

Part IV System Administrator's Guide "A": Recommended and Supported Implementations

Chapter 14: *Installing Fermi Kerberos on a UNIX (non-Linux) System*

In this chapter we provide instructions for installing the Fermilab **kerberos** product on a UNIX machine (Linux is treated separately in Chapter 15: *Installing Fermi Kerberos on a RedHat Linux System*) and for installing Kerberized **ssh**, as the combination works very well. These products are available from *fnkits.fnal.gov*. We describe how to install them using **UPS/UPD**. The information is valid for all supported flavors of UNIX, namely: SunOS, IRIX and OSF1.

Chapter 15: *Installing Fermi Kerberos on a RedHat Linux System*

In this chapter we provide instructions for installing the Fermilab **kerberos** product and Kerberized **ssh** on a RedHat Linux machine. These products are available as **UPS** products from *fnkits.fnal.gov*, and in **RPM** format.

Chapter 16: *Kerberized UNIX System Administration Issues*

In this chapter we discuss some UNIX system administration issues related to the installation of Kerberos software.

Chapter 17: *The Kerberos Configuration File: krb5.conf*

In this chapter we describe the Kerberos configuration file `krb5.conf`.

Chapter 18: *Additional UNIX Sysadmin Information for Off-Site Installations*

In this chapter, we discuss some miscellaneous issues that sysadmins of off-site Kerberos installations should be aware of. Also see Chapter 6: *Logging In from Off-Site*.

Chapter 19: *Installing and Configuring WRQ® Reflection on a Windows System*

In this chapter we describe how to install and configure the **WRQ® Reflection** software on your Windows system (Win 2k, NT4, 95, or 98) in order to access Kerberized machines and optionally encrypt your data transmissions.

Chapter 20: *Installing and Configuring the Windows AFS Client*

In this chapter we describe how to install and configure the **Windows AFS Client** software on your Windows system (Win 2k, NT4, 95, or 98) in order to transfer files between a Windows desktop and AFS space.

Chapter 14: Installing Fermi Kerberos on a UNIX (non-Linux) System

In this chapter we provide instructions for installing the Fermilab **kerberos** product on a UNIX machine (RH Linux is treated separately in Chapter 15: *Installing Fermi Kerberos on a RedHat Linux System*¹) and for installing Kerberized **ssh**, as the combination works very well. These products are available from *fnkits.fnal.gov*. We describe how to install them using **UPS/UPD**². The information is valid for all supported flavors of UNIX, namely: SunOS, IRIX and OSF1.

14.1 Before You Install Kerberos

14.1.1 Obtain a Kerberos Principal

Strictly speaking, you don't need a Kerberos principal to just install the software. It will be difficult to judge your results without one, however. You'll need to get a principal (plus an initial password) to have access to the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal* for information, and fill out the online form at <http://www.fnal.gov/cd/forms/strongauth.html>.

14.1.2 Create an Account that Matches your Principal



We strongly recommend that you create an account/login name on the machine that matches the “primary” (the username part) of your user principal. See section C.2 *If your Principal and Login Name do not Match* in Appendix C: *More about Choosing a Principal Name*. Note that even if your login name and principal don't match you can still log into your machine at the console after it's Kerberized, as long as your UNIX password is there.

-
1. The information is also valid for Fermi RedHat Linux, but more options are available for Linux.
 2. For documentation on **UPS/UPD**, see <http://www.fnal.gov/docs/products/ups>. Installing products from *fnkits* is described in Part II of the **UPS/UPD** documentation.

14.1.3 Understand your Installation Options

If you don't wish to maintain the **UPS/UPD** software on your machine, we recommend that you install it temporarily in order to install **ssh** and **kerberos**, and then remove it. Instructions for a temporary **UPS/UPD** install are online at <http://www.fnal.gov/docs/products/ups/ReferenceManual/misc/TemporaryInstall.html>.



If you choose not to use **UPS/UPD**, it will be difficult to install the Fermilab **kerberos** product (unless you install via RPM on RH Linux, discussed in Chapter 15: *Installing Fermi Kerberos on a RedHat Linux System*). Instead you can download the MIT Kerberos product in a variety of formats from the Web and install it. See Chapter 21: *Installing Kerberos on a non-Fermi-Supported Linux System*.

14.1.4 Install UPS/UPD (Recommended)

If **UPS/UPD** is not already installed on your machine, go ahead and install it (for instructions, see Part III of the *UPS, UPD and UPP v4 Complete Guide and Reference Manual* at

<http://www.fnal.gov/docs/products/ups/ReferenceManual/parts.html#partIII>). If your node is not in the fnal.gov domain, make sure that you first register your node for product distribution using the form at

http://www.fnal.gov/cd/forms/upd_registration.html.

14.1.5 Install Kerberized SSH (Recommended)

Using Kerberized **ssh** with the **kerberos** product in fully strengthened mode smoothes out several operations that can cause extra work in a non-ssh installation. Most importantly, ssh can be configured to always provide encrypted connections. Also, you get X11 connection forwarding so that you don't have to set the `$DISPLAY` variable, and the X11 connections are encrypted.

As of version 1_2_27, the first Kerberized ssh version, the ssh product components no longer reside in the `/usr/local` directory tree. The newer versions get installed in the `/usr/krb5` directory tree, which should be local to individual machines.



