

# **HP CIFS Client A.01.09 Administrator's Guide**

**HP-UX 11.0 and 11i version 1 and 2**



**Manufacturing Part Number : B8724-90044  
August, 2003**

U.S.A.

© Copyright 2003 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.

PAM NTLM includes a library derived from the Open Source Samba product. This library is subject to the GPL license. For detailed information, refer to the GPL license in Chapter 5 of the CIFS/9000 Server manual.

**Copyright Notices.** ©copyright 1983-2003 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.

©copyright 1998 Christian Starkjohann, All Rights Reserved.

**Trademark Notices.** UNIX is a registered trademark of The Open Group.



**1. Introduction to the HP CIFS Client**

Introduction to HP CIFS .....	15
What is the CIFS Protocol? .....	15
HP CIFS Client Description .....	17
HP CIFS Client Features.....	18
CIFS UNIX Extensions .....	18
NTLM PAM Integration.....	18
Kerberos Authentication: Integration with System Kerberos Cache .....	19
AutoFS 2.3 Support for HP CIFS Client .....	19
Support for Internationalized Clients .....	20

**2. Installing, Configuring, and Using the HP CIFS Client**

Overview of HP CIFS Client Installation and Configuration .....	23
Step 1: Checking HP CIFS Client Installation Prerequisites .....	24
Step 2: Installing HP CIFS Client and PAM Software .....	25
Step 3: Configuring the HP CIFS Client .....	27
Editing cifsclient.cfg .....	27
Step 4: Starting and Stopping the HP CIFS Client Daemon.....	29
Using the HP CIFS Client.....	30
More on Mounting CIFS Filesystems .....	33
Using /etc/fstab .....	33
How to Mount and Login in One Step.....	33
Deprecated mount and unmount commands.....	34
HP CIFS Client Files and Directories .....	35

**3. CIFS Security and Authentication**

Introduction .....	38
Authentication Protocols .....	38
User Authentication Methods.....	39

**4. CIFS Authentication Using Kerberos**

Introduction To Kerberos.....	44
Requirements and Limitations .....	45
Kerberos Key Distribution Center and CIFS Servers .....	45
Tickets and Ticket Acquisition.....	45
Using Kerberos with the HP CIFS Client .....	46
Step 1. Review fundamental Kerberos Operating Principals.....	46
Step 2. Set Up and Verify the Kerberos Infrastructure .....	47

---

# Contents

Step 3. Configure Kerberos on the HP CIFS Client . . . . .	49
CIFS Client Kerberos Authentication Policies . . . . .	50
Explicit login: cifslogin . . . . .	50
Automatic login: Integration with System Kerberos Cache (kinit(1) and PAM Kerberos) . . . . .	50
Ticket Lifetime . . . . .	50
Troubleshooting Kerberos in the HP CIFS Client . . . . .	51

## 5. Commandline Utilities

cifsclient . . . . .	55
Synopsis . . . . .	55
Description . . . . .	55
Commands . . . . .	55
Files . . . . .	57
See Also . . . . .	57
cifsmount . . . . .	58
Synopsis . . . . .	58
Description . . . . .	58
Options . . . . .	58
Examples . . . . .	61
Files . . . . .	61
See Also . . . . .	61
cifslogin . . . . .	62
Synopsis . . . . .	62
Description . . . . .	62
Options . . . . .	62
Examples . . . . .	64
Files . . . . .	65
See Also . . . . .	65
cifsumount . . . . .	66
Synopsis . . . . .	66
Description . . . . .	66
Options . . . . .	66
Files . . . . .	66
See Also . . . . .	67
cifslogout . . . . .	68

Synopsis . . . . .	68
Description . . . . .	68
Options . . . . .	68
Files . . . . .	68
See Also . . . . .	68
cifslist . . . . .	69
Synopsis . . . . .	69
Description . . . . .	69
mount_cifs, umount_cifs . . . . .	70
Synopsis . . . . .	70
Description . . . . .	70
Options . . . . .	70
Files . . . . .	72
See Also . . . . .	72
<b>6. Troubleshooting and Error Messages</b>	
Troubleshooting FAQs . . . . .	75
How to Kill the Daemon with cifsclient stop . . . . .	75
What to Do if the Daemon Terminates . . . . .	75
HP CIFS Client Error Messages . . . . .	76
<b>7. Configuration File</b>	
General Structure . . . . .	81
Configuration Variables . . . . .	83
<b>8. PAM NTLM</b>	
Introduction . . . . .	104
PAM NTLM . . . . .	106
PAM NTLM Features . . . . .	106
User Map File . . . . .	106
PAM NTLM Configuration . . . . .	107
Configuring the PAM NTLM Module . . . . .	107
Configuring a User Map File . . . . .	111
Using NIS Distribution of the User Map File . . . . .	111
<b>Glossary . . . . .</b>	<b>113</b>
<b>Index . . . . .</b>	<b>115</b>

---

# Contents

---

## **Preface: About This Document**

The latest version of this document can be found on line at:

*<http://www.docs.hp.com>*

This document describes how to install, configure, and troubleshoot HP CIFS Client on HP-UX platforms.

The document printing date and part number indicate the document's current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The document part number will change when extensive changes are made.

Document updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

### **Intended Audience**

This document is intended for system and network administrators responsible for installing, configuring, and managing HP CIFS Client. Administrators are expected to have knowledge of HP CIFS Client product.

### **New and Changed Documentation in This Edition**

Information about CIFS authentication using Kerberos was added.

CIFS security and authentication information was added.

Information about AutoFS 2.3 support for HP CIFS client was added

## Publishing History

Table 1

Publishing History Details

Document Manufacturing Part Number	Operating Systems Supported	Supported Product Versions	Publication Date
B8724-90022	IA 11.22 1	A.01.08	June 2002
B8724-90011	11.0 11i version 1	A.01.06 A.01.06	June 2001

## What's in This document

This manual describes how to install, configure and troubleshoot the HP CIFS Client software product.

The manual is organized as follows:

- Chapter 1      **Introduction to the HP CIFS Client** Use this chapter to learn the HP CIFS Client product features, requirements and limitations.
- Chapter 2      **Installing, Configuring, and Using the HP CIFS Client** Use this chapter to learn how to install, configure, and use the HP CIFS Client software.
- Chapter 3      **CIFS Security and Authentication** Use this chapter to understand the CIFS security and authentication methods.
- Chapter 4      **CIFS Authentication Using Kerberos** Use this chapter to describe information about the Kerberos authentication services.
- Chapter 5      **Commandline Utilities** Use this chapter to learn about UNIX man pages for all HP CIFS Client utilities.
- Chapter 6      **Troubleshooting the HP CIFS Client** Use this chapter to understand the detailed procedures to help diagnose HP CIFS Client problems.

- Chapter 7      **Configuration File** Use this chapter to know a list of all configuration variables if you want to customize HP CIFS Client software.
- Chapter 8      **PAM NTLM** Use this chapter to understand detailed information about the PAM NTLM authentication service.

## Typographical Conventions

This document uses the following conventions.

- Italics*              Identifies titles of documentation, filenames and paths
- Bold**                 Text that is strongly emphasized.
- monotype             Identifies program/script, command names, parameters or display.

## HP Encourages Your Comments

HP encourages your comments concerning this document. We are truly committed to providing documentation that meets your needs.

Please send comments to: [netinfo\\_feedback@cup.hp.com](mailto:netinfo_feedback@cup.hp.com)

Please include document title, manufacturing part number, and any comment, error found, or suggestion for improvement you have concerning this document. Also, please include what we did right so we can incorporate it into other documents.



---

# **1 Introduction to the HP CIFS Client**

This chapter provides a HP CIFS Client description.

It contains the following sections:

- Introduction to HP CIFS.
- HP CIFS Client Description.
- HP CIFS Client Features.

## Introduction to HP CIFS

HP CIFS provides HP-UX with a distributed file system based on the Microsoft Common Internet File System (CIFS) protocols. HP CIFS implements both the server and client components of the CIFS protocol on HP-UX.

The HP CIFS Server is based on the well-established open-source software Samba, and provides file and print services to CIFS clients including Windows 95, 98, NT, 2000, and HP-UX machines running HP CIFS Client software.

The HP CIFS Client enables HP-UX users to mount as UNIX filesystems shares from CIFS file servers including Windows servers and HP-UX machines running HP CIFS Server. The HP CIFS client also offers an optional Pluggable Authentication Module (PAM) that implements the Windows NT Lan Manager (NTLM) authentication protocols. When installed and configured within HP-UX's PAM facility, PAM NTLM allows HP-UX users to be authenticated against a Windows authentication server.

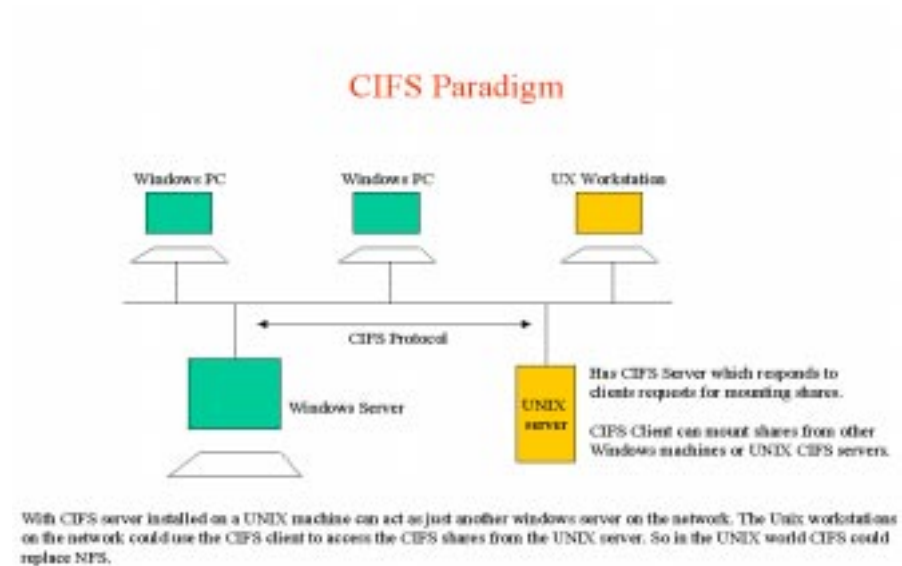
### What is the CIFS Protocol?

CIFS had its beginnings in the networking protocols, sometimes called Server Message Block (SMB) protocols, that were developed in the late 1980 for PCs to share files over the then nascent Local Area Network technologies (for example, Ethernet). SMB is the native file-sharing protocol in the Microsoft Windows 95, Windows NT, and OS/2 operating systems and the standard way that millions of PC users share files across corporate intranets.

CIFS is simply a renaming of SMB; and CIFS and SMB are the same. (Microsoft now emphasizes the use of CIFS, although references to SMB still occur.) CIFS is also widely available on UNIX, VMS(tm), Macintosh, and other platforms.

CIFS is a remote file access protocol; it provides access to files on remote systems. It sits on top of and works with the file systems of its host systems. CIFS defines both a server and a client: the CIFS client is used to access files on a CIFS server.

HP CIFS uses the CIFS protocol from the HP-UX machines, which enables directories from HP-UX servers to be mounted on to Windows machines and vice versa.



## PAM NTLM

The HP-UX PAM subsystem gives system administrators the flexibility of choosing any authentication service available on the system to perform authentication. The framework also allows new authentication service modules to be plugged in and made available without modifying the applications.

The PAM framework, *libpam*, consists of an interface library and multiple authentication service modules. The authentication service modules are a set of dynamically loadable objects invoked by the PAM API to provide a particular type of user authentication.

NT LAN Manager (NTLM) is the protocol by which CIFS clients are authenticated by CIFS servers. PAM NTLM is a PAM module that implements the NTLM protocol. It enables users logging in to an HP-UX system to have access to CIFS-mounted file systems without having to use the `cifslogin` command.

## **HP CIFS Client Description**

HP CIFS Client implements the CIFS protocols on HP-UX so that HP-UX users may mount shares from CIFS servers as UNIX file systems.

## HP CIFS Client Features

Following is a list of the HP CIFS Client major features:

- CIFS UNIX Extensions
- NTLM PAM Integration
- Kerberos Authentication, Integration with System Kerberos Cache
- ONC AutoFS 2.3 Support
- Support for Internationalized Clients

### CIFS UNIX Extensions

CIFS UNIX Extensions enable the CIFS Client and Samba server to implement standard UNIX file system features. These include:

- UNIX permission modes
- File ownership based on UNIX UIDs and GIDs
- Symbolic links and hard links
- Standard UNIX timestamps for file access, change, and modification
- Includes other data contained in the UNIX stat(2) data structure

---

#### NOTE

This feature only works with CIFS servers that support CIFS UNIX extensions.

---

### NTLM PAM Integration

NT LAN Manager (NTLM) is the default protocol by which CIFS clients are authenticated by CIFS servers. When used in conjunction with HP's NTLM Pluggable Authentication Module (PAM) and the HP CIFS Client, users who log in to an HP-UX system will have access automatically to CIFS-mounted file systems provided that PAM NTLM and the CIFS server are using the same database.

