, and will slow down the server, so you should only check the box if you are working with StarNine Technical Support and they recommend this course of action.

Log Archiving

The automated archiving saves a copy of your log file at a specified interval, with the date and time in the file name. This keeps the log file from getting too big and makes it easy to locate a specific time period. By default, mail log archiving is **off**. You should enable it if your mail server is at all busy.

For instructions, see “Log Archiving” on page 122.



When you use this option, the mail log files are extremely large, and can fill your hard drive if you are not careful.

REPORTING

In addition to monitor windows and logging, the WebSTAR Mail server can send you regular reports about email usage.

Report Statistics

The WebSTAR Mail server tracks how many messages are sent, by host name, user and protocol. It clears these statistics each time it sends a report, and starts fresh.

Mail Server Report Format

When the mail server sends you a report, the title is "Email Statistics", and the email message describes the mail traffic on the server. An enclosure with account usage information is attached.

Report Message

The message describes number of messages and size of messages received by the server (SMTP Incoming) and the number and size sent (SMTP Outgoing), divided up domain or host. This gives you a rough idea of the server load.

Current disk usage: 79.90% used, with 422,836 Kbytes of free disk space
Maximum disk usage: 79.90% used, with 422,836 Kbytes of free disk space

	SMTP Incoming		SMTP Outgoing	
	Messages	Kilobytes	Messages	Kilobytes
domain.com	15	3428	0	0
example.com	52	83	57	84
knickknacks.com	0	0	0	0
mail.domain.com	1	4	0	0
tchotchkeys.com	0	0	0	0
Other	0	0	0	0

	POP3	Sent	IMAP	Sent	IMAP	Received	SMTP	Sent	SMTP	Received
	messages	Kbytes	messages	Kbytes	messages	Kbytes	messages	Kbytes	messages	Kbytes
jan	0	0	23	17	0	0	0	0	3	6
jo@x.com	0	0	0	0	0	0	0	0	3	2
joe@x.com	0	0	138	31	0	0	0	0	18	160
postmaster	2	1	49	3426	0	0	0	0	10	3419

Remember, each time you get a report, the Mail server clears all statistics and starts fresh.

Setting the Report Schedule

Use the Reporting panel of the Mail Settings in the WebSTAR Admin application to set your report options. You can specify an address to get the report, and how often the server should send it, and send one right away.



Reportina
Reporting

Send Report to:

Email usage reports:

Send Report To

Enter an email address—yours or another mail administrator's address—in this field. You may want to use an address on another server for these reports, so if your WebSTAR Mail server has problems, you will notice that the server does not send you a message.

Setting the Usage Reports Schedule

By default, WebSTAR does not send mail server reports, so the **Email usage reports** popup menu is set to **none**. You can set it to send you reports daily, weekly, or monthly by choosing from the popup menu.

Clear Report

This button resets all statistics to 0, so you can start fresh.

Run Now

When you click this button, the server runs all reports immediately, and sends them to the designated address. It also resets all statistics.



See also “How to Get Help” on page 106, “WebSTAR Debug Plug-In” on page 107 and “General Server Troubleshooting Guidelines” on page 108.

If you see errors on startup, in monitors, logs or users report problems, use this list of common problems to fix your Mail server.

Repairing Damaged Mail Files

If you have a disk crash or other disaster, and lose your mail database, the WebSTAR Mail server can recreate it for you.

- 1 Quit the WebSTAR server.
- 2 Remove the *WebSTAR Mail Users* file from the *WebSTAR Mail Data* folder in the *Plug-Ins* folder. Make sure you keep the other files in that folder. You may be able to retrieve some messages from the Mail Users file later.
- 3 Launch the WebSTAR application again.
- 4 The server will auto-recreate a new file containing all the previous email messages and account information. It does this by comparing the latest backup (*WebSTAR Mail Backup.1*) and the *Transaction Log* and rebuilding the *WebSTAR Mail Users* file based upon the information contained within.
- 5 You will see a message in the Mail Monitor window when this is successful.

The automatic recovery is dependent on the backup snapshots and transaction logs being present and current. Unless you delete the backup files, they should always be in place and ready for recovery

Server Not Getting Messages

If your server does not get messages that you send from other systems, there are several possible troubleshooting steps:

- Verify with your ISP or network administrator that you are allowed to run an email server. If there is a firewall, they will have to make holes on the mail ports for your server as well.
- Look at any “bounce” messages and see if the reasons given provide any useful information.
- Send yourself a message and watch the Mail Monitor window: you should see an SMTP IN / Connect From entry.
- Check your DNS record for your server. If you are getting Web and FTP requests, that means your general DNS record is probably right. So make sure that the MX (Mail Exchange) record does not send your email to some other mail host. For more information, see “Checking Your DNS Entries” on page 102.

Log Error Messages

Internet address not found — the recipient's mail host could not be located. The WebSTAR Mail server will put the message in the queue and try again.

Internet connection failed, try later — there was a TCP/IP error, such as a network failure at the router, DNS server, or somewhere between your server and the recipient's mail server. The WebSTAR Mail server will put the message in the queue and try again.

Mail Trace File

The WebSTAR Mail server contains a great deal of consistency checking and detection of potential problems. If there are internal errors, the server will write a file named *mail.trace* in the main *WebSTAR Server Suite* folder. StarNine Tech Support may request that you send them this file.

Client Problems and Error Messages

As mail administrator, you'll have to help your users with their email problems, including error messages and other client problems.

Error: We do not relay

This message means that the WebSTAR Mail SMTP server will not send a message for this client.

- Have the user log in and read mail before trying to send messages. This is a spam-prevention measure ensuring that your users are the only ones sending messages from this server. You can extend the open period for sending mail: see "Timeout" on page 381.
- Check the Mail Settings Connections panel to see if Enable SMTP Forwarding (described on page 380) is checked. If not, the server will not send messages, so check this box.
- Check the Mail Settings Allow/Deny list as described in "Restricting Access to SMTP Incoming" on page 387. If you deny access to a particular domain name or IP address range, any otherwise legitimate user who tries to send mail from one of those hosts will have their messages rejected.

Insufficient memory to accept posted message

If users see this message, they have reached the message storage limit for the user account. POP users should make sure they do not have their client set to leave messages on the server and IMAP users should

move messages from the server to their local mailboxes, or delete them.

No Trash Mailbox on server

When using IMAP, if a user deletes a message, the mail client may put it into a Trash mailbox on the server. However, if the account does not already have a Trash box, and the IMAP Privileges are not set to allow them to create mailboxes, they will see this error. To fix it, go into the WebSTAR Admin, Mail Settings, Users & Accounts panel and check the box by **Create Mailboxes**.

IMAP messages not deleting

Some clients do not delete IMAP messages by default, they just mark them for deletion. WebSTAR Mail does not perform the delete until the client sends it the command. If your client does this, you may be able to override the default behavior, for example, in Netscape Communicator 4.5, go to the Preferences, select Mail Server, click on the mail server, select IMAP and change the "When I delete a message:" radio button to "Remove it immediately".

Can't use @ in User Name Field

If a user puts their entire email address in a POP or IMAP client user name field, they may get an error. They should enter the user name in that field, and the host name in the POP (or IMAP) and SMTP host name field. As there is only one user of a given name for a mail host, that is enough to identify them uniquely.

Web Mail Login Error When Accounts Exist

When logging into the web browser mail interface, users must enter the entire email address if there is more than one user of that name on any mail host on the server.

If users enter an ambiguous user name without the mail host name, they will see the error:

The name or password you entered was incorrect - please try again.

XTND XMIT Problems

Some clients use the XTND XMIT (extended transmittal) protocol to send messages without using the standard SMTP login. WebSTAR Mail server 4.0 does not support this protocol.



The Web mail interface does require users to log in using the email@host format, but POP clients construct it from separate fields.

Changing Passwords

Some clients, such as Eudora, help users change their POP or IMAP password remotely. WebSTAR Mail server 4.0 does not support this process, so you will have to change the passwords manually.

Postmaster Problem Messages

When incoming mail is not accepted due to insufficient disk space, or when automatic backups fail for any reason, the Mail server will send a message to the Postmaster account. That's another reason to make sure you check mail for this account frequently.

This section covers the concepts and design of the WebSTAR Proxy server, which provides shared data caching and security for web browsers. The next chapters describe Proxy administration, the Proxy monitor window and log file, and troubleshooting.

ABOUT THE WEBSTAR PROXY SERVER

A **proxy server** acts as a go-between for a browser when it requests information over a network such as the Internet. Institutions use proxy servers because they offer security and performance benefits for groups of people who share the same connection to the Internet.

Normally when you request a document over the Web, your browser talks to the **origin server**—the computer that has the information—and requests it directly. The server then returns the data to your browser, and your browser displays the data for you. When you use a proxy server, you instruct your browser to contact the proxy instead. Then the proxy server retrieves the information from the origin server, and the proxy delivers the information to your browser.

One benefit that proxy servers offer is data caching. Often, a large group of people sharing the same connection to the Internet will look at many of the same documents. By keeping copies of the documents that it retrieves, the proxy can avoid always having to get the document from the origin server and instead get it from disk. This results not only in faster service for the person requesting the document, but in less traffic going over the group's internet connection.

The other advantage is security. A proxy server can be used to allow a group of people access to network services outside of their local firewall without compromising internal security, or to restrict the Internet sites that a group can access. In addition, you can limit which machines can access the proxy server.

Privacy Issues

If you expect to view the Proxy Monitor Window or track usage in the Proxy log file, we recommend that you **notify your users**. People may be very surprised to learn that their web browsing is not private, so it is **vital to warn them of this monitoring**.



Note that the WebSTAR Proxy server is implemented for HTTP requests only: it does not provide proxy services for FTP or other protocols.



For step-by-step instructions for getting started, see “Connect to Your Proxy Server” starting on page 63.

Cache Issues

Caching is a technique that allows many browsers to share web pages stored in a special database on the server disk. If you have a slow Internet connection, you'll find that retrieving files over your local network is faster than getting them from the original Web server. And because your colleagues are getting more of their data from the cache, the Internet connection is available for those files which are not cached.

Proxy Cache Flushing

To avoid serving obsolete files, the Proxy cache will flush files from the cache on a regular basis. No file will be kept more than the specified maximum length of time (14 days, by default). In addition, when the Proxy cache is full, it will remove unpopular files first, based on the average last use of the files.

Some pages, such as stock quotes, search results, and news headlines, are time-sensitive, and should not be cached. The Proxy cache will not cache any pages that do **not** have a "Last Modified Date" in the HTTP header. Most pages created by CGIs do not have this field, so they will never be cached.

Time-To-Live Calculation

In addition, some pages include an **Expiration Date** in the HTTP header, indicating when the data will become obsolete. The Proxy cache will honor that date, and remove the file from the cache on or before the day it expires.

For other pages, the Proxy cache uses an algorithm based on the interval between the "Last Modified Date" field in the HTTP header, and the date that the file is cached. The default Time-To-Live Ratio is "0.2". This means the Proxy cache will flush the file in 2% of the time between when the file was modified and when it was received.

For example, if a file created or modified on January 1 and requested on February 11, its **age** is 42 days. Multiply that age by the Time-To-Live ratio of 0.2, and the result is 8.4, so the file will be flushed on or before February 19.

Proxy Cache and Obsolete Pages

While these procedures will provide the most recent version of a page in most cases, there are still a few situations where the browser will receive an obsolete page. For example, if a simple page is updated



To change the ratio, see "Time-To-Live" on page 417.



If there is no super reload, try reloading the page twice. Most browsers send a “nocache” command in the second reload request.

once a year, and the first browser accesses it one day before it is updated, the other browsers will get the obsolete version until the file is flushed from the cache after the maximum length of time.

If someone suspects that they have an obsolete page, they can use the browser’s “Super Reload” (usually shift+Reload), so that it will include a “nocache” option in the request. In that case, the WebSTAR Proxy server will pass the request to the origin server, rather than returning the file in the cache.

Cache and Hard Disks

The default location for the cache itself is in *Plug-Ins : WebSTAR Proxy Extensions : Cache Files*. If you would like to move this to another hard disk, you can make a folder named *Cache Files* on the other disk, and replace the original folder with an alias to that new folder. The Proxy cache will resolve the alias correctly and access the files on the other disk.

Disk Optimization

As most cached files are small, the Proxy cache benefits greatly from the smaller block sizes of the Mac OS Extended File Format (also known as HFS Plus), introduced in Mac OS 8.1. If you have a large hard drive (over 1 GB) the files will take up substantially less room in this format—you will regain from 50% to 90% of your disk space, without losing any speed.

In addition, the Proxy cache may be faster if you increase the size of the Mac OS Disk Cache (set in the Memory control panel).

WebSTAR Proxy cache Status Window

The WebSTAR Proxy cache Window in the WebSTAR Server application displays some information about the number of files cached, the cache efficiency and the total number of bytes sent.

Browsers and the Proxy Server

To take advantage of the WebSTAR Proxy server, you must configure the browsers. Find the preferences for your browser, and locate the Proxy panel (usually in the “Networking” section). Select the manual proxy option, and enter the default host name of your WebSTAR primary server (do not use a virtual host name), or use the IP number. Enter the port number that you are using for the WebSTAR Proxy server (the default port is 8000), and save the preferences. From that

point onward, all requests for URLs beginning in “http://” from that browser will be made through the Proxy server.

If you have a fast internal network, you can reduce or remove the browser cache on the local disk by changing the browser preference. As the data is stored in the Proxy Server's cache, it doesn't have to be kept on the browser machine.



For step-by-step instructions see “Connect to Your Proxy Server” starting on page 63.

WebSTAR Proxy Server Design

The WebSTAR Proxy server is a group of Plug-Ins that work together. It is designed this way so third-party developers can add support for more protocols, expanded access control, logging features, and other features. The Plug-Ins are:

- **WebSTAR Proxy** instructs the server to listen for proxy requests, dispatches the request to the proper Plug-In for servicing, and generally glues the whole proxy system together.
- **WebSTAR Proxy HTTP** handles requests for HTTP objects, such as HTML pages and graphics.
- **WebSTAR Proxy cache** handles saving data to disk for future use, and retrieves cached data when it is available.
- **WebSTAR Proxy Log** enables logging of Proxy requests and provides the server with a monitor window to track connections.
- **WebSTAR Proxy Access** implements the Access Controls portion of the Proxy server for restricting access to the Proxy and from the Proxy connecting to other sites.

These Plug-Ins are stored in a *WebSTAR Proxy Extensions* folder inside the *Plug-Ins* folder.

The WebSTAR Proxy Plug-Ins are installed automatically when you install WebSTAR, and the server is enabled. To administer your server, use the WebSTAR Admin program. There are four Proxy Settings panels: Connections, Cache and Allow/Deny in this chapter, and Logging Options (described on page 422).

Proxy Connections

These settings control how the browsers access the Proxy server.

Connections

Proxy Connections

Increasing connection setting may require allocating additional RAM to the server.

Maximum Connections: 12

Timeout (Seconds): 60

Port: 8000

Upstream Proxy Server

Address:

Port: 8000

Maximum Connections: Limits the number of simultaneous connections that browsers can request via the WebSTAR Proxy server. Each browser normally uses four connections for each page (or frame) during the time that the data is being received. Just as with the web server, browsers will close connections once they get all the data.

