

Chapter 23: Installing and Configuring MIT

Kerberos on a Macintosh System

In this chapter we describe how to install and configure Kerberos for Mac OS X 10 in order to access Kerberized machines and encrypt your data transmissions. If you use an older Macintosh OS, we recommend that you upgrade. In case upgrading is not convenient for you, we still provide instructions for installing the MIT Kerberos 4.0x for pre-OS X Macintosh software.

Computing Division Macintosh Strategy

We quote from the (2001) Computing Division policy on Macintosh support. It is still valid as of January 2005.

“The Macintosh Operating System is no longer a supported operating system from the Computing Division and is not a strategic operating system for future plans...

... Specifically regarding the Strong Authentication realm, the supported access method from Macintoshes will be via the CRYPTOCard. Kerberos clients may be available and used, but there will be no effort expended to select, test or distribute them.”

That said, there is some community support for the Macintosh, primarily through *kerberos-users@fnal.gov* and *macusers@fnal.gov*.

23.1 Kerberos on Mac OS X 10

23.1.1 Install and Configure

MIT Kerberos for Macintosh is shipped as part of Mac OS X (as of the OS X 10.1 “Cheetah” update). There is a kit of “extras” for OS X 10.1 and later with some additions to what gets shipped with the OS.

- 1) Update to OS X 10.3 “Panther” if you have not already done so. It has the best Kerberos support, especially for connecting to Windows services

- 2) Optionally install MIT's "Kerberos extras for Macintosh". It provides a shortcut in /Applications/Utilities to the GUI ticket manager which is already present in /System/Library/CoreServices, and provides a support library for CFM-based applications such as Fetch and Eudora.

To install it, go to

<http://web.mit.edu/macdev/KfM/Common/Documentation/osx-kerberos-extras.html> and scroll down about 1/3 the way to "Where can I get Mac OS X Kerberos Extras?". Click as indicated to download:

http://web.mit.edu/macdev/Download/Mac_OS_X_Kerberos_Extras.dmg. Once it's on your desktop, open it and run the installer (called Mac OS X Kerberos Extras).

- 3) Obtain the Fermilab Kerberos configuration file template `krb5.conf.template` from the FNAL ftp server. Find the most recent version at <ftp://ftp.fnal.gov:8021/products/krb5conf/>. Edit the [libdefaults] section of `krb5.conf.template` to contain only:

```
[libdefaults]
default_realm = FNAL.GOV
dns_lookup_realm = TRUE
```

If you commonly work from behind a NAT, as is typical of many cable and DSL internet users, you should also add to the [libdefaults] section:

```
noaddresses = TRUE
```

- 4) The system expects to find this configuration file in one, and only one, of two places. Check for the existence of either of the following two files. (`/etc` is a private directory, requires sysadmin privileges):

```
/etc/krb5.conf
/Library/Preferences/edu.mit.Kerberos
```

If the second one is the only one there, overwrite it with your edited `krb5.conf.template` file, renaming the file `edu.mit.Kerberos`. In all other cases, delete the second one (if there) and overwrite the first with your edited `krb5.conf.template` file, renaming it `krb5.conf`.



Make sure it only exists in one of the two places!

- 5) If you only want Kerberos access from your Mac to other services (e.g., to log into Unix and/or connect to Windows file servers) you're done. If you want more, keep reading.
- 6) For AFS access: Download the latest "Darwin" release of OpenAFS from <http://www.openafs.org/release/latest.html>.

Click on Mac OS 10.3, then on `OpenAFS.pkg.tar.gz`. This unzips it, downloads the tar file, and untars it using Stuff-it.

- 7) Click on the untarred file (pkg file), and an installer pops up; run the installer.
- 8) Go to `/var/db/openafs/etc/` (requires sysadmin privileges) and edit `ThisCell.sample` such that it contains only the single line:

```
fnal.gov
```

- 9) Save it as `ThisCell`.

- 10) Restart your computer.