## **Kerberos Authentication: Integration with System Kerberos Cache**

The CIFS Client supports the Kerberos authentication mechanism. Kerberos is a secure, industry-standard authentication protocol. It provides significant improvements over the older NTLM protocol traditionally used by CIFS Clients and Servers. The CIFS servers in your network must support Kerberos in order for you to take advantage of Kerberos support in the HP CIFS Client. Kerberos must be properly configured both on the HP-UX host on which the Client runs and on your network.

An additional feature is that the HP CIFS Client is integrated with the system Kerberos cache. If the HP-UX host uses PAM Kerberos or other Kerberos-aware programs that utilize the system Kerberos cache, such as *kinit(1)*, the CIFS Client can utilize these cached credentials to provide automatic access to mounted CIFS servers without explicit user-initiated authentication for each server.

### **AutoFS 2.3 Support for HP CIFS Client**

The AutoFS is a service which is part of the HP ONC product set that automatically mounts or unmounts filesystems with near- transparency to the end users. The latest version of AutoFS 2.3 supports the mount and unmount of the HP CIFS Client mounted filesystems. AutoFS 2.3 can automatically perform direct and indirect mounts of the HP CIFS filesystems. AutoFS 2.3 only supports the HP CIFS Client with direct and indirect map files, it doesn't support CIFS Client with special or executable map files, or with multiple (replicated) servers.

In order to provide HP CIFS Client AutoFS support, AutoFS 2.3 must be installed and configured on the system. For detailed information on installing and configuring AutoFS, please refer to *“Configuring and Administering AutoFS”* in *NFS Services Administrator's Guide* on HP-UX at <http://www.docs.hp.com>.

---

**NOTE**

AutoFS 2.3 support for HP CIFS Client applies only to HP-UX 11i version 2. AutoFS doesn't support HP CIFS Client on HP-UX release 11.0 and 11i version 1.

---

## **Support for Internationalized Clients**

The CIFS Client is designed to work with a variety of internationalized clients and servers. It can use Unicode to transmit multi-byte characters on the network, or any of several character encoding tables located in */etc/opt/cifsclient/unitables*. See the *README* file in that directory for an index of the tables.

---

## 2

# Installing, Configuring, and Using the HP CIFS Client

This chapter describes the procedures for installing HP CIFS Client software on your system.

It contains the following sections:

- **Overview of HP CIFS Client Installation and Configuration**
- **Step 1: Checking HP CIFS Client Installation Prerequisites**
- **Step 2: Installing HP CIFS Client and PAM Software**
- **Step 3: Configuring the HP CIFS Client Configuration**
- **Step 4: Starting and Stopping the HP CIFS Client Daemon**

## Overview of HP CIFS Client Installation and Configuration

Installation of the HP CIFS Client includes checking installation prerequisites, loading the HP CIFS Client filesets using the *swinstall(1M)* utility, and completing HP CIFS configuration procedures.

The CIFS Client and PAM NTLM products are delivered in the same bundle, packaged for installation via HP Software Distributor (SD). HP recommends that both products be installed at the same time. This is not a requirement as each one can also be installed and run as a standalone product. To install and remove software, use the HP-UX commands `swinstall(1M)` and `swremove(1M)`. Detailed information on these commands are provided in the HP-UX man pages.

The CIFS Client forces a system reboot during installation and removal. The CIFS Client modifies the kernel so that it will recognize CIFS as a mountable filesystem.

When you install the bundles for the HP CIFS Client, there will be two products for you to install. The first one is the HP CIFS client software and the second one (optional) is the NTLM PAM module.

---

### NOTE

You can download the HP CIFS Client software from [www.software.hp.com](http://www.software.hp.com).

---

## Step 1: Checking HP CIFS Client Installation Prerequisites

Prior to loading the HP CIFS Client software onto your system, check that you have met the following hardware and software prerequisites:

1. The HP CIFS client runs on all HP workstations and Servers that are capable of running HP-UX version 11.0 or later, in either 32-bit or 64-bit mode. No specific system patches are required for the HP CIFS Client. See item 3 below.
2. The Kerberos libraries, *libkrb5.sl* and *libcom\_err.lib*, must be present on your system. For HP-UX version 11i (B.11.11) and future releases, these libraries should be on your system by default as part of your base HP-UX operating system installation. However, on HP-UX version 11.0 (B.11.00), these libraries may not be present (check in */usr/lib*). To acquire these libraries, install the product PAM Kerberos, available at <http://software.hp.com>
3. Check that you have the latest PAM library patch. Patches are available at HP's online patch catalogue, search for "libpam". You can use the `swlist` command to list software installed on your system. If a General Release patch is listed, you can check its contents for PAM patches with the following command:  

```
swlist -l fileset_patch-name_ | grep -i pam
```

Refer to the HP CIFS Client release notes for information about patch dependencies.
4. You must be root to perform the installation.

## Step 2: Installing HP CIFS Client and PAM Software

Follow the steps below to load HP CIFS Client software using the HP-UX *swinstall* program.

1. Log in as `root`.
2. Insert the software media (disk) into the appropriate drive.
3. Run the *swinstall* program using the command:

```
swinstall
```

This opens the Software Selection Window and Specify Source Window.

4. Change the Source Host Name if necessary, enter the mount point of the drive in the Source Depot Path field, and activate the `ok` button to return to the Software Selection Window. Activate the `Help` button to get more information.

The Software Selection Window now contains a list of available software bundles to install.

5. Highlight the HP CIFS Client software and press `Enter`.
6. Highlight one or both products and press `Enter`.  
There will be two software products for the client. One is for the Client software and the other is for the NTLM PAM plug-in authentication module.
7. Choose `Mark for Install` from the Actions menu to choose the product to be installed.
8. Choose `Install` from the Actions menu to begin product installation and open the Install Analysis Window.
9. Activate the `ok` button in the Install Analysis Window when the Status field displays a Ready message.
10. Activate the `yes` button at the Confirmation Window to confirm that you want to install the software. *swinstall* displays the Install Window.

View the Install Window to read processing data while the software is being installed. When the Status field indicates Ready and the Note Window opens.

*swinstall* loads the fileset, runs the control scripts for the fileset, and builds the kernel. Estimated time for processing is 3 to 5 minutes.

11. Activate the ok button on the Note Window to reboot the system.

The user interface disappears and the system reboots.

12. When the system reboots, check the log files in */var/adm/sw/swinstall.log* and */var/adm/sw/swagent.log* to make sure the installation was successful.

---

## Step 3: Configuring the HP CIFS Client

The configuration file for the HP CIFS Client, `/etc/opt/cifsclient/cifsclient.cfg`, can be used as delivered, with no modification of its default values.

### Editing `cifsclient.cfg`

If appropriate, edit the HP CIFS client configuration file `/etc/opt/cifsclient/cifsclient.cfg` as described below.

1. Update the domain variable with the name of the NT domain to which the client will belong. This step is recommended, but not required.

```
domain = hpnet_dom
```

2. Configure Internationalized Clients.

The CIFS Client is designed to work with a variety of internationalized clients and servers. It can use Unicode to transmit multi-byte characters on the network, or any of several character encoding tables located in `/etc/opt/cifsclient/unitables`. See the *README* file in that directory for an index of the tables.

Each table is a CharMap file which can be configured for encoding file and directory names on the client or server (file contents are left untouched). The character set displayed on the CIFS Client console is configured with the parameter `clientCharMapFile`, which selects any one of the many character mapping files provided with the product. Character translations for communications with CIFS Servers can be done either in Unicode or through the configuration parameter `serverCharMapFile`, which also is used to select a character mapping file. Use of Unicode is turned on and off with the `useUnicode` parameter.

The default settings in `cifsclient.cfg` are:

```
serverCharMapFile = "/etc/opt/cifsclient/unitables/unimapCP437.cfg";  
clientCharMapFile = "/etc/opt/cifsclient/unitables/unimap8859-1.cfg";
```

If, for example, your CIFS Client is configured as a Japanese system using the *Shift-JIS* locale, and it is connected to a Japanese CIFS Server that also uses *Shift-JIS*, you would configure the following:

### Step 3: Configuring the HP CIFS Client

```
serverCharMapFile = "/etc/opt/cifsclient/unitables/unimapShiftJIS.cfg";  
clientCharMapFile = "/etc/opt/cifsclient/unitables/unimapShiftJIS.cfg";
```

#### 3. Authentication Level

The configuration parameter, `authenticationLevel`, should be set to `ntlm` or `kerberos`. See “HP CIFS Authentication Using Kerberos” for details.

4. HP recommends that no other configuration modification be made to this file. Because of limitations of the Windows file system, however, two configuration settings must be carefully considered for your operating environment: *execMapping* and *caseSensitive*. These are discussed in *Configuration File* Chapter. Also, see the discussion of case sensitivity in the HP CIFS Server manual in the section “Other Samba Issues.”

Because of limitations of the Windows file system, however, two configuration settings must be carefully considered for your operating environment: *execMapping* and *caseSensitive*. These are discussed in Chapter 5. Also, see the discussion of case sensitivity in the HP CIFS Server manual in the section “Other Samba Issues.”

---

#### NOTE

As of this revision, Samba does not support Unicode. Windows NT and Windows 2000 use Unicode by default.

---

## Step 4: Starting and Stopping the HP CIFS Client Daemon

Use the `cifsclient` command to start and stop the HP CIFS client.

The syntax is:

```
/opt/cifsclient/bin/cifsclient <start | stop>
```

The default, when no arguments are used, is to start the daemon. If the HP CIFS client is already running when you execute the command, you will get a message indicating it is already up.

Use the `stop` option of the `cifsclient` command to stop the HP CIFS Client.

In this case, the script tries to unmount all of the shares before it stops the daemon. If there is a problem with the unmounting, the script does not stop the HP CIFS Client.

See `cifsclient` man page in *Commandline Utilities* Chapter for more details.

## Using the HP CIFS Client

This section presents summary of how the HP CIFS Client can be used. The basic procedure is (1) start the daemon, (2) mount shared directories, (3) log in to CIFS Servers. These steps and some useful tips follow:

### 1. Start the daemon.

Normally the system administrator, logged in as *root*, enters this command at system startup:

```
$ cifsclient start
CIFS Client started; process id: 12783
```

To check status at any time:

```
$ cifsclient status

path:          /opt/cifsclient/sbin/cifsclientd
version:       FILESET HP CIFS CLIENT: Version: A.01.09
               Compiled on HP-UX B.11.00, s785/C360,
               03/05/30, 13:34:15
               cifsclientd: ver_id=1291218999
cksum:         2781544263
status:        CIFS Client is up; process id 12783,
               started Apr 13
mntck:         ok
```

You can also configure your system to start the CIFS Client automatically at bootup by editing the file */etc/rc.config.d/cifsclient* such that the run flag is set to 1: *RUN\_CIFSCLIENT=1*. There must be no spaces on either side of the equal sign.

### 2. Mount and unmount shares on a CIFS server.

This must be done by *root*. Directories mounted by the HP CIFS Client must first be configured as shares on the HP CIFS Server.

In this example, the share *source*, configured as a share on the HP CIFS Server, is mounted by the CIFS Client using the directory */home/devl/source* as the mount point. The directory used as the mount point must already exist.

To mount:

```
$ mount -F cifs buildsys:/source /home/devl/source
```

To unmount:

```
$ umount /home/devl/source
```

### 3. Access the shared directory via the mount point on the Client.

The HP CIFS Client allows access to mounted directories only on a per-user basis. Therefore, each user must first be authenticated by the HP CIFS Server. This is accomplished through the *cifslogin* command.

In this example, the share *source* has been mounted by the system administrator. The *root* user on the Client wants to access the shared directory on *buildsys*. This is first attempted by changing directories to the mount point, but without first logging into the server (this fails).

Then, by logging into *buildsys* with the *cifslogin* command, the user is authenticated by *buildsys* and can access its shared *source* directory through the CIFS Client's mount point. Note that the user name used to login to the CIFS Server can be different than the current login name at the Client. The account and password pair used in *cifslogin* must exist on the system that does the authentication.

Further, if the CIFS Server is a HP-UX system, all users on the Client that access the Server should have the same *uid* on both systems, so that file ownership is consistent.

```
$ whoami
root
cd /home/devl/source
sh: /home/devl/source: not found
```

This fails because the user has not yet logged into the CIFS Server *buildsys*.

```
$cifslogin buildsys root
Remote user root's password: *****
```

**This succeeds. To verify the results:**

```
$ cifslist
=====
Server buildsys:
=====
Remote Username: root          Local Username: root
Share: \\BUILDSYS\source
      rw /home/dev1/source
$ cd /home/dev1/source
$ _
```

**Normal users (non-root) gain access to CIFS mounts in the same manner. Using the example above (*source* is mounted and root is authenticated on *buildsys*), a user named *lucy* accesses the mount as follows:**

```
$ cifslogin buildsys lucy
Remote user lucy's password: *****
```

**Verify results:**

```
$ cifslist
=====
server buildsys:
=====
Remote Username: root          Local Username: root
Remote Username: lucy         Local Username: lucy
Share: \\BUILDSYS\source
      rw /home/dev1/source
```

## More on Mounting CIFS Filesystems

In addition to the `mount` command discussed in the previous section, which was used to explicitly create a single mount, there are other methods to manage the mounting of CIFS file systems. See the reference for `mount_cifs` and `umount_cifs` in Chapter 4 for syntax details not contained in this section.