If you have ssh-afs installed from a previous version of ssh, you must remove it in order for the Kerberos, ssh and AFS to work together properly. The new Kerberized versions of ssh know how to work with AFS.



If you've already installed kerberos and want to add Kerberized ssh via UPS/UPD, make sure you run **ups install-sshd kerberos** after installing ssh, for reasons discussed below. (The Kerberized ssh RPM, described in section 15.2.3 *Fermi Kerberos and ssh RPM Descriptions*, can be installed either before or after kerberos.)

Why Install SSH First?



Make sure you install ssh BEFORE you install kerberos (and install the latter in fully-strengthened mode). The UPS kerberos installation checks for the sshd configuration file and, if it exists, makes the appropriate modifications to turn off the authentication methods that shouldn't be allowed, i.e., password and RSA hosts.

The ssh installation, on the other hand, only checks whether an sshd configuration already exists. If so, it simply keeps it, and if not, it creates a default one (a more permissive one). So, if you install ssh after kerberos, you end up with a too-permissive-for-kerberos ssh configuration. This can be fixed by running **ups install-sshd kerberos** which invokes the part of the kerberos install script which modifies the sshd configuration.

To Install SSH using UPD

- 1) First, log in as the appropriate user for product installation (usually *products* or *root*).
- 2) We recommend that you stop sshd prior to the installation (as *root*):

```
% /etc/rc.d/init.d/sshd stop
```
- 3) Setup UPD by running the command:

```
% setup upd
```
- 4) Next run the **upd install** command to retrieve **ssh** from the product server, and set it as “current” in the database:

```
% upd install ssh [v<N_M>] -G -c
```
- 5) Log out, if necessary, and log in now as *root* (or **su** to *root*).
- 6) Run the following configuration command (on each individual machine, if installing on a cluster):

```
% ups InstallAsRoot ssh
```
- 7) Note: The ssh installation sets the values of `RhostsRSAAuthentication`, `RSAAuthentication` and `PasswordAuthentication` in `/etc/sshd_config` to “yes”. They must be set to “no”! (`KerberosOrLocalPasswd` must also

be “no”.) If you proceed to install kerberos, these values will get set properly. If kerberos is already installed, you must either set the values to “no” by hand, or you can do it by running:

```
% ups install-sshd kerberos
```

8) Restart sshd (as *root*):

```
% /etc/rc.d/init.d/sshd start
```

9) Verify your \$PATH is pointing to the right ssh (in case you had an older version of ssh running previously). To test, run the command: **which ssh**. It should return `/usr/krb5/bin/ssh`. If not, go into `/usr/bin` and reset the ssh link to `/usr/krb5/bin/ssh`.

Documentation on **ssh** is provided under

<http://www.fnal.gov/docs/products/ssh/>.

14.1.6 Do you Need to Allow Incoming Kerberos Connections?

If you plan to log in to your machine over the network and/or offer services, your machine must allow incoming Kerberos connections (including portal mode connections). In this case, you must get a service principal for the host, and one for **FTP** if that is an offered service. These service principal names are of the form `host/<full.node.name>` and `ftp/<full.node.name>` (e.g., `host/mynode.fnal.gov` and `ftp/mynode.fnal.gov`, or for off-site nodes, something like `host/mynode.myuniv.edu` and `ftp/mynode.myuniv.edu`, according to your institution’s domain). We also recommend that you get a fixed IP address.

If you need host and ftp principals, first register yourself in the database of system administrators. Go to *System Administrator Registration* at <http://miscomp.fnal.gov/sysadmindb/> to register.

Before installing **kerberos** on a machine the first time, request the host-specific service principals (plus initial passwords) for that machine, using the form at <http://www.fnal.gov/cd/forms/strongauth.html>. You will need to provide the full hostname of the machine.



Notes:

- For a machine with two or more active (static) IP addresses or multiple node names, see section 16.12 *Multiple IP Addresses or Node Names*.
- If you are reinstalling **kerberos** on a machine, you should keep the same host and **FTP** principals. If the `krb5.keytab` is not lost, there’s nothing you have to do for these principals. If it is lost, contact compdiv@fnal.gov to get passwords reset on the principals.

If you don't intend to allow incoming connections, don't request these service principals, and just answer "no" when asked if you have the passwords for them during installation of the **kerberos** product. You can request and install them at a later date, if needed. To do so, log on as *root* and run the command:

```
% ups install-hostkeys kerberos
```

and provide the passwords as prompted.

14.1.7 Synchronize your Machine with Time Server

When using Kerberos, the client and server must be time-synchronized with each other, each in its local time zone. A wrong system clock is the single most common authentication problem (it typically appears as a "preauthentication failed" message). Use the command **date -u** to check the date/time that really counts. Kerberos is configured to allow a discrepancy of five minutes. **xntp** is a product that you can install on your machine to maintain the system time in agreement with Internet standard time servers. It is available from *fnkits* for some platforms¹.



