WU-FTPD 2.4 Release Notes

HP 9000 Series Computers

Version 2.4

Manufacturing Part Number: 5971-2286

E0698

United States

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett- Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY 3000 Hanover Street Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Contents

1. WU-FTPD 2.4 Release Notes

Overview 8

WU-FTPD Overview 9

What's New in this Version 10

New ftp Daemon Options 11

New ftp Support Commands 13

New ftp Configuration Files 15

The ftpaccess Configuration File 15

The ftpconversions Configuration File 21

The ftphosts Configuration File 22

The ftpusers Configuration File 22

The ftpgroups Configuration File 23

The xferlog Log File 23

Virtual ftp Support 26

Setting Up a Secure Version of ftp 28

Contents

1 WU-FTPD 2.4 Release Notes

Overview

- What's New in this Version of ftp
- New ftp Daemon Options
- New ftp Support Commands
- New ftp Configuration Files
  - The ftpaccess Configuration File
  - The ftpconversion Configuration File
  - The ftphosts Configuration File
  - The ftpusers Configuration File
  - The ftpgroups Configuration File
  - The xferlog Configuration File
- Setting Up Virtual ftp Support
- Setting Up a Secure Version of ftp

WU-FTPD Overview

The new version of ftp has been made available for HP-UX as follows:

HP-UX Release	ftp Patch June 1998
11.0	PHNE_14479, released in June 1998, superseded by PHINE_17188
11i	part of the core networking products

All the features of the existing (“legacy”) ftp are present in the new version of ftp along with additional functionality. This June 1998 version of ftp contains WU-FTPD 2.4 ftp server changes and its therefore also referred to as WU-FTPD 2.4.

NOTE PHNE_17188 is the latest ftp patch.

CAUTION In general, existing installations do not have to modify their ftp configurations unless they want to use the new features. There is one exception; there is a difference in the ftp daemon options between legacy ftp and the new June 1998 version of ftp. In the older version of ftp, the -A option enables Kerberos authentication. In the new version of ftp, the -K option enables Kerberos authentication, and the -A option is used to disable the ftpacess file. See the section “New ftp Daemon Options” for more information.

What's New in this Version

WU-FTPD 2.4 introduces new configuration files, daemon options and support commands, detailed below, to support the following new features:

- logging of transfers
- logging of commands
- on the fly compression and archiving
- classification of users on type and location
- per-directory upload permissions
- restricted guest accounts
- system-wide and per-directory messages
- directory aliases
- cdpath
- filename filter
- virtual host support
- per-class limits

New ftp Daemon Options

The following new options are used for the ftp daemon, `/usr/lbin/ftpd`. You specify these options in the ftp entry of the inetd configuration file (typically `/etc/inetd.conf`).

An example ftp entry in the `/etc/inetd.conf` file might look like this:

ftp stream tcp nowait root `/usr/lbin/ftpd` ftpd -l -d -a

The preceding example sets the -l, -d, and -a options, which are explained below:

- **-l**

  Using this option with ftpd enables logging of the ftp session to the syslog file.

- **-d**

  Using this option logs debugging information to the syslog file.

- **-a**

  This option enables the use of the `/etc/ftpd/ftpaccess` file, which contains information for configuring ftpd.

- **-A**

  This option disables the use of the ftpaccess configuration file.

- **-K**

  This option is used to enforce Kerberos Authentication. In the legacy version of ftp, the -A option was used to enforce Kerberos Authentication.

- **-i**

  This option logs all incoming (received) files by the ftpd server to the `/var/admin/syslog/xferlog` log file.

  Note that the “logs transfers” entry in the `/etc/ftpd/ftpaccess` file will overwrite this option.

- **-o**

  This option logs all outgoing (transmitted) files by ftpd to `/var/admin/syslog/xferlog`.

  Note that the “log transfers” entry in the `/etc/ftpd/ftpaccess` file will overwrite this option.

