

# **WU-FTPD 2.6.1 Release Notes**

**First Edition**



**Manufacturing Part Number: <5969-4306>  
<E0801>**

U.S.A.

© Copyright 2001 Hewlett-Packard Company

---

## 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.

---

## Copyright Notices

Copyright © 2001 Hewlett-Packard Company. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

iCOD and iCOD CPU Agent Software are products of Hewlett-Packard Company, and all are protected by copyright.

Copyright © 1979, 1980, 1983, 1985-93 Regents of the University of California. This software is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

Copyright © 1988 Carnegie Mellon University

Copyright © 1990-1995 Cornell University

Copyright © 1986 Digital Equipment Corporation.

Copyright © 1997 Isogon Corporation

Copyright © 1985, 1986, 1988 Massachusetts Institute of Technology.

Copyright © 1991-1997 Mentat, Inc.

Copyright © 1996 Morning Star Technologies, Inc.

Copyright © 1990 Motorola, Inc.

Copyright © 1980, 1984, 1986 Novell, Inc.

Copyright © 1989-1993 The Open Software Foundation, Inc.

Copyright © 1996 Progressive Systems, Inc.

Copyright © 1989-1991 The University of Maryland

Copyright © 1986-1992 Sun Microsystems, Inc.

---

## Trademark Notices

UNIX® is a registered trademark in the United States and other countries, licensed exclusively through The Open Group.



---

# Contents

## 1. New and Changed Features

New Features . . . . .	9
Virtual Hosts Support . . . . .	9
privatepw . . . . .	10
New Clauses for ftpaccess . . . . .	10
Enabling RFC 1413 . . . . .	19
New Features related to data transfer . . . . .	19
Field added to xferlog . . . . .	20
New Command Line Options . . . . .	20
IPv6 Support . . . . .	22
HP-specific features . . . . .	24
Other Features . . . . .	25
Changed Features . . . . .	26
Removed Features . . . . .	28

## 2. Installation Information

Compatibility with Previous Versions . . . . .	30
System Requirements . . . . .	32
Installing WU-FTPD 2.6.1 . . . . .	34
Installing WU-FTPD . . . . .	36

## 3. Documentation

WU-FTPD Information . . . . .	38
-------------------------------	----

## 4. Known Problems, Limitations, and Fixes

Known Problems . . . . .	40
Limitations and Fixes . . . . .	41
Defects Closed in this Release . . . . .	42

---

# Contents

---

# **1** **New and Changed Features**

WU-FTPD2.6.1 is available on HP-UX 11.0 and 11i platforms as a web upgrade. For 11i customers, WU-FTPD 2.6.1 adds new functionality to WU-FTPD 2.4, which is the version delivered as part of the core HP-UX networking products. For systems on HP-UX 11.0, this version allows

customers to upgrade to WU-FTPD 2.6.1 from either the legacy ftp version, delivered with the core networking products on 11.0, or from WU-FTPD 2.4, which has been made available with patch PHNE\_14479 (now superseded by PHNE\_21936).

---

**IMPORTANT**

---

In general, existing installations do not have to modify their existing configuration unless they want to use the new features. There are a few exceptions that are listed below, for both the HP-UX 11.0 users and the HP-UX 11i users:

*For HP-UX 11.0*

- If upgrading from legacy ftp: There is a difference in the ftp daemon options between legacy ftpd and WU-FTPD. In the legacy ftpd, the `-A` option enables Kerberos authentication whereas in the WU-FTPD, the `-K` option enables Kerberos authentication, and the `-A` option is used to disable the ftpaccess file.
- If upgrading from WU-FTPD 2.4: The two options `"suppresshostname"` and `"suppressversion"` that were present in WU-FTPD 2.4 have been replaced by the new `"greeting"` option.

*For HP-UX 11i*

- The option `"sendfiletransfer"` in the ftpaccess configuration file has been replaced with `'-U'` option in this version.
- The two options `"suppresshostname"` and `"suppressversion"` that were present in WU-FTPD 2.4 have been replaced by the new `"greeting"` option.

