

NAME

client.conf – client configuration file for cups (deprecated on macos)

DESCRIPTION

The **client.conf** file configures the CUPS client and is normally located in the */etc/cups* and/or *~/cups* directories. Each line in the file can be a configuration directive, a blank line, or a comment. Comment lines start with the *#* character.

Note: Starting with macOS 10.7, this file is only used by command-line and X11 applications plus the IPP backend. The **ServerName** directive is not supported on macOS at all. Starting with macOS 10.12, all applications can access these settings in the */Library/Preferences/org.cups.PrintingPrefs.plist* file instead. See the NOTES section below for more information.

DIRECTIVES

The following directives are understood by the client. Consult the online help for detailed descriptions:

AllowAnyRoot Yes**AllowAnyRoot No**

Specifies whether to allow TLS with certificates that have not been signed by a trusted Certificate Authority. The default is "Yes".

AllowExpiredCerts Yes**AllowExpiredCerts No**

Specifies whether to allow TLS with expired certificates. The default is "No".

DigestOptions DenyMD5**DigestOptions None**

Specifies HTTP Digest authentication options. **DenyMD5** disables support for the original MD5 hash algorithm.

Encryption IfRequested**Encryption Never****Encryption Required**

Specifies the level of encryption that should be used.

GSSServiceName name

Specifies the Kerberos service name that is used for authentication, typically "host", "http", or "ipp". CUPS adds the remote hostname ("name@server.example.com") for you. The default name is "http".

ServerName hostname-or-ip-address[:port]**ServerName /domain/socket**

Specifies the address and optionally the port to use when connecting to the server. **Note: This directive is not supported on macOS 10.7 or later.**

ServerName hostname-or-ip-address[:port]/version=1.1

Specifies the address and optionally the port to use when connecting to a server running CUPS 1.3.12 and earlier.

SSLOptions [AllowDH] [AllowRC4] [AllowSSL3] [DenyCBC] [DenyTLS1.0] [MaxTLS1.0] [MaxTLS1.1] [MaxTLS1.2] [MaxTLS1.3] [MinTLS1.0] [MinTLS1.1] [MinTLS1.2] [MinTLS1.3] [NoSystem]

SSLOptions None

Sets encryption options (only in */etc/cups/client.conf*). By default, CUPS only supports encryption using TLS v1.0 or higher using known secure cipher suites. Security is reduced when *Allow* options are used. Security is enhanced when *Deny* options are used. The *AllowDH* option enables cipher suites using plain Diffie-Hellman key negotiation (not supported on systems using GNU TLS). The *AllowRC4* option enables the 128-bit RC4 cipher suites, which are required for some older clients. The *AllowSSL3* option enables SSL v3.0, which is required for some older clients that do not support TLS v1.0. The *DenyCBC* option disables all CBC cipher suites. The *DenyTLS1.0* option disables

TLS v1.0 support - this sets the minimum protocol version to TLS v1.1. The *MinTLS* options set the minimum TLS version to support. The *MaxTLS* options set the maximum TLS version to support. The *NoSystem* option disables applying system cryptographic policy. Not all operating systems support TLS 1.3 at this time.

TrustOnFirstUse Yes

TrustOnFirstUse No

Specifies whether to trust new TLS certificates by default. The default is "Yes".

User name

Specifies the default user name to use for requests.

UserAgentTokens None

UserAgentTokens ProductOnly

UserAgentTokens Major

UserAgentTokens Minor

UserAgentTokens Minimal

UserAgentTokens OS

UserAgentTokens Full

Specifies what information is included in the User-Agent header of HTTP requests. "None" disables the User-Agent header. "ProductOnly" reports "CUPS". "Major" reports "CUPS/major IPP/2". "Minor" reports "CUPS/major.minor IPP/2.1". "Minimal" reports "CUPS/major.minor.patch IPP/2.1". "OS" reports "CUPS/major.minor.path (osname osversion) IPP/2.1". "Full" reports "CUPS/major.minor.path (osname osversion; architecture) IPP/2.1". The default is "Minimal".

ValidateCerts Yes

ValidateCerts No

Specifies whether to only allow TLS with certificates whose common name matches the hostname. The default is "No".

NOTES

The **client.conf** file is deprecated on macOS and will no longer be supported in a future version of CUPS. Configuration settings can instead be viewed or changed using the **defaults(1)** command:
 defaults write /Library/Preferences/org.cups.PrintingPrefs.plist Encryption Required
 defaults write /Library/Preferences/org.cups.PrintingPrefs.plist TrustOnFirstUse -bool NO

defaults read /Library/Preferences/org.cups.PrintingPrefs.plist Encryption

On Linux and other systems using GNU TLS, the */etc/cups/ssl/site.crl* file, if present, provides a list of revoked X.509 certificates and is used when validating certificates.

SEE ALSO

cups(1), **default(1)**, CUPS Online Help (<http://localhost:631/help>)

COPYRIGHT

Copyright © 2020-2025 by OpenPrinting.