- **-L**

  This option logs all user commands sent to the ftpd server into syslog. Be aware that using this option will log any user command, that is if the user accidently enters a password for a command instead of the username, it will cause the password to be logged via syslog.

  Note that the “log transfers” entry in the `/etc/ftpd/ftpaccess` file will overwrite this option.

- **-m <number of tries>**

  This option is used to specify the number of tries for a bind() socket call.

New ftp Support Commands

The following new support commands are available with this version of ftp:

- **ftpcount**

  This command shows the current number of users for each class and the limit for each class as defined in the `/etc/ftpd/ftpaccess` file. If the ftpaccess file does not exist, the ftpcount command will not display anything. However, if the ftpaccess file exists and is 0 bytes, then an error message will be displayed.

  For more details, see the **ftpcount (1)** manpage.

- **ftpwho**

  This command shows the current process information for each user logged into the ftp server. If the ftpaccess file does not exist, the ftpwho command will not display anything. However, if the ftpaccess file exists and is 0 bytes, then an error message will be displayed.

  For details, see the **ftpwho (1)** manpage.

- **ckconfig**

  This command verifies the pathnames of all the ftp configuration files.

  For details, see the **ckconfig(1)** manpage.

- **ftpshut**

  This command allows superusers to create a shutdown message file that warns users before ftpd shuts down. An ftp daemon checks this file at intervals to determine the shutdown time.

  To use the ftpshut command, perform the following steps:

  1. Edit the `/etc/ftpaccess file`, so that the “shutdown <path>” entry specifies a path to the shutdown message file.

(You will create the shutdown message file with the ftpshut command in a later step.)

2. To enable the ftpaccess file, specify the -a option in the ftp entry of the inetd configuration file (typically `/etc/inetd.conf`). For example, ftp stream tcp nowait root `/usr/lbin/ftpd ftpd -a`

   NOTE: If the "shutdown <path>" entry is not specified in ftpaccess file and you try to execute ftpshut command, then the following error message will be displayed:

   No shutdown file defined in ftpaccess file.

   Execute the ftpshut command to create a shutdown message file (with the path specified in the "shutdown" entry of ftpaccess file) in the home directory of real, anonymous and virtual users. Note that in guest users' home directories the ftpshut command will not create the shutdown message file; you must do it manually.

   The shutdown message file indicates the time of a planned shutdown and notifies users. This file can also specify that new connections be denied after a specified time before shutdown and that current connections be dropped at a specified time before shutdown.

   For details, see the **ftpshut(1)** manpage.

- **ftprestart**

  The ftprestart command removes all the shutdown message files from the real, anonymous, and virtual user accounts. These message files are created by the ftpshut utility in the path specified by the "shutdown" entry in the `/etc/ftpd/ftpaccess file`. For guest user accounts the message files have to be removed manually.

  The ftprestart command is always used after the ftpshut command is executed.

  For details, see the **ftprestart(1)** manpage.

New ftp Configuration Files

The following configuration files have been newly introduced in ftp:

- **`/etc/ftpd/ftpaccess`**

  This is the primary configuration file for defining the operation of the ftp daemon.

- **`/etc/ftpd/ftpconversions`**

  This file defines options for compression/decompression and tar/un-tar operations.

- **/etc/ftpd/ftphosts**

  This file lets you allow/deny ftp account access according to source IP addresses and hostnames.

- **`/etc/ftpd/ftpusers`**

  This file is now in a new location, `/etc/ftpd/ftpusers`.

- **`/etc/ftpd/ftpgroups`**

  This file is a group password file for use with the SITE GROUP and SITE GPASS commands.

The ftpaccess Configuration File

The `/etc/ftpd/ftpaccess` configuration file is the primary configuration file for defining the operation of the ftp daemon. A sample file is provided in `/usr/newconfig/etc/ftpd`. You can edit this file and copy it to its correct location `/etc/ftpd/ftpaccess`.