The default is **12** connections, which is enough for a small network. To add proxy support for more browsers, increase this number and increase the RAM allocated to the WebSTAR server by 50 K per connection.

Port: The port number is used when setting up the browser preferences. If your network administrator is using port 8000 for another purpose, you can set this to any port you prefer, as long as you make sure the browser preferences use the same port.

Timeout (Seconds): If browser or server is idle for a time, the Proxy server will close these connections and accept others in their places. Note that busy servers may be slow sending all the requested data,



To add memory see “Application Memory and Connections” on page 88.



For port and firewall information, see “Port Numbers” on page 102.

and may not respond in the specified time. In that case, the browser will display a truncated download. If your users report this kind of problem, increase the timeout delay.

The default is **60** seconds.

Upstream Proxy

WebSTAR Proxy can now route all requests through another Proxy server. This is useful in situations where a school district has a master Proxy server (perhaps it's doing content filtering) and each school (connected to the school district via a slow net connection) wants to also host their own WebSTAR Proxy server to help improve performance.

Enter the full HTTP proxy server host name and the port number. The default port number is **8000** (the standard proxy port).



Be sure to check with the upstream proxy server before enabling this feature.

Caching

The Proxy Caching panel allows you to specify the sizes and settings for the proxy cache. For more background information, see “Cache Issues” on page 412.

Caching

Cache Size

Maximum Cache Size (MB):

Maximum File Size to Cache (K):

Ram Cache Size (K):

Time-To-Live

Amount of time an HTTP object is allowed to remain cached.

Maximum Time-To-Live (Days):

The expiration ratio is used when an HTTP object is received without an explicit expiration date.

Time-To-Live Expiration Ratio:

Maintenance

Maintenance Priority:

Cache Size

The cache size settings control how much of your server's hard drive will be used for Proxy caching. If you have a lot of room on your hard



You do not have to increase the RAM allocated to WebSTAR, because the Proxy Cache is a disk cache.

drive, you can store more data, improving performance for the browsers.

Maximum Cache Size (MB): Increase this number to enlarge your cache, if you have many people sharing the cache. If you run out of cache space, the Proxy Cache will automatically flush those files which have not been requested by browsers recently.

The default is **10 MB**.

Maximum File Size to Cache (K): If you increase the cache size, you can also increase the size of files kept in the cache. If proxy users often download the same large files, this can be very helpful.

The default is **100K**.

Cache RAM Size: Specifies how much of WebSTAR's memory allocation is dedicated to the Proxy Cache in RAM. This stores information about the files in the Proxy Cache, such as their expiration date, last use, number of times used and location. If there is enough room, files which are heavily used are also stored in RAM.

The default is **512K**, and is enough for small sites. If you are using the Proxy Cache for many browsers, you will want to increase the Cache RAM size to several thousand K, and performance will improve substantially. Be **sure** to allocate more memory to WebSTAR to accommodate this increase: see "Server Application Issues" on page 87.

Time-To-Live

The Proxy Cache must balance cache coverage against the possibility that a page will be obsolete. It flushes files from the cache at specified times, according to these settings.

Maximum Time-To-Live (Days): This setting controls the maximum length of time that the file can stay in the cache before it is flushed. The default value is **14**.

Time-To-Live Expiration Ratio: This slider controls the ratio used by the Proxy Cache to estimate the frequency of file changes, and define an expiration date, described in "Time-To-Live Calculation" on page 412. A lower value will make the expiration date interval very small, while a high value will make it many days or even weeks. However, all files are flushed when they reach the maximum time, as set above.



For background, see "Proxy Cache Flushing" on page 412.

Maintenance

Maintenance Priority Level: The cache is constantly checking the files to flush old files. If you have an extremely large cache, and you feel that files are not being removed fast enough, you can increase this priority. The **lower the number, the more priority you are assigning**. Note that if you decrease this number, other WebSTAR server functions may be slower.

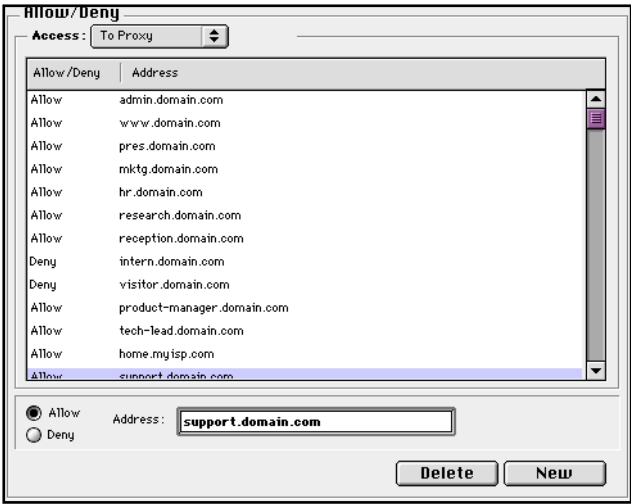
The default is fast enough to check all files in a large cache at least twice a day.

Proxy Allow/Deny

By default, anyone can use WebSTAR Proxy. If you choose, you can specify that it will only accept proxy requests from certain IP addresses and host names. This protects your server from exploitation by anyone outside your organization.

In addition, you can specify the sites that browsers using the proxy may access or not access. For schools and other institutions, this allows some control over the Web use in the organization.

Allow/Deny Access To Proxy



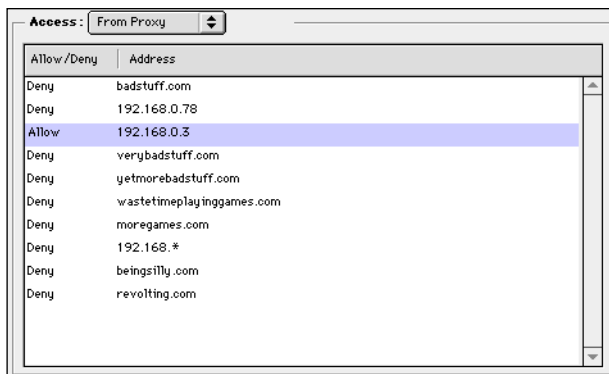
If this list is empty, all browsers can access the proxy. To restrict browsers from the proxy, create a Deny entry with the IP address, subnet, host name or domain name. To restrict access to a small number of browsers, create a Deny * entry and then allow specific

 These entries are stored in the *WebSTAR Settings* file.

 You can use wildcards (“*”) at the beginning **or** the end of a host name or IP address. Wildcards will match anything.

machines. WebSTAR Proxy will compare the host name or IP address of all requests to this list.

Allow/Deny Access To Sites From Proxy



The screenshot shows a window titled 'Access:' with a dropdown menu set to 'From Proxy'. Below the menu is a table with two columns: 'Allow/Deny' and 'Address'. The table contains the following entries:

Allow/Deny	Address
Deny	badstuff.com
Deny	192.168.0.78
Allow	192.168.0.3
Deny	verybadstuff.com
Deny	getmorebadstuff.com
Deny	wastetimeplayinggames.com
Deny	moregames.com
Deny	192.168.*
Deny	beingsilly.com
Deny	revolting.com



Be thoughtful in your use of wildcards. For example, denying `*sex.com` will also deny `essex.com`.

You can also specify which IP addresses, subnets, host names or domain names are accessible through the proxy. If there are sites that you do not approve, you can add them as “deny” entries, and browsers will not be able to access them. They will see an error message saying “You are not allowed access to that URL”.

For situations where you have very restricted access to the Web, you can add a deny `*` entry, then limited “allow” entries, and all other entries will be denied.

This chapter covers the Proxy Server Monitor Window and Log files, including the format of the transactions logged.

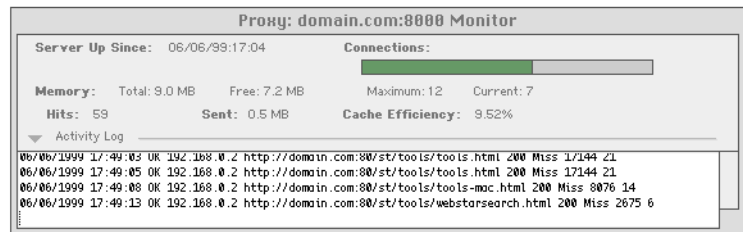
PROXY STATUS WINDOW & LOG FILE

Privacy Issues: If you expect to view the Proxy Status Window or track usage in the Proxy log file, be **sure** to notify your users. People may be very surprised to learn that their web browsing is not private, so it is **important to warn them of this monitoring**.

The Proxy status window in the Admin and the server are similar.

In the Admin, the status pane displays the number of bytes sent, the number of files matched in the cache, a bar indicating the percentage of connections used, the maximum number of connections and the current number of connections.

Below it, and in the server monitor window, the log pane shows the proxy server transactions.



- **Date:** month, day and year of the transaction.
- **Time:** time of day, using the 24-hour clock.
- **Status:** result status from the origin server: OK, ERR, etc..
- **IP Address:** address of the requesting browser machine.
- **URL:** the full URL path requested by the browser.
- **Status:** result code from the origin server.
- **Proxy Cache Status:**
 - **Hit:** the requested file was served from the cache.
 - **Miss:** the requested file was retrieved from the origin server, and a copy was stored in the cache.
 - **Pass:** the requested file was retrieved from the origin server, but was not a cacheable object, and was not stored.
- **Bytes Sent:** number of bytes transferred.
- **Time Taken:** number of ticks (60 per second) taken to perform the transaction.



see also "Cache Issues" on page 412.

PROXY LOG OPTIONS

The Proxy Logging Options panel in the WebSTAR Admin application includes a section for controlling the logging functionality, and one for Log Archiving (described on page 122).

Logging Options



Logging On and Off

When you click the Logging “Off” radio button, and press the **Save** button, the log file will no longer be updated. You must select the Logging On radio button and press Save to start logging again.

The default is Logging **On**.

Log File Name

The default file name is : logs:WebSTAR Proxy . log, specifying that the log file will be named *WebSTAR Proxy.log* and will be located in a *logs* folder in the WebSTAR root folder. A record of all Proxy transactions is maintained in this file. If the file does not exist, the WebSTAR server will create it.

The **Choose** button allows you to select a file on the server and append all future log information to that file. You cannot create a new log file this way, but you can select any file on your server as a log file, so be careful that you do not start appending log information to HTML or other files.

Log Archiving

Log Archiving allows you to save separate log files covering specified periods of time, such as every day, every week on Thursday, or monthly. The log files are automatically created at the time you set, filled, and then closed when the next one is created.

For information on these settings, see “Log Archiving” on page 122.



See also “How to Get Help” on page 106, “WebSTAR Debug Plug-In” on page 107 and “General Server Troubleshooting Guidelines” on page 108.

This chapter provides advice on locating and solving problems with the WebSTAR Proxy Server.

Proxy Server Troubleshooting

Check these entries if your Proxy server does not respond as expected.

The WebSTAR Proxy server isn't working correctly

- Check to see if the **browsers are configured** to work with your Proxy server. There is an option in browsers to specify a server and port to act as a Proxy, consult the browser documentation for specifics.
- If your Proxy server is behind a **firewall**, the network administrator needs to ensure that specific ports are available for access. Or configure the specific IP address for the server machine to be outside the firewall.
- The **Proxy server is crashing**. You may have too many connections. The maximum total connections that WebSTAR can handle, under Open Transport, is 498 (although very few sites would have the kind of bandwidth to come close to supporting that number). This total includes HTTP, FTP and Proxy servers, plus the 2 connections allocated to the Admin application.

Browsers display truncated downloads

- If the origin server is very busy and the download is delayed for longer than the Proxy Timeout value, it will close the connection to the server. To increase the timeout value, see “Proxy Connections” on page 415.

Error 500 host could not be found

This may happen the first time a particular host is contacted, because the DNS server did not respond in time. It is a problem with slow DNS servers, and cannot be fixed by the proxy.

Suffix Mapping Defaults

A

For an introduction, explanation and examples, see “Suffix Mapping” starting on page 154.

DEFAULT FILE SUFFIX MAPPINGS

These Suffix Mappings will allow the WebSTAR Web server to serve the most common file types without any additional configuration. Remember that order matters: the Web server uses the first matching suffix, serves the file using the Action and sets the header to the MIME type for the browser or other client to recognize.

Predefined Suffix Mappings

KIND OF FILE	ACTION	SUFFIX	TYPE	CREATOR	MIME TYPE
Graphics	BINARY	.GIF	GIFf	ogle	image/gif
	BINARY	.JPG	JPEG	ogle	image/jpeg
	BINARY	.JPEG	JPEG	ogle	image/jpeg
	BINARY	.PNG	PNGf	ogle	image/png
HTML	BINARY	.HTML	TEXT	R*ch	text/html
	BINARY	.HTM	TEXT	R*ch	text/html
CGI Applications	ACGI	.ACGI	APPL	*	text/html
	CGI	.CGI	APPL	*	text/html
BinHex	BINARY	.Hqx	TEXT	BnHq	application/mac-binhex40
MacBinary	BINARY	.BIN	BINA	SITx	application/x-macbinary
Stuffit	BINARY	.SIT	SITD	SIT!	application/x-stuffit
Adobe Acrobat (PDF)	BINARY	.PDF	PDF%20	CARO	application/pdf
PC executable	BINARY	.EXE	PFCA	SWIN	application/octet-stream
Java	BINARY	.CLASS	Clss	CWIE	application/octet-stream
	BINARY	.JAVA	TEXT	CWIE	application/octet-stream
JavaScripts	BINARY	.JS	TEXT	R*ch	application/javascript

APPENDIX A: SUFFIX MAPPING DEFAULTS

Predefined Suffix Mappings (Continued)

KIND OF FILE	ACTION	SUFFIX	TYPE	CREATOR	MIME TYPE
Style Sheets	BINARY	.CSS	TEXT	R*ch	text/css
Text (ASCII)	TEXT	.TEXT	TEXT	R*ch	text/plain
	TEXT	.TXT	TEXT	R*ch	text/plain
XML & SGML Text	BINARY	.XML	TEXT	R*ch	text/xml
	BINARY	.SGML	TEXT	R*ch	text/sgml
QuickTime video	BINARY	.MOV	MOOV	TVOD	video/quicktime
	BINARY	.QT	MOOV	TVOD	video/quicktime
	BINARY	.QTVR	MOOV	TVOD	video/quicktime
	BINARY	.DV	dvc!	TVOD	video/octet-stream
	BINARY	.QTC	*	*	video/x-qtz
MPEG video	BINARY	.MPG	MPEG	TVOD	video/mpeg
	BINARY	.MPEG	MPEG	TVOD	video/mpeg
AVI video	BINARY	.AVI	Vfw%20	TVOD	video/x-msvideo
RealAudio	BINARY	.RA	PNRM	PNst	application/x-pn-reaudio
	BINARY	.RAM	PNRM	PNst	application/x-pn-reaudio
Audio Format (Sun)	BINARY	.AU	ULAW	TVOD	audio/basic
AIFF (Audio Interchange File Format, Apple)	BINARY	.AIF	AIFF	TVOD	audio/x-aiff
	BINARY	.AIFF	AIFF	TVOD	audio/x-aiff
	BINARY	.AIFC	AIFF	TVOD	audio/x-aiff
PureVoice (Qualcomm)	BINARY	.QCP	celp	Blad	audio/vnd.qcelp
WAVE (Microsoft)	BINARY	.WAV	WAVE	TVOD	audio/x-wav
UNIX TAR files	BINARY	.TAR	TARF	S691	application/x-tar
GZIP compressed files	BINARY	.GZ	Gzip	Gzip	application/x-gzip
ZIP compressed files	BINARY	.ZIP	ZIP%20	ZIP%20	application/zip

Predefined Suffix Mappings (Continued)

KIND OF FILE	ACTION	SUFFIX	TYPE	CREATOR	MIME TYPE
PostScript	BINARY	.EPS	EPSF	vgrd	application/postscript
	BINARY	.PS	TEXT	vgrd	application/postscript
VRML	BINARY	.WRL	TEXT	R*ch	x-world/x-vrml
PICT graphics	BINARY	.PICT	PICT	ttxt	image/pict
XBM graphics	BINARY	.XBM	XBM%20	GKON	image/x-xbm
Microsoft Word	BINARY	.WORD	WDBN	MSWD	application/msword
	BINARY	.DOC	WDBN	MSWD	application/msword
Microsoft Excel	BINARY	.XL	XLS%20	XCEL	application/vnd.ms-excel
	BINARY	.XLS	XLS%20	XLS8	application/vnd.ms-excel
MS PowerPoint	BINARY	.PPT	SLD3	PPT3	application/vnd.ms-powerpoint
MacroMedia Director, Shockwave, Flash and Future Splash	BINARY	.DCR	FGDM	AFTB	application/x-director
	BINARY	.DIR	FGDM	AFTB	application/x-director
	BINARY	.DXR	FGDM	AFTB	application/x-director
	BINARY	.SWA	FGDM	AFTB	application/x-director
	BINARY	.SWF	SWFL	SWF2	application/x-shockwave-flash
	BINARY	.SPL	TEXT	Fspl	application/futuresplash
RAW	RAW	.RAW	RAW!	WWW%BD	application/x-raw-stuff

RAW Files

Files with a type of “RAW!” and creator code of “WWWΩ” are always served as binary, no matter what the suffix is. Therefore, it’s not possible to write CGIs or Plug-Ins that perform any actions on these files.