---

**NOTE**

---

A more detailed information on WU-FTPD 2.4 for HP-UX 11i customers as well as migration information for HP-UX 11.0 customers is available in the WU-FTPD 2.4 Release Notes on <http://docs.hp.com>.



---

## New Features

The following new features have been added in WU-FTPD 2.6.1. Please refer to the WU-FTPD 2.4 Release Notes at <http://docs.hp.com> for information on the new features that were made available with WU-FTPD 2.4.

### Virtual Hosts Support

Virtual Hosts are now fully supported in WU-FTPD 2.6.1. A new configuration file named `/etc/ftpd/ftpservers` has been added. This configuration file contains a set of virtual domain configuration file names that the WU-FTPD server can use. Thus, WU-FTPD has the ability to use separate configuration files for each virtual domain.

The new configuration file is placed in the directory `/etc/ftpd/`. A sample configuration file can be found in directory `/usr/newconfig/etc/ftpd/`.

WU-FTPD 2.4 partially supported virtual servers, that is it supported setting the root ftp directory, the log file and the banner for each virtual domain. All other directives in the `ftppass` file had to be shared globally across all virtual servers.

With WU-FTPD 2.6.1, the `ftppass`, `ftpusers`, `ftpgroups`, `ftphosts` and `ftpconversions` files can now be specified on a per domain basis. The Master WU-FTPD configuration files present under the directory `/etc/ftpd` can now be overridden with a local copy specific to that domain. If you do not wish to place a copy of one or all the files listed above in the virtual host directory for any specific host, then the master copy can be used.

The following example illustrates a possible entry in the `ftpservers` configuration file:

#### Example 1-1

```
123.123.123.123 /etc/ftpd/somedomain
```

In this example, when a ftp client connects to the server, using the IP Address 123.123.123.123, the WU-FTPD server searches for the configuration files `ftppass`, `ftphosts`, `ftpusers`, `ftpgroups` and `ftpconversions` under the directory `etc/ftpd/somedomain`. If a match is not found or an invalid directory path is encountered, the default master

## New Features

configuration files in directory `"/etc/ftpd"` are used instead.

### **privatepw**

The admin utility `"privatepw"` allows modification of the WU-FTPD group access file information (`/etc/ftpd/ftpgroups`). A site currently supports the `ftp` commands `SITE GROUP` and `SITE GPASS`. When necessary, the administrator should be able to add, delete and list enhanced access group information needed for these two commands. The `privatepw` utility is used to update this information in the group access file (`/etc/ftpd/ftpgroups`). This command requires read/write permission for the appropriate `ftpgroups` file.

---

#### **NOTE**

For more details on the different options available in `privatepw`, refer to the `privatepw (8)` manpage.

---

### **New Clauses for ftpaccess**

Several new `ftpaccess` clauses have been added to the file `"/etc/ftpd/ftpaccess"`. The `/etc/ftpd/ftpaccess` file is used to configure the operation of `ftpd`. The new clauses have been listed below:

- **Email-on-load:**

Using this feature, email addresses can be specified for anonymous upload notifications. The sender's email address can also be specified. By default, the sender's address is specified as `'wu-ftp'`. This can also be specified for virtual hosts. To avoid any problems if the recipient attempts to reply to a notification, or if downstream mail problems generate bounces, ensure that the mailfrom address is deliverable.

The general syntax for this is:

```
mailserver <hostname>
incmail <emailaddress>
virtual <address> incmail <emailaddress>
defaultserver incmail <email address>
mailfrom <emailaddress>
virtual <address> mailfrom <emailaddress>
```

```
defaultserver incmail <emailaddress>
deny-email <case-insensitive-email-address>
```

**NOTE**

For more details on the email-on-load feature, refer to the ftpaccess (4) manpage.

**Example 1-2**

```
mailserver <abc.com>
```

Specifying the name of a mail server that will accept upload notifications for the WU-FTP daemon. This option is relevant only if someone has to be notified of anonymous uploads.

```
incmail <def@abc.com>
```

Specifying the email addresses to be notified of anonymous uploads.

```
mailfrom <ghi@abc.com>
```

Specifying the sender's email address for anonymous upload notifications.

