

NAME

cups-files.conf – file and directory configuration file for cups

DESCRIPTION

The **cups-files.conf** file configures the files and directories used by the CUPS scheduler, **cupsd**(8). It is normally located in the */etc/cups* directory.

Each line in the file can be a configuration directive, a blank line, or a comment. Configuration directives typically consist of a name and zero or more values separated by whitespace. The configuration directive name and values are case-insensitive. Comment lines start with the *#* character.

DIRECTIVES

The following directives are understood by **cupsd**(8):

AccessLog

AccessLog *filename*

AccessLog **stderr**

AccessLog **syslog**

Defines the access log filename. Specifying a blank filename disables access log generation. The value "stderr" causes log entries to be sent to the standard error file when the scheduler is running in the foreground, or to the system log daemon when run in the background. The value "syslog" causes log entries to be sent to the system log daemon. The server name may be included in filenames using the string "%s", for example:

```
AccessLog /var/log/cups/%s-access_log
```

The default is *"var/log/cups/access_log"*.

CacheDir *directory*

Specifies the directory to use for long-lived temporary (cache) files. The default is *"var/spool/cups/cache"* or *"var/cache/cups"* depending on the platform.

ConfigFilePerm *mode*

Specifies the permissions for all configuration files that the scheduler writes. The default is "0644" on macOS and "0640" on all other operating systems.

Note: The permissions for the *printers.conf* file are currently masked to only allow access from the scheduler user (typically root). This is done because printer device URIs sometimes contain sensitive authentication information that should not be generally known on the system. There is no way to disable this security feature.

CreateSelfSignedCerts **yes**

CreateSelfSignedCerts **no**

Specifies whether the scheduler automatically creates self-signed certificates for client connections using TLS. The default is yes.

DataDir *path*

Specifies the directory where data files can be found. The default is usually *"usr/share/cups"*.

DocumentRoot *directory*

Specifies the root directory for the CUPS web interface content. The default is usually *"usr/share/doc/cups"*.

ErrorLog

ErrorLog *filename*

ErrorLog **stderr**

ErrorLog syslog

Defines the error log filename. Specifying a blank filename disables error log generation. The value "stderr" causes log entries to be sent to the standard error file when the scheduler is running in the foreground, or to the system log daemon when run in the background. The value "syslog" causes log entries to be sent to the system log daemon. The server name may be included in filenames using the string "%s", for example:

```
ErrorLog /var/log/cups/%s-error_log
```

The default is "/var/log/cups/error_log".

FatalErrors none

FatalErrors all *-kind [... -kind]*

FatalErrors kind *[... kind]*

Specifies which errors are fatal, causing the scheduler to exit. The default is "config". The *kind* strings are:

none

No errors are fatal.

all All of the errors below are fatal.

browse

Browsing initialization errors are fatal, for example failed connections to the DNS-SD daemon.

config

Configuration file syntax errors are fatal.

listen

Listen or Port errors are fatal, except for IPv6 failures on the loopback or "any" addresses.

log Log file creation or write errors are fatal.

permissions

Bad startup file permissions are fatal, for example shared TLS certificate and key files with world-read permissions.

Group *group-name-or-number*

Specifies the group name or ID that will be used when executing external programs. The default group is operating system specific but is usually "lp" or "nobody".

LogFileGroup *group-name-or-number*

Specifies the group name or ID that will be used for log files. The default group is operating system specific but is usually "lp" or "nobody".

LogFilePerm *mode*

Specifies the permissions of all log files that the scheduler writes. The default is "0644".

PageLog *[filename]*

PageLog stderr

PageLog syslog

Defines the page log filename. The value "stderr" causes log entries to be sent to the standard error file when the scheduler is running in the foreground, or to the system log daemon when run in the background. The value "syslog" causes log entries to be sent to the system log daemon. Specifying a blank filename disables page log generation. The server name may be included in filenames using the string "%s", for example:

```
PageLog /var/log/cups/%s-page_log
```

The default is "/var/log/cups/page_log".

PassEnv *variable [... variable]*

Passes the specified environment variable(s) to child processes. Note: the standard CUPS filter and backend environment variables cannot be overridden using this directive.