### Using */etc/fstab*

By creating entries in */etc/fstab* you can mount CIFS filesystems automatically at boot time, or mount multiple CIFS file systems on one or more CIFS Servers, with a single command entered manually. The format for such entries is:

```
server:/share mount_point cifs defaults 0 0
```

Then, to mount all CIFS entries in */etc/fstab* manually, enter:

```
$ mount -aF cifs
```

To unmount all currently mounted CIFS filesystems, enter:

```
$ umount -aF cifs
```

These commands will occur automatically, at bootup and shutdown, if the system is configured to start the CIFS Client at bootup, as explained above.

---

#### NOTE

Automounting a CIFS filesystem using the HP ONC+ AutoFS service is only supported on HP-UX release 11i version 2. For HP-UX release 11.0 and 11i, attempting mount CIFS filesystems via AutoFS may cause hung processes to remain in the system process table and may make the mount point directory inaccessible

---

### How to Mount and Login in One Step

The root user has the option to mount a CIFS filesystem and login to the CIFS Server in one step, obviating the need to explicitly issue the `cifslogin` command. Using the names from the examples above:

```
$ mount -F cifs -o username=x,password=y buildsys:/source home/dev1/source
```

where *x* and *y* are the name and password pair recognized by the server.

## **Depricated mount and unmount commands**

The `cifsmount` and `cifsumount` commands provide equivalent functionality to `mount` and `umount`, but HP discourages their use. They require different syntax and may not be available in future releases of the HP CIFS Client. `man` pages for these commands are provided in Chapter 5 of this manual for historical reasons.

---

## HP CIFS Client Files and Directories

This section lists the important files that comprise the HP CIFS Client.

**Table 2-1** HP CIFS Client Files and Directories

<b>File/Directory</b>	<b>Description</b>
<i>/opt/cifsclient/</i>	Base directory for all CIFS Client core files and administrative files.
<i>/opt/cifsclient/bin/</i>	CIFS Binaries.
<i>cifsmount</i>	Mounts CIFS Shares from CIFS Servers. Can only be used by root user.
<i>cifsumount</i>	Unmounts CIFS shares. Can only be used by root user.
<i>cifslogin</i>	For ordinary users to use the CIFS shares (already mounted), they first login to the CIFS domain/machine with their username and password (according to CIFS configuration).
<i>cifslogout</i>	User logout from the CIFS domain. Cannot use the mounted shares in the CIFS domain.
<i>cifslist</i>	Lists the mounted shares on the Client.
<i>cifsclient</i>	Start/Stop script for CIFS Client. Please refer to "Step 4: Starting and Stopping CIFS Client" for more details on this script.
<i>/opt/cifsclient/pam</i>	HP CIFS PAM files.

**Table 2-1 HP CIFS Client Files and Directories (Continued)**

<b>File/Directory</b>	<b>Description</b>
<i>/opt/cifsclient/sbin</i>	CIFS Clients for use by the administrator or root user. The CIFS Client daemon is contained in this directory.
<i>/etc/opt/cifsclient</i>	Directory for CIFS Client configuration and localization files.
<i>cifsclient.cfg</i>	Configuration file accessed by CIFS Client daemon.
<i>cifsclient.cfg.default</i>	Default configuration file. Should be copied as <i>cifsclient.cfg</i> for your use. Do not modify.
<i>/etc/opt/cifsclient/unitalles</i>	Character-mapping tables for internationalized clients.
<i>pam/smb.conf</i>	PAM configuration file. You may need to modify according to your needs. Refer to "Chapter 6: PAM NTLM" for more details on this file.
<i>pam/smb.conf.default</i>	Default PAM file. Should be copied as <i>pam/smb.conf</i> for your use. Do not modify.
<i>/var/opt/cifsclient</i>	Directory for the CIFS Client log files, <i>pid</i> files and any temporary files created for client's own use.

---

# 3

## **CIFS Security and Authentication**

This chapter provides a description for CIFS Security and Authentication Methods

## Introduction

One of the important characteristics of the CIFS file-sharing protocol is its security model. Before a user on a CIFS client can access the mountpoint of a CIFS server, the user must be authenticated by the server (the user must login to the server). Four login methods are available, they are explained in the following pages. Restrictions at the file or directory level on the server's filesystem are also enforced by the server.

In contrast, NFS relies solely upon file and directory level permissions on the server's filesystem, in conjunction with the user's UNIX uid.

## Authentication Protocols

The CIFS Client supports two authentication protocols. These protocols are configured on a global or server specific basis in the CIFS Client configuration file (*/etc/opt/cifsclient/cifscient.cfg*) by the system administrator:

- Windows NT LanManager (NTLM)

NTLM is a challenge-response strategy protocol. The server sends a challenge key to the client which the client returns to the server encrypted with the user's password. The server decrypts the key and authenticates the user. No semblance of the user's password is transmitted over the network.

- Kerberos

Kerberos is a distributed authentication service that allows a client running on behalf of a user to prove its identity to an application server without sending data across the network that might allow an attacker to subsequently impersonate the user. Kerberos is a secure, industry standard authentication protocol. It provides significant improvements over the NTLM protocol.

---

## User Authentication Methods

- Explicit Login (`cifslogin`)

Users on the CIFS Client can authenticate themselves to CIFS servers explicitly with the `cifslogin` command. Please see the `cifslogin` man page in *Commandline Utilities* Chapter.

- Automatic Login

The CIFS Client provides methods for accessing CIFS mountpoints automatically. The initial request for access to a CIFS mountpoint (`cd`, `ls`, etc.) causes the CIFS Client to log the user in, in the background. If the background login succeeds, the user's request for access succeeds, and the `cifslogin` command is not required.

The CIFS Client's automatic login policy follows:

1. Kerberos: integration with `kinit` and PAM Kerberos

If Kerberos authentication has been configured and the user has a Ticket-Granting Ticket (TGT) in the system Kerberos credentials cache (created explicitly with the `kinit(1)` command or automatically by PAM Kerberos), the CIFS Client will use the TGT to perform an automatic login. Please refer Chapter 4 for more information on using Kerberos Authentication with the CIFS Client.

2. Integration with PAM NTLM

If PAM NTLM has been configured on the system (in `/etc/pam.conf`) and the user has logged into the CIFS Client HP-UX host with PAM NTLM, the CIFS Client will attempt to reuse the user's cached PAM NTLM credentials to authenticate the user to the CIFS server. Please see Chapter 8 for more information on PAM NTLM.

3. User Database

If no PAM NTLM credentials are found, but the user has an entry in the CIFS Client user database, the CIFS Client will attempt to log the user into the CIFS server using the encrypted password in the user's database entry. You can use the `cifslogin -s` command to save an entry in the user database or

use the `cifslogout -d` command to delete an entry from the user database. Please see man pages *cifslogin*, *cifslogout* for details.

---

**NOTE**

---

Automatic login using user database is not supported with Kerberos

#### 4. Guest User

This feature enables all users on the HP CIFS Client host who are not logged into a mounted CIFS server to access the server's mountpoints, with the privileges of a guest user. Please also see the detailed information on the `guestUser` parameter in Chapter 7.

The following example explains how to set up guest user capabilities.

In this example, we use arbitrary names for users, systems, directories, and shares. You can use any legal names. Perform the following steps as `root`:

- a. In the CIFS Client configuration file, set the `guestUser` parameter to `cifsunix`:

```
guestUser = "cifsunix"
```

- b. We recommend that you set up a generic HP-UX account for this purpose. Create the user `cifsunix` on the CIFS Client HP-UX host. For security reasons, set any legal password for this user:

```
$useradd cifsunix
```

```
$passwd cifsunix
```

- c. On the CIFS server `ntsrv01`, create the user `cifsguest` with password `cifspass`, and create the share `cifspub` for some directory.

- d. On the CIFS Client host, mount the shared directory `cifspub` on the CIFS server `ntsrv01`, at the local mountpoint, `/mnt/cifs01`:

```
$ mount -F cifs ntsrv01:/cifspub /mnt/cifs01
```

e. As the HP-UX user `cifsunix`, log in to `ntsrv01` as `cifspub`:

```
$ su cifsunix -c "cifslogin ntsrv01 cifsguest -s"
```

```
Remote user cifsguest's password:cifspass
```

Now, when any other UNIX users on the CIFS Client HP-UX host who have not logged into the CIFS server `ntsrv01` try to access the mountpoint, `/mnt/cifs01`, they will automatically access it as if they were UNIX user `cifsunix` and CIFS server user `cifsguest`. The `-s` option to `cifslogin` (step e) saves the username/password pair in the CIFS Client user database. This allows all future guest users access to occur without any user having to previously invoke `cifslogin` as user `cifsunix`.



---

## **4 CIFS Authentication Using Kerberos**

This chapter provides a description for CIFS Authentication using Kerberos.

## Introduction To Kerberos

Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or only a server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal. Kerberos optionally provides integrity and confidentiality for data sent between the client and server. [Neuman, Ts'o: *Kerberos: An Authentication Service for Computer Networks*]

Kerberos was developed at the Massachusetts Institute of Technology (MIT).

Use of Kerberos in the CIFS environment provides significant security improvements over the older NT LanManager (NTLM) protocol traditionally used by CIFS Clients and Servers.

## Requirements and Limitations

### Kerberos Key Distribution Center and CIFS Servers

For this release, only Windows 2000 is supported for Kerberos authentication. Specifically, Key Distribution Centers (KDCs) and CIFS file servers that participate in Kerberos authentication with the HP CIFS Client must be Windows 2000 systems. Any other supported server platform can be used for traditional NTLM authentication.

### Tickets and Ticket Acquisition

For this release, the following ticket types are not acquired by the HP CIFS Client:

- Renewable
- Proxiable
- Forwardable

---

**NOTE**

Cross-realm authentication is not supported in this release.

---

## Using Kerberos with the HP CIFS Client

These procedures should be followed to use Kerberos with the HP CIFS Client:

- Step 1. Review fundamental Kerberos operating principals
- Step 2. Set up and verify the Kerberos infrastructure
- Step 3. Configure Kerberos in the HP CIFS Client

### Step 1. Review fundamental Kerberos Operating Principals

If you are not familiar with the fundamental features and operation of Kerberos, consult one or more of the following references.

These HP-UX resources explain the essentials of Kerberos (in the respective *Overview* chapters in each manual). This level of detail may be sufficient for most installations.

- *Configuration Guide for Kerberos Client Products on HP-UX:*  
<http://docs.hp.com/hpux/onlinedocs/T1417-90005/T1417-90005.html>
- *Installing, Configuring and Administering the Kerberos Server on HP-UX 11i:*  
<http://docs.hp.com/hpux/onlinedocs/T1417-90001/T1417-90001.html>
- *Installing, Configuring and Administering the Kerberos Server V 2.0 on HP-UX 11i:*  
<http://docs.hp.com/hpux/onlinedocs/T1417-90003/T1417-90003.html>

Other HP-UX resources can be found by searching for `kerberos` at <http://docs.hp.com>

In-depth discussion of the Kerberos protocol can be found in the following excellent documentation:

- *Kerberos: An Authentication Service for Computer Networks*, B. Clifford Neuman and Theodore Ts'o:

*<http://www.isi.edu/gost/publications/kerberos-neuman-tso.html>*

- The documentation repository at Massachusetts Institute of Technology (the developer of Kerberos):

*<http://web.mit.edu/kerberos>*

- The Kerberos specification, RFC 1510. An excellent introduction (section 1) and descriptions of message exchanges (section 3):

*<http://ftp.rfc-editor.org/in-notes/rfc1510.txt>*

- Several informative papers can also be found at the Microsoft web site. Most of these documentation also include practical information on how you should set up security in networks of Windows computers. Please search for `kerberos` or related topics at:

*<http://www.microsoft.com>*

## **Step 2. Set Up and Verify the Kerberos Infrastructure**

In order to utilize Kerberos with the HP CIFS Client, you must have a working Kerberos infrastructure on your network (completely independent of the CIFS Client) which consists of:

- A Key Distribution Center (KDC)
- At least one CIFS server that supports Kerberos and is a member of the KDC's domain (called a "realm" in the Kerberos terminology)
- At least one user principal account on the KDC
- A properly configured HP-UX Kerberos Client installation on the system running the HP CIFS Client

---

### **NOTE**

A domain name server (DNS) is recommended to be active on a Windows server on your network. CIFS servers to which you want to connect should be configured in the Windows DNS table in order to be recognized by the KDC.

---

If you are setting up a Key Distribution Center on a Windows 2000 server, consult your Microsoft documentation.

The CIFS servers to which you want to connect via Kerberos with the CIFS client must be joined to the Windows Domain. Windows online help contains information on how this can be accomplished.

If you want to set up user principals on a Windows 2000 KDC, consult online help for managing user Domain accounts.

To set up the HP-UX Kerberos client, consult the Configuration Guide cited above in step 1. The following HP-UX man pages also contain useful information: *kerberos(9)*, *krb5.conf(4)*, *kpasswd(1)*, *kinit(1)*, *klist(1)*, *kdestroy(1)*.