- 11) Edit `/etc/sshd_config` and make sure that every non-comment line containing the string “Authentication” (in any combination of upper and lower case!) ends with a “no”, except this one:

```
KerberosAuthentication yes
```

In particular, make sure that

```
PasswordAuthentication no
```

Is NOT commented out with a '#'.

- 12) If your Mac is a DHCP client, make sure it gets a stable hostname when connected: Go to System Preferences, click “Network”, choose each network interface in turn that you intend to use (probably “Built-in Ethernet” and “Airport”). For each one, click Configure, go to the TCP/IP tab, and fill in the “DHCP Client ID” box with just your hostname (not the fully qualified name). E.g., let’s suppose you’ve registered in MISNET with the hostname `mackinac`. Just put `mackinac` in the box, even though your full domain name is `mackinac.dhcp.fnal.gov`.

- 13) Go to http://computing.fnal.gov/cd/forms/extra_kerb_req_form.html and request a “host principal” for that name. In the additional info box at the bottom, specify that you do NOT need an ftp principal.

- 14) When you get email back with an initial host principal password, open a Terminal session (Applications > Utilities > Terminal), and under an administrator account run this command:

```
sudo /usr/sbin/kadmin -p host/mackinac.dhcp.fnal.gov -q  
"ktadd host/mackinac.dhcp.fnal.gov"
```

Provide the password when prompted -- it can only be used one time. If successful the terminal will display a message to the effect of "Entry for principal host/mackinac.dhcp.fnal.gov ... added to keytab WRFILE:/etc/krb5.keytab."

15) Open System Preferences, pick "Sharing" and with the "Services" tab selected, click "Remote Login" to enable incoming ssh. Make sure your correct hostname (not the fully qualified name) is in the Computer Name field.

16) Add a `.k5login` file to the home directory of any account to which you want to be able to log in remotely, and include the appropriate principals (full principal with no spaces). This file must be writable only by the account itself and/or root.

Once you have set up Kerberos, you have:

- Kerberos telnet and ssh clients
- A Kerberos ssh server (if you completed steps 8-11)
- Kerberos access to WIN.FNAL.GOV Windows 2000 servers

You will not have Kerberos ftp, rlogin, and rsh.

23.1.2 Kerberized Ftp Client

You may be able to get by with `sftp`, an ssh subsystem, if the servers you use support it. Otherwise, you can get Fetch, an easy-to-use, full-featured FTP client for the Apple Macintosh. As of this writing (Dec 04), 4.0.3 is the latest version. Download it from <http://www.fetchsoftworks.com/>.

23.1.3 X Client

Download the X Client from the Apple site:
<http://www.apple.com/macosx/features/x11/>.

23.1.4 Authenticate to Kerberos

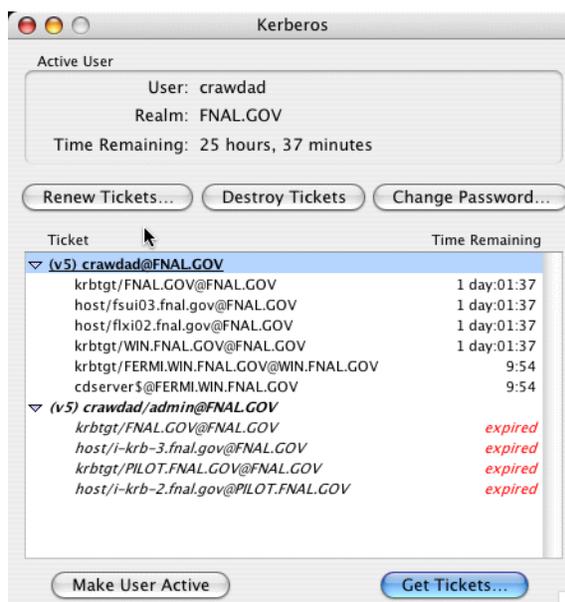
To authenticate, use either the command line `kinit` as you would on a Unix system, or the OS X GUI that will now (after installing the "Extras") be visible as "Kerberos" in the /Applications/Utilities folder.