If your system runs AFS, don't install **xntp** or any other synchronizing software; AFS does its own time synchronization. But beware: AFS doesn't set the hardware clock, so, for example, when daylight savings time starts or ends, your clock may be an hour off. Choose ONLY ONE of the following solutions:

- start **xntp**, let it sync the clock, then turn it off
- see if the **afsd** has a **-nosettime** option; if so, set it and run **xntp** to handle the timekeeping instead
- (Linux) make sure the date is correct, then run **/sbin/hwclock --systohc** to change the hardware clock to match the system clock (or edit your `crontab` to run the above command at some frequency; e.g., to sync it up once a month, add the line `33 3 3 * * /sbin/hwclock --systohc`)

14.1.8 Determine Kerberos Access Mode(s)

Before installing you must first determine whether you want **kerberos** configured in fully strengthened mode, in mixed mode (Kerberos plus **ssh**), or in a customized mode.

1. If your node is not in the `fnal.gov` domain, make sure that you first register your node for product distribution via `fnkits` using the form at http://www.fnal.gov/cd/forms/upd_registration.html

Fully Strengthened Mode (Kerberos Only)

This mode enables only Kerberized access to the node. This includes Kerberized ssh. It disables *all* non-Kerberized means of accessing the node. This is the mode on-site Kerberized systems are obliged to choose beginning Jan. 1, 2002.

Mixed Mode (Kerberos plus SSH)

This mode enables Kerberized access to this node, does not disable any existing non-Kerberized **ssh** access to the node, but disables *all other* non-Kerberized means of accessing the node. This mode is incompatible with Kerberized **ssh**.



For ON-SITE SYSTEMS, this mode is not in compliance with the Computing Policy, and thus is NOT ALLOWED as of January 1, 2002.

Other

If neither of these configurations applies, read the file `README.INSTALL.DETAILS` which describes all of the possible installation options in detail.



This is recommended only for experts.

14.1.9 Choose Login Program

Secondly, you can choose to use the standard UNIX login program or to install the Kerberos login program¹. As of September 2001 the installation of Fermi **kerberos** automatically replaces the system login program with the Kerberized version. The Kerberos login program is required for CRYPTOCard support.

14.2 Installing Fermi Kerberos using UPS/UPD

The Fermilab **kerberos** product is preconfigured and in general should require no further actions beyond the installation instructions found here (this information has been taken from its `README.INSTALL` file). **kerberos**

1. Not applicable to IRIX systems or to Linux or Solaris if using the GUI login box; the login program isn't run in these cases.

must be properly installed on each individual node. For more information, or to do a custom install, see the the various README files that come with the product.

1) First, log in as the appropriate user for product installation (usually *products* or *root*).

2) Setup **UPD** by running the command:

```
% setup upd
```

3) Next run the **upd install** command to retrieve **kerberos** from the product server, and set it as “current” in the database¹:

```
% upd install kerberos [v<N_M>] -G -c
```

4) Log out, if necessary, and log in now as *root* (or **su** to *root*).

5) Choose the configuration option appropriate to your situation (as described in section 14.1.8 *Determine Kerberos Access Mode(s)*) and issue the corresponding **ups install** command (note the **ups** in place of the **upd**) to complete the installation of the **kerberos** product. You need to include the version (**v<N_M>**) only if **kerberos** has not been declared as “current”. (See section 16.1 *Alterations Made to your System when Fermi Kerberos is Installed* for information on what changes this portion of the installation makes to your system.)

a) For fully strengthened mode (required for on-site systems):

```
ups install kerberos [v<N_M>]
```

b) For mixed mode (allowed for off-site systems):

```
ups install-keep-ssh kerberos [v<N_M>]
```

c) For any other configuration, refer to the file

```
README.INSTALL.DETAILS (recommended for experts only)
```

6) If you wish to override the standard UNIX login program on the machine with a Kerberized login program as discussed in section 14.1.9 *Choose Login Program*, issue the command:

```
% ups install-login kerberos [v<N_M>]
```

where **v<N_M>** is not needed if the **kerberos** product is chained to “current”.

7) If you had installed **kerberos** v0_1 or v0_2 and are now reinstalling **kerberos** on the node, you need to clean out the files which had been copied to `/usr/local` (and are now copied to `/usr/krb5`). To so

1. Running the **upd install** command just puts the kerberos files in the products area. At this point you can run **setup kerberos** and you can get Kerberized network connections or do password maintenance. You cannot yet do any thing requiring a host key.

so, run the command:

```
% ups clean kerberos [v<N_M>]
```

where **v<N_M>** refers to the newly installed version, and is not needed if the new version is chained to “current”.

Also, if you are reinstalling, keep the same host and FTP service principals to reuse the identity of the machine.

Chapter 15: Installing Fermi Kerberos on a RedHat Linux System

In this chapter we provide instructions for installing the Fermilab **kerberos** product and Kerberized **ssh** on a RedHat Linux machine via **RPM**.¹ These products are also available as **UPS** products from *fnkits.fnal.gov*.



For your reference, the Fermilab Linux pages are online at <http://www-oss.fnal.gov/projects/fermilinux/>.

15.1 Before You Install Kerberos

15.1.1 Choose your Installation Method

Both the UPS/UPD and RPM installation frameworks are available for Kerberos on Linux machines. Both methods perform the installation of all the Fermilab Kerberos tools and configuration settings.

The UPS/UPD method has been around longer, and much work has gone into ensuring that it satisfies the Fermilab policy requirements. We recommend this for people running servers in the UPS framework.