- **timeouts:**

This feature is used to control the various timeouts used within the daemon. The following daemon timeout values are now available:

- **accept** - The time period the daemon waits for an incoming (PASV) data connection. The default value is 120 seconds.
- **connect** - The time period the daemon waits before attempting to establish an outgoing (PORT) data connection. The default value is 120 seconds.
- **data** - The time period the daemon will wait for some activity on the data connection. The default value is 1200 seconds.
- **idle** - The time period the daemon will wait for the next command. The default value is 900 seconds.
- **RFC931** - The maximum time the daemon allows for the entire RFC931 (AUTH/ident) conversation. The default value is 10 seconds.
- **maxidle** - The SITE IDLE command allows the remote client to

### New Features

establish a higher value for the idle timeout. With a new option in `ftpaccess (MaxIdle)` this can be overridden. The default value is 1200 seconds.

The general syntax for timeout is:

```
timeout accept <seconds>
timeout connect <seconds>
timeout data <seconds>
timeout idle <seconds>
timeout maxidle <seconds>
timeout RFC931 <seconds>
```

#### Example 1-3

```
timeout idle 200
```

Displays the following message "Current IDLE time limit is 200 seconds; max 7200"

```
timeout maxidle 6200
```

Displays the following message "Current IDLE time limit is 200 seconds; max 6200"

```
timeout RFC931 0
```

Disables RFC931 based authentication since 0 has been specified.

- **Enhanced DNS extensions:**

This feature is used for refusing (or overriding) an FTP session when a reverse DNS lookup fails.

The general syntax for this is:

```
dns refuse_mismatch <filename> [ override ]
dns refuse_no_reverse <filename> [ override ]
dns resolveroptions <options>
```

- **Control of the address reported:**

This feature allows control of the address reported in response to a `PASV` command and the TCP port numbers, which may be used for a passive data connection.

---

**NOTE**

---

This feature will not work in the IPv6 environment.

The general syntax for this is:

```
passive address <externalip> <cidr>
```

```
passive ports <cidr> <min> <max>
```

**Example 1-4**

```
passive address 10.0.1.15 10.0.0.0/8
```

In this example, clients connecting from the class-A network 10 will be told that the passive connection is listening on the IP-address 10.0.1.15

```
passive ports 10.0.0.0/8 90 100
```

In this example, if there is a control connection from the class-A network 10, the port range within 90 and 100 will be randomly selected for the daemon to listen on.

- Selectively allow PORT and PASV data connections:

This feature enables the site admin to selectively allow PORT and PASV data connections. Usually a connection is not established if the remote IP address of the data connection does not match the remote IP address of the control connection data. Multiple passive addresses may be specified to handle complex, or multi-gatewayed, networks.

---

**NOTE**

---

This feature will not work in the IPv6 environment.

The general syntax for this is:

```
pasv-allow <class> [ addrglob ...]
```

```
port-allow <class> [ addrglob ...]
```

- **SO\_KEEPALIVE:**

This feature sets the TCP option **SO\_KEEPALIVE** for data sockets. This can be used to control network disconnect. You could specify "Yes" to set this option or "No" to use the system default, which is usually off.

## New and Changed Features

### New Features

The general syntax for this is:

```
keepalive yes|no
```

- **ftppass log:**

The feature `ftppass log` clause has been changed to allow logging transfers to both the `syslog` and `xferlog`. This option enables you to redirect the logging messages for incoming and outgoing transfers to `syslog`. If this option has not been specified, the messages are written to `xferlog`.

The general syntax for this is:

```
log syslog
```

```
log syslog+xferlog
```

- **Clauses to control access to areas on the FTP site:**

The following clauses control whether areal or guest user is allowed access to areas on the FTP site outside their home directories. These clauses are not meant to replace the use of `guestgroup` and `guestuser`. Instead, you can use these clauses to supplement the operation of guests. The `unrestricted-uid` and `unrestricted-gid` clauses may be used to allow users to use their home directories who would otherwise be restricted.