Command Line `kinit`

Open a terminal window and run the command `kinit`. See section 12.1 *kinit*.

GUI

- 1) Open /Applications/Utilities/Kerberos or, if you did not install Kerberos Extras, point to /System/Library/Core Services/Kerberos.
- 2) Click Get Tickets.



- 3) Check that your username is right and the realm is FNAL.GOV. Optionally click Show Options. Enter your Kerberos password and click OK.
- 4) You'll see your principal name appear and a Time Remaining for your tickets. You can click the triangle to reveal a list of the tickets.
- 5) Now you are ready to connect to a Unix system with telnet or ssh, or to a Windows 2000 domain file server with the Finder's Command-K function. You can quit the Kerberos GUI application without losing your tickets.

23.1.5 Time Synchronization

If¹ you get the error “KDC reply did not match expectations”, your computer's date and time are different than the date and time on the Kerberos server. Should you see this error, make sure your date and time are correct.

On a Macintosh, the Date and Time in the System Preferences or Control Panel has an option for using a network time server. To set the date and time:

1. This text is adapted from MIT IS&T Stock Answer #5897.

- First quit all Kerberos-using applications.
- On Mac OS 10.3 or higher, open System Preferences and click the Date & Time. Check the field “Set Date & Time automatically”, then in the field to the right of it, enter the Fermilab core router 131.225.8.200 as the time server. (You could use the secondary router 131.225.17.200.)
- On Mac OS 10.2 or previous, click the Network Time tab and enter the time server to in the field. Click the “Set Time Now” button.

If the problem persists, restart your computer.

23.2 Installing MIT Kerberos for Mac OS 9 and Earlier

Before you go on, remember that the best advice is to upgrade to OS X! If you choose not to, then follow these instructions which apply only to OS 9 and earlier. First, obtain a Kerberos principal and initial password for the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal*.

This section was originally written for version 3.5 of the MIT Kerberos software for Macintosh. Various versions 4.x have since been made available. Installation can be accomplished by clicking on the “Kerberos for Mac 4.0” installer application. This should install everything into the disk containing your System Folder. This version includes the Kerberos Floating Window (for status), and Kerberos Menu on the menubar (a quick way to create/destroy tickets and to open the Kerberos Control Panel). You will need to reboot probably twice, then, assuming your Kerberos Preferences file is configured properly, you should successfully get a ticket for your principal.

23.2.1 Changes in MIT Kerberos for Macintosh 4.0

See

<http://web.mit.edu/macdev/Development/MITKerberos/Common/Documentation/release-4.0.html>. A big change is better OS X support. User interface changes relative to v3.5 include:

- The **KERBEROS CONTROL PANEL** is a changed version of the **KERBEROS MANAGER**.
- The **KERBEROS MENU** on the menu bar shows the status of the active user’s TGT and can be used to quickly get/destroy/renew tickets or open the control panel.

- The **KERBEROS CONTROL STRIP** is similar to the **KERBEROS MENU** but a module in the control strip.
- Kerberos Floating Window
- Optional status display of all user's TGTs.

Regarding installation, version 4.0 includes two installer programs, one for OS X and the other for OS 8/9 (supports 8.1 through 9.2.1) but is otherwise much the same as version 3.5.

23.2.2 Download Kerberos from the MIT Web Site

- 1) Bring up the **MIT Kerberos for Macintosh** web page, at URL `http://web.mit.edu/macdev/www/kerberos.html`.
- 2) Select *Getting MIT Kerberos for Macintosh*.
- 3) On this page, look for the paragraph that starts "If you are outside of MIT but still in the US or Canada...". Click on the *download page* link in that paragraph.
- 4) This brings you to the **Kerberos Distribution Authorization Form**. Answer the three questions, and submit the form to arrive at the download page. (There is a link on this page for Canadian users, which we have not tried or documented.)
- 5) Click on the link for MIT Kerberos for Macintosh 4.
- 6) Under the small heading "Binaries and SDKs", click *Binhexed self mounting disk image*.