WEBSTAR PLUG-IN SUFFIX MAPPINGS

The Suffix Mappings for the WebSTAR Plug-Ins:

WebSTAR Plug-In Suffix Mappings

ACTION	SUFFIX	PLUG-IN
ADMIN	.ADMIN	WebSTAR Admin (only used by server and Admin application)
BINHEX	.HQX	WebSTAR Auto BinHex (BinHex files)
BYTE_SERVE	.PDF	WebSTAR Byte Server (Adobe Acrobat files)
CACHE	.CACHE	WebSTAR Data Cache (files you wish to cache)
DIRECTORY	.DIR	WebSTAR Directory Indexer (linked to “.message” files)
UPLOAD	.UPLOAD	WebSTAR File Upload (linked to “.upload” files)
IMAGE_MAP	.MAP	WebSTAR Image Map (image map files)
SERVLET	.SERVLET	WebSTAR JRun Servlet Runner (Java “/servlet/” URLs)
LOG_ROLLER	.ROLL	WebSTAR Log Archiver, used by WebSTAR server
PROXY	.PROXY	WebSTAR Proxy, used by the Proxy server
FORMMAIL	.FORMMAIL	WebSTAR Form Mail (linked to “x.formmail” forms)
SEARCH	.SEARCH	WebSTAR Search, used for index files to be searched
SSI	.SSI	WebSTAR SSI, used for HTML files to be processed by the SSI Plug-In
VHOST	.VHOST	Virtual Hosts, used by the WebSTAR server.
WOADAPTOR	.WO	WebSTAR WebObjects Adaptor

This chapter provides reference charts for WebSTAR SSI commands, environmental variables and field descriptors for date and time formatting.

For complete information, see “WebSTAR SSI” starting on page 275.



In this table, commands and tags implemented according to the NCSA standards are entered in **bold**.

SSI COMMAND REFERENCE TABLE

The following table provides a complete reference for SSI commands. These commands are described in detail in the “SSI Command List” starting on page 280.

SSI Command Reference

Command	Tag	Values	Notes
config (see page 292)	errmsg	your own wording	Configure format for displaying the time and file size. Also used to customize the SSI error message, or change character translation, or generate a new random number. <pre><!--#config timefmt="%B %D %Y"--> <!--#config errmsg="An error was encountered in the processing of this SSI command"--> <!--#config sizefmt="abbrev"--> <!--#config charset="latin1"--> <!--#config newrandom="500"--></pre>
	timefmt	See “Timefmt Field Descriptors” on page 433.	
	sizefmt	bytes, abbrev	
	charset	normal, latin1, ascii	
	newrandom	integer between 2 and 10,000 inclusive	
counter (see page 284)	var	name of counter	The counter command increments a named counter variable, and inserts the new value into the HTML output stream. <pre><!--#counter var="my_page_counter"--> <!--#counter display="off"--></pre>
	display	true, false, off, on, yes, no	
echo (see page 280)	var	See “Environmental Variables” on page 431.	Echo an environment or WebSTAR API variable. <pre><!--#echo var="HTTP_USER_AGENT"--></pre>
exec (see page 288)	cgi	path to be executed by the CGI script	Execute a command, CGI, script or WebSTAR API service. <pre><!--#exec cgi="/ProcessSale.qry" post="sales=19.95"--> <!--#exec script="/salescript" post="sales=19.95"--> <!--#exec pIService="FORMMAIL_SSI" param="from=eric@starnine.com&to=marc@starnine.com&subject=Hello&body=I%20hope%20you're%20having%20fun!&host=email.starnine.com"--></pre>
	script	path to the CGI script	
	pIService	name of the WebSTAR API service to execute	

SSI Command Reference (Continued)

Command	Tag	Values	Notes
flastmod (see page 283)	virtual	file path to local URL	File's last modification date. <pre><!--#flastmod virtual="/stuff/address.shtml"--> <!--#flastmod file="Macintosh HD:WebSTAR:stuff:address.shtml"--></pre>
	file	Macintosh file pathname	
fsize (see page 283)	virtual	file path to local URL	File's size in bytes or kilobytes. <pre><!--#fsize virtual="/stuff/address.shtml"--> <!--#fsize file="Macintosh HD:WebSTAR 4.0:stuff:address.shtml"--></pre>
	file	Macintosh file pathname	
hide (see page 285, see also "show" below)	none required	defaults to =	To conditionally turn off the HTML output stream based upon environmental variables, operators and values. <pre><!--#hide--> <!--#hide variable="date_gmt"--> <!--#hide variable="date_gmt" operator="contains" value="1998" --></pre>
	operator	contains, start, end, =, ==, !=, <>, <, <=, =<, >, >=, =>	
	value	optional (defaults to empty string)	
	variable	See "Environmental Variables" on page 431.	
include (see page 282)	virtual	file path to local URL	Include another document into the HTML output stream. <pre><!--#include virtual="/stuff/address.shtml"--> <!--#include file="Web HD:WebSTAR 4.0:stuff:address.shtml"--></pre>
	file	Macintosh file pathname	
postarg (see page 291)	var	name of the form variable from the page	Display named variables that have been sent to an SSI page from an HTML form. <pre>Hello, <!--#postarg var="your_name"-->!</pre>

SSI Command Reference (Continued)

Command	Tag	Values	Notes
show (see page 285, see also "hide" above)	none required	defaults to =	To conditionally turn on the HTML output stream based upon environmental variables, operators and values. <pre><!--#show--> <!--#show variable="date_gmt"--> <!--#show variable="date_gmt" operator="contains" value="1997" --></pre>
	operator	contains, start, end, =, ==, !=, <>, <, <=, =, >, >=, => (see "Operators for Show and Hide Commands" on page 287)	
	value	optional (defaults to empty string)	
	variable	See "Environmental Variables" on page 431.	
store (see page 291)	variable	your preferred variable name, up to 33 characters	Saves text or numbers for later use by the echo, hide, or show commands. <pre><!-- #store special_offer="Upgrade for only \$299!"--></pre>
	kind	optional: local (default), shared or persist	

SSI ENVIRONMENTAL VARIABLES

The following table provides a reference to SSI environmental variables. You can use these variables in the Echo command, and as part of the condition for the Show and Hide commands. You can also use the WebSTAR API parameters for such useful features as the MIME type requested, servers's domain name, path to the file on the disk, free memory available and so on. For details, see the "WebSTAR API Parameter Definitions" on page 455.

Environmental Variables

PARAMETER NAME	DESCRIPTION	SAMPLE VALUE
CONTENT_LENGTH	Form posting info to SSI page: length of posted data	1024
CONTENT_TYPE	Form posting info to SSI page: Type of information sent to server.	application/x-www-form-urlencoded
DATE_GMT	The current date/time, GMT.	1997/10/31:00:45:10
DATE_LOCAL	The current local date/time.	1997/10/30:16:45:10
DOCUMENT_NAME	The document's path and filename.	Mac HD:webstar:widgets:blue.html
DOCUMENT_URI	The URL of the document	/widgets/blue.html
GATEWAY_INTERFACE	The CGI or API version the server uses	WebSTAR API (version 1)

Environmental Variables (Continued)

PARAMETER NAME	DESCRIPTION	SAMPLE VALUE
HTTP_ACCEPT	MIME Types browser can accept	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
HTTP_REFERER	The document the user just came from.	http://www.starnine.com/default.html
HTTP_USER_AGENT	The name and version of the user's browser.	Mozilla/4.03 (Macintosh; I; PPC)
LAST_MODIFIED	Date and time the document was last modified or created.	1997/10/21:11:29:07
PATH_INFO	Text of the path arguments, after the \$ character in the URL.	sales%20territory
PATH_TRANSLATED	Decoded path arguments, after the \$ character in the URL.	sales territory
QUERY_STRING	Text of the search arguments, after the \$ character in the URL.	sample=region%201&name=pat
QUERY_STRING_UNESCAPED	Decoded search arguments, after the \$ character in the URL.	sample=region 1&name=tina
REMOTE_ADDR	Client's IP address	192.168.24.16
REMOTE_HOST	Client host name, if "use DNS" is turned on, otherwise, the IP address	leslie.domain.com 192.168.24.16
REMOTE_USER	<i>User name as passed by the browser</i>	Obsolete
REQUEST_METHOD	The request method	GET
SCRIPT_NAME	Path of the requested URL	/cgi-bin/myscript.cgi
SERVER_NAME	The server host name	www.domain.com
SERVER_PORT	The port number used	80
SERVER_PROTOCOL	The HTTP version used by the server	HTTP/1.0
SERVER_SOFTWARE	Name and version of your servers's software.	SERVER_SOFTWARE: WebSTAR/4.0 ID/55512

SSI FIELD DESCRIPTORS FOR TIMEFMT

The following table provides a complete reference for timefmt field descriptors. They allow you to reformat date and time display, so it is easier to read.

Timefmt Field Descriptors

FIELD DESCRIPTOR	DESCRIPTION	EXAMPLE
%a	Abbreviated weekday name	Mon
%A	Full weekday name	Monday
%b	Abbreviated month name	Jun
%B	Full month name	June
%c	Date and time (like %A, %d %B %Y %l:%M:%S %P)	Monday, 10 November, 1997 11:08:59 AM
%d	Day of month from 01 through 31	05
%H	Hour in military time from 00 through 23	22
%I	Hour in civilian time from 00 through 12	10
%j	Day of year	156
%m	Month from 01 through 12	06
%M	Minute from 00 through 59	21
%p	AM or PM	PM
%S	Seconds from 00 through 59	14
%U	Week number of year, beginning on Sunday	23
%w	Day of week as a number (Sunday is day 0)	0
%W	Week number of year, beginning on Monday	22
%x	Date, in the form "Day Month, Year" (%d %B, %Y)	10 November, 1997
%X	Time, using the HH:MM:SS (Hours:Minutes:Seconds) format	22:21:14
%y	Year in two digit format, from 00 through 99	97
%Y	Year in four digit format	1997
%%	A percent sign (%)	%

Descriptors Not Supported

The following NCSA timefmt descriptors are not supported: %C, %D, %e, %h, %k, %l, %n, %r, %R, %s, %t, %Z.

This chapter provides a list of Lasso Document Markup Language Tags available for the WebSTAR Lasso Publisher Plug-In. For additional information, see the files in the *Documentation* folder.

Lasso Tag Table

LESSO TAG	NAME	TYPE	MODULE
==	Equals Operator	Operator	Lasso_Tags
!=	Does Not Equal Operator	Operator	Lasso_Tags
>	Greater Than Operator	Operator	Lasso_Tags
>=	Greater Than or Equal To Operator	Operator	Lasso_Tags
<	Less Than Operator	Operator	Lasso_Tags
>>	Contains Operator	Operator	Lasso_Tags
<=	Less Than or Equal To Operator	Operator	Lasso_Tags
	Or Operator	Operator	Lasso_Tags
&&	And Operator	Operator	Lasso_Tags
[Else]	Else Statement	Sub-Container	Lasso_Tags
[Else:If]	Else If	Sub-Container	Lasso_Tags
[If] ... [/If]	If Statement	Container	Lasso_Tags
[Loop] ... [/Loop]	Loop Statement	Container	Lasso_Tags
[While] ... [/While]	While	Container	Lasso_Tags
[Server_Date]	Server Date	Substitution	Lasso_Tags
[Server_Day]	Server Day	Substitution	Lasso_Tags
[Server_Time]	Server Time	Substitution	Lasso_Tags
-Email.BCC	Email BCC	Command	Lasso_Tags
-Email.CC	Email CC	Command	Lasso_Tags
-Email.Format	Email Format	Command	Lasso_Tags

APPENDIX C: LASSO TAG REFERENCE

LESSO TAG	NAME	TYPE	MODULE
-Email.From	Email From	Command	Lasso_Tags
-Email.Host	Email Host	Command	Lasso_Tags
-Email.Subject	Email Subject	Command	Lasso_Tags
-Email.To	Email To	Command	Lasso_Tags
[Checked]	Checked	Sub-Container	FM_Tags
[Option]	Option	Substitution	FM_Tags
[Portal] ... [/Portal]	Portal	Container	FM_Tags
[Relation] ... [/Relation]	Relation	Container	Lasso_Tags
[Repeating] ... [/Repeating]	Repeating	Container	FM_Tags
[RepeatingValueItem]	Repeating Value Item	Sub-Container	FM_Tags
[Total_Records]	Total Records	Substitution	FM_Tags
[Value_List] ... [/Value_List]	Value List	Container	FM_Tags
[ValueListItem]	Value List Item	Sub-Container	FM_Tags
Action.lasso	Lasso Action Call	Other	Lasso_Tags
-Add	Add Action	Action	Lasso_Tags
-AddError	Add Error	Command	Lasso_Tags
-AddResponse	Add Response	Command	Lasso_Tags
-AnyError	Any Error	Command	Lasso_Tags
-AnyResponse	Any Response	Command	Lasso_Tags
-Database	Database Command	Command	Lasso_Tags
-Datasource	Datasource Command	Command	Lasso_Tags
-DBNames	Database Names Command	Command	DB_Info_Tags
-Duplicate	Duplicate Action	Action	Lasso_Tags
-DuplicateResponse	Duplicate Response	Command	Lasso_Tags
-Image	Image Action	Action	FM_Tags

