

CUPSd - plik konfiguracyjny

Położenie: /etc/cups/cupsd.conf

© Imagine Studio 2005, <http://myGentoo.tk>

```
# "$Id: cupsd.conf.in,v 1.10 2002/12/17 22:08:08 mike Exp $"
##### Server Identity #####
# ServerName: the hostname of your server, as advertised to the world. By default CUPS will use the hostname of the system. To set
the default server used by clients, see the client.conf file. Może to być nazwa lub numer IP. Każdy użytkownik może sobie to zmienić
poprzez założenie pliku ~/.cupsrc z poniższym wpisem. Tak więc zadania drukowania mogą być wysyłane na inny serwer (nie na
lokalny spool).
```

ServerName [server.imagine](#)

```
# ServerAdmin: the email address to send all complaints/problems to. By default CUPS will use "root@hostname".
```

ServerAdmin robertSurma@op.pl

```
##### Server Options #####
# AccessLog: the access log file; if this does not start with a leading / then it is assumed to be relative to ServerRoot. By default set to
"/var/log/cups/access_log". You can also use the special name "syslog" to send the output to the syslog file or daemon.
```

AccessLog [/var/log/cups/access_log](#)

```
# Classification: the classification level of the server. If set, this classification is displayed on all pages, and raw printing is disabled. The
default is the empty string.
```

Classification [classified](#)
Classification [confidential](#)
Classification [secret](#)
Classification [topsecret](#)
Classification [unclassified](#)

```
# ClassifyOverride: whether to allow users to override the classification on printouts. If enabled, users can limit banner pages to before
or after the job, and can change the classification of a job, but cannot completely eliminate the classification or banners. The default is
off.
```

ClassifyOverride [off](#)

```
# Katalog główny serwera CUPS, domyślnie ("/usr/share/cups").
```

DataDir [/usr/share/cups](#)

```
# DefaultCharset: the default character set to use. If not specified, defaults to "utf-8". Note that this can also be overridden in HTML
documents...
```

DefaultCharset [iso-8859-2](#)

```
# DefaultLanguage: the default language if not specified by the browser. If not specified, the current locale is used.
```

DefaultLanguage [pl](#)

```
# DocumentRoot: the root directory for HTTP documents that are served. By default "/usr/share/doc/cups".
```

DocumentRoot [/usr/share/doc/cups-1.1.20/html](#)

```
# ErrorLog: the error log file; if this does not start with a leading / then it is assumed to be relative to ServerRoot. By default set to
"/var/log/cups/error_log". You can also use the special name "syslog" to send the output to the syslog file or daemon.
```

ErrorLog [/var/log/cups/error_log](#)

```
# FileDevice: determines whether the scheduler will allow new printers to be added using device URIs of the form "file:/foo/bar". The
default is not to allow file devices due to the potential security vulnerability and due to the fact that file devices do not support raw
printing.
```

FileDevice [No](#)

FontPath: the path to locate all font files (currently only for pstoraster). By default "/usr/share/cups/fonts".

FontPath /usr/share/cups/fonts

LogLevel: controls the number of messages logged to the ErrorLog file and can be one of the following:

debug2 Log everything.

debug Log almost everything.

info Log all requests and state changes.

warn Log errors and warnings.

error Log only errors.

none Log nothing.

LogLevel info

MaxLogSize: controls the maximum size of each log file before they are rotated. Defaults to 1048576 (1MB). Set to 0 to disable log rotating.

MaxLogSize 0

PageLog: the page log file; if this does not start with a leading / then it is assumed to be relative to ServerRoot. By default set to "/var/log/cups/page_log". You can also use the special name "syslog" to send the output to the syslog file or daemon.

PageLog /var/log/cups/page_log

PreserveJobHistory: whether or not to preserve the job history after a job is completed, cancelled, or stopped. Default is Yes.

PreserveJobHistory Yes

PreserveJobFiles: whether or not to preserve the job files after a job is completed, cancelled, or stopped. Default is No.

PreserveJobFiles No

AutoPurgeJobs: automatically purge jobs when not needed for quotas. Default is No.

AutoPurgeJobs No

MaxCopies: maximum number of copies that a user can request. Default is 100.

MaxCopies 40

MaxJobs: maximum number of jobs to keep in memory (active and completed.). Default is 500; the value 0 is used for no limit.

MaxJobs 10

MaxJobsPerPrinter: maximum number of active jobs per printer. The default is 0 for no limit.

MaxJobsPerPrinter 10

MaxJobsPerUser: maximum number of active jobs per user. The default is 0 for no limit.