23.2.3 Items that Appear on your Desktop

You'll find three new items on your desktop once the transfer finishes (This section has not been updated since v3.5; you will find similar things for v4.0.):

- MIT Kerberos for the Mac folder
- MIT_Kerberos_for_Mac_3.5.hqx file
- MIT Kerberos for Mac 3.5.smi file

There will also be a new disk volume from mounting the .smi (if the disk is not present, double-click the .smi file).

Discard the .hqx file, and open the MIT Kerberos for the Mac folder. This folder contains:

- two subfolders:

- Mac OS 9 Binaries 3.5, which contains four sub-subfolders labelled as per their destination folders (the names are of the form ->Into <Foldername>)
- Mac OS 9 SDK 3.5; this is the software development kit and can be ignored.
- one application program **Kerberos for Mac 3.5**
- three links/HTML files: to the MIT Kerberos home page, to the Kerberos for Macintosh Bugs page, and to the KfM 3.5 Release Notes.
- one text file KfM 3.5 Read Me, which contains installation instructions



The Kerberos for Macintosh 4.0 disk will have similar contents with the addition of the "Kerberos for Mac OS X 4.0" application and a link "Mac OS X SDK Information". Note that 4.0 supports both Mac OS 8.1 through 9.1 as well as Mac OS X.

23.2.4 Installation Instructions

(This section has not been updated since v3.5; v4.0 is similiar.) We refer you to the Read Me file to complete the installation of MIT Kerberos for the Mac, but we provide a few clarifications here:

- On the MIT download page, double-click the Kerberos for Mac 3.5 application to install.
- The downloaded files no longer need to be copied manually into folders under the System Folder on your system.
- The ->Into Preferences folder contains three subfolders. Choose Kerberos Preferences v5.

After installation, if you get the error message “preauthentication fails” when you attempt login via the **GET TICKETS** button, it is most likely caused by a password or time-sync error. First verify your password is correct. Then, synchronize your machine with the network time (see section 23.7.3 *Time Synchronization (Pre-OS X 10)*).

23.3 Configuring the Kerberos Software v4 for Mac

23.3.1 The Preferences File

The Kerberos Preferences file needs to contain information for Fermilab's strengthened realm(s). Edit the file or just replace the initial contents with that of the `krb5.conf` file from either the **krb5conf** product in KITS or a machine in the Fermilab FNAL.GOV realm (note that pasting text directly from a web browser may cause end-of-line problems). A Fermi-configured Preferences file is now available for download from <http://www.fnal.gov/docs/strongauth/ps/> (see `Kerberos_Preferences.sit` for the StuffIt archive file, or `Kerberos_Preferences.hqx` for the BinHexed (ASCII encoding) version of that file). We reproduce the text of the file here:

```
[libdefaults]
    default_realm = FNAL.GOV
    ticket_lifetime = 1560
    checksum_type = 1
    ccache_type = 2
    default_tkt_enctypes = des-cbc-crc
    default_tgs_enctypes = des-cbc-crc
    noaddresses = true

[realms]
    FNAL.GOV = {
        kdc = krb-fnal-1.fnal.gov:88
        kdc = krb-fnal-2.fnal.gov:88
        kdc = krb-fnal-3.fnal.gov:88
        kdc = krb-fnal-4.fnal.gov:88
        kdc = krb-fnal-5.fnal.gov:88
        admin_server = krb-fnal-admin.fnal.gov
        master_kdc = krb-fnal-admin.fnal.gov:88
        default_domain = fnal.gov
    }
    WIN.FNAL.GOV = {
        kdc = newpckits.fnal.gov:88
        admin_server = newpckits.fnal.gov
        default_domain = fnal.gov
    }

[domain_realm]
    .fnal.gov = FNAL.GOV
```

```
.hep.net = FNAL.GOV
.minos-soudan.org = FNAL.GOV
```

Note: if you have to deal with Network Address Translation (NAT), see section 6.5 *Network Address Translation*.