LASSO TAG	NAME	TYPE	MODULE
-KeyField	Key Field Name Command	Command	Lasso_Tags
-KeyValue	Key Field Value Command	Command	Lasso_Tags
-Layout	Layout Command	Command	Lasso_Tags
-LayoutNames	Layout Names Command	Command	Lasso_Tags
-ModuleAdmin	Module Admin	Command	Lasso_Tags
-ModuleName	Module Name	Command	Lasso_Tags
-NoResultsError	No Results Error	Command	Lasso_Tags
-NoResultsError	No Results Error	Command	Lasso_Tags
-Nothing	Nothing Action	Action	Lasso_Tags
-Random	Random Action	Action	Lasso_Tags
-RecordID	Record ID	Command	FM_Tags
-Required	Required	Command	Lasso_Tags
-RequiredFieldMissingError	Required Field Missing Error	Command	Lasso_Tags
-Response	Response	Command	Lasso_Tags
-ReturnField	Return Field	Command	Lasso_Tags
-Search	Search Action	Action	Lasso_Tags
-Show	Show Action	Action	Lasso_Tags
-Table	Table Command	Command	Lasso_Tags
-Timeout	Timeout Command	Command	Lasso_Tags
[Include]	Include	Substitution	Lasso_Tags
[Inline] ... [/Inline]	Inline	Container	Lasso_Tags
[SQL_Inline] ... [/SQL_Inline]	SQL Inline	Container	ODBC_DataSource

APPENDIX C: LASSO TAG REFERENCE

LESSO TAG	NAME	TYPE	MODULE
EncodeBreak	Encode Break Keyword	Encoding Keyword	Lasso_Tags
EncodeNone	Encode None Keyword	Encoding Keyword	Lasso_Tags
EncodeRaw	Encode Raw Keyword	Encoding Keyword	Lasso_Tags
EncodeSmart	Encode Smart Keyword	Encoding Keyword	Lasso_Tags
EncodeURL	Encode URL Keyword	Encoding Keyword	Lasso_Tags
[Lasso_Abort]	Lasso Abort	Process	Lasso_Tags
[Lasso_Process]	Lasso Process	Process	Lasso_Tags
[LoopAbort]	Loop Abort	Process	Lasso_Tags
[Client_Address]	Client Address	Substitution	Lasso_Tags
[Client_IP]	Client IP	Substitution	Lasso_Tags
[Client_Password]	Client Password	Substitution	Lasso_Tags
[Client_Type]	Client Type	Substitution	Lasso_Tags
[Client_UserName]	Client User Name	Substitution	Lasso_Tags
[Database_Name]	Database Name	Substitution	Lasso_Tags
[DB_LayoutNameItem]	Layout Name Item	Sub-Container	DB_Info_Tags
[DB_LayoutNames] ... [/DB_LayoutNames]	Layout Names	Container	DB_Info_Tags
[DB_NameItem]	Database Name Item	Sub-Container	DB_Info_Tags
[DB_Names] ... [/DB_Names]	Database Names	Container	DB_Info_Tags
[Error_AddError]	Add Error	Substitution	Lasso_Tags
[Error_CurrentError]	Current Error	Substitution	Lasso_Tags
[Error_DatabaseConnectionUnavailable]	Database Connection Unavailable	Substitution	Lasso_Tags
[Error_DatabaseTimeout]	Database Timeout	Substitution	Lasso_Tags

LESSO TAG	NAME	TYPE	MODULE
[Error_FileNotFound]	File Not Found	Substitution	Lasso_Tags
[Error_InvalidDatabase]	Invalid Database	Substitution	Lasso_Tags
[Error_InvalidPassword]	Invalid Password	Substitution	Lasso_Tags
[Error_InvalidUsername]	Invalid User Name	Substitution	Lasso_Tags
[Error_ModuleNotFound]	Module Not Found	Substitution	Lasso_Tags
[Error_NoError]	No Error	Substitution	Lasso_Tags
[Error_NoRecordsFound]	No Records Found	Substitution	Lasso_Tags
[Error_OutOfMemory]	Out Of Memory	Substitution	Lasso_Tags
[Error_ReqFieldMissing]	Required Field Missing	Substitution	Lasso_Tags
[Field]	Field	Substitution	Lasso_Tags
[Field_Name]	Field Name	Substitution	Lasso_Tags
[Form_Param]	Form Parameter	Substitution	Lasso_Tags
[KeyField_Name]	Key Field Name	Substitution	Lasso_Tags
[KeyField_Value]	Key Field Value	Substitution	Lasso_Tags
[Lasso_CurrentAction]	Current Action	Substitution	Lasso_Tags
[Lasso_DataSourceModuleName]	Datasource Module Name	Substitution	Lasso_Tags
[Lasso_TagExists]	Tag Exists	Substitution	Lasso_Tags
[Lasso_Version]	Lasso Version	Substitution	Lasso_Tags
[Layout_Name]	Layout Name	Substitution	Lasso_Tags
[LoopCount]	Loop Count	Sub-Container	Lasso_Tags
[RecordID_Value]	Record ID Value	Substitution	FM_Tags
[Referrer] ... [/Referrer]	Referrer	Container	Lasso_Tags
[Referrer_URL]	Referrer URL	Substitution	Lasso_Tags
[Repetition]	Repetition	Sub-Container	Lasso_Tags
[Required_Field]	Required Field	Substitution	Lasso_Tags

APPENDIX C: LASSO TAG REFERENCE

LASSO TAG	NAME	TYPE	MODULE
[Response_FilePath]	Response File Path	Substitution	Lasso_Tags
[Selected]	Selected	Sub-Container	FM_Tags
[Server_Name]	Server Name	Substitution	Lasso_Tags
[Server_Port]	Server Port	Substitution	Lasso_Tags
[Variable]	Variable	Substitution	Lasso_Tags
bw	Begins With	Operator	Lasso_Tags
cn	Contains	Operator	Lasso_Tags
eq	Equals	Operator	Lasso_Tags
ew	Ends With	Operator	Lasso_Tags
[Found_Count]	Found Count	Substitution	Lasso_Tags
gt	Greater Than	Operator	Lasso_Tags
gte	Greater Than or Equal To	Operator	Lasso_Tags
[Image]	Image URL	Substitution	FM_Tags
[Link_CurrentSearch]	Link with Current Search	Substitution	Lasso_Tags
[Link_Detail]	Link Detail	Substitution	Lasso_Tags
[Link_NextRecord] ... [/Link_NextRecord]	Link Next Record	Container	Lasso_Tags
[Link_NextRecordURL]	Link Next Record URL	Substitution	Lasso_Tags
[Link_PrevRecord] ... [/Link_PrevRecord]	Link Previous Record	Container	Lasso_Tags
[Link_PrevRecordURL]	Link Previous Record URL	Substitution	Lasso_Tags
-LogicalOperator	Logical Operator	Command	Lasso_Tags
[LogicalOperator_Value]	Logical Operator Value	Substitution	Lasso_Tags
lt	Less Than	Operator	Lasso_Tags
lte	Less Than or Equal To	Operator	Lasso_Tags

LESSO TAG	NAME	TYPE	MODULE
-MaxRecords	Max Records	Command	Lasso_Tags
[MaxRecords_Value]	Max Records Value	Substitution	Lasso_Tags
neq	Not Equal To	Operator	Lasso_Tags
-Operator	Operator Command	Command	Lasso_Tags
-OperatorBegin	Operator Begin	Command	Lasso_Tags
-OperatorEnd	Operator End	Command	Lasso_Tags
[Records] ... [/Records]	Records	Container	Lasso_Tags
[Search_Arguments] ... [/Search_Arguments]	Search Arguments	Container	Lasso_Tags
[SearchFieldItem]	Search Field Item	Sub-Container	Lasso_Tags
[SearchOperatorItem]	Search Operator Item	Sub-Container	Lasso_Tags
[SearchValueItem]	Search Value Item	Sub-Container	Lasso_Tags
[Shown_Count]	Shown Count	Substitution	Lasso_Tags
[Shown_First]	Shown First	Substitution	Lasso_Tags
[Shown_Last]	Shown Last	Substitution	Lasso_Tags
[Shown_NextGroup] ... [/Shown_ NextGroup]	Shown Next Group	Container	Lasso_Tags
[Shown_NextGroupURL]	Shown Next Group URL	Substitution	Lasso_Tags
[Shown_PrevGroup] ... [/Shown_ PrevGroup]	Shown Previous Group	Container	Lasso_Tags
[Shown_PrevGroupURL]	Shown Previous Group URL	Substitution	Lasso_Tags
-SkipRecords	Skip Records	Command	Lasso_Tags
[SkipRecords_Value]	Skip Records Value	Substitution	Lasso_Tags
-Token.Name	Token Command	Command	Lasso_Tags
[Token_Value]	Token Value	Substitution	Lasso_Tags
[Variable_Set]	Set Variable	Process	Lasso_Tags

CGIs, Plug-Ins and Java

WebSTAR's extensible architectures allow you to add powerful features to your server by using CGIs, Plug-In modules, and Server-Side Java. These modules are triggered by URL requests and internal conditions, and can communicate with other applications, such as databases, then send results to users or perform tasks. Or they can be called as a Pre-Processor, Post -Processor, or Filter, checking each request.

CGIs (Common Gateway Interface applications) use Apple Events for communication. They can be written in AppleScript, Frontier, MacPerl, C, or any other language that supports Apple Events. For more information, see "Developing CGIs" starting on page 445.

WebSTAR API implements a modular architecture for extending the server in C and C++, using an system much like Adobe Photoshop and modern web browsers. For more information, see "Developing WebSTAR API Plug-Ins" starting on page 454.

WebSTAR supports Java Servlets according the JavaSoft Servlet API: for more information see "WebSTAR JRun Servlet Runner" on page 255 and "Developing Java Servlets for WebSTAR" on page 464.

The information here provides a brief overview of the approaches to writing these modules, and tables of the most important calls and parameters.

WEBSTAR DEVELOPMENT INFORMATION

For information on writing your own CGIs, Plug-Ins and Java servlets, see:

<http://dev.starnine.com/>

There is also an active and helpful mailing list, WebSTAR-Dev. To sign up on the Web, see:

<http://www.starnine.com/address-list-editor.html>

Or send an email message with the word "subscribe" in the subject to:

<mailto:webstar-dev-request@starnine.com>

If you are also interested in the **WebSTAR API** and discussions about furthering it, see the Development site for information as well as instructions on signing up for the WebSTAR-API mailing list.

Scripting Tools

Scripting tools for WebSTAR include:

- WebSTAR SSI (described on page 275)

The Server-Side-Include commands are extremely powerful and may allow you to avoid writing a CGI altogether.

- AppleScript <<http://www.apple.com/applescript/>>

Simple but slow language lets you access many other applications on the server.

- WebSiphon <<http://www.purity.com/websiphon/>>

From Purity Software: A powerful embedded scripting language for building dynamic web sites that is easy to learn but rich enough to satisfy the needs of advanced programmers.

- Frontier <<http://www.scripting.com/frontier/>>

A powerful, widely-used scripting language developed by UserLand Software and based around an object database, Frontier is useful to web developers both as a development environment and a CGI framework, though it gives you rich system-level control as well.

- Typhoon <<http://www.pacific-coast.com/Typhoon/>>

Pacific Coast Software's Typhoon uses a subset of the WebDNA command language used by WebCatalog (their online commerce application) to add fast dynamic processing to your web pages.

MacPerl

WebSTAR supports the standard Perl language via MacPerl. For the simplest implementation, save the Perl script (using MacPerl) as a CGI or ACGI (those options are in the save dialog of MacPerl). However, it does not have all the Unix system support that many Perl scripts expect, so you may have to make changes or use another scripting language.

Install MacPerl onto your server, and address the CGI as you would anywhere else.

For more information, see:

<http://www.iis.ee.ethz.ch/~neeri/macintosh/perl.html>

<http://www.ptf.com/macperl/>

<http://www.perl.com/CPAN-local/doc/FAQs/mac/MacPerlFAQ.html>

THIRD-PARTY WEBSTAR ADD-ONS

There are hundreds of add-on products to the WebSTAR server, allowing you to provide features like database access, scheduling, forms and surveys, an online store, and more.

For information on third-party add-ons, you can browse the following web sites:

StarNine's "Extending WebSTAR" page

<http://www.starnine.com/extendingwebstar.html>

This page presents many add-on products via a searchable and browsable database.

NetPro Magazine

<http://www.netprolive.com/>

Another page with lists of useful add-ons. Use the Internet Products Search form and look for "Server - Helper" or "Server - Plugin/CGI".

DEVELOPING CGIs

A **CGI** is any application that uses the **Mac OS Common Gateway Interface** standard to interact with an information server such as WebSTAR. The CGI standard defines arguments that allow the server to pass data to applications and receive data back from them.

You can develop a CGI to integrate with databases, process forms, and perform all sorts of other useful functions. CGIs can be developed and programmed in high-level scripting languages such as AppleScript, Frontier or MacPerl, or in low-level languages like C, Pascal or Java. Developing an application in a low-level language requires more effort but results in much better performance than an application developed in a scripting language.



CGIs must perform all HTML formatting themselves. The WebSTAR web server expects your script or application to generate and return a proper HTTP header, and does no conversion of the return values from CGIs.

The WebSTAR server itself does not process the data it sends to the CGI application nor the pages it returns to the client software. The server's job is to handle connections, use the proper method to return pages and files, and handle communications between the client and the CGI.

See the WebSTAR Development site at <http://dev.starnine.com/> for specs and more information related to Mac OS CGI development.

ACGIs and Asynchronous Processing

The WebSTAR server can interact with a CGI **synchronously** or **asynchronously**. If the name application ends with “.cgi”, the server passes an Apple Event to the application and waits for the CGI to return a result (synchronous operation). If the application name ends in “.acgi”, the server passes an Apple Event to the application and then continues processing other tasks until it receives a reply. Writing a CGI to be processed asynchronously is usually preferable.

AppleScript CGI Issues

- If you use AppleScript to develop a CGI, save the CGI as an Application in the Script Editor and make sure you use the Keep Open and Never Show Startup Screen options.
- To avoid timeouts, you should name your AppleScript CGIs with the “.acgi” suffix (asynchronous CGI). Although the interaction is not actually asynchronous, this suffix enables the server to work more cooperatively with AppleScript.
- AppleScript CGIs can now use the new `on handle CGI request`, a method included in the new Standard Additions Scripting Addition of Mac OS 8.5 and greater. An example of the call is included in the *AppleScript CGIs* folder in *Tools & Examples*.

While the Mac OS CGI `'handle CGI request'` parameter provides a cleaner format for writing AppleScript-based CGIs, it does not support the “Full Request” and “DIRE” parameters supported by the WebSTAR CGIs ‘«event WWW2sdoc»’ format.

- For instructions in creating AppleScript CGIs, see:

<http://dev.starnine.com/>

WebSTAR Apple Events

The WebSTAR server includes Apple Events and application properties to set all configuration parameters. For the most part, the syntax of the data sent by the AppleScript Set commands, or returned by the AppleScript Get commands is the same as the syntax for setting parameters.

The WebSTAR server supports the four required Apple Events, plus a custom Apple Event suite for sending information to the WebSTAR server while it is running. The custom event suite provides the flexibility and power of WebSTAR CGIs.