To enable the ftpaccess file, specify the -a option for the ftp entry in the `/etc/inetd.conf file`.

Example:

ftp stream tcp nowait root /usr/lbin/ftpd ftpd -a -l -d

To disable the ftpaccess file, specify the -A option for the ftp entry in the

`/etc/inetd.conf file`.

You can use the ftpaccess configuration file to set access capabilities, informational capabilities, logging, permissions, regular expression capabilities, and others, which are explained below.

Setting Access Capabilities

NOTE For details on the following keywords, see the **ftpaccess(4)** manpage.

Options for setting access capabilities in the `/etc/ftpd/ftpaccess` file are:

autogroup

Allows you to define access to group-and-owner-read-only files and directories to a particular class of anonymous users.

class

Allows you to define classes of users according to the source IP addresses and/or hostnames, and to limit access according to user class.

deny

Allows you to deny access to any hosts matching specified hostnames, IP addresses, or domain names.

guestgroup

Allows you to restrict guest users so that they are only able to access the directory structure under their home directory (which will appear to be root /).

limit

Allows you to limit a particular class to a specified number of users at specified times, displaying a message file if a user is denied access. A limit check is performed at login time

only.

noretrieve <filename> <filename> ....

Allows you to deny retrievability of specified files.

For example you may wish to always deny retrievability of the `/etc/passwd` file.

loginfails <number>

This entry allows you to log a "repeated login failures" message and terminate the ftp connection after a specified number of login failures.

private <yes|no>

After the user logs in, the SITE GROUP and SITE GPASS commands may be used to specify an enhanced access group and associated password. If the group name and password are valid, the user becomes (via setgid()) a member of the group specified in the group access file, `/etc/ftpd/ftpgroups`.

Setting Informational Capabilities

The following key words can be used for setting up informational capabilities in the `/etc/ftpd/ftpaccess` file.

NOTE For details on the following keywords, see the **ftpaccess(4)** manpage.

banner

Works similarly to the message command, except that the banner is displayed before the user enters the username/password.

WARNING Use of this command can completely prevent non-HP-UX ftp clients from

making use of the ftp server. Not all clients can handle multi-line responses (which is how the banner is displayed).

email

Defines the email address of the ftp archive maintainer.

message

Allows you to define a message file so that ftp will display the file to the user at login time or when the user changes to the specified directory.

readme

Allows you to define a file such that ftpd will notify users at login time or upon using the change working directory command that the file exists and was modified on such-and-such a date.

Setting Logging Capabilities

The following keywords can be used for setting up logging capabilities in the `/etc/ftpd/ftpaccess` file.

NOTE For details on the following keywords, see the **ftpaccess(4)** manpage.

log commands

Enables logging of individual commands by users.

log transfers

Enables logging of file transfers for either real or anonymous ftp users to `/var/adm/syslog/xferlog`. Logging of transfers to the server (incoming) can be enabled separately from

transfers from the server (outbound).

Setting Permission Capabilities

The following keywords can be used for setting up permissions capabilities in the `/etc/ftpd/ftpaccess` file.

NOTE For details on the following keywords, see the **ftpaccess(4)** manpage.

chmod <yes|no>

delete <yes|no>

overwrite <yes|no>

rename <yes|no>

umask <yes|no>

Allows or disallows the ability to perform the specified function. By default, all users are allowed.

passwd-check

Defines the level and enforcement of password checking done by the server for anonymous ftp.

Setting Regular Expression Capabilities

The following keywords can be used for setting up regular expression capabilities in the `/etc/ftpd/ftpaccess` file.

NOTE For details on the following keywords, see the **ftpaccess(4)** manpage.

path-filter

For specified users path-filter defines regular expressions that control what a filename can or cannot be. If a filename is invalid due to a failure to match the path-filter specifications, a message

will be displayed to the user.

upload

Defines a directory that permits or denies uploads.