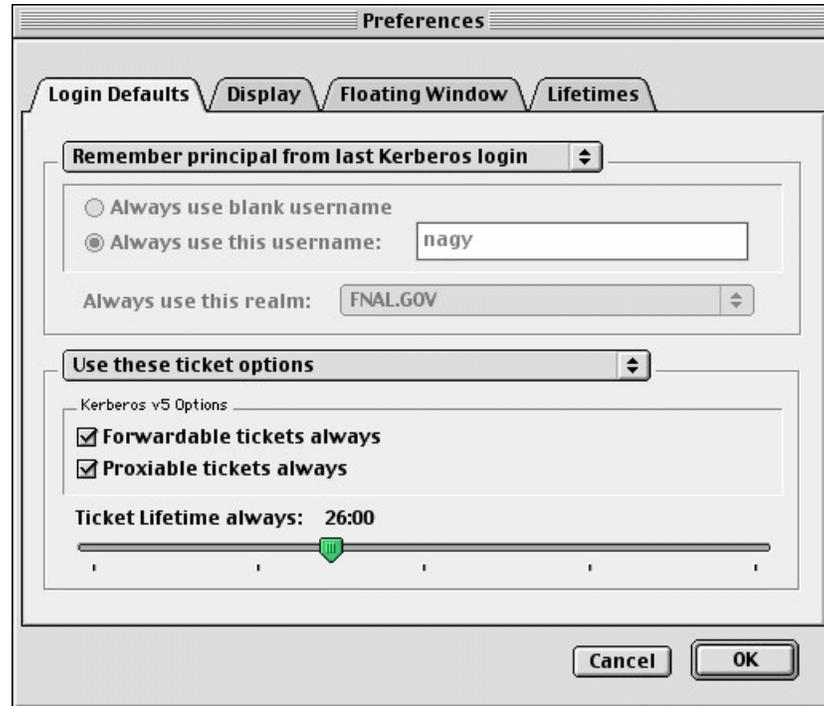
23.3.2 Select Favorite Realms

After modifying the **KERBEROS PREFERENCES**, start the **KERBEROS CONTROL PANEL** and select the **FAVORITE REALMS** item from the **EDIT** menu. Use the dialog box to copy your favorite realms from the right to the left-hand side of the screen.

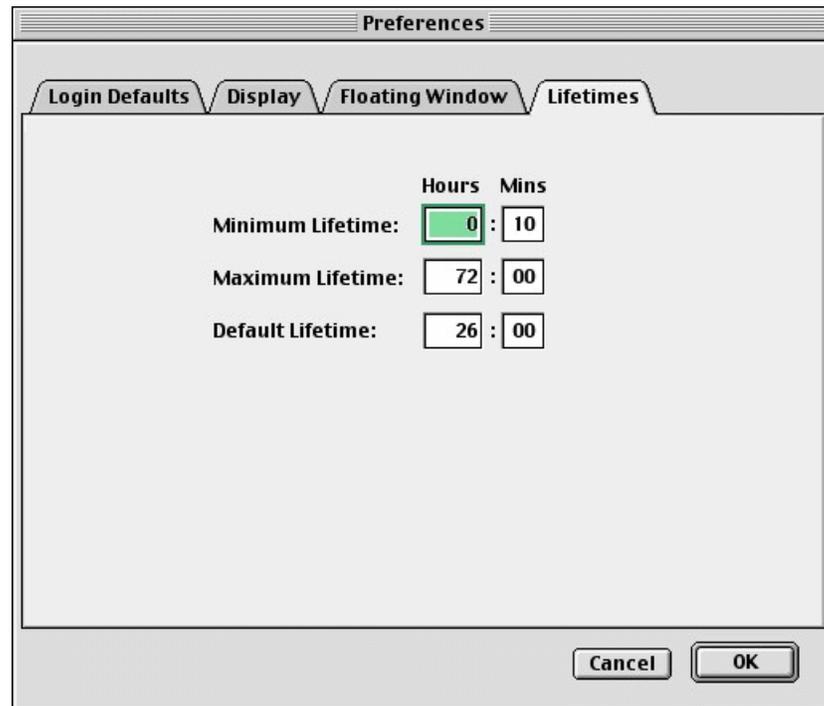


23.3.3 Edit Preferences

Edit your login preferences, and make sure you check **FORWARDABLE TICKETS ALWAYS**:



Edit your ticket lifetime preferences (the KDC limits the ticket lifetime to 26 hours):



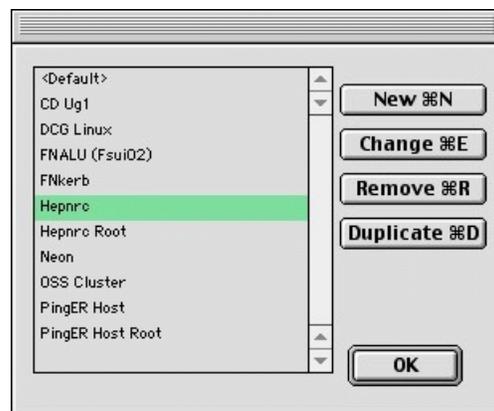
23.4 Installing Telnet Client

BetterTelnet and **NiftyTelnet** with Kerberos v5 support are the only **telnet** products that we know of at this time that work on the Macintosh. We document **BetterTelnet** here. You'll need both it and an associated plug-in installed on your machine.

- 1) Bring up the **MIT Kerberos for Macintosh** web page, at URL <http://web.mit.edu/macdev/www/kerberos.html>. Select *Frequently Asked Questions*.
- 2) Look for the Q/A that discusses **telnet** (you can search on "BetterTelnet"). Click on the link *BetterTelnet and Kerberos plugin*. This brings you to the FTP site:
`ftp://ftp.cmf.nrl.navy.mil/pub/chas/MIT_Kerberos_3.5/.`
- 3) If you don't already have **BetterTelnet** installed, click on *BetterTelnet 2.0f...* and install this software first.
- 4) Once **BetterTelnet** is installed, download `Telnet_Plugin.bin` from the same **FTP** site and copy it to the **BetterTelnet** folder on your machine.

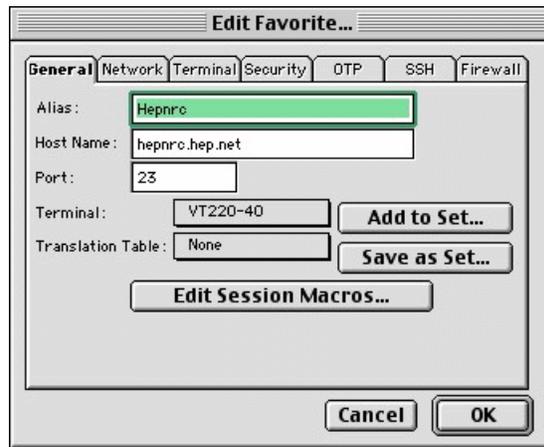
23.5 Configuring Telnet

- 1) Invoke **BetterTelnet**. On the **FAVORITES** menu, choose **EDIT FAVORITES**. You should create one configuration for each strengthened host you plan to access.

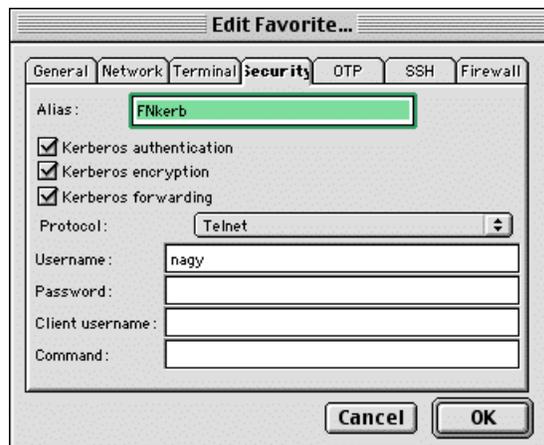


- 2) To create a new configuration, on the pop-up screen, click **NEW**. Then,

with the **GENERAL** tab selected, type in an **ALIAS** which will be used to identify the host (this can be any string) and the **HOST NAME**.



