

Connecting to UC SMB shares on linux [machine connected to Active Directory only]



Warning on login methods

This guide only applies to machine that have been connected to Active Directory for people who use their UC user code and password. The method below doesn't really work for login with ssh keys.



Warning on time limits

The guide below shows how to automount SMB shares on login using ticket generated by kerberos when using Active Directory. Kerberos tickets are limited in time and that time limit is enforced by the server. Expect to lose your mount if you stay logged in for more than 7 day at a time on a single session. Kerberos tickets have a lifespan of 10 hours and can be renewed for up to 7 days at UC. If you are using a setup connected to active directory by the eResearch support team (François Bissey at the time of writing), your ticket should be automatically renewed to the end of the 7 days by the login service. Finally the share may be unmounted when you log out which may be an issue if you rely on the share being present to execute scheduled work in the background.



Our team can do the setup for you according to your specifications (within reason). This page is mainly a document for people who want to manage and learn things on their own. It also document some limitations of the current storage solution at UC. It can also help you make an informed decision on the setup if you request it be done by the eResearch support team.

Pre-requisites

This setup will use [pam_mount](#) to magically mount the UC shared drive upon login. We will need the following packages on the machine

packages to install

```
sudo apt install libpam-mount cifs-utils hxttools keyutils
```

the above is of course for ubuntu/debian linux distributions. Look for the equivalent packages if you use a different flavor. Note, that some pre-requisites should already be present because your system has been hooked up with Active Directory.

You should already have the `krb5-user` package installed. Upon installation it should have generated a sample configuration of `krb5.conf` in the `/etc` folder of your machine. This configuration, usually based on the original setup at the MIT, can be safely removed in its entirety and replaced with the following

/etc/krb5.conf

```
[libdefaults]
    default_realm = CANTERBURY.AC.NZ
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    default_ccache_name = FILE:/tmp/krb5cc_%{uid}

[realms]
    CANTERBURY.AC.NZ = {
        default_domain = canterbury.ac.nz
    }

[domain_realm]
    canterbury.ac.nz = CANTERBURY.AC.NZ
    .canterbury.ac.nz = CANTERBURY.AC.NZ

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log
```

Managing the mounting process will take place in the file `/etc/security/pam_mount.conf.xml`. Further configuration can be devolved to the user inside a file in their home directory. This needs to be allowed, and the file location defined, in the general configuration file under `/etc/security`. The advantage of devolving some configuration to the user means that they can choose a mount point in a folder they own. But more on this in the next few sections.

Mounting file systems in central mount points

In this section we will configure `pam_mount` to mount all the shares you usually would need under a central point under `/file`, this mimics the setup of RedHat machine centrally managed by ITS. The only difference will be that don't make the `P` drive the home for your user, we just make it available.

You can use the `pam_mount.config.xml` file below to achieve mounting of all the `P` drive, `K` drive, bulk, research, share and scratch drives

sample pam_mount.conf.xml

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">
<!--
    See pam_mount.conf(5) for a description.
-->

<pam_mount>

    <!-- debug should come before everything else,
    since this file is still processed in a single pass
    from top-to-bottom -->

<debug enable="3" />

<!-- Volume definitions -->

<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Research"
    mountpoint="/file/research"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Bulk"
    mountpoint="/file/bulk"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Departments"
    mountpoint="/file/departments"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Scratch"
    mountpoint="/file/scratch"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Shared"
    mountpoint="/file/shared"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
```

```

/>

<!-- P drives -->
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersa$"
    mountpoint="/file/usersa"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersb$"
    mountpoint="/file/usersb"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersc$"
    mountpoint="/file/usersc"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersd$"
    mountpoint="/file/usersd"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Userse$"
    mountpoint="/file/userse"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersf$"
    mountpoint="/file/usersf"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersg$"
    mountpoint="/file/usersg"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersh$"
    mountpoint="/file/usersh"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"

```

```

    path="Usersi$"
    mountpoint="/file/usersi"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersj$"
    mountpoint="/file/usersj"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersk$"
    mountpoint="/file/usersk"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersl$"
    mountpoint="/file/usersl"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersm$"
    mountpoint="/file/usersm"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersn$"
    mountpoint="/file/usersn"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Userso$"
    mountpoint="/file/userso"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersp$"
    mountpoint="/file/usersp"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"
    server="file.canterbury.ac.nz"
    path="Usersq$"
    mountpoint="/file/usersq"
    uid="10000-640000"
    options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
    fstype="cifs"

```

```

server="file.canterbury.ac.nz"
path="Usersr$"
mountpoint="/file/usersr"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Userss$"
mountpoint="/file/userss"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Userst$"
mountpoint="/file/userst"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Usersu$"
mountpoint="/file/usersu"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Usersv$"
mountpoint="/file/usersv"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Usersw$"
mountpoint="/file/usersw"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Usersx$"
mountpoint="/file/usersx"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Usersy$"
mountpoint="/file/usersy"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
fstype="cifs"
server="file.canterbury.ac.nz"
path="Usersz$"
mountpoint="/file/usersz"
uid="10000-640000"
options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>

```

```

<!-- We need to over-ride the cifs mount command so that uid and gid are not
      set as they would by default. This would result in a permission denied error. -->
<cifsmount>mount -t cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o %(OPTIONS)"</cifsmount>

<!-- requires ofl from hxttools to be present -->
<logout wait="0" hup="no" term="no" kill="no" />