We are confident that the RPM install also satisfies the Fermilab policy requirements. It leaves the systems in a PAM-aware configuration such that more of the normal RedHat tools function as expected. We recommend this installation for people using the stock FRHL configuration. The major advantages of this method are seen to be:

- 1) the potential for automatic updates via the AutoRPM service
- 2) the closer alignment with stock RH product management tools
- 3) increased ease of use for non-FNAL/non-UPS/UPD configurations

15.1.2 Differences between the UPS/UPD and RPM Ker-

1. We describe installation for fully-strengthened mode only (see discussion in section ??); due to details of the PAM configuration, the mixed-mode installation would violate Fermilab policy.

beros Products

Configuration

The UPS product configuration uses a perl script, the RPMs use bash scripts. For the most part all the RPM install scripts immitate what is done during the UPS product install.

The UPS Kerberos product is designed to be installed interactively, whereas an RPM is designed to be installed without any interaction, except for the `makehostkeys` script which must be run manually after everything else is installed. The `makehostkeys` script creates the `/etc/krb5.keytab` file, which allows Kerberized logins to a machine.

There are two configuration files for RPM that, in order to work with the pam modules, currently differ from the UPD/UPS Kerberos product:

- `/etc/krb.conf` changed to use the kerberos servers to authenticate
- `/etc/krb5.conf` added a section containing instructions for the pam modules

Login Program

The RPM Kerberos login program authenticates users at the login prompt with their Kerberos passwords, but may prohibit users from starting X windows. We plan to eventually replace this program with PAM modules. For now, we recommend that you install login program and try it out with the rest of the RPM Kerberos package. If you have any problems starting X windows, just remove the login RPM.

15.1.3 Follow Same Pre-install Steps as for UNIX

Obtain a Kerberos principal	See section 3.1.2 <i>Requesting a Principal</i> .
Create an account on the machine that matches your principal	See section 14.1.2 <i>Create an Account that Matches your Principal</i> .
Determine if you need to allow incoming Kerberos connections and/or FTP access. If so get a fixed IP and obtain host and service principals.	See section 14.1.6 <i>Do you Need to Allow Incoming Kerberos Connections?</i> .
Synchronize your machine with a time server	See section 14.1.7 <i>Synchronize your Machine with Time Server</i> .

15.2 Kerberos Installation Steps (RPM)

The procedures outlined in this section are designed to get your Linux machine fully Kerberized. You may be able to skip some steps depending on the current status of your machine. The commands shown in the steps reflect program versions as of December 2001. Make sure you know what the current versions of the products are so that you can install them. Log in as *root* to perform the installations. For more information, or to do a custom install, see the various README files that come with the Fermi ssh and Kerberos products.

15.2.1 Installation Steps for RH 6.x Based systems



Kerberos is not implemented with PAM in the 6.x environment. Thus the passwords that you use in your desktop environment (e.g., for screensavers, graphical logins, etc.) will remain the same as they were before.

- 1) Install Kerberized ssh (see section 14.1.5 *Install Kerberized SSH (Recommended)*). Available to fnal.gov domain machines only.

```
% rpm -Uvh
ftp://linux.fnal.gov/linux/contrib/DONOTEXPORT/s
sh/ssh-current.rpm
```

- 2) Install the kerberos product. Issue the **rpm** command for each of the files:

```
% rpm -Uvh
ftp://linux.fnal.gov/linux/contrib/kerberos/61x/
krb5-fermi-current.rpm
```

```
% rpm -Uvh
ftp://linux.fnal.gov/linux/contrib/kerberos/61x/
krb5-fermi-config-current.rpm
```

- 3) If you plan to allow incoming Kerberos connections (i.e., to allow incoming remote log in) and/or offer services, you need to create a keytab file. Run the script:

```
% /usr/krb5/config/makehostkeys
```

- 4) If you did a fresh Linux install, you'll need to go to `/etc/inetd.conf` and turn the services on (e.g., telnet, ftp).

15.2.2 Installation Steps for RH 7.1 Based Systems



Kerberos is implemented with PAM in the 7.x environment. Thus the passwords that you use in your desktop environment (e.g., for screensavers, graphical logins, etc.) will become the same as your Kerberos password. If you want these passwords to remain unchanged, skip the last two steps shown here.

- 1) If not already done, install Fermi RedHat Linux v7.1. (When you install or reinstall this, be aware that all the services (e.g., telnet, ftp) are turned OFF by default. After you Kerberize, you will need to turn them on in `/etc/inetd.conf`.) FRHL installation instructions can be found at <http://www.fnal.gov/cd/unix/linux/>
- 2) Install Kerberized ssh (see section 14.1.5 *Install Kerberized SSH (Recommended)*). Available to fnal.gov domain machines only.

```
% rpm -Uvh
ftp://linux.fnal.gov/linux/contrib/DONOTEXPORT/ssh/ssh-current.rpm
```

- 3) Install kerberos:

```
% rpm -Uvh
ftp://linux.fnal.gov/linux/contrib/kerberos/71x/krb5-fermi-current.rpm

% rpm -Uvh
ftp://linux.fnal.gov/linux/contrib/kerberos/71x/krb5-fermi-config-current.rpm
```