Setting Additional Capabilities

The following keywords can be used for setting up additional capabilities in the `/etc/ftpd/ftpaccess` file.

NOTE For details on the following keywords, see the **ftpaccess(4)** manpage.

alias

Defines an alias for a directory. Aliases only apply to the cd command.

cdpath

Defines an entry in the cdpath. This defines a search path that is used when changing directories.

compress

Enables compress capabilities for any specified class. The actual conversions are defined in the configuration file `/etc/ftpd/ftpconversions` (discussed later in this document).

tar

Enables tar capabilities for the specified class. The actual conversions are defined in the configuration file `/etc/ftpd/ftpconversions` (discussed later in this document).

shutdown <path>

If the shutdown message file pointed to by <path> exists, the server will check the file regularly to see if the server is going to be shut down. You create the shutdown message file using the ftpshut command. The shutdown message file indicates the time of

a planned shutdown, so that users are notified and new connections are denied after a specified time before shutdown. The shutdown file can also specify that current connections are dropped at a specified time before shutdown.

See the **ftpshut (1)** manpage for details.

virtual

Enables the virtual ftp server capabilities.

The ftpconversions Configuration File

The new `/etc/ftpd/ftpconversions` configuration file defines options for the following:

- compression/decompression
- tar/un-tar operations

A sample file is provided in `/usr/newconfig/etc/ftpd`. You can edit this file and copy it to its correct location, `/etc/ftpd/ftpconversions`. The ftpconversions file lets you configure the ftp server so that if the user specifies a filename (when using a get command) certain compression and tar operations take place (as shown in the following table):

True Filename	Specified Filename	Action
<filename>.Z	<filename>	Decompress file before transmitting.
<filename>	<filename>.Z	Compress <filename> before transmitting.
<filename>	<filename>.tar	Tar <filename> before transmitting.
<filename>	<filename>.tar.Z	Tar and compress <filename> before transmitting.

Enabling/Disabling tar and compression

You enable/disable tar and compression in `/etc/ftpd/ftpaccess` file, by specifying yes or no with the tar and compression keywords. The default is "yes" to enable tar and compression.

NOTE For more details, see the **ftpconversions (4)** manpage.

The ftphosts Configuration File

The new `/etc/ftpd/ftphosts` configuration file can be used to deny/allow access to certain accounts from specified hosts.

A sample file is provided in `/usr/newconfig/etc/ftpd/ftphosts`. You can edit this file and copy it to its correct location, `/etc/ftpd/ftphosts`.

NOTE For more details, see the **ftphosts (4)** manpage.

The ftpusers Configuration File

The ftpusers configuration file defines security for ftpd. ftp rejects login connections to local user accounts that are named in the ftpusers file.

The ftpusers configuration file has been moved from /etc directory to the `/etc/ftpd` directory.

When you install ftp, the utility checks whether the `/etc/ftpusers` file already exists or not from a previous version of ftp. If a ftpusers file already exists in `/etc`, then a link is created from `/etc/ftpd/ftpusers` to `/etc/ftpusers`. If the `/etc/ftpusers` file does not exist, then it is created in the `/etc/ftpd` directory.

NOTE For more details, see the **ftpusers (4)** manpage.

The ftpgroups Configuration File

The `/etc/ftpd/ftpgroups` file is the group password file for use with the SITE GROUP and SITE GPASS commands. A sample file is provided in `/usr/newconfig/etc/ftpd/ftpgroups`. You can edit this file and copy it to `/etc/ftpd/ftpgroups`.

NOTE For more details, see the **ftpgroups (4)** manpage.

The xferlog Log File

The new `/var/adm/syslog/xferlog` file logs file transfer information from the ftp server daemon.

You enable/disable logging to the xferlog file in the `/etc/ftpd/ftpaccess` file, using the "log transfers" keyword. See the **ftpaccess (4)** and **xferlog (5)** manpages for details.

NOTE The xferlog display is informational only. You cannot edit this file.