- 3) **Very important!!** Change to the **SECURITY** tab, check Kerberos authentication and Kerberos encryption. Kerberos forwarding is recommended. The protocol should be left as telnet (the default). Filling in other fields is optional (even if you fill in your Kerberos password, you need to provide it again when you authenticate). Click **OK** to save the configuration.



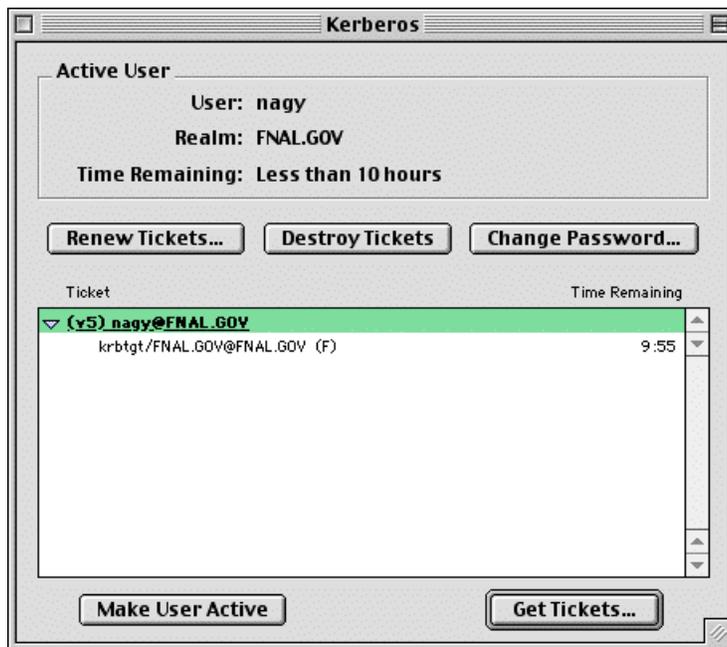
23.6 Kerberized FTP Client

Fetch is an easy-to-use, full-featured FTP client for the Apple Macintosh. As of this writing (Dec 04), 4.0.3 is the latest version. Download it from <http://www.fetchsoftworks.com/>.

23.7 Authenticating to Kerberos

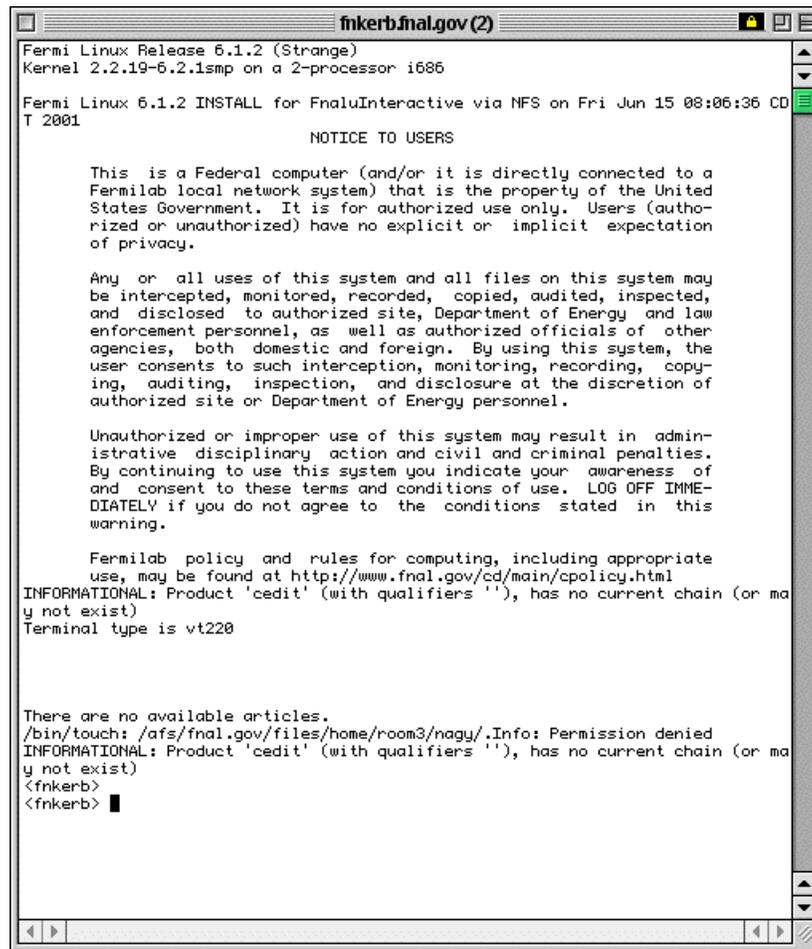
23.7.1 Authenticate via Kerberos Control Panel