The general syntax for this is:

```
restricted-uid <uid-range>[...]
```

```
restricted-gid <gid-range>[...]
```

```
unrestricted-uid <uid-range>[...]
```

```
unrestricted-gid <gid-range>[...]
```

#### Example 1-5

```
restricted-uid abtalt abtuser
```

```
restricted-gid users abt
```

- **Retrieval of files:**

This feature allows retrieval of files which would otherwise be denied by the `noretrieve` clause. This clause overrides the `noretrieve` clause.

The general syntax for this is:

```
allow-retrieve [ absolute|relative ] [ class= classname ]  
... [-] filename
```

- **Virtual Server:**

New virtual server clauses have been added. Using these clauses, the access for different users to both the virtual and non-virtual domain can be restricted. Also, the virtual hostname can be specified for printing by using one of the options below.

The general syntax for this is:

```
virtual <address> allow <username> [ username ...]
virtual <address> deny <username> [ username ...]
virtual <address> private
virtual <address> hostname|email string
defaultserver deny <username> [ username ...]
defaultserver allow <username> [ username ...]
defaultserver private
```

### Example 1-6

```
virtual xx.xx.xx.xx allow root
```

- Adding this entry will ensure that the user root is allowed to start the ftp session in the machine. By default, all real and guest users will be denied service. This is applicable only for virtual ftpservers.

```
virtual xx.xx.xx.xx allow *
```

```
virtual xx.xx.xx.xx deny root
```

- Adding this entry will deny root users and allow other users to start the ftp.

```
virtual xx.xx.xx.xx private
```

- Adding this entry will deny service for anonymous ftp.

```
virtual xx.xx.xx.xx hostname telnet2.abc
```

- Adding this entry will print the greeting (telnet2.abc) in place of the actual hostname at the beginning.

```
defaultserver deny root
```

- Adding this entry denies ftp on the default ftp server for the root user. The message "FTP LOGIN REFUSED" is displayed in syslog.

```
defaultserver private
```

## New Features

- Adding this entry anonymous ftp is denied on default server. The message "FTP LOGIN REFUSED" is logged in the syslog.

- Default host name:

This feature defines the default host name of the ftp server which will be displayed in the greeting message. If this clause is not specified, the default host name of the local machine is used.

The general syntax for this is:

```
hostname <some.host.name>
```

### Example 1-7

```
hostname telnet2.123.com
```

- Displays the default hostname specified (telnet2.123.com) in place of the actual hostname in the greeting message.

- Control information:

This feature allows you to control the information given out in the greeting message before a remote user logs in. The information specified can be either hostname and daemon version, only hostname or just the message "FTP server ready". By default, "greeting full" is set as the default greeting clause.

The general syntax for this is:

```
greeting full|brief|terse
```

```
greeting text <message>
```

- Using the "greeting text" clause a different text message from the standard greeting can be printed.

### Example 1-8

```
greeting text Hi!!! Welcome to FTP Server
```

- Displays the message "Hi!!! Welcome to FTP server" as the greeting message.

- Limit the total time of a session:

This feature allows you to limit the total time a session can take. By default, there is no limit set. Real users are never limited.

The general syntax for this is:

```
limit-time {*|anonymous|guest} <minutes>
```



- **Forcing all UID/GID's:**

This feature has the ability to force all UID/GID in a range to be treated as guests. This is a new feature that has been added.

The general syntax for this is:

```
guestuser <username> [ username ... ]
realgroup <groupname> [ groupname ... ]
realuser <username> [ username ... ]
```

- **Specification of UID and GID values:**

These clauses allow specification of UID and GID values, which will be denied access to the ftp server. By default, allow access is set.

The general syntax for this is:

```
deny-uid <uid-range>[...]
deny-gid <gid-range>[...]
allow-uid <uid-range>[...]
allow-gid <gid-range>[...]
```

- **access clauses:**

Detail counters and ftp access clauses set limitations of the user's ability to upload/download files.