Once you have set up these elements of your Kerberos infrastructure, you can use the following checks to verify that everything is working. Please do not proceed to step 3 without performing this verification.

- To verify that the user principals have been set up properly on the KDC, and that the Kerberos authentication service on the KDC and the HP-UX Kerberos client can communicate properly, enter:

```
$ kinit name
```

where *name* is one of the user principals. If the operation succeeds, a Ticket-Granting Ticket (TGT) will be issued for *name*. To verify that this actually occurred, execute the *klist* command to display the contents of the ticket stored in the system Kerberos cache.

- To verify that the CIFS server has been properly configured in the KDC, execute the test program, *cifsgetttkt*, located in */opt/cifsclient/bin*:

```
$ cifsgetttkt -s server
```

where *server* is one of the CIFS servers. This command will use the TGT acquired with *kinit* to request a service ticket (ST) from the Ticket-Granting Server (TGS). Because *cifsgetttkt* is used only for testing, it does not modify the system Kerberos cache. However, it produces an informative message at the console.

If these verification steps succeed, Kerberos authentication for CIFS clients and servers should succeed. You are ready to proceed to step 3.

### Step 3. Configure Kerberos on the HP CIFS Client

The configuration parameter, *authenticationLevel*, specified in the HP CIFS Client configuration file (*/etc/opt/cifsclient/cifsclient.cfg*) indicates which mechanism should be used by the CIFS Client to authenticate users to CIFS servers. Legal entries for this parameter are *ntlm* or *kerberos*. By default, the traditional Windows NT LAN Manager (NTLM) protocol is used. The configuration setting is:

```
authenticationLevel = ntlm;
```

If you wish to use Kerberos, change the line to:

```
authenticationLevel = kerberos;
```

In this case, the CIFS Client will request the use of Kerberos when negotiating an initial connection with the CIFS Server. If the server's response is affirmative, only Kerberos is used for authenticating users to this server; otherwise NTLM is used.

## CIFS Client Kerberos Authentication Policies

This section assumes that the CIFS server and client have negotiated the use of Kerberos.

### Explicit login: `cifslogin`

Kerberos authentication is implemented transparently into this command. Required Kerberos credentials (TGT and ST) are acquired from the KDC on behalf of the user and the Service Ticket (ST) is sent to the CIFS server within a `SESSION_SETUP` request. No special action is performed by the user.

### Automatic login: Integration with System Kerberos Cache (`kinit(1)` and PAM Kerberos)

This feature allows users to access mounted CIFS servers without using `cifslogin`. If you have a pre-existing Ticket-Granting Ticket (TGT) in the system Kerberos cache, established with `kinit(1)` or PAM Kerberos, you can attempt to access the CIFS mountpoint directly (`cd`, `ls`, etc.). The CIFS Client uses the TGT to acquire a Service Ticket (ST) for the mounted CIFS server and performs a CIFS login, all in the background. It is unnecessary for you to explicitly invoke `cifslogin` in this case.

### Ticket Lifetime

Maximum ticket lifetime is controlled by the configuration of the KDC. For `cifslogin`, the CIFS client requests a lifetime of 30 days for a TGT. Thus, the actual lifetime of a TGT issued to a CIFS client is the lesser of 30 days and the configured maximum at the KDC. For automatic login, the expiration time of a user's ST is equal to the expiration time of the TGT in the system cache.

---

## Troubleshooting Kerberos in the HP CIFS Client

- `cifsTrace`

Informative log messages will be produced by Kerberos processing in the HP CIFS Client log file if the `cifsTrace log level` is enabled.

- Temporary credentials files

When Kerberos authentication is used, the HP CIFS Client utilizes a temporary file to store users' credentials during login processing. There is one temporary credentials file per user per server. Kerberos tickets are not reused by the HP CIFS Client. Hence, when the user's login processing is completed, the temporary file is removed.

If the temporary credential files are required for troubleshooting, the files can be preserved by setting the configuration variable, `rmTempKerbCredFiles`, to `no`. You can then examine and remove the files with the standard Kerberos Client utilities, `klist(1)` and `kdestroy(1)`. Use the `-c cache_filename` option with these command, specifying filenames in the following form:

```
/var/opt/cifsclient/krb5_tmp/krb5cc_servername_uid
```

where *servername* is the CIFS server and *uid* is the user's Unix uid on the local HP-UX host on which the CIFS Client is running.

As a convenience, the `cifsclient` control script can also be used to operate on these credentials files without referring to file or path names. Enter `cifsclient -h` for a syntax summary.

- Basic Kerberos functionality

If you suspect that basic functionality of your Kerberos infrastructure is not working properly, repeat the verification checks in step 2.

- If you wish to set `authenticationLevel` for specific servers to a value different from the global setting in the `defaultServer` section of the configuration file, you can create server specific options in the `servers` section. The `servers` section of the configuration file is discussed near the end of Chapter 7, and the configuration file itself contains a sample `servers` entry.



---

## **5** **Commandline Utilities**

This chapter provides details for the CIFS Client Commandline Utilities.

The HP CIFSClient software package consists of the following programs:

<code>cifsclient</code>	Stop and start the CIFS client.
<code>cifsmount</code>	Mount a directory from a remote server.
<code>cifslogin</code>	Authenticates you to the remote server. You may then use any shares already mounted by other users.
<code>cifsumount</code>	The opposite of <code>cifsmount</code> . It removes the local mountpoint and disconnects it from the server if it is not mounted somewhere else.
<code>cifslogout</code>	The opposite of <code>cifslogin</code> . You cannot use any shares from the specified server after logging out.
<code>cifslist</code>	Lists connected servers, mountpoints, mounted shares, etc.
<code>mount_cifs</code>	Mounts the CIFS filesystem.
<code>umount_cifs</code>	Unmounts the CIFS filesystem.

Each of the utilities described above also accepts the options `-h` and `-v` if given as the only parameter. The option `-h` prints a short help to standard error and the option `-v` prints the current version numbers to standard output.

---

**NOTE**

The sequence of arguments to the CIFS Client command-line utilities is significant, and it is reversed from conventional UNIX commands. For example, in:

```
cifslogin server -U user
```

the argument pair `-U user` must appear after the argument `server`.

---

---

## cifsclient

### Synopsis

```
cifsclient { command }
cifsclient fuser [-v] mountpoint [...]
cifsclient force_umount mountpoint [...]
```

### Description

This shell script is used to start and stop the HP CIFS Client, and perform other useful tasks. Only users with `root` capabilities can invoke `start`, `stop`, `restart`, `fuser`, and `force_umount` (see also the `-a` option to `klist` and `kdestroy`). Any user can invoke `status`, `klist`, `kdestroy`, and `ver.cifsclient` without any additional command is equivalent to `cifsclient start`.

### Commands

<code>start</code>	Starts the daemon.
<code>stop</code>	Shut down the daemon.
<code>restart</code>	Stop, sleep 1 second, start.
<code>status</code>	Display information about daemon.
<code>klist [-a]</code>	Display the contents of all of the invoking user's CIFS Client Kerberos credentials files. This command provides a shortcut that invokes <code>klist(1)</code> on all of the user's credentials files, automatically appending the <code>-c {filename}</code> option for each file. <code>-a</code> (recognized only for <code>root</code> ) lists entries for all users. CIFS Client Kerberos credentials files will be present on the system only if the configuration parameter, <code>rmTmpKerbCredFiles</code> , has been set to <code>no</code> . The files are located in <code>/var/opt/cifsclient/krb5_tmp</code> .
<code>kdestroy [-a]</code>	Destroy all of the invoking user's CIFS Client Kerberos credentials files, using <code>kdestroy(1)</code> . To destroy a single CIFS Kerberos credentials file, use <code>kdestroy(1)</code>

directly, specifying the `-c {filename}` option. CIFS Client Kerberos credentials files are located in `/var/opt/cifsclient/krb5_tmp`. These files will be present on the system only if the configuration parameter, `rmTmpKerbCredFiles`, has been set to `no`. `-a` (recognized only for `root`) destroys all files for all users.

`ver [-vx]`

Report version information. The following modifiers are also recognized:

`-v` Verbose: display `what(1)` strings for binaries, scripts and configuration files.

`-x` Extra: display versions of component source files. This option is useful only to HP support personnel.

`fuser [-v] mountpoint [...]`

Run `fuser -fu` (see `fuser(1M)`) against the given CIFS filesystem mountpoint and each of its subdirectories. This is useful for determining which users are accessing the mount, in the event that unmounting fails with a “Device busy” message. You must be logged into the mounted CIFS fileserver for this command to be effective. `-v` produces verbose output (all subdirectories are shown), otherwise, only directories with active user processes are shown. NOTE: The execution time for this command is proportional to the number of entries in the mounted filesystems.

`force_umount mountpoint [...]`

Forcibly unmount given mountpoints; this is an emergency procedure to be used only in case of failure of the standard `umount` commands:

```
umount mountpoint
```

or

```
cifsumount mountpoint
```

Cannot be used unless the CIFS Client is down.

## Files

*/etc/opt/cifsclient/cifsclient.cfg*

This file contains run-time configuration options for the HP CIFS Client. For detailed information see Chapter 7.

*/var/opt/cifsclient/krb5\_tmp/krb5cc\_<server>\_<uid>*

Temporary CIFS Client Kerberos credentials file. *<server>* is the name of the CIFS server to which the user has been authenticated, *<uid>* is the decimal UID of the user.

## See Also

*cifslist, cifslogin, cifslogout, fuser(1M), kdestroy(1), klist(1), mount\_cifs, umount\_cifs*

## cifsmount

You can use the *mount* command to execute the *cifsmount* command. Both commands are shown below.

### Synopsis

```
cifsmount //<server>/<share> <mountpoint> [<options>]
```

### Description

The *cifsmount* command is used to mount remote shares on the local file system. It mounts the share *<share>* from server *<server>* in the local file system at *<mountpoint>*. The mountpoint must exist. You are prompted for a password and the program uses the combination *username/password* to log in to the server. If you are already logged in to the given server, the password prompt is skipped. You can use the option *-N* to suppress password prompting.

---

#### NOTE

HP-UX does not support the SSL option.

---

### Options

*-c <clientname>*

Sets the Netbios name of client. CIFS is based on Netbios. Netbios requires that valid Netbios computer names are supplied during the connection establishment for the client and the server. The client name is usually taken from the hostname of your computer. If this does not work or if your computer's Netbios name is different, you may supply the value to be used with this parameter. This parameter is ignored if the server is already connected.

*-I <IP number>*

IP address of server. By default, the hostname of the server is taken from the server specification of the share. This must also be the Netbios host name of the server, if the server enforces correct Netbios names. HP CIFS Client uses Domain Name Server instead of Netbios to resolve server names to IP addresses. If the DNS name of the server is different from the Netbios name, you may supply the DNS name or the server's IP address with this parameter. It is ignored if the server is already connected.

`-p <portnumber>`

Sets the connection port. Netbios connections are usually made on port 139. If you want to connect on a different port, you can supply a decimal port number with this parameter. This parameter is ignored if the server is already connected.

`-r`

Mounts as read-only filesystem.

`-U <username>`

Username sent to server. By default, the HP CIFS Client accesses the server under the same user name as the login name of the user that issues the `cifs mount` command. If you have a different user name at the server, you may use this option to set that name. It is ignored if you are already logged in at the server.

`-P <password>`

Password given in commandline. Use this option only if necessary, because all commandline parameters may show up in the output of the `ps` command. It gives you the possibility to pass a dynamically generated password to the server. The password is ignored if the user is already logged in at the server.

`-S`

Reads the password from stdin. This option may be useful if you want to use `cifs mount` from a shell script or another program. The `-P` option is insecure for this purpose because the UNIX command `ps` can show the commandline parameters of running processes.

- N Do not prompt for a password. This option may be used to avoid prompting for a password if you do not have a password.
- u Enables plain text passwords. The HP CIFS Client refuses to send passwords in plain text to the server by default because this is a security risk. There are tools available that sniff the network for plain text passwords. If you really must send the password in plain text (e.g., because your server does not allow password encryption), you can enable it with this option. It is ignored if you are already logged in at the server.
- f Forces mount. When this option is used, the mount is done even if the server is not responding. No requests are sent to the server. Consequently, none of the parameters can be checked for validity.
- s Saves mount and password in database. Do not use unless you understand the security implications. HP CIFS Client can maintain a database of mounts, usernames, and passwords. This database is used at startup to re-establish stored mounts and to log in users on demand, even if you are not logged in at the client.

This option may be useful for automounting and to run programs by cron that cannot ask the user for a password. Passwords are stored in the HP CIFS Client's user database file. It is possible to get the HP CIFS hash values of the passwords (which is functionally equivalent to the passwords themselves) out of this file, although the file itself is not sufficient.

You can use this option safely only if you are the only one who has physical or root access to your machine or if you trust everyone who has this access. The HP CIFS Client does not store unencrypted passwords in the user database. If your server does not support encrypted passwords, you cannot use this option.