      <!-- pam_mount parameters: Volume-related -->

<mkmountpoint enable="1" remove="true" />

</pam_mount>

```

This is a big file since there are a lot of share to mount for the `P` drives. Some details

user volume details

```

<volume
  fstype="cifs"
  server="file.canterbury.ac.nz"
  path="Usersz$"
  mountpoint="/file/usersz"
  uid="10000-640000"
  options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERID),multiuser,vers=3.0"
/>

```

The file system type `fstype` is `cifs` which is a technical term for SMB shares as used by windows. `server` is the name of the SMB host and `path` is the name of the share on that host. Another syntax you may use with nautilus (gnome) or dolphin (KDE) would be `smb://file.canterbury.ac.nz/Usersz`. Note that when using `mount.cifs` as we are here the final `$` is important as it is a bit of SMB magic used for the `P` drives (the other shares don't need it). `mountpoint` is where the share will appear on our system, no need for a matching `$` here. The `uid` line makes sure we will go through with the mount only for user with `uid` in the given range. This should cover Active Directory users while leaving out local users defined on the machine, for which the mount would fail in any case.

Last but not least, the `options` line is very important. `user` is self explanatory, and `%(USER)` automatically fills in the right value. `sec` is for security and describe the method of authentication, here we will use the `krb5` (kerberos) ticket issued at login. `cuid` is the `uid` on behalf of which the mount is made and to which the file will look like they belong to (but you still won't be able to look or touch files that are not yours). This is usually required when login with `sec=krb5`. `multiuser` means several people can mount the same share concurrently without any issue. Finally `vers` is the version of the SMB protocol we want to negotiate.

The line

mountpoint management

```

<mkmountpoint enable="1" remove="true" />

```

means that the mount point will be created on demand and deleted once the last user mounting the share logs out.



Leave the empty lines alone

Finally the empty lines before `</pam_mount>` statement closing the file are an important part of the syntax. Don't remove them.

Delegation to the user

We can delegate some or all the mounting configuration to the user. For that we will need to tell `pam_mount`

- Where to look for the user configuration
- what options the users are allowed to use in their mount command
- if there are any options that are compulsory
- if there are any options that are forbidden

With that in mind, let's move on to a good sample of `pam_mount.conf.xml` for delegating mounting configuration to the user

Allowing user configuration

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">
<!--
    See pam_mount.conf(5) for a description.
-->

<pam_mount>

    <!-- debug should come before everything else,
    since this file is still processed in a single pass
    from top-to-bottom -->

<debug enable="3" />

<userconf name=".config/pam_mount.conf.xml" />

<cifsmount>mount -t cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o %(OPTIONS)"</cifsmount>

<mntoptions allow="nosuid,nodev,loop,nonempty,sec,cruid,multiuser,user,domain,vers,multiuser,noperm" />

<!-- commented out.
<mntoptions deny="*" />
-->

<mntoptions require="" />

<!-- requires ofl from hxttools to be present -->
<logout wait="0" hup="no" term="no" kill="no" />


    <!-- pam_mount parameters: Volume-related -->

<mkmountpoint enable="1" remove="true" />

</pam_mount>
```

First we see the `userconf` option which will point to the location of the user configuration file in their home directory. This is arbitrary but all end users will need to put their configurations in at a consistent location. We have three `mntoptions` statements, one to `allow` options, one to `deny` and one to `require`. They should be consistent with the filesystem you are planning to let the user mount. The options allowed above are good for a multiuser SMB setup like the one we have at UC.

The user configuration will look very similar to the general configuration from the previous section

user configuration

```
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">

<pam_mount>

<volume
  fstype="cifs"
  server="file.canterbury.ac.nz"
  path="Research"
  mountpoint=~ /UCDrive/research"
  options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>
<volume
  fstype="cifs"
  server="file.canterbury.ac.nz"
  path="Usersf$/frb15/Home"
  mountpoint=~ /Pdrive"
  options="user=%(USER),domain=uocnt,sec=krb5,cuid=%(USERUID),multiuser,vers=3.0"
/>

</pam_mount>
```

The main difference being that we create mount points in the user home directory. Note that `frb15` is used as an example, replace with your own usercode and be sure that the first letter of your usercode is set properly in the `Users` part of the `path`.

Odds and ends

Questions:

Can I use my password on login instead of the kerberos ticket?

By default on ubuntu, that will not work. You would have to alter the `pam` configuration in the file `/etc/pam.d/common-auth` the line

pam_mount authentication

```
auth optional pam_mount.so
```

has to be moved from its location at the bottom of the file to the top before

common-auth sample

```
auth    [success=2 default=ignore]    pam_unix.so nullok_secure
auth    [success=1 default=ignore]    pam_sss.so use_first_pass
```

otherwise `pam_mount` will not be able to access your password. You will also need to remove `sec=krb5` from the option for it to switch to using the password.

Even so, it will not work at UC. You would have to alter some of the options as such a configuration cannot be multiuser anymore and the options `cuid` and `multiuser` are meaningless now. UC doesn't let you mount SMB share with "unix extensions" which means that while you have mounted something the permissions are all garbled and you cannot access anything in your mount point. There is nothing you can do to fix this short of forcing central ITS to change the storage configuration.

Could I use a credential file instead of a kerberos ticket so I can login with ssh key?

The `mount.cifs` command support a `credential` option which can point to a file containing your login information in the format

credential format

```
user=$your_user_code  
domain=uocnt  
password=$your_password
```

However, you will suffer from the same limitation as in the previous question.