The general syntax for this is:

```
ul-dl-rate <rate> [ class ... ]
dl-free <filename> [ class ... ]
dl-free-dir <dirname> [ class ... ]
```

### **Example 1-9**

```
ul-dl-rate 2
```

d- For every 1 byte of data that is uploaded, the ftpserver will allow 2 bytes of data to be downloaded.

- **nice clause:**

The 'nice' clause allows modification of the nice value of the WU-FTPD server process for certain users. The process nice value is adjusted by the indicated nice-delta value, if the remote user is a member of the named class. If class is not specified, then use

## New and Changed Features

### New Features

nice-delta as the default adjustment to the WU-FTPD server process nice value. This default nice value adjustment is used to adjust the nice value of the server process only for those users who do not belong to any class for which a class-specific nice directive exists in the ftpaccess file.

The general syntax for this is:

```
nice <nice-delta> [ class ]
```

---

#### NOTE

Only negative values are considered. Positive values or 0 are ignored for the nice-delta.

---

- defumask clause:

The 'defumask' clause allows to set the umask for a file created by the daemon, if the remote user is a member of the named class. There can be multiple entries for defumask. If class is not specified for a defumask entry, then that umask is used as the default for those classes, which do not have a defumask entry specified.

The general syntax for this is:

```
defumask <umask> [ class ]
```

#### Example 1-10

```
defumask 0177  
defumask 0133 ClassA
```

- Specifying this will create files with the permission "-rw-r--r--" for a user of ClassA. For other users files will be created with the permission "-rw-----".

- Controlling the maximum number of lines of output:

A clause to set the maximum number of lines of output to be displayed on the screen has been added. By default, the limit is set to 20.

The general syntax for this is:

```
site-exec-max-lines <number> [ class ... ]
```

- Setting the root directory:

The clauses to set the root directory when the user logs in as

anonymous or guest have been added.

The general syntax for this is:

```
anonymous-root <root-dir> [ class ]
guest-root <root-dir> [ uid-range ]
```

- **Enabling the server to listen:**

A clause has been added to enable the server to listen on any particular address. If this value is not set, then the server will listen for connections on every IP addresses. Use of this clause is discouraged as it will break virtual hosting.

---

**NOTE**

This option will work only when WU-FTPD is running on a standalone mode. For more details, refer to ftpd (1m) manpage.

---

The general syntax for this is:

```
daemonaddress <address>
```

---

**NOTE**

For more details on the new clauses added to the ftpaccess utility, refer to the ftpaccess (4) manpage.

---

## Enabling RFC 1413

The Identification Protocol (RFC 1413) provides a means to determine the identity of a user of a particular TCP connection. Given a TCP port number pair, it returns a character string which identifies the owner of that connection on the server's system. Use the "-I" daemon option to enable RFC 1413 based authentication. By default, this authentication is disabled.

## New Features related to data transfer

Two new features related to data transfer have been introduced:

- For statistical purposes, you can keep track of the total bytes of data transferred. Also, you can limit the number of data bytes a user in any given class may transfer. A limit can be placed on the number of

## New and Changed Features

### New Features

bytes in, out or total. This clause can be specified for a particular class. If no class is specified for a data limit entry, that limit entry is the default for all classes for which this clause is not specified. When logging off the ftp session, it will print the number of files and the number of bytes transferred.

The general syntax for this is:

```
data-limit [raw] in|out|total count [class]
```

- Limit the number of data files a user in the given class may transfer in a session. The limit can be placed on the files in, out or total. If no class is specified, the limit is the default for classes, which do not have a limit specified.

The general syntax for this is:

```
file-limit [raw] in|out|total count [class]
```

### Field added to xferlog

A new field has been added in xferlog to indicate the completion status of the data transfer. "C" indicates complete transfer and "i" indicates incomplete transfer.

---

#### NOTE

For more details on the field that has been added to xferlog, refer to the xferlog (5) manpage.