The event suite for the WebSTAR server Apple Events is the same as the four-character creator code for the WebSTAR server application.



Many of the application properties can be found in the Apple Event dictionary for the WebSTAR server, viewable in the Script Editor.

The four-character Event Suite is WWWΩ—three uppercase Ws (WWW), followed by the omega character "Ω" (option-Z on the keyboard).

WebSTAR Apple Event Suite

EVENT	COMMAND	PARAMETERS	EXAMPLE
Verbose Messages Toggle Verbose Messages on or off	Verbose Messages <boolean value>	True or False	verbose messages false
Hide Window Toggle hiding status window in the background	Hide Window <boolean value>	True or False	hide window true
Refuse Connections Toggle incoming web connections on or off	Refuse Connections <boolean value>	True or False	refuse connections false
Suspend Logging Turn logging on or off	Suspend Logging <boolean value>	True or False	suspend logging true
flush cache Flushes the file info cache, the data cache and any Plug-In caches.	flush cache	none	flush cache
reset stats resets all server counters to zero	reset stats	none	reset stats
add user Add a user and password for a specific security realm	add user <username> password <password> realm <security realm>	user name, password and realm name as character strings	add user "President" password "speCial100" realm "HUMRES"
delete user Delete specified user from a particular security realm	delete user <username> realm <security realm>	user name and realm name strings.	delete user "President" realm "HUMRES"
import users import records into the user/password database	import users <importFile>	importFile: file specification, fileRefNum in AppleScript.	import users myUserFile
validate user Validate that a given password is correct for a user in a specific realm	validate user <username> password <password> realm <security realm>	user name, password and realm name as character strings	validate user "President" password "speCial100" realm "HUMRES"

WebSTAR Apple Event Suite (Continued)

EVENT	COMMAND	PARAMETERS	EXAMPLE
Get_AllowDenyInfo get allow/deny info for a specific realm Result: character string containing allow/deny info for specified realm	Get_AllowDenyInfo for <realmName>	realmName: name of the realm as a character string.	Get_AllowDenyInfo or "HUMRES"
Set_AllowDenyInfo set allow/deny info for a specific realm	Set_AllowDenyInfo <status><address> for <realmName>	status: allow or deny; address: host name, domain name or IP address as string; realmName: name of the realm as a string.	Set_AllowDenyInfo "dumb.com" for "HUMRES"
Status Report Return status information about the server Result: returns info about WebSTAR in a character string.	Status Report	none	status report true
request reporting Request real-time status reports be sent to caller. Result: status of request & name and port of remote WebSTAR server in a character string.	request reporting messages <boolean> status <boolean> id <requestor ID> client_version <admin client version number>	user name, password and realm name as character strings	request reporting messages true status false client_version 3.0
send partial Sends partial ACGI execution results to the WebSTAR web server for transmission to clients.	send partial <partialData> connection integer <connectionID> more <boolean>	partialData: data to return to the WWW client, as a character string. connectionID: connection ID to return data to, as an integer more: is there more data to send? True/False	send partial "this is a test" connection 24 more true

WebSTAR Apple Event Suite (Continued)

EVENT	COMMAND	PARAMETERS	EXAMPLE
WSAPI_ReadHTTPData Read incoming data from a HTTP client (e.g., POST args, etc.)	WSAPI_ReadHTTPData	The WebSTAR API parameter that you would like to read for that connection, along with the connection ID	WSAPI_ReadHTTPData
WSAPI_GetIndexedParameter Result: 'char' Retrieve a scalar WebSTAR API parameter (indexed or normal)	WSAPI_GetIndexedParameter <WebSTAR API parameter> [index <indexName> connection <connectionID>]	WebSTAR API parameter [index 'char'] -- index to retrieve connection integer -- connection ID to retrieve parameter from	WSAPI_GetIndexedParameter

Notes on WebSTAR API Apple Events

WSAPI_ReadHTTPData circumvents the old 32K limit on POST args by allowing you to call it multiple times. The dataLen parameter is limited to 32K at a time. If more than 32K is expected from the client, you'll have to send this event multiple times to read all the data. Note that calling this function when data **isn't** pending will likely result in a timeout.

The WSAPI_GetIndexedParameter event gets information about WebSTAR using WebSTAR API parameters (see "WebSTAR API Parameter Definitions" on page 455). Unlike the function of the same name in the WebSTAR API, the Plug-In parameter specifier is a character string instead of a 4 byte OSType character. Also, integer values are coerced to strings before being returned and non-integer, non-string parameters are not returned (e.g., FSSpecs, etc.).

For information about the equivalent API functions, use the WebSTAR Server Suite Installer to custom install "WebSTAR Development Resources", and see the WebSTAR API SDK.

Apple Event Properties

The WebSTAR server application Get and Set events can use these properties:

WebSTAR Apple Event Properties

PROPERTY	DATA TYPE	MEANING
dump_buf_size	small integer (256-10240)	Output buffer size for TCP/IP writes to clients.
maxusers	small integer (4-500)	Maximum number of simultaneous users. The upper limit is 500 under Open Transport.
no_dns	boolean (true = DNS off, false = DNS on)	Toggle for domain name resolution by the server.
time_out	small integer (5-600)	Timeout value for idle client connections and Apple Events in seconds
logging	boolean	Enable/Disable logging
verbose_messages	boolean	Toggle Verbose Messages on/off
refuse_connections	boolean	Refuse/Allow incoming web connections
default_mime_type	'char'	Default MIME type for untyped files
port	small integer	TCP/IP port for server to listen on
index_file	'char'	Name of the default "index" file
error_file	'char'	Name of the error message file
log_file	'char'	Name of server log file
log_format	'char'	String of keywords for log format
no_access_file	'char'	Name of "no access" file
pre_processor	'char'	Pre-processor application name
post_processor	'char'	Post-processor application name
suffix_mappings	'char'	Suffix and MIME Type mappings in text block format
access_controls	'char'	Allow/Deny access controls via IP address and domain name. Text block format
realms	'char'	Security realm entries in text block format.
actions	'char'	User-defined actions in text block format
version	'char' [r/o]	WebSTAR version number

WebSTAR Apple Event Properties (Continued)

PROPERTY	DATA TYPE	MEANING
CGI_Persistent_Connections	integer	If enabled all CGIs must support persistent connections
WNE_Threshold	integer	Time between Wait Next Event calls
report_delay	small integer (1-60)	Number of seconds delay between status report events
file_info_cache_size	integer (0 to max RAM)	Amount of memory to allocate for file info caching. The upper limit is the amount of RAM available to WebSTAR
keep_alive_connections	small integer (0 - 10)	Number of persistent connections per client to keep active
keep_alive_time	small integer (0 - 60)	Timeout delay for persistent connections
plugin_admin_info	'char' [r/o]	Information for configuring installed Plug-Ins (tab separated tokens)
server_name	'char'	Name of server to return in HTTP responses instead of DNS name
cgi_bin_only	boolean	Flag that indicates if only CGIs inside the cgi-bin directory will be executed

Calling CGIs

If the WebSTAR server receives a query (such as “GET”) from a browser requesting a file whose suffix mapping Action is “CGI” or “ACGI”, the WebSTAR server attempts to launch the CGI application and communicate with it via Apple Events.

The WebSTAR server implements the Mac OS Common Gateway Interface standard in the sdoc Apple Event. The four-character Event Suite is “WWWΩ”—three uppercase Ws (WWW), followed by the omega character (option-Z on the keyboard). The four-character event code is sdoc. For example:

```
on «event WWWΩsdoc»
```

The Apple Event keyword codes for the parameters passed by the WebSTAR server to CGI and ACGI applications are listed below. You

can name the variables associated with these parameters whatever you like.

CGI Parameters

PARAMETER	KEYWORD	DATA SIZE	DESCRIPTION
Path Args	----	1024	Contains arguments following the dollar-sign (\$) in a URL. For example, for this URL: <pre><form action="ProcessForm.cgi\$JimmyJones?14" method=post></pre> the value "JimmyJones" is contained in this parameter. This keyword is also the direct parameter of the Apple Event (keyDirectObject).
Search Args	kfor	1024	Contains arguments following a question mark ("?",) in a URL. For example, for this URL: <pre><form action="ProcessForm.cgi\$JimmyJones?14" method=post></pre> the value "14" is contained in this parameter.
Username	user	32	Passes the username if authentication was required.
Password	pass	32	Passes the password if authentication was required.
<i>From User</i>	<i>frmu</i>	<i>128</i>	(obsolete) email address of user.
Client Address	addr	256	Passes the domain name of the client (or the IP address if DNS look-ups are disabled).
Server Address	svnm	256	Passes the domain name of the server (or the server's IP address if DNS look-ups are disabled).
Server IP port	svpt	16	Passes the TCP/IP port the server is listening on.
Script name	scnm	1024	Passes the path of the CGI being executed. If the CGI is called as an ACTION, this parameter contains the file portion of the URL.
Content Type	ctyp	64	Passes the MIME type of post arguments if present.
Referrer	refr	1024	Passes the URL of the page from which this CGI was referenced. This information is useful for telling what sites are referencing your pages. It can also be useful in a script to add a "return" link to pages on-the-fly that would return users to whatever page they came from.

CGI Parameters (Continued)

PARAMETER	KEYWORD	DATA SIZE	DESCRIPTION
User Agent	Agnt	256	Passes the WWW client software (browser) name and version.
Action	Kact	1024	Passes the action being performed by the CGI. It will contain either the name of the user-defined action or one of these strings: CGI, ACGI, PREPROCESSOR, POSTPROCESSOR, ERROR, INDEX, or NOACCESS.
Action Path	Kapt	1024	Passes the path to this CGI if it is executing as an action (in which case, the script name parameter contains the URL file path sent from the client).
Post Arguments	post	32,768	Passes arguments sent from the WWW client as part of a POST request (such as form arguments). The actual form data (returned from running the CGI) is also placed in this parameter.
Method	meth	32	Passes the HTTP method being requested (such as GET, GET_CONDITIONAL, POST, etc.). For more information, see below.
Client IP Address	Kcip	32	Passes the IP address of the client as a string, even if NO_DNS is false.
Full Request	Kfrq	4096	Passes the complete, unmodified HTTP request as received from the WWW client.
Connection ID	Kcid	4	Passes a unique long integer identifying the TCP/IP connection over which the server is communicating to the client. This number is used for sending the “Send Partial” Apple Event to the WebSTAR web server.
DIRE	DIRE	70	An FSSpec pointing to the root folder of the virtual host, or, if the URL is not for a virtual host, the WebSTAR root folder.

The Method Parameter

This parameter passes the HTTP method being requested (such as GET, GET_CONDITIONAL, POST, etc.).

If the HTTP method is POST, the form data sent in the object body of the HTTP request is returned to the server in the `post_args` parameter. Otherwise, this parameter is empty.

If the HTTP method is GET, the form data overwrites the `http_search_args` parameter. If you are using a map-processing CGI, you might use the `method=get` argument to pass the name of a map

information file that the CGI should use to process the map. The URL might look like this:

```
/cgi/MapServe.acgi$jonsmap.map
```

When a user clicks on the map, the client software changes this URL so that the map coordinates are added in the search arguments. The full URL transmitted to the WebSTAR web server would look something like this:

```
/cgi/MapServe.acgi$jonsmap.map?223,1
```

CGIs and Virtual Hosts

When WebSTAR sends an Apple Event to CGIs, it includes a “DIRE” parameter. This enables CGIs to determine the correct root folder for the virtual host the request was made to.

More Information on CGIs

For more information about how to develop CGI applications that work with the WebSTAR server, see:

<http://dev.starnine.com/>

DEVELOPING WEBSTAR API PLUG-INS

The **WebSTAR Application Program Interface (API)** is a modular, high-performance technique for developers to extend the functionality of WebSTAR. The WebSTAR API uses CFM on PowerPC systems to implement these Plug-Ins.

Theory of Operation

WebSTAR API Plug-Ins exist as part of the web server's running code, can be called from threads within WebSTAR, and have access to data and services provided to the Plug-In by the web server. Plug-In developers have to take care to cooperate with the web server and other Plug-Ins. Provisions exist for giving Plug-Ins idle CPU time on a regular basis, so you aren't limited to performing all of your processing in the context of a single subroutine call. In addition, Plug-Ins can listen on multiple TCP ports, perform routing of browser requests, return to the server the HTTP response code they sent to the client, and display their own windows.

Complete documentation of the WebSTAR API is included in the WebSTAR API SDK, which is a custom install option in the *WebSTAR Server Suite Installer*. The SDK can also be found at:

ftp://ftp.starnine.com/pub/webstar_dev/wsapi_sdk.sea.hqx

Filter Plug-Ins

All Filter Plug-Ins get called immediately after the server has read the incoming HTTP request and before any processing has begun. They will receive all the request information, and can change it as appropriate. For example, the WebSTAR JRun Servlet Runner checks for the text `/servlet/` in a URL and adds the suffix `.servlet`. This ensures that the WebSTAR Suffix Mapping process will correctly direct requests for Java servlets. Then the filter passes the request back to the server, which may pass it to another filter. For WebSTAR, all Filter Plug-Ins are invoked in reverse alphabetic order (i.e., last to load is first to run). The details are contained in the WebSTAR API documentation.



Filters can only change request text, they can't return results.

There are good reasons to write a filter rather than a Pre-processor: Your filter can work with other filters, while each server can only have one Pre-processor, making filters much more compatible. And filters can automatically install the suffix data in the Suffix Mapping Table, while Pre-processors must be designated by the user.

WebSTAR API Parameter Definitions

This table contains a complete listing of WebSTAR API parameters, keywords and a short description describing the value returned.

While these WebSTAR API parameters are primarily for use by WebSTAR API Plug-In developers, they can also be used in connection with Plug-Ins like WebSTAR SSI which allow WebSTAR API parameter values to be returned from the echo command. For instance:

```
<!--#echo var="piTotalConnections"-->
```

In addition, the values of these parameters are accessible by the `WSAPI_GetIndexedParameter` Apple Event function.