MaxJobsPerUser 10

MaxPrinterHistory: controls the maximum number of history collections in the printer-state-history attribute. Set to 0 to disable history data.

MaxPrinterHistory 10

Printcap: the name of the printcap file. Default is /etc/printcap. Leave blank to disable printcap file generation.

Printcap /etc/printcap

PrintcapFormat: the format of the printcap file, currently either BSD or Solaris. The default is "BSD".

PrintcapFormat BSD

PrintcapGUI: the name of the GUI options panel program to associate with print queues under IRIX. The default is "/usr/bin/glpoptions" from ESP Print Pro. This option is only used under IRIX; the options panel program must accept the "-d printer" and "-o options" options and write the selected printer options back to stdout on completion.

PrintcapGUI /usr/bin/glpoptions

RequestRoot: the directory where request files are stored. By default "/var/spool/cups".

RequestRoot /var/spool/cups

RemoteRoot: the name of the user assigned to unauthenticated accesses from remote systems. By default "remroot".
RemoteRoot remroot

ServerBin: the root directory for the scheduler executables. By default "/usr/lib/cups".

ServerBin /usr/lib/cups

ServerRoot: the root directory for the scheduler. By default "/etc/cups".

ServerRoot /etc/cups

Fax Support

FaxRetryLimit: the number of times a fax job is retried. The default is 5 times.
#FaxRetryLimit 5

FaxRetryInterval: the number of seconds between fax job retries. The default is 300 seconds/5 minutes.
#FaxRetryInterval 300

Encryption Support

ServerCertificate: the file to read containing the server's certificate. Defaults to "/etc/cups/ssl/server.crt".
ServerCertificate /etc/cups/ssl/server.crt

ServerKey: the file to read containing the server's key. Defaults to "/etc/cups/ssl/server.key".

ServerKey /etc/cups/ssl/server.key

Filter Options

User/Group: the user and group the server runs under. Normally this must be lp and sys, however you can configure things for another user or group as needed. Note: the server must be run initially as root to support the default IPP port of 631. It changes users whenever an external program is run, or if the RunAsUser directive is specified...

User lp

Group lp

RIPCach: the amount of memory that each RIP should use to cache bitmaps. The value can be any real number followed by "k" for kilobytes, "m" for megabytes, "g" for gigabytes, or "t" for tiles (1 tile = 256x256 pixels.) Defaults to "8m" (8 megabytes).

RIPCach 8m

TempDir: the directory to put temporary files in. This directory must be writable by the user defined above! Defaults to "/var/spool/cups/tmp" or the value of the TMPDIR environment variable.

TempDir /var/spool/cups/tmp

FilterLimit: sets the maximum cost of all job filters that can be run at the same time. A limit of 0 means no limit. A typical job may need a filter limit of at least 200; limits less than the minimum required by a job force a single job to be printed at any time. The default limit is 0 (unlimited).

FilterLimit 0

Network Options

Ports/addresses that we listen to. The default port 631 is reserved for the Internet Printing Protocol (IPP) and is what we use here. You can have multiple Port/Listen lines to listen to more than one port or address, or to restrict access: Port 80, Port 631, Listen hostname, Listen hostname:80, Listen hostname:631, Listen 1.2.3.4, Listen 1.2.3.4:631. NOTE: Unfortunately, most web browsers don't support TLS or HTTP Upgrades for encryption. If you want to support web-based encryption you'll probably need to listen on port 443 (the "https" port...)

#Port 80

#Port 443

Port 631

HostNameLookups: whether or not to do lookups on IP addresses to get a fully-qualified hostname. This defaults to Off for performance reasons...

HostNameLookups On

KeepAlive: whether or not to support the Keep-Alive connection option. Default is on.

KeepAlive On

KeepAliveTimeout: the timeout before Keep-Alive connections are automatically closed. Default is 60 seconds.

KeepAliveTimeout 60

MaxClients: controls the maximum number of simultaneous clients that will be handled. Defaults to 100.

MaxClients 100

MaxClientsPerHost: controls the maximum number of simultaneous clients that will be handled from a specific host. Defaults to 10 or 1/10th of the MaxClients setting, whichever is larger. A value of 0 specifies the automatic (10 or 1/10th) setting.

MaxClientsPerHost 0

MaxRequestSize: controls the maximum size of HTTP requests and print files. Set to 0 to disable this feature (defaults to 0.)

MaxRequestSize 0

Timeout: the timeout before requests time out. Default is 300 seconds.

Timeout 300

Browsing Options

Browsing: whether or not to broadcast and/or listen for CUPS printer information on the network. Enabled by default.