The xferlog file displays the following log information:

- **current-time**

  This is the current local time in the form "DDD MMM dd hh:mm:ss YYYY". Where DDD is the day of the week, MMM is the month, dd is the day of the month, hh is the hour, mm is the minutes, ss is the seconds, and YYYY is the year.

- **transfer-time**

  This is the total time in seconds and micro-seconds for the transfer.

- **remote-host**

  This is the remote host name.

- **file-size**

  This is the size of the transferred file in bytes.

- **filename**

  This is the name of the transferred file.

- **transfer-type**

  This is a single character indicating the type of transfer. Can be one of

  1. for an ascii transfer
  2. for a binary transfer

- **special-action-flag**

  This is one or more single character flags indicating any of the following special action taken. Can be one or more of:

  C flag indicates that the file was compressed
  U flag indicates that the file was uncompressed
  T flag indicates that the file was tar'ed
  _ no action was taken

- **direction**

  This is the direction of the transfer. Can be one of:

  o outgoing
  i incoming

- **access-mode**

  This is the method by which the user is logged in. Can be one of:

a (anonymous)	for an anonymous guest user.
g (guest)	for a password guest user (See the guestgroup entry in the `/etc/ftpd/ftpaccess` file).
r (real)	for a local authenticated user.

- **username**

  This is the local username, or if guest, the ID string given.

- **servicename**

  This is the name of the service being invoked, usually ftp.

- **authentication-method**

  This is the method of authentication used. Can be one of:

  0 none
  1 RFC931 Authentication

- **authenticated-user-id**

  This is the user id returned by the authentication method. A * is used if an authenticated user id is not available.

- **current-time-in-seconds**

  This is the current local time in seconds.

- **cpu-utilization**

  This is the total cpu utilization for one ftp session. This field will be filled only in the last entry for the entire session.

Virtual ftp Support

Virtual ftp support allows you to manage an ftp server for two separate domains on the same machine.

Basically, virtual ftp allows an administrator to configure systems so that user1 connecting via ftp to ftp.domain1.com gets one ftp banner and ftp directory, while user2 connecting via ftp to ftp.domain2.com gets another banner and directory. (This occurs even though the users are on the same machine and are using the same ports).

NOTE Setting up a virtual ftp server requires IP address aliasing. This feature is supported in HP-UX Release 10.30 onwards.

Setting Up a Virtual ftp Server

Following is an example of how to set up a virtual ftp server:

1. Set up an IP alias for the ftp server machine using the ifconfig command. For example,

   ifconfig lan0:1 15.70.178.100 netmask 0xffffff00 up

   This will set 15.70.178.100 as an IP address alias for the interface lan0. Now you can access that particular machine with this IP address.

2. Declare the following directives in the `/etc/ftpd/ftpaccess` file:

   virtual 15.70.178.100 root/virtual
   virtual 15.70.178.100 banner / virtual/banner.msg
   virtual 15.70.178.100 logfile / virtual/xferlog

3. Create the /virtual directory and banner.msg and xferlog file inside it.
4. Login as anonymous on the virtual ftp server (ftp 15.70.178.100): it will display the banner.msg from the /virtual directory.

An anonymous user will be chrooted to the directory specified in the "virtual <IP ADDRESS> root" entry as specified in the `/etc/ftpd/ftpaccess` file. In this example, the user will be chrooted

to the /virtual directory.

You will need to make sure that any files referenced after the chroot are in the virtual server. (The same way it is done while setting up an anonymous ftp account.)

Setting Up a Secure Version of ftp

With HP-UX 11.0, a unified binary is available for ftp which can operate as both a Kerberos and non-Kerberos service. To have ftp operate in a secure environment, enable the secure environment using the following command on the command-line:

```
/usr/sbin/inetsvcs_sec enable
```

This command will update the system file `/etc/inetsvcs.conf` with an entry "kerberos true". The services obtain the type of authentication mechanism from the system file at run-time.

Index