---

### New Command Line Options

The following new options are available in WU-FTPD 2.6.1:

- -q & -Q

These options determine whether the WU-FTPD daemon uses the PID files. These files are required by the limit directive to determine the number of current users in each access class. Disabling the use of the PID files disables user limits. By default, the daemon uses the PID files. Specify -Q to disable using the PID files. The -Q option can be used for testing the server as a normal user since access permissions prevent the use of the PID files. Large, busy sites that do not wish to impose limits on the number of concurrent users may also consider disabling the PID files.

- **-r root dir**

This option instructs the daemon to chroot (see `chroot(2)`) to the specified `rootdir` immediately upon loading. This can improve system security by limiting the files which may be damaged should a break-in occur through the daemon. This option is like anonymous FTP.

- **-V**

This option causes the program to display copyright and version information, then terminate.

- **-w & -W**

These options determine whether user logins are to be recorded in the `wtmp` file. If the `-W` option is specified, user logins are not recorded in the `wtmp` file. By default, the `-w` option is used to record every login and logout.

- **-X**

If the `-X` option is specified, the output created by the `-i` and `-o` options is not saved to the `xferlog` file but written to `syslog`.

- **-I**

This option enables the use of RFC1413 (AUTH/ident) to attempt to determine the username on the client. By default, this authentication is disabled. If `identd` daemon is not running in the remote machine and if this option is set there will be a delay when the user logs in.

- **-s & -S**

These options run the daemon in standalone operation mode. The `-S` option runs the daemon in the background and is useful in start-up scripts during system initialization (i.e., in `rc.local`). The `-s` option leaves the daemon in foreground and is useful when running from `init` (see `init(1M)`).

To start the WU-FTP daemon in the standalone mode, give the following commands:

```
/user/lbin/ftpd -S
```

Also, ensure that the `ftp` entry in `/etc/inetd.conf` file is removed before executing the above command.

- **-c <ctrl port> & -C <data port>**

## New Features

These options override the control and the data port numbers that is used by the daemon. Normally, the daemon determines the port numbers by looking in `/etc/services` (see `services(4)`) for "ftp" and "ftp-data". If there is no `/etc/services` entry for "ftp-data" and the `-C` option is not specified, the daemon uses the port just prior to the control connection port. The `-c` and `-C` options are both available if running as a standalone daemon. Otherwise, only the `-C` option can be used.

- `-U`

For 11.0

By setting this option the user can switch from "sendfile()" system call to "send()" system call. By default, "sendfile()" is used.

For 11i

The option "sendfiletransfer" in the `ftppass` configuration file has been replaced with '-U' option in WU-FTPD. By setting this option the user can switch from "sendfile()" system call to "send()" system call. By default, "sendfile()" is used.

---

### NOTE

For more details on the command line options in WU-FTPD, refer to the `ftpd (1M)` manpage.

---

- Other Utilities

In version 2.6.1 a new option "`-V`" prints the copyright and the version information for all utilities (`ftpcount`, `ftprestart`, `ckconfig`, `ftpwho`, `privatepw` and `ftpshut`).

## IPv6 Support

After installing the stack, the `inetd.conf` file must be modified as follows, in order to support IPv6:

```
ftp stream tcp6 nowait root /usr/bin/ftpd ftpd -l
```

If `tcp` is specified instead of `tcp6`, FTP will operate in IPv4 mode. Note that FTP over IPv6 uses the `ipnodes` database entry in the `/etc/nsswitch.conf` file, the name service configuration file. Therefore, if you are using the name service switch, make sure that the `ipnodes` entry has been added.

The following are the new features incorporated in this release:

- **Implementation of RFC 2428**

This RFC specifies a method by which FTP clients and server exchange data connection information i.e. port, host address, and type of protocol family, for both IPv4 and IPv6 addresses.

In this release, FTP uses `EPRT` and `EPSV` instead of `PORT` and `PASV` respectively for IPv6 connections.

- `EPRT` - Extended Port

This command allows you to specify a host-port for both IPv4 and IPv6 connections.

### Example 1-11

For IPv4:

```
-----> EPRT | 1 | 132.235.1.2 | 50934 |
```

For IPv6:

```
-----> EPRT | 2 | fe80::260:b0ff:fec1:7b2f | 50934 |
```

- `EPSV` - Extended Passive

This command requests a server to listen on a data port and wait for a connection. The response to this command includes only the TCP port number of the listening connection.