WebSTAR API Parameter Definitions

PARAMETER NAME	KEYWORD	DESCRIPTION
Connection-related		Read-only values
<code>piPathArgKeyword</code>	<code>----</code>	Path argument portion of URL
<code>piSearchArgKeyword</code>	<code>'kfor'</code>	Search argument portion of URL

WebSTAR API Parameter Definitions (Continued)

PARAMETER NAME	KEYWORD	DESCRIPTION
piUserKeyword	'user'	Username for current authentication scheme
piPasswordKeyword	'pass'	Password for current authentication scheme
piFromUser	'frmu'	"From" header field (e-mail address when supplied)
piAddressKeyword	'addr'	domain name of client
piPostKeyword	'post'	first 24k of HTTP object body (e.g., form data, etc.)
piMethodKeyword	'meth'	HTTP method (e.g., GET, POST, HEAD, etc.)
piServerName	'svnm'	domain name of server
piServerPort	'svpt'	port number server is listening on
piScriptName	'scnm'	name of CGI or URL path if executing as an action
piContentType	'ctyp'	MIME type of the HTTP object body
piContentLength	'CLen'	data size of the HTTP object body
piRefererKeyword	'refr'	"Referer" HTTP header field value
piUserAgentKeyword	'Agnt'	"User-Agent" HTTP header field value
piActionKeyword	'Kact'	name of action associated with current URL request
piActionPathKeyword	'Kapt'	path to the CGI processing the current URL request
piClientIPAddress	'Kcip'	4 byte integer containing client's IP address
piFullRequestKeyword	'Kfrq'	Entire HTTP request as received from the client
piFileMIMEType	'Mime'	MIME type of requested URL as determined by server
piServerField	'SvFd'	preconstructed response header field for server name
piServerDirectoryPath	'SPth'	local file system path to the server's document tree
piURLPhysicalPath	'UPth'	local file system name for the requested file
piIfModifiedSince	'IfMS'	true/false if file has been modified since last client request
piURLFileRef	'Pufr'	server-specific reference to file in the native OS
piCurrentRealm	'CRlm'	name of security realm (if any) protecting requested file
piConnectionID	'LCID'	unique ID for this HTTP connection

WebSTAR API Parameter Definitions (Continued)

PARAMETER NAME	KEYWORD	DESCRIPTION
piServerUniqueID	'LSID'	unique ID for this execution of the server
Server Status Info		Read-only values
piTotalConnections	'STCn'	total number of connections served since start-up
piCurrentUserLevel	'SCLd'	current number of users connected to the server
piHighestUserLevel	'SMLd'	max number of users ever connected at one time
piCurrentFreeMemory	'SFMm'	current amount of free memory available to the server
piMinimumFreeMemory	'SMFM'	minimum amount of free memory ever available to server
piTotalConTimeouts	'STTm'	total number of connections that have timed out
piTotalConBusies	'STBz'	total number of connections refused because server was busy
piTotalConDenied	'STDn'	total number of connections denied for access violations
piTotalBytesSent	'TByt'	total bytes transmitted to clients
piVersionNumber	'Pvrs'	name and version number of server
piUpSinceDate	'SUPS'	date & time the server was launched in the format MM/DD/YY:HH:MM
piPluginAdminInfo	'Padm'	text block containing info on each Plug-In currently installed
Plug-in Info		Read-only values
piPluginParamInfo	'Pipi'	pointer to a WebSTAR API-specific data structure describing Plug-In parameter semantics
piPluginParamCount	'Pipc'	count of the number of WebSTAR API parameters in piPluginParamInfo
piPluginDirPath	'Pdph'	full path to the Plug-Ins folder
piPluginDirFSSpec	'PdFs'	platform-specific file system reference to Plug-Ins folder
Logging Info		Read-only values
piTransferResult	'LTRs'	result of processing URL (OK, ERR!, PRIV)
piBytesSent	'LByt'	bytes sent for current request

WebSTAR API Parameter Definitions (Continued)

PARAMETER NAME	KEYWORD	DESCRIPTION
piTransferTime	'LTrT'	time in ticks from connection open to close
Special Routing Settings		Read/Write access
piIndexFile	'Pixf'	name of file in each directory to return as a default
piErrorFile	'Perf'	relative path to Mac file/CGI handling file not found
piNoAccessFile	'Pnaf'	relative path to file/CGI handling access violations
Global Server Settings		Read/Write access
piDumpBufSize	'Dbuf'	chunk size for TCP/IP output
piPigDelay	'PigD'	time in ticks between WaitNextEvent calls
piMaxUsers	'MaxU'	maximum number of simultaneous connections allowed
piNoDNS	'Ndns'	toggle DNS look-ups on/off.
piTimeOut	'TimO'	timeout in seconds for inactive connections
piMaxListens	'MaxL'	same value as Max Users. Should be set to the same value
piLogging	'Plog'	toggle log file output on/off (1/0)
piVerboseMessages	'Pvrb'	toggle server debugging messages on/off (1/0)
piRefuseConnections	'Pcon'	toggle connection refusal on/off (1/0)
piHideWindow	'Phid'	toggle status window hiding on/off (1/0)
piDefaultMIMEType	'Pmim'	default MIME types for files with no suffix mapping
piPort	'Pprt'	port for server to make HTTP connections on
piLogFile	'Plgf'	relative path to server log file
piSuffixMappings	'Psuf'	text block defining suffix mapping info
piAllowDeny	'Pa/d'	text block defining allow/deny IP security
piAllowDenyByRealm	'PADr'	This is an indexed value and you must use the <code>WSAPI_GetIndexedParameter</code> or <code>WSAPI_SetIndexedParameter</code> call to manipulate it. The Index is the name of the realm to get or set allow/deny info for.
piRealms	'PrIm'	text block defining realm security

WebSTAR API Parameter Definitions (Continued)

PARAMETER NAME	KEYWORD	DESCRIPTION
piActions	'Pact'	text block defining user-defined actions
piLogFormat	'Plfm'	text block defining log file format
piPreProcessor	'Ppre'	relative path to CGI/Plug-In handling preprocessor
piPostProcessor	'Ppst'	relative path to CGI/Plug-In handling postprocessor
piReportDelay	'Prdl'	amount of time in seconds between status report events
piCacheFlush	'Pcfl'	setting this flag indicates the server should flush any cached data
piFileInfoCacheSize	'Pfic'	amount of memory to allocate to file info caching
piKeepAliveConnections	'Pkac'	number of connections per client to keep alive
piKeepAliveTime	'Pkat'	seconds to keep alive idle client connections
piServerCName	'Pscn'	canonical name of server to be used in HTTP responses, regardless of DNS name
piCGIBinOnly	'Pcbo'	flag determining if CGIs will be executed from the /cgi-bin folder only
piServiceAddress	'Pisa'	table of registered service addresses
WebSTAR-specific		
piSSLInterface		See starnine.h file in the SDK for details
piBrowserBufferBag		See starnine.h file in the SDK for details
piDefaultAction		See starnine.h file in the SDK for details
piByteServerAction		See starnine.h file in the SDK for details
piCGIPersist		See starnine.h file in the SDK for details
piSSLPort		See starnine.h file in the SDK for details
piWNEThreshold		See starnine.h file in the SDK for details
piSSLAvailabale		See starnine.h file in the SDK for details
piFragList		See starnine.h file in the SDK for details
piFagVers		See starnine.h file in the SDK for details

Error Checking

If the path to a Plug-In processed URL request is incorrect, the WebSTAR Web server will now serve the user-defined Error file.

Under previous versions of WebSTAR when a bad URL request (i.e. `http://www.domain.com/bogus.ssi`) was sent to a Plug-In, that Plug-In was responsible for returning an error message to the user saying that the file did not exist. Note that in this situation the defined Error file was not being processed. Now if a Plug-In returns a `WSAPI_E_MessageNotHandled` from a non-existent file request, the WebSTAR Web server will now handle normal processing of the Error file (instead of just returning a 404 status code).

Additional information on WebSTAR API Plug-ins

For more information about how to develop Plug-Ins that work with the WebSTAR server, see:

<http://dev.starnine.com>

ClearWay's WebSTAR API Plug-In Cookbook:

<http://dev.clearway.com/>

USING WEBSTAR PLUG-IN SERVICES

Many of StarNine's WebSTAR Plug-Ins provide *services*, meaning that other Plug-Ins can use their features. Plug-ins can take advantage of the functionality of other Plug-Ins and work together, for example, WebSTAR SSI calls WebSTAR Data Cache to cache static data. Third-party Plug-Ins may also support services.

You can call the standard WebSTAR Plug-Ins according to the instructions below. Be sure to do a "preflight" to make sure that the Plug-In is installed, and deal with the errors if it is not.

Calling WebSTAR Auto BinHex

At WebSTAR API Registration time, WebSTAR Auto BinHex registers a service named "BINHEX". This service references routines with the following C prototype:

```
void BinHex(WSAPI_CommandPBPtr pb, char *fileName);
```

where 'pb' is a WebSTAR API parameter block and 'filename' is a Macintosh path (absolute or partial) pointing to the file to be

BinHexed and send to the client. The path must also include a trailing “.hqx” extension.

Calling WebSTAR Data Cache

If your Plug-In returns static data, you can take advantage of the WebSTAR Data Cache to have that data stored in memory, rather than requested from your Plug-In at all times.

At WebSTAR API Registration time, WebSTAR Data Cache registers services named “DATACACHE” and “CACHE_PIXO”. Both services perform similar functions: to return the contents of a specified file to the caller (retrieving the data from the cache if possible), and to cause the file to be cached for subsequent retrievals.

The DATACACHE service uses a simple WebSTAR API service routine calling interface defined by the following C prototype:

```
char * DataCacheService (WSAPI_CommandPBPtr pb, char *filename, char
                        *mimetype)
```

The CACHE_PIXO service uses the PIXO interface (<http://dev.clearway.com/pixo/>) defined by the following C prototype:

```
PIXO_RunResult HandlePIXOService
                (PIXO_ParameterBlockPtr pixoPB)
```

WebSTAR Data Cache now defines some additional and much improved services for handling of cached data. They are:

```
struct cacheFileData {
    // INPUTS
    char *filename;
    // OUTPUTS from Cache_GetFileData, INPUTS for Cache_ReleaseFileData
    unsigned long len;    // how many bytes in the file data
    char *data;    // the file data
    unsigned long cookie[4]; // Needed to "unlock" the item. There's enough
                          // room here for unplanned uses. Our implementation
                          // only uses cookie[0..1]
};

/* Use with Cache_FlushItem to specify the file you want flushed. */
struct cacheFlushFile {
    char *filename; // the name of the file to flush from memory
};
```

```
typedef struct {
    Cache_Command  command;
    union {
        struct cacheAPIInfo api;
        struct cacheFileInfo finfo;
        struct cacheFileData data;
        struct cacheFlushFile flush;
    };
} Cache_Params, *Cache_ParamsPtr ;
```

Calling WebSTAR Proxy

This flexible architecture allows for third party developers to easily augment features in the Proxy or replace the default features that already exists. The Proxy server in WebSTAR Server Suite is not just one Plug-In but rather several Plug-Ins working together. For example, a third party developer could easily replace our WebSTAR Proxy Cache Plug-In with one of their own, or write a “WebSTAR Proxy FTP” Plug-In to handle Proxy FTP requests.

- Main “Dispatch” plug-in that accepts connections from browsers, calls the other plug-ins when they need to be called, and then releases the connection. The other plug-ins register themselves with the Dispatcher to let it know they are available.
- Multiple “Access” plug-ins. They control which users have access to what kinds of data.
- Multiple “Protocol” plug-ins. They handle requests with specific protocols. (e.g.: the HTTP plug-in handles requests for Web information.)
- Multiple “Postprocess” plug-ins, which do logging and other after-the-fact processing.
- Multiple “Munger” plug-ins, which have an opportunity to change data while it is being delivered to the browser.

In addition to these plug-ins, we have also included a *WebSTAR Proxy Cache* Plug-In that works with the *WebSTAR Proxy HTTP* plug-in to cache and manage data that the WebSTAR Proxy Server receives.

Proxy Log Information

You can get and set the WebSTAR Proxy log name and location via AppleEvents:

```
#define kPLEventClass 'Pxyl'
        // set log file name - typeChar
#define kPLEventSetFile 'stlg'
```

```
// get the log file name - typeChar
#define kPLEventGetFile 'gtlg'
```

Calling WebSTAR Form Mail

At WebSTAR API Registration time, WebSTAR Form Mail registers three services named “FORMMAIL”, “FORMMAIL_MIME” and “FORMMAIL_SSI”. The service “FORMMAIL” uses the following C prototype to pass parameters needed to send mail:

```
void FormMail (WSAPI_CommandPBPtr pb, char *from, char *to, char *subject,
char *body, char *host);
```

The service “FORMMAIL_MIME” uses the following C prototype to pass strings to become MIME-encoded:

```
void FormMailMime (WSAPI_CommandPBPtr pb, char *data);
```

The service “FORMMAIL_SSI” uses the following C prototype to receive text from the WebSTAR SSI #exec pIService command.

```
char *FORMMAIL_SSI(WSAPI_CommandPBPtr pb, char *text)
```

Calling WebSTAR SSI

At WebSTAR API Registration time, WebSTAR SSI registers two services named “SSISend” and “SSIParse”. These services references routines with the following C prototype:

```
char *Service(WSAPI_CommandPBPtr pb, char *text)
```

Both services perform SSI processing on the null-terminated text parameter. The SSISend service will send the results back to the client via `WSAPI_SendHTTPData()`. The SSIParse service will return the results to the caller as a null-terminated string. The caller must dispose of the result string via `WSAPI_FreeMemory`.

Service routines must be defined as follows to be a valid target of this exec command extension:

```
char *Service (WSAPI_CommandPBPtr pb, void *param);
```

If no character value is returned by the service, it is assumed that the service routine inserted any results directly into the HTTP output stream (via the `WSAPI_SendHTTPData` call). Otherwise, the character string returned by the service is processed by SSI, sent to the client, and then disposed of (via the `WSAPI_FreeMemory` call).

DEVELOPING JAVA SERVLETS FOR WEBSTAR

The WebSTAR JRun Servlet Runner includes support for JDK 1.1 through the use of MRJ 2.1.1 or above, as well as support for the JDK 1.2 Servlet API, including persistent session tracking. This version now uses a Java application for JRun configuration. The application is written using JFC 1.1.

Because the Macintosh has a file length limit, the Servlet API docs are included as a ".zip" icon. You should view these on an alternate file system or view each file individually.

The WebSTAR Java Servlet Runner is developed by Live Software:

<http://www.livesoftware.com>

Overview of JRun

JRun, is a set of Java classes and native code that can extend your Web server to support Java Servlets. By using Servlets as an extensible, well-defined Java component model across all environments, sophisticated applications for both client and server become easier to develop, faster to deploy, and more cost effective to maintain.

JRun 2.3 fully implements the Java Servlet API. In addition, JRun also implements many of the advanced features found in the Java Web Server. Following are some of JRun 2.3's feature highlights:

- dynamic reloading of modified servlets
- packaging of servlets in .zip files
- dynamic reloading of modified .zip files
- servlet initialization parameters
- servlet chaining
- servlet filtering
- servlet chains within filters
- software virtual server support
- separate servlet and logging directories for each virtual server
- <SERVLET> tag support

- persistent session tracking support
- administration JFC 1.1 application

Using JRun

The WebSTAR Server Suite Installer does not install the WebSTAR JRun Servlet Runner and related files automatically—this is a custom install option. Once installed, run the JRun Admin application to administer JRun. For more information, see the examples in the *WebSTAR Server Suite* folder.