- 4) If you plan to allow incoming Kerberos connections (i.e., to allow incoming remote login) and/or offer services, you need to create a keytab file. Run the script:

```
% /usr/krb5/config/makehostkeys
```

- 5) Deactivate afs-pam:

```
% rpm -q afs-pam
```

- a) If the output from this command is `package afs-pam is not installed`, skip to step 6.
- b) Otherwise, determine the release and version from the output generated by this command. The release is after the second dash (well, “third” given the dash in `afs-pam`), version is after the following dash. E.g., `afs-pam-nonis-1` gives release as `nonis`, and version as `1`. Then run
`/usr/sbin/uninstall-afs-pam <release>`
`<version>` (e.g., `/usr/sbin/uninstall-afs-pam`

nonis 1)

- 6) Run `/usr/sbin/authconfig` to enable the Kerberos PAM.
- 7) If you did a fresh Linux install, you'll need to turn the services on. Go to the `/etc/xinetd.d` directory, and in each service-specific configuration file, set the flag `disable=yes` to `disable=no` (or remove the flag).

15.2.3 Fermi Kerberos and ssh RPM Descriptions

krb5-fermi

This contains the binaries and man pages from the Fermi kerberos product (except `/bin/login`). These files get installed in `/usr/krb5`, the same place as the product. If you installed an earlier version of Fermi kerberos and want a quick way to upgrade, install this rpm only. It doesn't perform any configuration in the files `inetd.conf`, `sshd_config`, `services`, or `krb5.conf` (though it does install a default `krb5.conf` if you don't already have one; you will need to edit it).

krb5-fermi-login

This rpm replaces your `/bin/login` with the Kerberized login. To get your old login back, just remove the rpm (using `rpm -e krb5-fermi-login`). You may not want this rpm because of one shortcoming regarding X.

krb5-fermi-config

This rpm has been made to work with Fermi RedHat 7.1.x and its corresponding Kerberos V5 rpms, in addition to FRHL 6.1.x. For FRHL 6.1.x it performs the configuration that you need to be fully Kerberized and configured for Fermi features, whereas for RH 7.1.x, it only configures Fermi features. It edits your `krb5.conf`, `inetd.conf`, `services`, and `sshd_config`. In addition, for FRHL 6.1.x it edits the `inetd.conf` file, and for 7.1.x it edits the configuration files in `xinetd.d`.

It also contains a `makehostkeys` script that you must run manually if this is your initial kerberos install. All the other included scripts are run just by installing the rpm. All of the scripts are stored in `/usr/krb5/config/` so that you can rerun any of them if necessary. Scripts in the configuration rpm include:

`makehostkeys` This creates your `/etc/krb5.keytab` file which allows Kerberized logins to your machine. If you want to log into your machine remotely, you must **run this**

script manually (host and ftp principals and passwords are required, and must be supplied at the start of the installation procedure).

`config-krb5.conf`

Builds (or rebuilds) the `/etc/krb5.conf` file to set your machine's default realm to `FNAL.GOV`.

`config-inetd.conf`

This kerberizes any normal inetd services that you have turned on (e.g., ftp).

`config-xinetd`

This kerberizes any normal xinetd services that you have turned on (e.g., ftp).

`config-services`

Ensures that all the Kerberos services are in your `/etc/services` file

`config-sshd_config`

Tightens down security on your `/etc/sshd_config` file so that a person has to have a Kerberos ticket to login via `ssh`¹.

ssh

At the heart of this rpm is the `sshd` startup script. It determines whether you have AFS and/or kerberos, and starts up the appropriate `sshd` accordingly. It is dynamic, in that it performs this check everytime the `sshd` is started.

Everything is put in `/usr/krb5`. Then a network of links is made to ensure that `ssh` is found in all of its usual places. In addition, we make sure that `/usr/krb5` gets added to your `$PATH`.

15.2.4 Kerberos and PAMs

A number of applications on Linux (most notably the screensavers) use authentication checks via the PAM libraries. The instructions earlier in this chapter enable most of these applications to use Kerberos. However, you may have to adjust modules in `pam.d` for custom configurations.

1. If you already have `ssh` running, and you want to keep it running, note that you can have either password-based `ssh` logins to an AFS machine OR kerberos-based logins via `ssh`, but not both. For the former, make sure that Password Authentication is "yes". If it's not, change it to yes, then run **kill -HUP** on the `sshd`.

We recommend the use of the standard RH `/bin/login` for Linux¹. This has the advantage of avoiding the problems with console ownership that occur using the FNAL `login.krb5` (it is not currently PAM-aware). However, it does require that you modify your standard PAM configuration. You may create a local account using standard methods, add the KRB5 authentication to the appropriate PAM modules (this is as easy as running `authconfig` with the 7.1 PAM version), or both.

For individuals administering their own desktops, we recommend that you do both. It is often convenient to have a local account for the cases when trouble arises. A local account is permitted, provided the following three conditions are met:

- the password hash is stored locally (no NIS, LDAP, etc.),
- the password cannot be used for network access (restrict to `securetty`)
- your local password does not contain your Kerberos password and is not similar to it

1. Note that the RH `/bin/login` doesn't support inbound portal mode (CRYPTOCard) logins, but this shouldn't be a problem. The Fermilab `sshd` (and `telnetd`) execute `/usr/krb5/sbin/login.krb5`. The `ftpd` never executes a login program.