### Example 1-12

```
ftp> passive
```

Passive mode on.

```
-----> EPSV
```

```
229 Entering Extended Passive Mode (| | | 9495 |).
```

- **Implementation of RFC 1639**

This RFC describes a convention for specifying an address other than the default data port for the transport connection over which data is transferred.

Two new commands to accommodate FTP operations over network and transport protocols have been added in this release.

## New and Changed Features

### New Features

#### — LPRT

This command allows you to specify a long address for the transport connection.

#### Example 1-13

```
-----> LPRT
6,16,254,128,0,0,0,0,0,2,96,176,255,254,193,123,47,2,198,244
200 LPRT command successful
```

#### — LPSV

This command requests a server to listen on data port other than its default port and to wait for a connection rather than initiate one upon the receipt of a transfer command.

#### Example 1-14

```
ftp> passive
Passive mode on.
-----> LPSV
228 Entering Long Passive Mode
(6,16,254,128,0,0,0,0,0,2,96,176,255,254,193,123,47,2,134,7)
```

---

#### NOTE

The `-l` option must be used by the FTP client in order to use the LPRT LPSV commands.

For more information on `-l` option, refer to the FTP manpage.

A new FTP session command “longaddr” toggles the use of the LPRT (extended port) and LPSV (extended passive) commands.

The GSSAPI feature is not included in this release, as IPv6 modifications are not available for the GSSAPI library.

---

### HP-specific features

The following features have been incorporated in HP’s port of WU-FTPD 2.6.1:



**Command line options:**

The options discussed below are present in WU-FTPD 2.4. These options are not present in the open-sourced version of WU-FTPD 2.6.1, but have been incorporated in HP's port for backward compatibility:

- **-m number\_of\_tries**  
Specifies the number of tries for a bind() socket call.
- **-n nice\_value**  
Sets the nice value for an WU-FTPD process. When using this option, make sure that the nice clause in /etc/ftpd/ftpaccess file (see ftpaccess(4)) is not set.
- **-B**  
Sets the buffer size of the data socket to blocks of size of 1024 bytes. The valid range for size is from 1 to 64 (default is 56). The new clause 'tcpwindowsize' in the "/etc/ftpd/ftpaccess" file also sets the buffer size. The -B option overrides the tcpwindow clause in the ftpaccess file.

---

**NOTE**

A large buffer size will improve the performance of WU-FTPD on fast links (e.g. FDDI), but may cause long connection times on slow links (e.g. X.25).

---

- **-p & -P**  
The -p option is used to allow private port access to the client. The -P option is used to allow Third Party Access as well as private port access.

**Other Features**

In addition to the above, WU-FTPD 2.6.1 on HP-UX also supports:

- Files greater than 2 GB;
- Large UIDs/GIDs;
- Trusted System features.

---

## **Changed Features**

There are no changed features in this release of WU-FTPd.



New and Changed Features

**Removed Features**

---

## **Removed Features**

There are no removed features in this release of WU-FTPD.

---

## **2** **Installation Information**

Read this chapter and WU-FTPD 2.4 Release Notes available at <http://docs.hp.com> before installing version 2.6.1 of WU-FTPD.

## **Compatibility with Previous Versions**

Customers currently using WU-FTPD 2.4 do not need to modify their configuration file. It is compatible with this release of WU-FTPD. However, it is highly recommended to use the WU-FTPD 2.6.1 configuration file (.cf) delivered with this release in order to effectively use the new features and changes incorporated in this version.



## **System Requirements**

To install WU-FTPD 2.6.1, you must have the following system components:

- Hewlett-Packard 9000 Computer
- HP-UX operating system version 11.0 or 11i





## **Installing WU-FTPD 2.6.1**

Read the following special installation directives before installing WU-FTPD 2.6.1 depot:

### ***For HP-UX 11.0***

The existing installations do not have to modify their ftp configuration unless they want to use the new features. There is one exception; there is a difference in the ftp daemon options between legacy ftpd and wu-ftp. In the legacy ftpd, the -A option enables Kerberos authentication. In wu-ftp, the -K option enables Kerberos authentication, and the -A option is used to disable the ftpaccess file. So if you are using Kerberos authentication, and you are using legacy ftpd, you will need to edit /etc/inetd.conf to change the existing -A option to -K.