Browsing On

BrowseProtocols: which protocols to use for browsing. Can be any of the following separated by whitespace and/or commas: all - Use all supported protocols; cups - Use the CUPS browse protocol; slp - Use the SLPv2 protocol. The default is "cups". NOTE: If you choose to use SLPv2, it is *strongly* recommended that you have at least one SLP Directory Agent (DA) on your network. Otherwise, browse updates can take several seconds, during which the scheduler will not response to client requests.

BrowseProtocols cups

BrowseAddress: specifies a broadcast address to be used. By default browsing information is not sent! Note: HP-UX does not properly handle broadcast unless you have a Class A, B, C, or D netmask (i.e. no CIDR support). Note: Using the "global" broadcast address (255.255.255.255) will activate a Linux demand-dial link with the default configuration. If you have a LAN as well as the dial-up link, use the LAN's broadcast address. The @LOCAL address broadcasts to all non point-to-point interfaces. For example, if you have a LAN and a dial-up link, @LOCAL would send printer updates to the LAN but not to the dial-up link. Similarly, the @IF(name) address sends to the named network interface, e.g. @IF(eth0) under Linux. Interfaces are refreshed automatically (no more than once every 60 seconds), so they can be used on dynamically-configured interfaces, e.g. PPP, 802.11, etc.

#BrowseAddress x.y.z.255

#BrowseAddress x.y.255.255

#BrowseAddress x.255.255.255

#BrowseAddress 255.255.255.255

BrowseAddress @LOCAL

BrowseShortNames: whether or not to use "short" names for remote printers when possible (e.g. "printer" instead of "printer@host"). Enabled by default.

BrowseShortNames Yes

BrowseAllow: specifies an address mask to allow for incoming browser packets. The default is to allow packets from all addresses. BrowseDeny: specifies an address mask to deny for incoming browser packets. The default is to deny packets from no addresses. Both "BrowseAllow" and "BrowseDeny" accept the following notations for addresses: All; None; *.domain.com; .domain.com; host.domain.com; nnn.*; nnn.nnn.*; nnn.nnn.nnn.*; nnn.nnn.nnn.nnn; nnn.nnn.nnn.nnn/mm; nnn.nnn.nnn.nnn/mmm.mmm.mmm.mmm; @LOCAL; @IF(name). The hostname/domainname restrictions only work if you have turned hostname lookups on!

BrowseAllow @LOCAL

BrowseDeny All

BrowseInterval: the time between browsing updates in seconds. Default is 30 seconds. Note that browsing information is sent

whenever a printer's state changes as well, so this represents the maximum time between updates. Set this to 0 to disable outgoing broadcasts so your local printers are not advertised but you can still see printers on other hosts.

BrowseInterval 120

BrowseOrder: specifies the order of BrowseAllow/BrowseDeny comparisons.

BrowseOrder Deny,Allow

BrowsePoll: poll the named server(s) for printers

BrowsePoll 192.168.0.2:631

BrowsePort: the port used for UDP broadcasts. By default this is the IPP port; if you change this you need to do it on all servers. Only one BrowsePort is recognized.

BrowsePort 631

BrowseRelay: relay browser packets from one address/network to another.

BrowseRelay source-address destination-address

BrowseRelay @IF(src) @IF(dst)

BrowseTimeout: the timeout for network printers - if we don't get an update within this time the printer will be removed from the printer list. This number definitely should not be less the BrowseInterval value for obvious reasons. Defaults to 300 seconds.

BrowseTimeout 300

ImplicitClasses: whether or not to use implicit classes. Printer classes can be specified explicitly in the classes.conf file, implicitly based upon the printers available on the LAN, or both. When ImplicitClasses is On, printers on the LAN with the same name (e.g. Acme-LaserPrint-1000) will be put into a class with the same name. This allows you to setup multiple redundant queues on a LAN without a lot of administrative difficulties. If a user sends a job to Acme-LaserPrint-1000, the job will go to the first available queue. Enabled by default.

ImplicitClasses Off

ImplicitAnyClasses: whether or not to create "AnyPrinter" implicit classes. When ImplicitAnyClasses is On and a local queue of the same name exists, e.g. "printer", "printer@server1", "printer@server1", then an implicit class called "Anyprinter" is created instead. When ImplicitAnyClasses is Off, implicit classes are not created when there is a local queue of the same name. Disabled by default.

ImplicitAnyClasses Off

HideImplicitMembers: whether or not to show the members of an implicit class. When HideImplicitMembers is On, any remote printers that are part of an implicit class are hidden from the user, who will then only see a single queue even though many queues will be supporting the implicit class. Enabled by default.