Chapter 16: Kerberized UNIX System

Administration Issues

In this chapter we discuss some UNIX system administration issues related to the installation of Kerberos software.

16.1 Alterations Made to your System when Fermi Kerberos is Installed

When you issue one of the `ups install ...` commands to complete the installation of the **kerberos** product (see step 5 of section 14.2 *Installing Fermi Kerberos using UPS/UPD*, step 7 of 15.2.1 *Installation Steps for RH 6.x Based systems*, or step 6 of section 15.2.2 *Installation Steps for RH 7.1 Based Systems*), the following changes are made to your environment:

- new directory `/usr/krb5` and directories/files underneath are created
- some service (port) definitions are added to `/etc/services` (if not already present). Note that these changes must be made known to the system: for Sun and Linux, make sure `/etc/nsswitch.conf` points to the correct `services` file.
- `/etc/krb5.conf` and `/etc/krb5.keytab` files are added
- `/etc/inetd.conf` is altered to enable Kerberized services and disable non-Kerberized ones, then `SIGHUP` is sent to `inetd`¹. The default **kerberos** install preserves pre-existing usage of `tcpwrappers` on a service-by-service basis.
- if `ups install-keep-ssh` isn't chosen, `/etc/sshd_config` is also altered

1. If two `inetd` processes are running, some nonKerberized services like `rlogin` may get handled by a different file than `/etc/inetd.conf` and thus won't be disabled by the **kerberos** installation script as they should be.

16.2 Setting Defaults for Tickets/Applications

The `/etc/krb5.conf` file, described in Chapter 17: *The Kerberos Configuration File: `krb5.conf`*, contains configuration information needed by the Kerberos V5 library. This includes information describing the default Kerberos realm, and the location of the KDC. You can use it to set default flags for tickets (e.g., forwardable, renewable) and application parameters (e.g., tell application to forward “forwardable” tickets). If your machine is in a domain other than `fnal.gov`, you’ll need to add your domain to the `[domain_realm]` section of the file (see section Chapter 18: *Additional UNIX Sysadmin Information for Off-Site Installations*). For complete information, refer to <http://www.osxfaq.com/man/5/krb5.conf.html>.

Note that as of January 2001, the current `krb5.conf` file available from KITS does not turn on ticket forwarding by default (for applications that check this file, e.g., **telnet**, **rlogin**, **FTP**, **rsh**). This was changed in response to users’ concerns about inadvertently forwarding credentials to an untrustworthy machine. However if the sysadmin turns it on by editing `krb5.conf`, a later update or re-installation will leave that change alone.

16.3 The `/etc/hosts` File



In the `/etc/hosts` file, the first-listed name for the local system must be the full name, including the domain, and must not be a nickname. The line should be of the form:

```
<IP address> <node>.<domain> <node>
```

E.g.,:

```
<131.225.11.11> mynode.fnal.gov mynode
```

or, depending on your home institution, something like

```
<111.111.11.11> mynode.myuniv.edu mynode
```



Note regarding `tcpwrappers`: If in `/etc/hosts.deny` there is an entry `ALL : ALL`, then all `tcp` connections are disabled, unless explicitly enabled in `/etc/hosts.allow`.

16.4 Portal Mode Configuration

A UNIX host running **kerberos v1_0** or later performs the portal function by default when accessed via telnet or FTP from the untrusted realm, unless this mode is specifically disabled. Host and **FTP** principals must exist for the node in order to enable portal mode.

In the `inetd.conf` file (which resides in either `/etc` or `/etc/inet`) you should find a line for **telnet** similar to:

```
telnet stream tcp nowait root /usr/krb5/sbin/telnetd telnetd
-Pa valid
```

And for **FTP**:

```
ftp stream tcp nowait root /usr/krb5/sbin/ftpd ftpd -aOP
```

The **P** flag in these lines enables portal mode. To disable this mode, remove the **P** flag. (This still leaves unencrypted **rsh** and **rlogin** open¹.)

16.5 Register yourself as an Administrator

If you need to allow remote logins to your machine or offer services, you need host and ftp principals for the machine. First register yourself in the database of system administrators. Go to *System Administrator Registration* at <http://miscomp.fnal.gov/sysadmindb/> to register.

16.6 User Accounts and Passwords

16.6.1 User Account Names

Set up each user's account such that the account name (login id) is the same as the person's principal. Otherwise, the user is subject to the problems listed in *C.2 If your Principal and Login Name do not Match*.

1. To eliminate those, take out the klogin service from inetd (leave eklogin) and add an 'e' flag to the kshell service.

16.6.2 Determine if a Particular Principal Exists

If you need to check whether a principal has been created for a user, run the **kinit** command with the principal name you want to test. Enter at least one character at the password prompt. The text of the error message will indicate whether the principal exists or not. If the principal exists, it will give a message indicating the password is wrong:

```
% kinit tez
Password for tez@FNAL.GOV: x
kinit: Preauthentication failed while getting initial
credentials
```

If the principal doesn't exist, it will give a "Client not found..." message instead:

```
% kinit tezNOT
Password for tezNOT@FNAL.GOV: x
kinit: Client not found in Kerberos database while getting
initial credentials
```

16.6.3 User Passwords

A Kerberized machine uses the Kerberos login program by default, and that login program accepts Kerberos passwords. Standard UNIX passwords can be used for non-Kerberos-authenticated login at the console. If a user will only access the gateway remotely, the user's account doesn't need a local UNIX password. Using **!!** in the password field for that account in `/etc/shadow` will disable local login, while leaving remote Kerberos login available.