This version of FTP has some new configuration files that can be used to take advantage of new functionality. Sample of the new configuration files are provided in /usr/newconfig/etc/ftpd. You can edit these files as per your need and copy them to the location /etc/ftpd.

---

#### **NOTE**

WU-ftp does not support sublogins on anonymous ftp.

Two options, "suppresshostname" and "suppressversion" that were present in the previous version of wu-ftp have been removed from the ftpaccess file (ftpd configuration file) as all those features are already present in the new greeting option. So, if you are using any of these two options, you need to modify your ftpaccess configuration file accordingly. More details on these can be found in the ftpaccess(4) man page.

---

### ***For HP-UX 11i***

This version of FTP has a new configuration file (ftpservers), which can be used to take advantage of the new virtual hosting functionality. A sample of the new configuration files is provided in /usr/newconfig/etc/ftpd. You can edit these files as per your need and copy them to the location /etc/ftpd.

---

#### **NOTE**

WU-ftp does not support sublogins on anonymous ftp.

Two options, "suppresshostname" and "suppressversion" that were present in the previous version of wu-ftpd have been removed from the ftpaccess file (ftpd configuration file) as all those features are already present in the new greeting option. So, if you are using any of these two options, you need to modify your ftpaccess configuration file accordingly. More details on these can be found in the ftpaccess(4) manpage.

The option "sendfiletransfer" in the ftpaccess configuration file has been replaced with '-U' option in ftpd.

---

## **Installing WU-FTPD**

This release of WU-FTPD is available as a web upgrade on HP-UX 11.0 and HP-UX 11i platforms at <http://www.software.hp.com>.

You need to run the following command to install WU-FTPD 2.6.1:

```
swinstall -s <source>
```

where <source> is the source depot where you downloaded the WU-FTPD web upgrade depot to.

---

### **NOTE**

The WU-FTPD 2.6.1 files are installed into the `/usr/contrib/wuftp` directory. During installation, the `/usr/bin/enable_inet` script backs up the existing WU-FTPD files into `/usr/contrib/wuftp/save_custom/backup` directory and enables the WU-FTPD upgrade by linking the new files to the existing file locations

The `enable_inet -r wuftp` command allows reverting back to the older FTP version. `enable_inet status ftp` shows the currently active FTP version. If you want to install a GR patch, you need to disable WU-FTPD 2.6.1 by running the command `"/usr/bin/enable_inet -r wuftp"` in the command line to revert back to the base version delivered with your operating system prior to patching.

---

---

## **3** **Documentation**

The following product documentation is available with WU-FTPD 2.6.1:

## **WU-FTPD Information**

The README files for WU-FTPD are available in /usr/share/doc. You may also need to read WU-FTPD 2.4 Release Notes, posted on <http://docs.hp.com> for more information about the product.

The following are the manpages distributed with the FTP depot:

- ftp.1
- ftpd.1m
- ckconfig.1
- ftprestart.1
- ftpwho.1
- ftpcount.1
- ftpshut.1
- privatepw.a
- ftpaccess.4
- ftpgroups.4
- ftpservers.4
- ftpconversions.4
- ftpusers.4
- ftphosts.4
- xferlog.5

The following RFCs have been implemented in WU-FTPD 2.6.1:

RFC 959  
RFC 1639  
RFC 2428

---

## **4 Known Problems, Limitations, and Fixes**

This chapter discusses the known problems, limitations, workarounds, and defects closed in this release of WU-FTP.

**Known Problems**

---

**Known Problems**

There are no problems in this release of WU-FTP.



## **Limitations and Fixes**

There are no limitations and Fixes in this release of WU-FTPD.

**Defects Closed in this Release**

---

**Defects Closed in this Release**

There are no defects closed in this release.