Additional information on Java Servlets

- Apple's Mac OS Java site: <<http://www.apple.com/java/>>
- Live Software: <<http://www.livesoftware.com>>
- Gamelan Java software repository <<http://www.gamelan.com>>

Index

Symbols

\$ (dollar sign), in URLs 189
 ((left bracket), in URLs 189
 .message File 242
 / (slash), in URLs 189
 > (right bracket), in URLs 189
 ~error.html 131
 ~noaccess.html 132
 “#” (SSI) 275
 “-” (Dash) in Log Files 201

Numerics

192.168.0.2 (temporary IP address) 47

A

Absolute File Path
 URLs 188
 Web Admin 121
 Access Control
 FTP 344
 Proxy 418
 Web (see also “Realms”) 164
 Accounts, Mail Server 391
 ACGI Action 158
 ACGIs 446
 Acrobat
 Byte-Range Serving 240
 suffix 425
 Actions 161
 Editing 162
 Using 163
 Suffix Mapping 158
 ACGI 158
 BINARY 158
 CGI 158
 Editing 161, 162
 Example 163
 IMAGE MAP 159
 RAW 159
 SSI 159
 TEXT 158
 Active Server, in Admin 114
 Admin
 Application 113
 Browser 55
 FTP 341
 Mail Settings 373
 Troubleshooting 327
 (see also “WebSTAR Admin”)
 AIAT Search Plug-In 261
 AIFF suffix 426
 Aliases
 Web 190
 Aliases, in FTP Folders 338
 Allow/Deny 172
 DNS 173, 389
 Domain Matching 173, 389
 Editing 173, 388
 Error File 183
 Examples 175
 Host Matching 173, 389
 IP Address Matching 173, 389
 Mail Server 387
 Number Denied Status 79
 Alternate DNS Server (Mail) 374
 Anonymous FTP 347
 APOP (Mail Server) 359
 Apple Events 446
 Properties 450
 Apple Events for WebSTAR 446
 Apple Information Access Toolkit 261
 AppleScript for CGIs 446
 Archiving Logs 200, 353, 422
 ASCII
 Definition 189
 FTP 339
 Suffix 426
 Asynchronous CGIs 446
 Authentication
 (see also “Web Users”) 168
 Auto BinHex 238
 Caching 239
 Calling Programmatically 460
 Other Suffixes 239
 Security 239
 Auto Flush Cache Setting 143
 Available Memory (Status) 78

B

Background-Only Server 91
 Backup
 Mail Server 370, 374

BINARY Action 158
 BinaryData Type in FTP 339
 BinHex suffix 425
 Brackets (“<>”) in URLs 189
 Broken Pipe Error 334
 Browser Admin 55
 Action List 163
 Allow/Deny List 174
 Auto-Flush Cache 143
 Buffer Size 136
 Data Cache 141
 Default MIME Type 133
 Error File Path 131
 Flush Cache Now 86
 Index File Name 131
 KeepAlive 137
 Log File Format 207
 Log File Path 199, 353, 422
 Log Options 199
 Max Connections 134
 Misc. Settings 134
 Monitor 78
 No Access File Path 132
 Plug-Ins 237
 Port Number (Web) 135
 PostProcess 133
 PreProcess 132
 Realms List 167
 Refuse Connections 86
 Restrict CGIs 137
 Server Name 130
 Status Report Delay 200
 Suffix Mapping Table 157
 Suspend Logging 85
 Timeout 136
 Troubleshooting 327
 Use DNS 136
 Verbose Messages 85
 Browsers 50
 Access Secure Server 211
 Accessing Email 363
 Broken Pipes 334
 Crash Troubleshooting 333
 Mail Access 363
 Proxy Configuration 63
 Secure/Unsecure Error 233
 Using Proxy Server 413
 WebSTAR Compatibility 50

- Buffer Size, Setting 136
- Busy Connections (Status) 79
- Byte Server 240
 - Example, PDF 240

C

- Cache
 - Auto Flushing 143
 - Data Cache 140
 - DNS 136
 - File Info Cache 139
 - Flush Command 86
 - Mail Server 382
 - Proxy 412
 - Settings 139
- Case Sensitivity
 - URLs 67
 - Web Admin File Paths 122
- CGI Action 158
- CGI suffix 425
- CGIs 154
 - Developing 445
 - Parameters 451
 - Restrict to CGI-BIN folder 86
 - Restricting 137
 - Security 86, 94
 - Setting Actions 161
 - Third-Party 445
 - Using 154
 - Writing 445
- CLF (Common Log Format) 202
- Client
 - Browser 50
 - FTP 337, 341, 355
 - Mail 358
 - Web 50
- Client-Side Image Maps 253
- Common Log Format 202
- Config Command (SSI) 292
- Connecting Admin to Server 113
- Connection Files for Admin 114
- Connection Meter (Status) 78
- Connection Refused (SSL) 232
- Connections
 - Busy Count 79
 - Current 78
 - Denied Count 79
 - Dropping Inactive 136
 - Duration 138
 - High 78
 - HTTP 179
 - Mail 377
 - Maximum
 - Setting 134
 - Status 78
 - Persistent 137
 - Session Total 78
 - Settings 134
 - SMTP 378
 - Status 78
- Cookies 180
- Core Plug-Ins, installing 35
- Core WebSTAR Plug-Ins 42
- Counter Command (SSI) 284
- Crashes
 - Browsers 333
 - Troubleshooting 327
- Creator Code 154
 - Suffix Mapping Example 156
 - WebSTAR 103
- Cryptography 209
- Current (Active) Connections 78
- Current Server, in Admin 114
- Custom Installer Options 34

D

- Dash ("-") in Log Files 201
- Data Block Size 136
- Data Cache 140
 - Calling Programmatically 461
 - Info Window 142
 - Optimizing Size 141
- Data Sent (Status) 78
- Default Host 145
- Default Index File Name 65
 - Setting 131
 - Virtual Hosts 150
- Default MIME Type 133
- Default Page 65
- Default Root Folder 122
- Default.html 131
- Defaults, Mail Settings 373
- Delimiters
 - Admin File Paths 121
 - URLs 189
- Denied Connections (Status) 79
- Deny (see also "Allow/Deny") 172
- DES Encryption 209
- Development 443
 - CGIs 445
 - Java Servlets 464
 - Plug-In Services 460
 - Plug-Ins 454
 - URL 443
 - W*API Parameters 455
 - WebSTAR-Dev Mailing List 443
- Digital ID Pair
 - Thawte 218
- Directory Indexer 241
 - Administration 244
 - Default Index Page Issues 244
 - Enabling with .message 242
 - Footer 242
 - Header 242
 - Icons and Caching 243
 - Upload 242
- Distinguished Name (SSL) 222
- DNS 100
 - In Allow/Deny Matching 173, 389
 - Log File Format 201
 - Mail Hosts 362
 - Setting Server Lookup 136
- DNS Server, Mail Alternate 374
- Dollar sign ("\$\$") in URLs 189
- Domain Name Service 100
- Domain Names 98
 - Access Control 172
 - see also "Host Names"
 - Top-Level (TLD) 99
 - Virtual Hosts 193
- Domestic Encryption (SSL) 210
- Download, FTP 337

E

- Echo Command (SSI) 280
- Email Access from Browsers 363
- Email Server (see also Mail Server) 357
- Email Support 107, 327
- Email Web Forms 249
- Empty Caches 86
- Encoding, File Name 189
- Encryption
 - Admin to and from Server 113
 - SSL 209

- Energy Saver Server Settings 110
- Error File Path
 - Default Host 131
 - Virtual Hosts 150
- Error Messages 334
- Exec Command (SSI) 288
 - Security 153
- ExLF (Extended Log Format) 203
- Export
 - FTP Users 347
 - Mail Users 395
 - Web Users 170
- Extended Log Format 203
- Extending WebSTAR 443
- Extra Plug-Ins, installing 35

F

- File Creator Code 154
- File Info Cache 139
- File Listing Plug-In 241
- File Names 186, 189
 - Hex Encoding 189
 - Mac Special Characters 189
 - Rules for Web 189
 - Virtual Hosts 150
 - Web Default Host 130
- File Paths 186
 - Absolute
 - URLs 188
 - WebSTAR Admin 121
 - Delimiter
 - URLs 189
 - WebSTAR Admin 121
 - FTP Root Folder 346
 - in HTML Links 187
 - Relative
 - URLs 188
 - WebSTAR Admin 122
 - SSI 277
 - URL 181
 - WebSTAR Admin
 - Delimiters 121
- File Security 95
- File Type Code 154
- File Upload 247
 - see also “FTP” 337, 341, 355
 - Administration 248
 - Enabling with .upload 247
 - Upload Form 247

Files

- Aliases 190
- Created by WebSTAR 103
- Creator Code 154
- Installed by WebSTAR 40
- Paths in WebSTAR Admin 121
- Suffixes 154
- Type Code 154
- Web Aliases 190
- Web Redirect 190
- Web Serving 186
- Filter Plug-Ins 455
- Firewall Issues 103
- FLastMod Command (SSI) 283
- Flush Cache 86
- flush the caches 143
- Folder Hierarchy 186
 - Example 186
 - Introduction 65
 - Virtual Hosts 187
- Folders
 - Aliases 190
 - FTP Root 346
 - Links 187
 - URL Rules 189
 - Web Aliases 190
 - Web Hierarchy 186
 - Web Redirect 190
 - Web Root 122
- Formats of Logs 200
- Forms
 - Email 249
 - Search 269
- Forwarding Email 380, 393
- Frontier 444
- FSize Command (SSI) 283
- FTP 337, 341, 349, 355, 357, 407
 - Access Control 344
 - Administration 341
 - Anonymous Access 347
 - ASCII 339
 - BINARY 339
 - Command List 350, 351
 - Connections, Max 341
 - Conventions 355
 - Data Types 339
 - FAQs 355
 - File and Folder Names 340
 - Flushing Cache 337

- Folders 337
- Getting Started 57
- Logging 349
- MacBinary 339
 - Setting 344
- Max Connections 341
- Monitor 82, 116, 349
- Port 340
- Root Folder 346
- Security 337
 - User Accounts 344
- Specifications 355
- Standards 355
- Status Window 349
- Timeout 341
- Troubleshooting 355
- URLs 339
- Use MacBinary 344
- Users 344
 - Allow Login 346
 - Anonymous 347
 - Create Folders 346
 - Delete and Change 346
 - Delete Folders 346
 - Download 346
 - Import & Export 347
 - Name and Password 345
 - Privileges 346
 - Root Folder 346
 - Upload 346
- Users File 105
- FTP Root Folder 337
- FTP Users File 105

G

- GIF
 - Suffix Mapping Example 155

Graphics suffixes 425
GZIP suffix 426

H

Handshake Failed Error 232
Hardware Requirements 29
Hexadecimal Encoding 189
Hide Command (SSI) 285
Hide Window in Background 86
High Connections (Status) 78
High-Water Mark (Status) 79
Hits This Session (Status) 78
Host Names 98
 (see also "Virtual Domains") 194
 Mail Server 375
 Setting Your Server 99
 Virtual Host Routing 146
Host, Default 145
Hot Spots (Image Maps) 253
HTTP 64
 Connections 179
 Persistent Connections 137
 Web Serving 179
HTTPS 211

I

Image Map 249
 Format 254
 Suffix Mapping Example 155
IMAGE MAP Action 159
Images, Troubleshooting 332
IMAP 360
 Connections 381
Import
 FTP Users 347
 Mail Users & Mailboxes 396
 Web Users 170
Inactive Connections, Timeout 136
Include Command (SSI) 282
 Security 153
Index File Name 65
 see also "Default Index File"
 Setting 131
 Virtual Hosts 150

Index Files for Search 266
Index.html 131
Indexing for Search 266
Installation
 Custom Options 34
 Files 40
 New 32
 Options 34
 Plug-Ins 236
Installing Plug-Ins 35
Interval, Status Report 200
IP Address 97
 Control Access Using 172
 Host 97
 Temporary 47
 Virtual Hosts 194
IP Multihoming 194
 Special Issues 195
 Troubleshooting 335
 WWW3 Recommendation 194

J

Japanese
 CharSet SSI Tag 294
 Default SSI Character Set 152
Java Servlet Runner 255
 Developing For 464
Java suffix 425
Java Virtual Machine 29
JavaScript suffix 425

K

Kanji
 CharSet SSI Tag 294
 Default SSI Character Set 152

Keep Alive 137
Key Password (SSL) 228

L

Language Routing 147
Launch Troubleshooting 327
LDAP 360
LDAP Connections 382
LED (Status) 78
License and Serial Numbers 84
Listen Port, Setting 135
Listing Plug-In 241
Load Histogram (Status) 78
Log Archiving 200, 353, 422
Log File
 Analysis Programs 200
 Created by WebSTAR 105
 Name and Path 199, 353, 422
 Proxy 421
Log Formats
 Administration 200
 Common Log Format (CLF) 202
 Configuration 207
 Dash (" ") 201
 Extended Log Format (ExLF) 203
 Host Name 201
 Options 202
 Setting 207
 Tokens 201, 203
 WebSTAR (WLF) 202
Logging
 Archive Settings 200, 353, 422
 File Path 199, 353, 422
 Files 105
 Formats 200
 FTP 349
 On and Off 199, 353, 422
 Proxy 419, 421
 Status Report Delay 200
 Suspending 85
Lookups, DNS 136
Lowercase (see also "Case Sensitivity")

67
Low-Water Mark (Status) 79

M

Mac OS Energy Saver 110
Mac OS Versions 29
Mac Special Characters 189
MacBinary 342
MacBinary (FTP) 339
MacBinary suffix 425
MacPerl 444
Mail Administration 367
Mail Client Login Requirement 380
Mail Clients 358
Mail Routing 384
Mail Server 357
 Accounts 391
 Administration 367
 Allow/Deny 387
 APOP 359
 Backup 370, 374
 Caching 382
 Client Login Requirement 380
 Client Problems & Errors 408
 Connections 377
 Defaults 373
 DNS 362
 Files 357
 Forwarding 393
 Hosts 375
 IMAP 360
 LDAP 360
 POP 359
 Postmaster 367
 Repairing Damage 407
 Routing 384
 SMTP 358
 Spam 370
 Troubleshooting 407
 Usage 368
 Users
 Characters Allowed 398
 Import/Export 395
 Naming Systems 398
 Users & Accounts 391
 Web Mail 363
Mailing Lists for WebSTAR 107, 327
Map, Image 249
 Suffix Mapping Example 155

Match Strings, Realm 164
Max Connections
 Setting 134
 Status 78
Max Mem (Status) 79
Maximum Data Cache Size 141
Memory
 Available 78
 Maximum Used 79
 Minimum Used 79
 Requirements 29
Memory Meter (Status) 78
Menus
 Server Application 83
 WebSTAR Admin 116
Message (.message) File 242
Message Form 364
Microsoft Excel suffix 427
Microsoft Word suffix 427
MIME Type
 Default 133
 Suffix Mapping 160
Min Mem (Status) 79
Monitors
 in Admin 116
 in Server 80, 81
Moving a Web Site to WebSTAR 66
Multihoming 193
 see also "IP Multihoming"
 see also "Virtual Hosts"
 Troubleshooting 335
Multiple Servers 92
 Virtual Hosts 193

N

Names, File (see also "File Names") 186
Network Requirements 30
No Access File Path
 Default Host 132
 Virtual Hosts 150

O

Open Transport
 Keep Loaded Setting 31
 MultiHoming 195
 Multiple IP Troubleshooting 335
 Version Compatibility 29

Operating System Requirements 29
Optimization
 Data Cache 141
 Proxy Cache 418
Optimizing Server 90
Options Menu 85
Origin Server (Proxy) 411

P

Parameters
 CGI 451
 W*API 455
Passwords 96
 Admin Password 83
 Choosing and Securing 96
 FTP 345
 FTP Users File 105
 Mail Users 392
 SSL Key 228
 Web Users 168
 WebSTAR.pass File 104
Paths, see "File Paths"
PC executable suffix 425
PDF
 Byte-Range Serving 240
 Searching 261
 suffix 425
Performance, Optimizing 90
Perl 444
Persistent Connections 137
PI_ADMIN
 (see also "Browser Admin") 126
 Password 55
Pipe, Broken Error 334
PIService (SSI Tag) 290
Plug-Ins 154, 275
 Installing 236
 Removing 236
 Acrobat 240
 Administration 237
 Auto BinHex 238
 BinHex 238
 Browser Admin 237
 Byte Server 240
 Core 35, 42
 Developing 454
 Directory Indexer 241
 Extra 35
 File Upload 247