## Examples

The following command mounts the share `entiredisk` from the server `bigserver` at the local mountpoint `/mounts/bigserver` and stores the mount and the user/password combination in the user database.

```
cifsmount //bigserver/entiredisk /mounts/bigserver -s
```

## Files

Mounts, usernames, and passwords are stored encrypted in the HP CIFS Client's user database file. The path to the user database file can be configured in the HP CIFS Client configuration file. The default path is

```
/var/opt/cifsclient/cifsclient.udb
```

## See Also

*cifslogin, cifsumount, cifslogout, cifslist*

## cifslogin

### Synopsis

```
cifslogin <servername> [<username>] [<options>]
```

### Description

The `cifslogin` command is used to authenticate additional users at a server. Only authenticated users may access mounted files. Each user accesses the file at the server with his or her privilege status at that server. Because there must be a one-to-one (many-to-one) mapping from local users to remote user names, every user can log in only once at a given server. By default, `cifslogin` sends the user's login name to the server. If this is not desired, the username can be given in the commandline.

### Options

`-c <clientname>`

Sets the Netbios name of the client. HP CIFS is based on Netbios. Netbios requires that valid Netbios computer names are supplied during the connection establishment for the client and the server. The client name is usually taken from the hostname of your computer. If this does not work or if your computer's Netbios name is different, you may supply the value to be used with this parameter. This parameter is ignored if the server is already connected.

`-I <IP number>`

IP address of server. By default, the hostname of the server is taken from the server specification of the share. This must also be the Netbios host name of the server, if the server enforces correct Netbios names. The HP CIFS Client uses DNS instead of Netbios to resolve server names to IP addresses. If the DNS name of the server is different from the Netbios name, you

may supply the DNS name or the server's IP address with this parameter. It is ignored if the server is already connected.

`-p <portnumber>`

Sets the connection port. Netbios connections are usually made on port 139. If you want to connect on a different port, you can supply a decimal port number with this parameter. This parameter is ignored if the server is already connected.

`-P <password>`

Password given in commandline. Use this option only if you really have to, because all commandline parameters may show up in the output of the `ps` command. It gives you the possibility to pass a dynamically generated password to the server. The password is ignored if the user is already logged in at the server.

`-S`

Reads the password from stdin. This option may be useful if you want to use `cifslogin` from a shell script or another program. The `-P` option is insecure for this purpose because the Unix command `ps` can show the commandline parameters of running processes.

`-N`

Do not prompt for a password. This option may be used to avoid prompting for a password if you are already logged in at the server or if the user does not have a password.

`-u`

Enables plain text passwords. The HP CIFS Client refuses to send passwords in plain text to the server by default because this is a security risk. There are tools available that sniff the network for plain text passwords. If you really must send the password in plain text (e.g., because your server does not allow password encryption), you can enable it with this option. It is ignored if you are already logged in at the server.

- f Forces login. When this option is used, the login is done even when the server is not responding. No requests are sent to the server. Consequently, none of the parameters can be checked for validity.
- s Saves password in database. Do not use unless you understand the security implications. This option can maintain a database of mounts, username, and passwords. This database is used at startup to re-establish stored mounts and to log in users on demand, even if you are not logged in at the client.  
  
This option may be useful for automounting and to run programs by cron that have no possibility to ask the user for a password. Passwords are stored in the HP CIFS Client's user database file. It is possible to get the CIFS hash values of the passwords (which is functionally equivalent to the passwords themselves) out of this file, although the file itself is not sufficient.  
  
You can use this option safely only if you are the only one who has physical or root access to your machine or if you trust everyone who has this access. The HP CIFS Client does not store unencrypted passwords in the user database. If your server does not support encrypted passwords, you cannot use this option.

## Examples

If local user *steve* has mounted a share from server *bigserver*, local user *bill* has no access to the mounted files because he is not logged in at the server. *Bill*, who has an account on *bigserver* under his real name *miller*, can do the following to gain access:

```
cifslogin bigserver miller
```

*Bill* will be prompted for a password and if it is correct, he will be given access to the share with the same privileges that user *miller* has on *bigserver*.

## **Files**

Username and passwords are stored encrypted in the HP CIFS Client's user database file. The path to the user database file can be configured in HP CIFS Client's configuration file. The default path is

*/var/opt/cifsclient/cifsclient.udb*

## **See Also**

*cifsmount, cifsumount, cifslogout, cifslis*

## cifsumount

You can use the `umount` command to execute the `cifsumount` command. Both commands are shown below.

### Synopsis

```
cifsumount <mountpoint> [<options>]  
cifsumount -a [<options>]
```

### Description

The `cifsumount` command is used to unmount any shares mounted with *cifsmount*. Shares can only be unmounted by the user that mounted the share at the given mountpoint or the superuser. The second variant (with the `-a` option) unmounts all mounts that are currently served.

### Options

- d Delete mount from database. If the mount associated with *<mountpoint>* is stored in the user database, it is deleted from that database.
- l Logs out all users from server, if no more shares are mounted from the server (the default behaviour).
- k Keeps users logged in at the server, even if no shares are mounted.
- f Forces unmount: Avoids requests to the server (useful if the server is down).

### Files

Mounts, usernames, and passwords are stored encrypted in the HP CIFS Client's user database file. The path to the user database file can be configured in the HP CIFS Client's configuration file. The default path is:

```
/var/opt/cifsclient/cifsclient.udb
```

## **See Also**

*cifsmount, cifslogin, cifslogout, cifslist*

## **cifslogout**

### **Synopsis**

```
cifslogout <servername> [<options>]
```

### **Description**

The `cifslogout` command is used to log the user who uses the command out of the server specified. After issuing `cifslogout`, the user cannot access any files from that server unless he or she is still stored in the user database.

### **Options**

`-d`                      Deletes password from database. If the user's password is stored in the user database, it is deleted from that database.

### **Files**

Mounts, usernames, and passwords are stored encrypted in the HP CIFS Client's user database file. The path to the user database file can be configured in the HP CIFS Client's configuration file. The default path is

```
/var/opt/cifsclient/cifsclient.udb
```

### **See Also**

*cifsmount, cifslogin, cifsumount, cifslist*

## **cifslist**

### **Synopsis**

```
cifslist -A      lists servers with shares and mountpoints
cifslist -U      lists users in database
cifslist -M      lists mounts in database
cifslist -S      lists connected servers
cifslist -s <server> lists shares open at server
cifslist -u <server> lists users logged in at server
cifslist -m <share> lists mountpoints for share
```

### **Description**

The `cifslist` command is used to view internal tables of HP CIFS Client.

## mount\_cifs, umount\_cifs

Mounts and unmounts CIFS file systems.

### Synopsis

```
mount -F cifs [-ar] [-o option[,option...]] [server:/share mount_point]
umount -aF cifs | mount_point
```

### Description

The `mount` command mounts file systems. Only a superuser can mount file systems. Other users can use `mount` to list mounted file systems. Use `cifslist -A` to view CIFS-specific mounts and user connections.

The `mount` command attaches `server:/share` to `mount_point`. `server` is a remote system. `share` is a directory on this remote system and `mount_point` is a directory on the local file tree. `mount_point` must already exist, and be given as an absolute path name. It will become the name of the root of the newly mounted file system.

If `mount` is invoked without any arguments, it lists all of the mounted file systems from the file system mount table, `/etc/mnttab`.

The `umount` command unmounts currently-mounted file systems. Only a superuser can unmount file systems.

### Options

- |                      |   |
|----------------------|---|
| <code>-F cifs</code> | Filesystem-specific identifier. Always required for mounting and unmounting CIFS file systems, except for the command form <code>umount mount_point</code> .                                |
| <code>-a</code>      | Used with <code>mount</code> , mounts all CIFS filesystems that have entries in <code>/etc/fstab</code> . Used with <code>umount</code> , unmounts all currently mounted CIFS file systems. |
| <code>-r</code>      | Mounts as read-only.  |
| <code>-o</code>      | This class of options is specified with the following syntax:   |

```
-o keywrdr[,keywrdr...],keywrdr=value[,keywrdr=value...]
```

Some keywords are specified as keyword/value pairs, some are not. `-o` options must be delimited by commas; no white space is allowed. For example:

```
-o ro,username=fulton,password=pokey
```

Following are the `-o` options to *mount* supported by the CIFS Client (keywords that require values are indicated by "keyword=*value*"):

- `nbname=nbname` Set NetBios name of client. HP CIFS is based on NetBios. NetBios requires that valid NetBios computer names are supplied during the connection establishment for the client and the server. The client name is usually taken from the hostname of your computer. If this does not work or if your computer's NetBios name is different, you may supply the value to be used with this parameter. This parameter is ignored if the server is already connected.
- `ipaddr=addr` IP address of server. By default, the hostname of the server is taken from the server specification of the share. This must also be the NetBios host name of the server, if the server enforces correct NetBios names. The HP CIFS Client uses DNS instead of NetBios to resolve server names to IP addresses. If the DNS name of the server is different from the NetBios name, you may supply the DNS name or the server's IP address with this parameter. It is ignored if the server is already connected.
- `port=port` Set connection port. NetBios connections are usually made on port 139. If you want to connect on a different port, you can supply a decimal port number with this parameter. This parameter is ignored if the server is already connected.
- `ro` Mount as read-only filesystem.
- `username=name` Username sent to server. By default, the HP CIFS Client accesses the server under the same user name as the login name of the user. If you have a different

user name at the server, you may use this option to set that name. It is ignored if you are already logged in at the server.

`password=passwd` Password given in commandline. Use this option only if you really have to, because all commandline parameters may show up in the output of the `ps` command. It makes it possible to pass a dynamically generated password to the server. The password is ignored if the user is already logged in at the server.

`plaintext` Enable plain text passwords. The HP CIFS Client refuses to send passwords in plain text to the server by default because this is a security risk. There are tools available that sniff the network for plain text passwords. If you really must send the password in plain text (e.g., because your server does not allow password encryption), you can enable it with this option. It is ignored if the user is already logged in at the server.

`forcemnt` When this option is used, the mount is done even if the server is not responding. No requests are sent to the server. Consequently, none of the parameters can be checked for validity.

## Files

`/etc/mnttab` Table of mounted file systems.  
`/etc/fstab` List of default parameters for each CIFS file system.

## See Also

`mount` (1M), `umount`(1M), `cifslogin`, `cifsumount`, `cifslogout`, `cifslist`

---

## **6** **Troubleshooting and Error Messages**

This chapter includes information about problems that you may encounter when using the HP CIFS client and explanations of error

messages that might occur with HP CIFS commands.

- Troubleshooting FAQs
- HP CIFS Client Error Messages

## Troubleshooting FAQs

This section includes commonly asked questions about HP CIFS.

### How to Kill the Daemon with `cifsclient stop`

You should never kill the daemon process directly. Although HP CIFS tries to unmount all mounted shares, it may not be successful and the stale mounts will become unusable and cause problems. The correct way to do it is with `cifsclient stop`.

Refer to “Step 4, Starting and Stopping the Client” in chapter 2 in this manual for more detailed information about `cifsclient stop`.

### What to Do if the Daemon Terminates

If the daemon terminates, all shares served by HP CIFS will immediately become unusable. Every access will hang until the NFS timeout (configured in the configuration file) elapses. You can probably get away without rebooting if you immediately terminate all processes using the mounts, change all current directories from within the mounts and then use the `cifsclient force_umount <mountpoint>` command to unmount the stale mounts. Report the event to HP Technical Support and describe how the problem can be reproduced.

## HP CIFS Client Error Messages

This section contains information about HP CIFS Client error messages for the following commands:

- `cifsclient`
- `cifsmount`
- `cifslogin`
- `cifsumount`
- `cifslogout`
- `cifslist`

```
userdb: cannot open file
/var/opt/cifsclient/cifsclient.udb
```

`cifsclient` was unable to open the user database file for the reason given in the message. This is normal if HP CIFS is started the first time or if nothing has been stored in the user database so far.

```
userdb: database file is incompatible
```

`cifsclient` has found a user database file, but this file was written by a different version of HP CIFS Client. For security reasons, all versions of HP CIFS Client (even from different compiler runs) are incompatible in this respect.

```
ipccclient: error connecting to daemon: ...
```

The commandline utility was not able to connect to the HP CIFS Client daemon. The detailed unix error message is given. Most probably the daemon is not running.

```
LOC: Server can't encrypt passwords, use option to override
```

Your server does not support encrypted passwords. HP CIFS Client refuses to send passwords in clear text by default. You can override this with the `-u` option. You should be aware, however, that anyone with a network sniffer can read your unencrypted password on the network.

Almost every Unix machine can be turned into a network sniffer. HP CIFS Client also refuses to store unencrypted passwords in the user database.

```
error: DOS: Access denied
```

The username/password pair you supplied was not accepted by the server. You may try to supply the username explicitly with the `-U` option.



---

# 7

## Configuration File

The default configuration file should work without modifications. Do not modify the configuration file unless you are sure you know what you are doing.

The configuration file is parsed by the HP CIFS Client daemon at startup and when edited. Although it is re-read by the running daemon, not all configuration changes will work immediately. Most options are read into internal variables when they are used. The server configuration, for instance, is transferred into internal structures when a connection to the server is opened. Therefore, if a change to the server configuration should become active, you must first unmount all shares and log out all users from that server.