- Invoke the **Kerberos Control Panel** (from **CONTROL PANELS** under the Apple menu, from the **KERBEROS MENU** in the menu bar, or from the **KERBEROS CONTROL STRIP** module).



- Select principal, and click **GET TICKETS**.
- Enter your Kerberos password on the pop-up screen.

You should see a ticket appear. Now you can invoke your **telnet** product (**BetterTelnet** or **NiftyTelnet**) and connect to one or more strengthened hosts without having to provide your password again.



```
fnkerbfnal.gov (2)
Fermilab Linux Release 6.1.2 (Strange)
Kernel 2.2.19-6.2.1smp on a 2-processor i686

Fermilab Linux 6.1.2 INSTALL for FnalInteractive via NFS on Fri Jun 15 08:06:36 CD
T 2001

NOTICE TO USERS

This is a Federal computer (and/or it is directly connected to a
Fermilab local network system) that is the property of the United
States Government. It is for authorized use only. Users (author-
ized or unauthorized) have no explicit or implicit expectation
of privacy.

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site, Department of Energy and law
enforcement personnel, as well as authorized officials of other
agencies, both domestic and foreign. By using this system, the
user consents to such interception, monitoring, recording, copy-
ing, auditing, inspection, and disclosure at the discretion of
authorized site or Department of Energy personnel.

Unauthorized or improper use of this system may result in admin-
istrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of
and consent to these terms and conditions of use. LOG OFF IMME-
DIATELY if you do not agree to the conditions stated in this
warning.

Fermilab policy and rules for computing, including appropriate
use, may be found at http://www.fnal.gov/cd/main/cpolicy.html
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
Terminal type is vt220

There are no available articles.
/bin/touch: /afs/fnal.gov/files/home/room3/nagy/.Info: Permission denied
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
<fnkerb>
<fnkerb> █
```

23.7.2 Authenticate at Login

Invoke **BetterTelnet** or **NiftyTelnet** and connect to a strengthened host. You will be prompted for your Kerberos password, and then authenticated once you have provided it.

23.7.3 Time Synchronization (Pre-OS X 10)

If¹ you get the error “KDC reply did not match expectations”, your computer’s date and time are different than the date and time on the Kerberos server. Should you see this error, make sure your date and time are correct.

1. This text is adapted from MIT IS&T Stock Answer #5897.

On a Macintosh, the Date and Time in the System Preferences or Control Panel has a setting for using a network time server. For a time server, use the Fermilab core router 131.225.8.200 as primary and 131.225.17.200 as secondary. First quit all Kerberos-using applications. On Mac OS 9, click the 'Network Time Server' button and add the time server to the list. Click the 'Set Time Now' button to sync your computer. If the problem persists, restart your computer.