- Filter 455
- Image Map 249
- Installing 35
- Java Servlet Runner 255
- Menu 86
- PDF 240
- QuickSend 249
- Search 261
- Security 94
- Services 460
- Setting Action 161
- Settings 237
- SSI 275
- Third-Party 445
- Troubleshooting 327
- WebObjects Adaptor 272
- WebSTAR Core 42
- POP Connections 381
- POP Mail 359
- Port Numbers 102
 - Admin 102
 - FTP 103, 340
 - IMAP 103
 - LDAP 103
 - Mail Server 103
 - POP 103
 - Proxy Server 103
 - Setting 135
 - SMTP 103
 - SSL Web Server 103
 - Web 102
- PostArg Command (SSI) 291
- Postmaster Account 367
- Post-Processor Setting 133
- PostScript suffix 427
- Pre-Processor Setting 132
- Problems, Troubleshooting 327
- Proxy 411, 415
 - Access Control 418
 - Allow/Deny 418
 - Access From Proxy 419
 - Access To Proxy 418
 - Browser Configuration 63
 - Browsers 413

- Cache 412
 - Expiration 412
 - Flushing 412
 - Maintenance 418
 - Maximum File Size 417
 - Maximum Size 417
 - RAM Size 418
 - Time-To-Live 412, 417
 - Expiration Ratio 417
 - Maximum 417
 - Ratio 417
- Cache Optimization 418
- Calling Programmatically 462
- Configuring Browsers 413
- Connections 415
 - Maximum Connections 415
 - Port 415
 - Timeout 415
- Expiration 417
- Flushing Cache 412
- Getting Started 63
- Log File 421
- Logging 419, 421
- Monitor 82, 421
 - Admin 117
 - Server 83
- Origin Server 411
- Privacy 411
- Server Plug-Ins 414
- Status Window 421
- Public Key Cryptography 209
- Public/Private Key
 - Thawte 216
 - VeriSign 220

Q

- QuickSend 249
 - Administration 251
 - Calling Programmatically 463
 - Custom Return & Error Pages 252
 - Examples 250
 - Mail Host 252
- QuickTime suffix 426
- Quit Server from Admin 119

R

- RAM
 - (see also "Memory")

- RAW Action 159
- RAW files 191
- RC4-128 Encryption 209
- RC4-40 Encryption 209
- RealAudio suffix 426
- Realms 164
 - Allow/Deny 172
 - Editing 165
 - Examples 165
 - Match Strings 164, 165
 - Users and Passwords 168
- Redirect Web Files 190
- Refuse New Web Connections 86
- Refused Connections (Status) 79
- Relative File Path
 - URLs 188
 - Web Admin 122
- Relay Restrictions, Mail 380
- Removing Plug-Ins 236
- Require Prior Client Login 380
- Restart Server
 - Application 90
 - Development 90
- Restrict CGIs to CGI-BIN 86, 137
- Root Folder 122
 - Default 66
 - FTP 346
 - Serving Files 181
 - Virtual Hosts 149, 196
- Routing to Virtual Hosts 146
- Routing, Mail 384
- RSA Encryption 209

S

- Safe Passwords 96
- Scripting 444
- Search
 - Auto-Update 271
 - Boolean Operators 262
 - Dictionaries 269
 - Examples 264
 - Forms 269
 - Index Root Folder 267
 - Indexing 266
 - Installation 264
 - Merging Indexes 268
 - Parameters 271
 - Queries 261
 - Search Index Files 266

- SSI Tags 270
- Stopwords 269
- Substitution 269
- Update 266
 - Automatic 271
- URLs and Links 270
- Secure/Unsecure Error 233
- Security 93
 - CGIs 86
 - Files 95
 - FTP 337
 - Passwords 96
 - Realms 164
 - Web Server 183
- Sent (Status) 78
- Serial Numbers 48, 84
 - Test 49
- Server
 - Admin Password 83
 - Background-Only (BG) 91
 - CGI security 86
 - Hide Status Window 86
 - Host Name 99
 - Identity 96
 - Menus 83
 - Multiple 92
 - Optimization 90
 - Performance 90
 - Plug-Ins Menu 86
 - Port Numbers
 - Admin 102
 - FTP 103, 340
 - Mail Server 103
 - Proxy 103
 - SSL 103
 - Web 135
 - Web Server 102
 - Quit from Admin 119
 - Refuse New Web Connections 86
 - Restart After OT Errors 90
 - Security 93
 - Serial Numbers 84
 - Session Length 79
 - Startup Troubleshooting 327
- Status
 - Busy 79
 - Connections 78
 - Current Connections 78
 - Denied 79
 - High Number 78
 - Hits 78
 - Max Mem 79
 - Mem 78
 - Min Mem 79
 - Sent 78
 - Up Since 79
 - Suspend Logging 85
 - Troubleshooting 327
 - Verbose Messages 85
 - WebSTAR Admin Connection 113
- Server Certificate (SSL) 224
- Server Fails To Respond
 - (Troubleshooting) 109
- Server Name 98
 - IP, Host Name and DNS 96
 - Redirect Name 130
 - Virtual Hosts Redirect 150
- Server-Side Includes ("SSI") 275
- Services, Plug-In 460
- Servlets, Java 255
 - Developing 464
- Sessions 180
- Shockwave suffix 427
- Show Command (SSI) 285
- signed Certificate pair 218
- Single-Link Multihoming 194
- Slash ("/") in URLs 189
- SMTP 358
 - Connections 378
 - Forwarding 380
- SMTP Web Forms 249
- Spam Prevention 380
- Spam, Dealing With 370
- SSI 275
 - Action 159
 - Administration 296
 - Aliases 278
 - Browser Admin 296
 - Calling Programmatically 463
 - Character Set 294
 - Commands 280
- Config Command 292
 - CharSet 294
 - NewRandom 295
 - SizeFmt 294
- Counter Command 284
- Counters
 - Display 280
 - Editing 297
- Date
 - Example 279
 - Field Descriptor List 433
 - Formatting 293
- Default Character Set 152
- Echo Command 280
 - Example 279
 - W*API Values 282
- Encoding 277
- Environmental Variables 280
- ErrMsg Tag 293
- Error Handling 279
- Example 279
- Exec Command 288
 - CGI Tag 289
 - PIService Tag 290
 - Script Tag 289
- Extensions 306
- File Paths 277
- FLastMod Command 283
- FSize Command 283
- Hide Command 285
 - Operator 286
 - Value 286
 - Variable 286
- Include Command 282
- New Random Number 295
- Path Names 277
- PostArg Command 291
- Random Value
 - Display 281
 - New 295
- Security Settings 153
- Server Environment Variables 280
- Show Command 285
 - Operator 286
 - Value 286
 - Variable 286
- SizeFmt 294
- Special Characters 277
- SSI Suffix 298

- Store Command 291
- Stored Values, Editing 297
- Stored Variable Display 281
- Suffixes
 - Default 298
 - HTML 160
- Tags 306
- TimeFmt (Config) 293
- Using for HTML Files 160
- Virtual Paths 277
- W*API Values 282
- Web Admin 152
- SSI Settings 39
- SSL
 - Browser Access 211
 - Requirements 213
 - Configuration 213, 229
 - Connection Refused 232
 - Distinguished Name
 - Thawte 222
 - Encryption 209
 - Setting Level 228
 - Example Connection 229
 - Handshake Failed Error 232
 - HTTPS 211
 - Installation 213
 - Installation Details 214
 - Key Password 228
 - Launch Troubleshooting 231
 - Proxy Compatibility 232
 - Public/Private Key
 - Thawte 216
 - VeriSign 220
 - Secure/Unsecure Error 233
 - Server Certificate 224
 - SSL Protocol 209
 - Thawte Certificate Authority 220
 - Tools 215
 - VeriSign Certificate Authority 216
- SSL Tools Folder 215
- Startup Troubleshooting 327
- Status Report Delay 200
- Status Window
 - Error Messages 334
 - Hide in Background 86
 - Top Panel 78
 - Update Interval 200
- Stopwords Dictionary (Search) 269
- Store Command (SSI) 291
- Stuftit suffix 425
- Substitution Dictionary (Search) 269
- Suffix 154
- Suffix Mapping 154
 - Symbol 158
 - Defaults 425
 - WebSTAR Plug-Ins 428
 - Action Popup Menu 158
 - Actions
 - ACGI 158
 - BINARY 158
 - CGI 158
 - IMAGE MAP 159
 - RAW 159
 - SSI 159
 - TEXT 158
 - Examples 155
 - Locked Entries 158
 - Match Fields 159
 - MIME Type 160
 - SSI 298
 - SSI Example 160
 - Suffix 159
 - Table 156
- Suffix, File 154
- Support 107, 327
- Suspend Logging 85
- System Requirements 29
 - Network 30
 - RAM 29
 - System Software 29
- T**
 - Tags, SSI 306
 - TAR suffix 426
 - Technical Support 107, 327
 - Test Server
 - Temporary IP Address 47
 - Temporary Serial Number 49
 - TEXT Action 158
 - Thawte Certificate Authority for SSL 220
 - Third-Party Add-Ons 445
 - Timeout
 - Admin 115
 - FTP 341
 - Web Server 136
- Tokens, Log 201
 - Details 203
- Tools & Examples Folder 44
- Top-Level Domains (TLDs) 99
- Total Number (Connections) 78
- Troubleshooting 327
 - Mail Server 407
- Type Code 154
 - Suffix Mapping Example 156
- Typhoon 444
- U**
 - Up Since (Status) 79
 - Upload
 - FTP 337
 - HTTP 247
 - Uppercase (see also "Case Sensitivity") 67
 - URLs 64, 180, 183
 - Brackets ("<>") 189
 - Delimiters 189
 - Encoding 189
 - Example 186
 - FTP 339
 - Links 187
 - Redirecting 191
 - Security Processing 183
 - Slash ("/") 189
 - WebSTAR Processing of 180
 - US Domestic Encryption (SSL) 210
 - Usage, Mail Server 368
 - Use DNS for Lookups 136
 - Users
 - (see also "Web Users") 168
 - FTP 344
 - Mail Server 391
 - Web 168
- V**
 - Verbose Messages 85
 - VeriSign Certificate Authority 216
 - Version History URL 69
 - Virtual Domains 194
 - see also "Virtual Hosts"
 - Special Issues 197
 - WWW3 Recommendation 194
 - Virtual Hosts 144, 193
 - "Any" Entries 145

- Default Host 145
- Default Index File Name 150
- Editing Entries 144
- Error File Path 150
- Folder Hierarchy 187
- Host Name 146
- IP Address 146
- IP Multihoming 194
 - Special Issues 195
- Language Routing 147
- No Access File Path 150
- Preparation 194
- Root Folder 149
- Root Folders 196
- Routing Concepts 193
- Routing Examples 146
- Server Name Field 150
- Settings 144
- Third-Party Alternatives 193
- Third-Party Options 193
- Troubleshooting 334
- Virtual Domains 194
 - Special Issues 197
- WWW3 Recommendation 194
- VRML suffix 427
- V-Twin Search Plug-In 261

W

- W*API Parameters 455
- W*API Plug-Ins 454
- WAV suffix 146
- Web Admin
 - Actions 161
 - Allow/Deny 172
 - Editing 173, 388
 - Examples 175
 - Auto Flush Cache 143
 - Buffer Size 136
 - Caching 139
 - Client, Connections Per 138
 - Connections 134
 - Data Cache 140
 - Default Index File Name 131
 - Default MIME Type 133
 - Duration, Connection 138
 - Error File Path 131
 - File Info Cache 139
 - File Mapping 154
 - File Names 130

- File Paths
 - Absolute 121
 - Relative 122
- Index File Name 131
- Log Formats 200
 - Configuration 207
- Max Connections 134
- No Access File Path 132
- Password (Admin) 83
- Passwords (Web Users) 168
- Persistent Connections 137
- Port Number 135
- Post-Processor 133
- Pre-Processor 132
- Realms 164
 - Editing 165
- Restrict CGIs 137
- Server Name 130
- SSI 152
- Status Report Delay 200
- Suffix Mapping 154
 - Editing Entries 156
 - Example 160
 - Table 156
- Timeout 136
- Use DNS 136
- Users (Web) 168
 - Editing 168
 - Example 170
 - Import/Export 170
- Virtual Hosts 144
 - Editing 144
 - Routing Examples 146
- Web Users 168
 - Editing 168
 - Example 170
- Web File Paths 186
- Web Log File Formats 202
- Web Mail 363
- Web Monitor 80
 - Admin 116
 - Server 80
- Web Port Number 135
- Web Server
 - Absolute File Paths 188
 - Access Control 164, 183
 - Aliases 190
 - Cookies 180
 - File Name Rules 189

- File Paths 181
- Host Name
 - Default 99
 - Virtual Hosts 144
- HTTP 179
- Redirect 190
- Relative File Paths 188
- Security Processing 183
- Sessions 180
- URL Processing 180
- Web Site 57
 - Example Hierarchy 186
 - File Security 95
 - Folder Hierarchy 65, 186
 - Troubleshooting 330
 - Virtual Hosts Hierarchy 187
- Web Status Window 80
- Web Users
 - Editing 168
 - Example 170
 - Export File Format 171
 - Import and Export 170
 - Passwords 168
 - Server File 104
 - WebSTAR.pass File 104
- Web-Based Email, Enabling 374
- WebObjects 180
- WebObjects Adaptor 272
- WebSiphon 444
- WebSTAR 52
 - Admin 113
 - Server 113
- WebSTAR Admin 113
 - see also "FTP" 341
 - Connection Files 114
 - Current Server 114
 - Getting Started 52
 - Menus 116
 - Monitor Windows 116
 - Multiple Servers 114
 - New Connection 52
 - Password 83
 - Quit WebSTAR Command 119
 - Security and Passwords 115
 - Windows 116
- WebSTAR API 454
- WebSTAR Apple Events 446
 - Properties 450

- WebSTAR BG 91
 - Troubleshooting 334
- WebSTAR Byte Server 240
- WebSTAR Development 443
- WebSTAR Directory Indexer 241
- WebSTAR FTP 337, 341, 349, 355, 357, 407
- WebSTAR Log Format 202
- WebSTAR Mail Data Files 357
- WebSTAR Mail Server 357
- WebSTAR Mailing List File 45
- WebSTAR Plug-Ins 275
 - (see also "Plug-Ins")
 - Auto Binhex 238
 - Byte Server 240
 - Core 42
 - Directory Indexer 241
 - File Upload 247
 - Image Map 249
 - Java Servlet Runner 255
 - QuickSend 249
 - Search 261
 - Services 460
 - SSI 275
 - WebObjects Adaptor 272
- WebSTAR Proxy 411, 415
- WebSTAR Scripting 444
- WebSTAR Security 93
- WebSTAR Serial Number 48
- WebSTAR Settings File 104
- WebSTAR.pass File 104
- WebSTAR.pass file 70
- WebSTAR-Talk Mailing List 107, 327
- Windows
 - in Server 77
 - in WebSTAR Admin 116

Z

- ZIP suffix 426