---

**NOTE**

---

SSL Options are not supported in HP CIFS.

---

## General Structure

Configuration files are built from the following simple syntactic structures:

- remarks
- strings
- arrays
- dictionaries

Strings, arrays and dictionaries are classified by the generic term "property".

Remarks can be written in three forms:

```
/* remark */
```

as in C,

```
// remark to end of line
```

as in C++ or Objective-C

```
# remark to end of line
```

as in shell scripts.

Strings are sequences of alphanumeric characters, including the underscore. If a string should consist of other characters like spaces, it must be quoted in double quotes. Within double quotes, the same escape sequences as in C strings can be used. There is no separate syntax for numeric arguments. Numeric arguments are regarded as strings and converted when used.

Arrays are ordered lists of other properties. An array is delimited by parentheses and the properties constituting the array may be separated by commas. The following example is an array consisting of several string elements:

```
(1, 2, 3, hello, "how are you")
```

Dictionaries are unordered lists of named properties. These lists are delimited by curly braces. Each dictionary entry consists of a left -hand side (key), which must be a string, an equal sign, and a right -hand side (value) which may be any property. Entries may be separated by

semicolons. The following is an example of a dictionary consisting of three entries named `property1` to `property3`; where the first one has a string value, the second an array value, and the third a dictionary value:

```
{
    property1 = "value of property1";
    property2 = (value, of, property2);
    property3 = {
        firstWord = value;
        secondWord = of;
        thirdWord = property3;
    };
}
```

The configuration file itself is a dictionary (the surrounding curly braces are optional because other properties are not allowed). The keys at the top level are the names of the configuration variables.

Properties that have been parsed as strings may be interpreted in one of the following ways:

- string
- number
- enumeration
- boolean

String needs no further explanation. Numbers are interpreted in decimal, unless they are prefixed with `0` (meaning octal), or `0x` (meaning hexadecimal). Enumerations are strings from a predefined set of strings. Boolean variables are a special case of enumeration where the set consists of the strings `yes` and `no`.

---

## Configuration Variables

The following is a list of all variables that may be configured at the top level:

### **logLevels**

The value of this variable is an array enumerating all logging modes that are active. A logging mode is a string out of the following set:

info

[0] Logging of informational messages. Should be turned on.

error

[1] Logging error messages. Should be turned on.

debug

[2] General debug messages. Used only during debugging.

resource

[3] Messages about allocation and deallocation of objects. Used only during debugging.

netbiosError

[4] Logging error messages from the Netbios layer. Should be turned on, unless too many errors occur. This is separated from general error logging because not all of Netbios is implemented in HP CIFS Client, and the unimplemented features result in Netbios error messages.

netbiosDebug

[5] Debug messages from the Netbios layer. Used only during debugging.

netbiosTrace

[6] Generates hex-dumps of all outgoing and incoming Netbios traffic. This is very useful during debugging but should be turned off for normal operation.

nfsTrace

[7] Provides detailed information about all NFS requests done by the kernel and the respective return values. It is very useful for debugging NFS but should be turned off for normal operation.

rare

[8] Logging of rare conditions. Used only during debugging.

cacheDebug

[9] Debugging of the cache's operation. Used only during debugging.

cifsTrace

[10] Logging of all CIFS commands issued and the respective return values. Very useful together with netbiosTrace for debugging, but should really be turned off during normal operation.

oplock

[11] Debugging of opportunistic lock mechanism. Used only during debugging.

warn

[12] Warnings of any kind, mostly used by the configuration file parser. Should be turned on.

smbSequence

[13] Debugging messages about the order of HP CIFS requests and the respective messages. Used only during debugging.

debugAttributes

[13] Debugging of file attribute routines. Useful only during debugging.

The numbers in square brackets which precede the descriptions are used to denote messages of the respective logging mode in the logging output.

- cfgParseInterval** HP CIFS Client can reparse the configuration file while running. For this feature to work, the HP CIFS Client must poll the file regularly. The variable *cfgParseInterval* defines the time of this poll cycle in milliseconds. If it is set to 0, the file is only parsed once during startup. The default is 0.
- sockMode**  
**sockOwner**  
**sockGroup** File access mode and ownership for the UNIX domain socket that is used for communication between the HP CIFS Client daemon and the commandline utilities. The access mode may be given in octal notation, if prefixed with a leading 0; in hexadecimal notation if prefixed with a leading 0x; or in decimal notation if not prefixed with any of the above. Owner and group may be given by name or as numeric id. Do not set these values to anything other than *mode=0600* and *owner=root* unless you really know what you are doing. The file access modes of this UNIX domain socket are used to provide secure authentication of the user that requests a service to the daemon. If these variables are not configured from the file, they default to the correct values.
- runAsUser** The HP CIFS Client daemon must be started as root. To improve security, it switches to a different user-id if root privileges are not needed. The user id used for this purpose can be configured with this value. It may be either a user name or a numeric id.
- pidFile** HP CIFS Client can maintain a file with the process id of the daemon, if desired. If this variable is defined, it is interpreted as the path of the file where the pid should be stored. If it is not defined, no such file is created.
- databaseFile** This variable configures the path to the user database file. It stores passwords, mounts, and the registration key. The default is */var/opt/cifsclient/cifsclient.udb*.
- allowSaving** This boolean variable defines whether user passwords and mounts may be stored in the user database. Setting it to *no* disables storing. The default is *yes*.

**caseConvertFile** This variable configures the path to the case conversion table. This file defines the mapping to upper and lower case for all unicode characters. The default is to use no table file and retain the default ISO 8859-1 mapping. A mapping file derived from the Unicode standard is part of the HP CIFS Client distribution. You can find it at *unitables/unicase.cfg*.

#### **serverCharMapFile**

This variable configures the path to the character mapping file for the server. This file is only used when client and server do not agree on using Unicode. It defines the mapping from the internal Unicode representation to the ASCII strings sent to the server (and vice versa). The default is a codepage 437 mapping, which is the US-Latin DOS character set. Mapping files for various character sets are distributed with HP CIFS Client in the directory *unitables*.

#### **clientCharMapFile**

This variable configures the path to the character mapping file for the client. This file defines the mapping from internal Unicode representation to the ASCII strings seen at the client. Together with the *serverCharMapFile*, any conversions between server and client character code can be accomplished. These tables can be used to compensate for vendor-specific character sets and to cope with various national character sets such as JIS and ShiftJIS for Kanji, etc. The default is ISO 8859-1 mapping.

#### **uniTableCompressBlocks**

This integer variable customizes the compression of the Unicode table. A higher value reduces conversion speed but improves memory efficiency. Values higher than the number of contiguous unused code blocks have no effect. The default is 3.

**nfsSockRxBuf** This integer variable sets the receive buffer size of the socket used to communicate with the kernel. If the value given is out of the acceptable range for your

machine, the HP CIFS Client automatically limits the range. Increase the buffer size if you have extremely slow writes.

**nfsSockTxBuf** This integer variable sets the transmit buffer size of the socket used to communicate with the kernel. It is not necessary to set an explicit buffer size.

**nfsTransferSize** This integer variable defines the maximum block size used in data transfer between the kernel and HP CIFS Client. The maximum allowed value is 8k (8192). It may be necessary to reduce the value if the NFS socket has frequent overflows, as it may be the case with AIX 3.x. It is useful to use only powers of 2 as block sizes. The default is 8192.

**scopeID** This string variable defines the Netbios name scope of the client. If it is not defined, no scope ID is used. If you do not know what a scope ID is, you do not need one.

#### **rmTmpKerbCredFiles**

When kerberos authentication is used, the CIFS Client utilizes a temporary file to store users' credentials during login processing. There is one temporary credentials file per user per server. Kerberos tickets are not reused by the CIFS Client, thus when the user's login processing is complete, the temporary file is removed. If required for troubleshooting, the files can be preserved by setting this variable to "no". The files are located in */var/opt/cifsclient/krb5\_tmp*.

**defaultServer** The baroque structure of CIFS has its mirror in the multitude of configuration options for CIFS connections. This variable defines a default behavior which can be overridden by specific configurations for each server. The value is a dictionary with the following keys:

localNetbiosName

This entry can be used to set the Netbios name for the client that is sent to the server.

<code>mtabName</code>	<p>This string variable defines the hostname used in mount table entries and in the output of <code>mount (1M)</code> and <code>bdm (1M)</code>. If it is set to the null string:</p> <pre>mtabName = " "</pre> <p>the entry is displayed in the standard UNIX format for mounted filesystems.</p>
<code>connectTimeout</code>	<p>This integer variable defines the maximum time in milliseconds that is waited for a connection to succeed. You probably have to increase the time if you are on a slow network. The default is 2000ms (2 seconds).</p>
<code>requestTimeout</code>	<p>This integer variable defines the maximum time in milliseconds a server response may take (if the connection is already established). The default is 60000ms (60 seconds).</p>
<code>authenticationLevel</code>	<p>This entry specifies the method that the HP CIFS Client should use to authenticate users to the CIFS server. Allowed values are <code>ntlm</code> or <code>kerberos</code>. If the value is set to <code>ntlm</code>, only the NTLM protocol will be used for logins to the server. If the value is set to <code>kerberos</code>, then if the server supports Kerberos, only Kerberos will be used for logins. Otherwise, NTLM will be used.</p>
<code>nfsTimeout</code>	<p>This integer variable defines the initial timeout in 1/10 seconds that is used by the kernel when it requests data from HP CIFS Client. This value is doubled on each retry. Together with <code>nfsRetransmit</code>, this defines the</p>

absolute timeout for NFS requests. A value of 50 (5 seconds) avoids frequent retries of already running (slow) requests and ensures a total timeout of about 2 minutes. This should be sufficient even for the slowest devices and links. If you use a jukebox, it may also be necessary to increase *requestTimeout*.

**nfsRetransmit** This integer variable defines the number of retries the kernel attempts when HP CIFS Client does not reply in time. The timeout starts with *nfsTimeout* and is doubled on each retry. Retransmissions should not be necessary, because HP CIFS Client should not lose any requests. However, if your system's NFS client puts high loads on NFS servers and has small maximum socket buffer sizes, requests can get lost due to buffer overflows. A value of 5 (which is also the default) should be a good choice. You may want to experiment with *nfsTimeout* to get the optimum performance even with frequent buffer overflows.

#### **nfsAttributeCaching**

A boolean variable that can enable file-attribute caching by NFS, effectively overriding the CIFS client's attribute cache). This improves performance of certain types of operations (such as creating *tar(1)* archives of large numbers of files residing on mounted CIFS filesystems), by reducing the number of get attribute calls sent over the network. The default setting is no.

**lookupStrategy** As you probably know, the HP CIFS Client maps between NFS requests and SMB/CIFS requests. On the NFS side, files are referenced by unique identifiers, called NFS file handles. On the HP CIFS side, files are referenced simply by their path. The HP CIFS Client must be able to determine the path given to an NFS file handle. There are two strategies available to do this:

- **pseudoInode**

This strategy derives the NFS file handle as a hash value from the path. The hash is chosen in a way that makes efficient lookups possible, as long as the depth of the file in the directory hierarchy is lower than 27. The advantage of this strategy is the low memory consumption: Files can be looked up on demand, nothing has to be stored. The main disadvantage is that NFS file handles change when files are renamed. This leads to a conflict with Unix semantics when open files are renamed: After renaming, the handle of the open file is stale and the file can not be accessed without reopening. It also conflicts with a bug in the caching code of the Solaris NFS client where the writeback occurs only after closing the file, not during closing the file.

- **database**

In this strategy all NFS file handle to file path relations are stored in an internal database.

This is the most secure and most compatible approach. The disadvantage is that all this information must be kept in memory. The HP CIFS Client needs about 500kB more real memory and about 10MB more virtual memory for each share that uses this strategy.

The *database* strategy is the default.

- caseSensitive** This is a boolean variable (possible values *yes* or *no*) which specifies whether filenames on the server are case sensitive. By default, they are case sensitive in order to be consistent with the UNIX file system. If you use a case mapping different from *none* (see next parameter), you must set this parameter to *no*.
- caseMapping** This variable (of type enumeration) defines whether file names are mapped to all upper case (*upper*), all lower case (*lower*) or preserved as they are on the server (*none*).
- capitalizeShares** This boolean variable defines whether share names are converted to all uppercase characters before a connection is attempted. Share names should be case insensitive, but Windows 95 does not accept lowercase names. If this option occurs in section *serverClasses*, it can override a *no* to a *yes*, but not a *yes* to a *no*. The default is *yes*.
- useUnicode** This boolean variable specifies whether the HP CIFS Client will use Unicode if the server supports it.

**domain** This string variable defines the domain name the client sends to the server. If undefined, it defaults to an empty string which should be suitable for all known servers.

**alwaysEncryptData**

If this boolean variable is set to *yes*, only SSL (Secure Socket Layer) connections with the server are accepted. If set to *no*, SSL is negotiated with the server.

**guestUser**

The *guestUser* configuration solves the following problem: each UNIX user must be logged in at the server (be mapped to a CIFS username/password pair) in order to access anything, even if the share is public. It may be impractical to log in each user if there is a large number of Unix users who want to access a public share where access permissions are not important. If you define a *guestUser*, all Unix users that are not logged in are treated as if they were the given Unix user. The UNIX user named in *guestUser* should be logged in, of course, e.g. with the *-s* option to *cifsmount* or *cifslogin*.