Disable NIS passwords and AFS passwords. There should be no passwords in the `yp` password files. Standard UNIX passwords can be used for non-Kerberos-authenticated login at the console.

16.6.4 Providing Access to Sensitive Accounts

You as the system administrator can choose to require that users of the *root* account and/or any other sensitive accounts obtain a *root instance* of their principal. This is described in section 9.4 *Using Root Instance of your Principal*.

To allow authorized users to log in directly to a sensitive account via `ssh`, `telnet`, `rsh`, `rlogin` or `ftp`, add the person's principal (or the person's */root* principal if you use that method) to the `.k5login` file in the account's home directory (`/root/` for Linux, `/` for the other supported flavors). This file is described in section 9.3 *Account Access by Multiple Users*.

For the *root* account, an alternative is for the authorized user to log in to the machine under his own login id, and provided he has a forwardable ticket on the machine, he can use **ksu** (instead of **su**) to run as *root*.

16.7 Non-user Accounts

There are often accounts maintained for file ownership/permissions reasons, and people don't log into these accounts. Typically these accounts have names that don't correspond to user names (e.g., "products"), but it is best to prevent accidental login in case a user's principal matches this account name. To do so, create an empty `.k5login` file in the account's home directory (see section 9.3.1 *The .k5login File*).

16.8 Searching KDC Log Files and the Principal List

The KDC log files and the list of principals are available in AFS space for users who are registered system administrators (see section 16.5 *Register yourself as an Administrator*). If you are a registered system administrator and can't access the KDC logs as described here, please contact nightwatch@fnal.gov.¹

The AFS directory `/afs/fnal.gov/files/data/k5logs` contains various KDC log files and a list of KDC principals. These files can be used by system administrators to understand error messages and to diagnose problems. All the directories referred to below reside under this directory.

The `princ/`, `kdc/`, `log/` and `adm/` directories contain subdirectories for the year and month. The format for the names of these directories is YYYY-MM (e.g., 2001-08). Under each YYYY-MM directory are the actual log files as listed here:

- `princ/` contains the weekly list of KDC principals, plus the `diag_user.pl` which allows you to look at yesterday's log file.
- `kdc/` contains the daily KDC transaction log files (the transaction records for each KDC are maintained in separate files)
- `log/` contains the daily KDC log files (not much here)

1. If your AFS username is different than your email username, it's likely that the script that built the AFS group that controls access to the KDC log files doesn't have your correct username and you can't access the files.

adm/ contains the daily KDC administration log files

The format for the names of the log files in these directories is

i-krb-<n>.YYYY-MM-DD (e.g., i-krb-3.2001-08-15). The meaning of i-krb-<n> is the DNS CNAME for a KDC as follows:

- i-krb-2 Pilot realm (PILOT.FNAL.GOV) master KDC (alias krb-pilot-1)
- i-krb-3 Production realm (FNAL.GOV) master KDC (alias krb-fnal-1)
- i-krb-4 FNAL.GOV realm backup KDC (alias krb-fnal-2)
- i-krb-5 PILOT/FNAL realm backup located in D0 (alias krb-fnal-5, krb-pilot-3)
- i-krb-6 PILOT/FNAL realm backup located in CDF (alias krb-fnal-4, krb-pilot-4)
- i-krb-7 PILOT/FNAL realm backup located in BD (alias krb-fnal-3, krb-pilot-5)
- i-krb-8 FNAL realm backup located in Soudan (alias krb-fnal-6)

The list of principals under the princ/ directory is only maintained for the master KDCs, i-krb-2 and i-krb-3. The list of principals includes the attributes for each principal and the expiration dates for the principal and password. Each principal record has comma-separated fields. The format of the records is as follows:

Field number	Field value	Description
1	principal name	full principal name including realm
2	principal expiration	number of days till principal expires, "*" for no expiration, "E" for expired
3	password expiration	same as for principal expiration
4 and beyond	principal attributes	

Most principal attributes are self explanatory such as "DISALLOW_FORWARDABLE". The attribute "DISALLOW_ALL_TIX" is used to disable a principal (except in the case of CRYPTOCard principals¹). The KDC transaction log files reside under the tmp/ and kdc/ directories:

1. Every user in possession of a CRYPTOCard has an "RB1" instance associated with his or her principal (e.g., username/RB1@FNAL.GOV), which we call a "CRYPTOCard principal". CRYPTOCard principals are given the "DISALLOW_ALL_TIX" attribute because the credentials obtained via a CRYPTOCard are associated with the principal name "username@FNAL.GOV".

`tmp/` contains the real-time KDC transaction log file, plus recent historical transaction log files, so look there to diagnose a problem in real-time.

`kdc/` contains the KDC transaction log files which are at least one day old.