HideImplicitMembers On

Security Options

SystemGroup: the group name for "System" (printer administration) access. The default varies depending on the operating system, but will be "sys", "system", or "root" (checked for in that order.)

SystemGroup lp

RootCertDuration: How frequently the root certificate is regenerated. Defaults to 300 seconds.

RootCertDuration 300

Access permissions for each directory served by the scheduler. Locations are relative to DocumentRoot...

AuthType: the authorization to use: None - Perform no authentication; Basic - Perform authentication using the HTTP Basic method (używa haseł i użytkowników systemowych); Digest - Perform authentication using the HTTP Digest method (używa haseł z / etc/cups/passwd.md5). (Note: local certificate authentication can be substituted by the client for Basic or Digest when connecting to the localhost interface)

AuthClass: the authorization class; currently only "Anonymous", "User", "System" (valid user belonging to group SystemGroup), and "Group" (valid user belonging to the specified group) are supported.

AuthGroupName: the group name for "Group" authorization.

Order: the order of Allow/Deny processing.

Allow: allows access from the specified hostname, domain, IP address, network, or interface.

Deny: denies access from the specified hostname, domain, IP address, network, or interface.
Both "Allow" and "Deny" accept the following notations for addresses: All; None; *.domain.com; .domain.com; host.domain.com; nnn.*; nnn.nnn.*; nnn.nnn.nnn.*; nnn.nnn.nnn.nnn; nnn.nnn.nnn.nnn/mm; nnn.nnn.nnn.nnn/mmm.mmm.mmm; @LOCAL; @IF (name). The host and domain address require that you enable hostname lookups with "HostNameLookups On" above. The @LOCAL address allows or denies from all non point-to-point interfaces. For example, if you have a LAN and a dial-up link, @LOCAL could allow connections from the LAN but not from the dial-up link. Similarly, the @IF(name) address allows or denies from the named network interface, e.g. @IF(eth0) under Linux. Interfaces are refreshed automatically (no more than once every 60 seconds), so they can be used on dynamically-configured interfaces, e.g. PPP, 802.11, etc.
Encryption: whether or not to use encryption; this depends on having the OpenSSL library linked into the CUPS library and scheduler. Possible values: Always - Always use encryption (SSL); Never - Never use encryption; Required - Use TLS encryption upgrade; IfRequested - Use encryption if the server requests it. The default value is "IfRequested".
Dostęp do wszystkich operacji napływających. Są one nadpisywane przez opcje podkatalogów.

```
<Location />  
Order Deny,Allow  
Deny From All  
Allow From 127.0.0.1  
Allow From 192.168.0.1  
Allow From @LOCAL  
</Location>
```

Dostęp do parametrów classes.
#<Location /classes>
You may wish to limit access to printers and classes, either with Allow and Deny lines, or by requiring a username and password.
#</Location>
#<Location /classes/name>
You may wish to limit access to printers and classes, either with Allow and Deny lines, or by requiring a username and password.
#</Location>

Dostęp do zadań wysłanych na drukarkę
#<Location /jobs>
You may wish to limit access to job operations, either with Allow and Deny lines, or by requiring a username and password.
#</Location>

Dostęp do drukarek.
#<Location /printers>
You may wish to limit access to printers and classes, either with Allow and Deny lines, or by requiring a username and password.
#</Location>

```
#<Location /printers/name>  
# You may wish to limit access to printers and classes, either with Allow and Deny lines, or by requiring a username and password.  
## Anonymous access (default)  
#AuthType None  
## Require a username and password (Basic authentication)  
#AuthType Basic  
#AuthClass User  
## Require a username and password (Digest/MD5 authentication)  
#AuthType Digest  
#AuthClass User  
## Restrict access to local domain  
#Order Deny,Allow  
#Deny From All  
#Allow From .mydomain.com  
#</Location>
```

Dostęp do wszystkich operacji administratorskich (np. dodawanie drukarek).
<Location /admin>
You definitely will want to limit access to the administration functions. The default configuration requires a local connection from a

user who is a member of the system group to do any admin tasks. You can change the group name using the SystemGroup directive.

AuthType Digest

AuthClass Group

AuthGroupName Ip

Restrict access to local domain

Order Deny,Allow

Deny From All

Allow From 127.0.0.1

Allow From 192.168.0.1

Allow From 192.168.0.2

Encryption IfRequested

</Location>

End of "\$Id: cupsd.conf.in,v 1.10 2002/12/17 22:08:08 mike Exp \$".

Ostatnia aktualizacja: 22 marzec 2005.