**fakeMountpointDate**

If this boolean variable is *yes*, the modification and access times of the mount point always read the current time. This is useful for servers that return bogus values for the modification dates of root directories, such as Windows NT or Windows 95. The default is *no*.

`execMapping` This enumeration variable is useful for files stored on Windows servers. It defines which DOS attribute should be mapped to the UNIX *execute* permission. The following keywords are valid: `archive`, `system`, `hidden`, `on`, or `off`. Default is *on*. A side-effect of *execMapping* is that if the configured attribute is set on the NT server, the file will be listed on the UNIX Client with the execute bit set for all users (`owner`, `group`, and `other`).

---

**WARNING**

**If you plan to store UNIX executables on an NT server and invoke them on a UNIX Client, then the default setting *execMapping = on* is required. In this case, as seen by the UNIX Client, the execute bit is set on *all* file listings from the Windows server. Using *execMapping = on* will not affect the attributes of files on HP CIFS Servers; those will still behave like normal UNIX files.**

`execInvert` When this boolean variable is *yes*, the execute bit (as derived with the *execMapping* setting) is inverted.

`dirDefaultLinks` If the server does not supply a number of hard-links for directories, this number is used. The value defaults to 2, if not specified. Some implementations of the UNIX utility `find` determine whether recursion is necessary or not from the link count. If your `find` uses this optimization, you may want to fake a high number

of links for directories. Alternatively you can switch off the optimization with a commandline switch to find.

**enableFakeLinks** If this boolean variable is set to *yes*, the HP CIFS Client can do softlinks on Windows-servers. These softlinks can be used by the HP CIFS Client clients only. On the Windows server they look like ordinary files with special attributes set (*system* and *hidden* attributes, if you have not modified the configuration).

**linkModeMask, linkMode**

These two integer variables define the file attributes that are used to distinguish faked softlinks from ordinary files. *linkModeMask* is 7 by default, which means that the attributes *read-only*, *hidden* and *system* are taken into account. *linkMode* defines the actual state that these attributes must have. It is 6 by default, which means that *hidden* and *system* must be set, but not *read-only*. The configuration value is calculated as the sum of the following components:

**Table 7-1**

1	read-only	2	hidden	4	system	32	archive
---	-----------	---	--------	---	--------	----	---------

**linksAreUnicode** If this boolean variable is set to *yes*, the HP CIFS Client stores faked links in Unicode format on the server. This is incompatible with the *CygWin32* format for symbolic links, but allows lossless storage of client paths. If it is set to *no*, symbolic links are more or less compatible to those of *CygWin32* on Windows, but a conversion to the

server character set is performed. Regardless of this variable, the HP CIFS Client can read symbolic link files in both formats.

**attributesCacheTime**

File attributes are cached for this amount of time (in milliseconds).

**dirCacheTime** Directory contents are cached for this amount of time (in milliseconds).

**maxCachedFiles** This is the maximum number of file objects that are held as cache of NFS file handles. If an NFS file handle is requested which is not in the cache, it must be looked up recursively, which may result in a notable performance loss. Recursive lookups are logged as rare events.

**maxOpenFiles** This is the maximum number of files that will be kept open at the server.

**dataCacheSize** This is the size of the data cache that is allocated for open files in bytes. The value is rounded to a multiple of the cache's page size, which is derived from the maximum transferable size. The page size will always be a power of two.

**closeDelay** This variable defines the time a file is kept open when it is not used. The value is a dictionary with the following keys:

**exclusiveLock**

The keep-open time in milliseconds if an exclusive *oplock* has been acquired.

**batchLock**

The keep-open time in milliseconds if a batch *oplock* has been acquired.

noLock

The keep-open time in milliseconds if no lock has been granted.

dataCacheTimeNoLock

If no *oplock* has been granted, no caching should be done. This might result in bad performance on servers that do not support *oplocks*. This value sets a cache-valid time (in milliseconds) that is used if no *oplock* was granted.

readAhead

This variable defines the number of cache pages to read ahead. It is a dictionary with the following keys:

lock

The number of pages to read ahead if an *oplock* was granted.

noLock

The number of pages to read ahead of no *oplock* was granted.

useWriteBack

This variable defines whether cache write-back techniques should be used. Write back is insecure (in terms of error recovery) if used with NFS2, but it may increase performance notably. The value is a dictionary with the following keys:

lock

Boolean value which configures whether write back should be used when an *oplock* has been granted.

noLock

Boolean value which configures whether write back should be used when no *oplock* has been granted.

If you care about reliability, always leave these options off. This configuration variable is also passed to the server. There are server/OS combinations (notably Samba/Linux) which become very slow in write-through mode. You may want to configure write back for these.

**requestOplock** This boolean variable defines whether oplocks should be requested from the server. It should be set to `no` for Windows95 machines because they grant an *oplock* although there is no support for it.

**closeForSetattr** This boolean variable defines whether files should be closed before attributes (write protection, modification dates) are changed. This is very useful for Windows 95 servers because these servers can not set the attributes of open files. However, with this feature enabled, the UNIX semantics mapping does not work completely. The default is `no`.

**disableSmbs** Not every server supports every SMB command equally well. In fact, many commands are unusable on certain server types. The value of this variable is an array which enumerates the SMB commands that should not be used. The respective commands will be replaced by a workaround automatically. The enumeration constants may be taken from the following set:

`getattrFind`

Suppresses the use of the *trans2/findfirst2* command for reading file attributes.

*trans2/findfirst2* is the best way to query attributes, so only disable it if you need to.

getattrTrans2QueryPath

Suppresses the use of the *trans2/query\_pathinfo* command for reading file attributes.

*Trans2/query\_pathinfo* seems to be broken on Windows 95.

attrUnix

Disables the UNIX extensions for file attributes.

setattrTrans2SetFile

Suppresses the command *trans2/setfileinfo* to be used for setting file attributes. This SMB command does not work properly on NT.

setattrTrans2SetPath

Suppresses the command *trans2/setpathinfo* to be used for setting file attributes. This SMB command does not work properly on NT.

setattrSetFile2

Suppresses the use of *SET\_INFORMATION2* for setting attributes.

setattrCoreWithTime

Suppresses the use of the core *SET\_INFORMATION* command for setting modification dates.

createOpenX

Suppresses the use of *SMB\_COM\_OPEN\_ANDX* for creating files.

openOpenX

Suppresses the use of *SMB\_COM\_OPEN\_ANDX* for opening files.

readReadX

Suppresses the use of *SMB\_COM\_READ\_ANDX* for reading files.

readOpenRead

Suppresses the use of *SMB\_COM\_OPEN\_ANDX* batched with *SMB\_COM\_READ\_ANDX* for reading files.

writeWriteX

Suppresses the use of *SMB\_COM\_WRITE\_ANDX* for writing files.

writeOpenWrite

Suppresses the use of *SMB\_COM\_OPEN\_ANDX* batched with *SMB\_COM\_WRITE\_ANDX* for writing files.

findUnix

Disables the CIFS UNIX extensions for reading directories.

findTrans2

Disables the use of *trans2/find* for reading directories.

fsinfoTrans2

Suppresses the use of *trans2/query\_fs\_info* for reading file system infos.

`sessionSetup`

Suppresses the session setup command (only used for core dialect).

`treeconAndX`

Suppresses the *TREE\_CONNNECT\_ANDX* command (*TREE\_CONNECT* is used instead).

`setDirDates`

Suppresses setting directory modification dates when files are created or deleted in a directory. This may be useful if the server sets the date automatically when directories are modified.

## **servers**

This variable may modify the values configured with *defaultServer* for specific servers. It consists of a dictionary where the keys are the Netbios names of servers. The value for each server key is also a dictionary. This dictionary has the same structure as the *defaultServer* dictionary. In addition, the following keys may be used:

**ipAddress** This entry may contain an IP address or a DNS name for the server. By default, the Netbios name is used for a DNS query. This parameter may be overridden from the `cifsMount` commandline.

**netbiosName** This entry is a last chance to change the Netbios name that is sent to the server for a given server.

tcpPort	You may change the TCP port that is used to connect to the server here. Default is 139, the Netbios session service port.
<b>serverClasses</b>	This variable may modify the values configured with <i>defaultServer</i> and <i>servers</i> after the connection has been established based on the information derived from session setup. The decision can depend on the server's operating system and LAN manager type. The format for this variable is an array of dictionaries. Each dictionary must have all of the following three keys:
OS	This entry contains a matching pattern in shell style syntax (* matches any character sequence, ? matches one character, [<characters>] matches any of the given characters and [^<characters>] matches none of the given characters). It is matched against the operating system name derived from session setup.
LanManager	This entry also consists of a matching pattern in shell- style syntax. It is matched against the LAN manager name derived from session setup. The operating system name and LAN manager name are printed to <i>syslog</i> if log level <i>info</i> is enabled.
config	If the previous two patterns match, the content of this variable (which must be a dictionary) is used as a server configuration which may contain all definitions that <i>defaultServer</i> may contain. If an option is given, it overrides the respective option from the other configurations. The option <i>disableSmb</i> s is an exception: all disabled SMBs add up to give the final list of disabled SMBs.

The array is searched from the first to the last entry. If an entry matches, the corresponding configuration is used and the search is aborted.

---

## **8** **PAM NTLM**

This chapter provides a description of PAM NTLM.

## Introduction

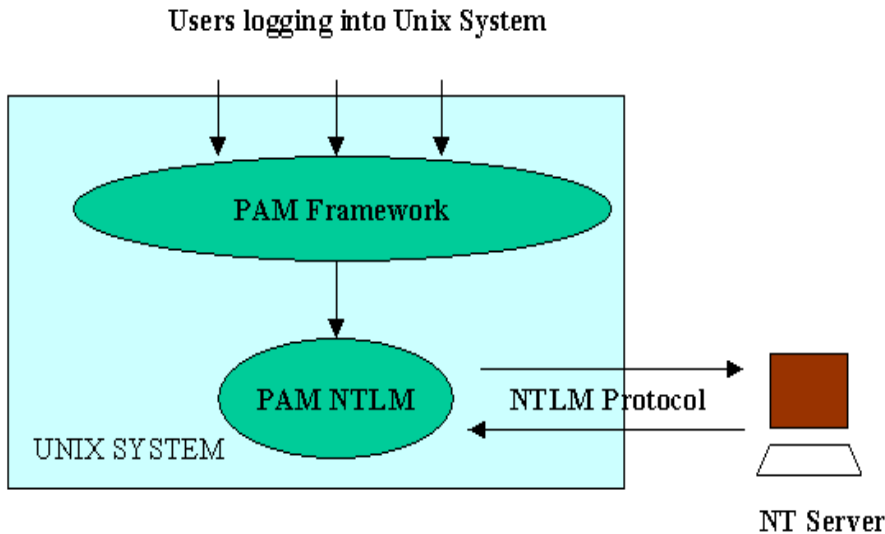
PAM NTLM ( NT Lan Manager) is a Pluggable Authentication Module (PAM) that enables HP-UX users to be authenticated against Windows servers during system login.

PAM is an authentication framework in UNIX, used to authenticate users logging into a UNIX system. PAM loads a dynamically loadable module (shared library) that performs the actual authentication. PAM can also be configured to use multiple shared library modules.

PAM NTLM uses NT servers to authenticate users logging into an HP-UX system. In other words, PAM NTLM uses the NT LanManager protocol to authenticate the UNIX users. It sends the UNIX user's name and password to the NT server for validation and returns the result to the PAM framework. The HP CIFS client uses the PAM NTLM authentication information to access the shares on the HP CIFS server. Thus, users logging into an HP-UX system can access CIFS-mounted file systems without having to use the *cifslogin* command.

Configuring PAM NTLM requires you to understand the PAM framework in general. Refer to *pam(3)*, *pam.conf(4)*, and *Managing Systems and Workgroups* at <http://docs.hp.com/hpux/os> for more information about PAM.

**Figure 8-1 PAM Introduction**



PAM NTLM is a dynamically loadable Module. PAM Framework passes user name and password to the PAM NTLM module, which uses the NTLM protocol to authenticate against a Windows server.

## PAM NTLM

This section provides a list of PAM NTLM features and a description of the User Map File.

### PAM NTLM Features

- PAM NTLM supports authentication and password management.
- PAM NTLM uses a subset of the Samba *smb.conf* file as its configuration file. See the PAM NTLM Post-installation Instructions below for further information.
- PAM NTLM supports *username mapping* to map a local UNIX user name to a remote NT domain user name to use for authentication. See the PAM NTLM Configuration section for more detailed information.
- Successful user/password authentications are cached for use by the CIFS client.
- Login authentication to CIFS Servers using NTLM encrypted passwords.
- Updating CIFS user passwords on NT 4.0 Primary Domain Controller (PDC) using the HP-UX *passwd(1)* command.

Refer to Chapter 2 for installation steps.

### User Map File

PAM NTLM supports a *user map file* that maps UNIX user names to NT domain user names before authentication by the CIFS server. PAM NTLM will search the user map file for the UNIX user name. If found, the mapped NT domain user name will be used to authenticate the user on the CIFS server. You must enter the correct password for the mapped NT user in order to be authenticated.