PeerCred *off***PeerCred** *on***PeerCred** *root-only*

Specifies whether peer credentials are used for authorization when communicating over the UNIX domain socket. When **on**, the peer credentials of any user are accepted for authorization. The value **off** disables the use of peer credentials entirely, while the value **root-only** allows peer credentials only for the root user. Note: for security reasons, the **on** setting is reduced to **root-only** for authorization of PUT requests.

RemoteRoot *username*

Specifies the username that is associated with unauthenticated accesses by clients claiming to be the root user. The default is "remroot".

RequestRoot *directory*

Specifies the directory that contains print jobs and other HTTP request data. The default is "/var/spool/cups".

Sandboxing *relaxed***Sandboxing** *strict*

Specifies the level of security sandboxing that is applied to print filters, backends, and other child processes of the scheduler. The default is "strict". This directive is currently only used/supported on macOS.

ServerBin *directory*

Specifies the directory containing the backends, CGI programs, filters, helper programs, notifiers, and port monitors. The default is "/usr/lib/cups" or "/usr/libexec/cups" depending on the platform.

ServerKeychain *path*

Specifies the location of TLS certificates and private keys. The default is "/Library/Keychains/System.keychain" on macOS and "/etc/cups/ssl" on all other operating systems. macOS uses its keychain database to store certificates and keys while other platforms use separate files in the specified directory, *.cert for PEM-encoded certificates and *.key for PEM-encoded private keys.

ServerRoot *directory*

Specifies the directory containing the server configuration files. The default is "/etc/cups".

SetEnv *variable value*

Set the specified environment variable to be passed to child processes. Note: the standard CUPS filter and backend environment variables cannot be overridden using this directive.

StateDir *directory*

Specifies the directory to use for PID and local certificate files. The default is "/var/run/cups" or "/etc/cups" depending on the platform.

StripUserDomain *Yes***StripUserDomain** *No*

Specifies whether to remove domain from user name during local user authentication (e.g., "user@example.com" -> "user"). This practice can be beneficial for maintaining compatibility with older versions of Kerberos. However, enabling this option can have negative consequences. It may result in confusion between domain and local users with identical names, potentially leading to incorrect assignment of user permissions and unintentional permission escalation, thus creating a security risk. Therefore, it is advisable to avoid using this option in most cases.

SyncOnClose Yes**SyncOnClose No**

Specifies whether the scheduler calls **fsync(2)** after writing configuration or state files.

SystemGroup *group-name* [... *group-name*]

Specifies the group(s) to use for **@SYSTEM** group authentication. The default contains "admin", "lpadmin", "root", "sys", and/or "system".

TempDir *directory*

Specifies the directory where short-term temporary files are stored. The default is "/var/spool/cups/tmp".

User *username*

Specifies the user name or ID that is used when running external programs. The default is "lp".

DEPRECATED DIRECTIVES

The following directives are deprecated and will be removed from a future version of CUPS:

FileDevice Yes**FileDevice No**

Specifies whether the file pseudo-device can be used for new printer queues. The URI "file:///dev/null" is always allowed. File devices cannot be used with "raw" print queues - a PPD file is required. The specified file is overwritten for every print job. Writing to directories is not supported.

Printcap *filename*

Specifies a file that is filled with a list of local print queues.

PrintcapFormat **bsd****PrintcapFormat** **plist****PrintcapFormat** **solaris**

Specifies the format to use for the Printcap file. "bsd" is the historical LPD printcap file format. "plist" is the Apple plist file format. "solaris" is the historical Solaris LPD printcap file format.

NOTES

The scheduler **MUST** be restarted manually after making changes to the **cups-files.conf** file. On Linux this is typically done using the **systemctl(8)** command, while on macOS the **launchctl(8)** command is used instead.

SEE ALSO

classes.conf(5), **cups(1)**, **cupsd(8)**, **cupsd.conf(5)**, **mime.convs(5)**, **mime.types(5)**, **printers.conf(5)**, **subscriptions.conf(5)**, CUPS Online Help (<http://localhost:631/help>)

COPYRIGHT

Copyright © 2020-2025 by OpenPrinting.