If you configure *password(1M)* to use PAM NTLM, then the password of the mapped NT domain user will be changed on the NT server.

## PAM NTLM Configuration

Configure the following to set up PAM-NTLM:

- The PAM-NTLM module
- The system file */etc/pam.conf* to use the PAM-NTLM module
- A usermap file (optional)

### Configuring the PAM NTLM Module

The PAM-NTLM configuration file is */etc/opt/cifsclient/pam/smb.conf*. A default configuration file is also provided (*smb.conf.default*). Do no change the default configuration file because you may need to refer to it in the future.

**Table 8-1**

```
##
## Name: smb.conf
##
## Set the values below to the actual names used in your environment
##
## Any line which starts with a semi-colon(;) or a hash(#)
## is a comment and is ignored.
##
##===== Global Settings =====
[global]

## workgroup: NT-Domain-Name or Workgroup-Name
workgroup = workgroup

## password server: the netbios name of the system which will be
## used to authenticate logins.
password server = pdc_name bdc1_name bdc2_name

## wins server: the system used to locate password servers,
## specified as a fully-qualified DNS name or an IP address.
wins server = winserv.mycorp.com
```

## Configuring the system to use the PAM NTLM Module

This task consists of editing the global HP-UX PAM configuration file `/etc/pam.conf`.

---

### IMPORTANT

You may not be able to log into the system if PAM is not correctly configured. Make sure that you understand the PAM framework before you modify `pam.conf`. For information on PAM, see these sections of HP-UX manpages: `pam.conf(4)`, `pam_unix(5)`.

For security reasons, HP strongly recommends you set up your system such that, for both authentication and password change, the host system (PAM UNIX), not the password server configured by PAM NTLM, authenticates root and other privileged users. Access on a per-user basis can be controlled through the use of `libpam_updbe` in `pam.conf`, and the `ignore` option to `libpam_ntlm` in `pam_user.conf`. See `pam.conf(4)`, `pam_user.conf(4)`, and `pam_updbe(5)` for explanations and examples of usage.

HP also recommends using PAM NTLM services in addition to, not in place of, PAM-UNIX. This configuration is depicted in the sample `pam.conf` file below.

---

PAM NTLM provides the following services:

- Password Authentication
- Password Change
- Password Change Upon Notice of Expiration

Each service corresponds to a specific section of `pam.conf`. Add entries for the services you wish to use:

- For Password Authentication, modify the Authentication management section of `pam.conf`.
- For Password Change, modify Password management.
- For Password Change Upon Notice of Expiration, modify Authentication management, Password management, and Account management (in order to utilize Password Change Upon Notice of expiration, you must also enable both Password Authentication and Password Change).

The following are sample *pam.conf* files with all three PAM NTLM services configured. Each PAM NTLM entry consists of a line that refers to the shared library *libpam\_ntlm.1*. In the authentication management section, when PAM NTLM is used in conjunction with PAM UNIX, it is recommended that the option *try\_first\_pass* be specified with the PAM-UNIX entry, as shown.

---

**WARNING**

**If incorrect paths are used in *pam.conf*, it can become impossible to login to the system. Ensure that you refer to the *pam.conf* file that matches the version of HP-UX installed on your system (use `uname -r` to check the version). In particular, you should add lines to *pam.conf* exactly as shown *without modifying paths*. Starting with versions B.11.22 of HP-UX, paths to the PAM libraries are different than in earlier versions.**

---

The following sample *pam.conf* file is for version B.11.22 of HP-UX:

**Example 8-1**

**Sample file for HP-UX version B.11.22**

```

=====
#
# PAM configuration
#
# Authentication management
# Note: For PA applications, /usr/lib/security/libpam_unix.so.1 is a
# symbolic link that points to the corresponding PA PAM module.
#
#
login    auth sufficient  /usr/lib/security/$ISA/libpam_ntlm.so.1
login    auth required    /usr/lib/security/$ISA/libpam_unix.so.1 try_first_pass
su       auth required    /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  auth required    /usr/lib/security/$ISA/libpam_unix.so.1
dtaction auth required    /usr/lib/security/$ISA/libpam_unix.so.1
ftp      auth required    /usr/lib/security/$ISA/libpam_unix.so.1
OTHER    auth required    /usr/lib/security/$ISA/libpam_unix.so.1
#
# Account management
#
login    auth sufficient  /usr/lib/security/$ISA/libpam_ntlm.so.1
login    account required /usr/lib/security/$ISA/libpam_unix.so.1
su       account required /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  account required /usr/lib/security/$ISA/libpam_unix.so.1
dtaction account required /usr/lib/security/$ISA/libpam_unix.so.1
ftp      account required /usr/lib/security/$ISA/libpam_unix.so.1
#
OTHER    account required /usr/lib/security/$ISA/libpam_unix.so.1
#
# Session management

```

## PAM NTLM

### PAM NTLM Configuration

```
#
login    session required    /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  session required    /usr/lib/security/$ISA/libpam_unix.so.1
dtaction session required    /usr/lib/security/$ISA/libpam_unix.so.1
OTHER    session required    /usr/lib/security/$ISA/libpam_unix.so.1
#
# Password management
#
login    auth sufficient     /usr/lib/security/$ISA/libpam_ntlm.so.1
login    password required   /usr/lib/security/$ISA/libpam_unix.so.1
passwd   password required   /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  password required   /usr/lib/security/$ISA/libpam_unix.so.1
dtaction password required   /usr/lib/security/$ISA/libpam_unix.so.1
OTHER    password required   /usr/lib/security/$ISA/libpam_unix.so.1
=====
```

The following sample *pam.conf* file is for versions B.11.00 and B.11.11 of HP-UX:

#### Example 8-2

#### Sample file for HP-UX versions B.11.00 and B.11.11

```
#
# PAM configuration
#
# Authentication management
#
login    auth sufficient     /usr/lib/security/libpam_ntlm.1
login    auth required       /usr/lib/security/libpam_unix.1 try_first_pass
su       auth required       /usr/lib/security/libpam_unix.1
dtlogin  auth required       /usr/lib/security/libpam_unix.1
dtaction auth required       /usr/lib/security/libpam_unix.1
ftp      auth required       /usr/lib/security/libpam_unix.1
OTHER    auth required       /usr/lib/security/libpam_unix.1
#
# Account management
#
login    account required    /usr/lib/security/libpam_ntlm.1
login    account required    /usr/lib/security/libpam_unix.1
su       account required    /usr/lib/security/libpam_unix.1
dtlogin  account required    /usr/lib/security/libpam_unix.1
dtaction account required    /usr/lib/security/libpam_unix.1
ftp      account required    /usr/lib/security/libpam_unix.1
OTHER    account required    /usr/lib/security/libpam_unix.1
#
# Session management
#
login    session required    /usr/lib/security/libpam_unix.1
dtlogin  session required    /usr/lib/security/libpam_unix.1
dtaction session required    /usr/lib/security/libpam_unix.1
OTHER    session required    /usr/lib/security/libpam_unix.1
#
# Password management
```

```
#
login      password sufficient /usr/lib/security/libpam_ntlm.1
login      password required  /usr/lib/security/libpam_unix.1
passwd     password required  /usr/lib/security/libpam_ntlm.1
dtlogin    password required  /usr/lib/security/libpam_unix.1
dtaction   password required  /usr/lib/security/libpam_unix.1
OTHER      password required  /usr/lib/security/libpam_unix.1
```

## Configuring a User Map File

To configure PAM NTLM to use the user map file, add the following line to the [Global] section of the `/etc/opt/cifsclient/pam/smb.conf` file:

```
Domain user map = /etc/opt/cifsclient/pam/domain_user.map
```

You can configure the name and location of the user map file. For name and location, HP recommends the line as shown above.

The format of a domain user file entry is:

```
UNIXusername = [\\DOMAIN_NAME\\] DomainUserName
```

`UNIXusername` is an existing account on the HP-UX system;  
`DomainUserName` is the name of the user that is mapped in the NT domain. `DOMAIN_NAME` is optional.

The user map file is parsed line by line. If any line begins with a `#` or `a;` then the line is ignored. Each line should contain a single UNIX user name on the left and then a single NT Domain User name on the right, separated by a tabstop or '='. If either name contains spaces then you must enclose it in quotes.

## Using NIS Distribution of the User Map File

The user map file is enabled to be distributed via NIS in a similar manner to the distribution of `/etc/passwd` to NIS clients.

To use this feature:

1. Convert the master user map file into an NIS map file named *domainusermap.byname* on the NIS master server.

---

**NOTE**

The NIS map file name *domainusermap.byname* is the default name that PAM NTLM uses for the NIS map file. You can configure a different NIS user map name in the PAM NTLM configuration file (*/etc/opt/cifsclient/pam/smb.conf*) of each NIS client. The configuration option is:

`nis ntuser mapname = <new usr map filename>`

---

2. In the user map file of each NIS client that will receive the distributed map file, add an entry with the plus sign (+) in the first column of the line. The plus sign is used to indicate that parsing the file should stop at that point and the remaining search of the user map file should use NIS calls to the NIS server.

---

## Glossary

### A

**ACL** Access Control List, meta-data that describes which users are allowed access to file data and what type of access is granted to that data. ACLs define access rights. In this scheme, users typically belong to "groups," and groups are given access rights as a whole. Typical types of access rights are read (list), write (modify), or create (insert). Different file systems have varying levels of ACL support and different file systems define different access rights. For example, DOS has only one set of rights for a file (since only one user is considered to use a DOS system). A POSIX 6-compliant file system allows multiple rights to be assigned to multiple files and directories for multiple users and multiple groups of users.

**Authentication** Scheme to ensure that a user who is accessing file data is indeed the intended user. A secure networked file system uses authentication to prevent access occurring from someone pretending to be the intended user.

### C

**CIFS** Common Internet File System, a specification for a file access protocol designed for the Internet.

**Credential** A piece of information that identifies a user. A credential may be as simple as a number that is uniquely associated with a user (like a social security number), or it may be complicated and contain additional identifying information. A strong credential contains proof, sometimes called a verifier, that the user of the credential is indeed the actual user the credential identifies.

### E

**Encryption** Encryption ensures that data is viewable only by those who possess a secret (or private) key. Encrypted data is meaningless unless the secret key is used to decrypt the data. Encryption and decryption of data is called ciphering.

### K

**Kerberos** An authentication and authorization security system developed by MIT and the IETF working group. It is based on secret key technology, and is generally easier to manage than a public key infrastructure because of its centralized design. However, Kerberos is not as scalable as a public key infrastructure.

### S

**Samba** An open source product that first appeared in the mid-1990's. Samba provides NT file and print server capability for UNIX systems, including most of the capabilities of Advanced Server for UNIX, with the exception of the Primary Domain Controller (PDC) and Backup Domain Controller (BDC) synchronization protocols. Although Samba is widely used, vendor support for it is not generally available.

**SMB** Server Message Block, the file-sharing protocol at the heart of Windows networking. SMB is shared by Windows NT, Windows 95, Windows for Workgroups, and OS/2 LAN Manager. CIFS is essentially a renaming of this protocol.



**C****CIFS**

- description, 15
- protocol, 15
- cifsclient, 30, 55, 76
- cifsclient.cfg, 27
- cifslist, 54, 69
- cifslogin, 54, 62
- cifslogout, 54, 68
- cifsmount, 54, 58, 70
- cifsumount, 54, 66
- Common Internet File System. See CIFS
- configuration
  - defaultServer, 87
  - file, 81
  - logLevels, 83
  - servers, 100
- configuring
  - HP CIFS client, 27
  - overview, 23

**D**

- daemon
  - killing, 75
  - when it crashes, 75
- diagnostic, 76
  - cifsclient, 76
  - cifsmount, 76

**E**

- error messages, 76

**F**

- file and directories, 35

**H**

- HP CIFS
  - file and directories, 35
  - introduction, 15
  - starting, 29
  - stopping, 29
- HP CIFS Client
  - features, 18
  - internationalized, 20, 27
  - troubleshooting, 75
  - UNIX Extensions, 18
- HP product enhancements, 17

**I**

- installing
  - loading software, 25
  - overview, 23
  - prerequisites, 24
- internationalized clients, 20, 27

**L**

- loading software, 25

**M**

- mount command, 30
- mount\_cifs, 70

**N**

- netbios, 58, 70
- NIS and the user map file, 111
- NTLM PAM, 25

**O**

- overview
  - configuring, 23
  - installing, 23

**P**

- PAM NTLM
  - configuration, 107
  - configuration file, 107
  - description, 16, 104
  - features, 50, 106
  - secure storage integration, 18, 19
- password(1M), 106

**S**

- Server Message Block, 15, 17
- serverClasses, 101
- SMB. See Server Message Block
- software, loading, 25
- SSL options, 80
- starting HP CIFS, 29
- stopping HP CIFS, 29
- swinstall(1M), 25

**T**

- troubleshooting the HP CIFS client, 75

---

# Index

## U

unmount command, 30  
unmount\_cifs, 70  
user map file, 106  
user map files, 111  
using client, 30  
utilities, summary, 53