The format of a KDC transaction log file is variable. The `diag_user.pl` perl script in the `tmp/` directory can be used to view the KDC transaction log file for a specific user. For example, if user `johndoe` is having a problem, try the command (from the directory `tmp/`):

```
% ./diag_user.pl johndoe
```

This command uses `grep` to search the current KDC transaction log file `kdc.log` for records with the string `johndoe`. The command will also output specific error records from the log file that pertain to “johndoe” transactions. The error records appear immediately before the transaction record and are missed if the standard `grep` command is used. Interpreting these KDC error messages is more art than science(!) For example, here is an error that indicates `johndoe` is using the wrong password (from the `tmp/` directory)

```
% ./diag_user.pl johndoe
```

```
ERROR->No such file or directory - pa verify failure
08:30:31=>AS_REQ from fnkerb.fnal.gov(131.225.68.13) PREAUTH_FAILED
johndoe@FNAL.GOV for krbtgt/FNAL.GOV@FNAL.GOV, Preauthentication failed
```

The “No such file or directory” output means wrong password. The next record containing “Preauthentication failed” is the message user `johndoe` receives.

There is another version of the `diag_user.pl` tool in the `princ/` directory. If used from there, the tool defaults to looking at yesterday’s log file.

16.9 Changing a Machine’s Node Name

If you need to change the node name of a Kerberized machine, the host and **FTP** service principals and keys, if any, must also be changed. There is no “rename” function on the principal database, so the old service keys must be deleted and new ones added. Request new service principals `host/<newname>.<domain>` and `ftp/<newname>.<domain>` using the form at <http://www.fnal.gov/cd/forms/strongauth.html>. When you get them, follow one of these procedures to change your node name.

16.9.1 Using UPS

If you have installed Fermi Kerberos, have **UPS** running and don't mind an interruption, the easiest way to change your node name is to:

- 1) Change the node name
- 2) Delete `/etc/krb5.keytab`
- 3) Run the command: **ups install-hostkeys kerberos** and provide the new password(s) when prompted.

16.9.2 Using Kerberos Utilities

If you're not running UPS, you'll need to use the native Kerberos utilities. You can avoid interruptions of service during the name change if you want to prepare in advance.

Once you get your new service principals, follow the procedure outlined in section 16.10 *Installing Service Host Keys* to install the new keys.

Then change the node name, and reboot as necessary. You may delete the old host and **FTP** keys from the `keytab` using the **ktutil** command:

```
% /usr/krb5/sbin/ktutil
```

```
ktutil: rkt /etc/krb5.keytab
```

```
ktutil: list
```

```
slot KVNO Principal
-----
1 2 host/oldname.domain@FNAL.GOV
2 2 ftp/oldname.domain@FNAL.GOV
3 2 host/newname.domain@FNAL.GOV
4 2 ftp/newname.domain@FNAL.GOV
```

```
ktutil: delent 2
```

```
ktutil: delent 1
```

Note: Delete entry 2 before entry 1 because they all drop down a slot after **delent**. Continue:

```
ktutil: wkt /etc/krb5.keytab.new
```

```
ktutil: quit
```

```
% mv /etc/krb5.keytab.new /etc/krb5.keytab
```

Done!

16.10 Installing Service Host Keys

With new host and FTP service principals and their assigned password(s) in hand, log in as *root* and run the **kadmin** command as shown below to install the keys (use appropriate values of **hostname**, **domain** and **REALM**). Note that Kerberos clients append the machine's default realm to the principal names typed in the **kadmin** command (**hostname.domain**). If the default realm of the machine does not match the realm for which the principals/keys were created, then include the **-r <REALM>** option.

```
% /usr/krb5/sbin/kadmin -p host/<hostname.domain> \  
-q "ktadd host/<hostname.domain>" [-r <REALM>]  
Enter password: <type in host principal's password>  
% /usr/krb5/sbin/kadmin -p ftp/<hostname.domain> \  
-q "ktadd ftp/<hostname.domain>" [-r <REALM>]  
Enter password: <type in ftp principal's password>
```

16.11 Static IP vs. DHCP Addresses



You can get host and FTP principals for a DHCP-based machine, but your service principals will work only for your nominal node name (e.g., `host/mynode.dhcp.fnal.gov` and `ftp/mynode.dhcp.fnal.gov`). Whenever that name does not resolve to your current IP address, then the service principal is of no use, and you can't authenticate to your host (you can still authenticate yourself to other hosts). A different machine using your node name cannot impersonate your node or steal Kerberized connections intended for your machine, so there's no risk, just inconvenience. However, if you plan to offer reliable services, a static IP address is the better solution.

16.12 Multiple IP Addresses or Node Names

If your machine is configured to have two or more active (static) IP addresses, as long as there's just one node name, you do not need multiple service principals. Just make sure all the IP addresses are listed in DNS. There should be no problems using credentials which have been *forwarded to* such a single-named host.

If you have multiple node names (which are not nicknames), get a host service principal for each name. This will take care of telnet and the r-commands. FTP will not work properly under these circumstances, and credentials forwarded to such a host will be only partly usable.

16.13 Laptops

The feature that sets laptops apart as regards authentication is the fact that they may have different host names and/or IP addresses depending on where they're being used. Install the Kerberos product on it as you would on any other machine, but first decide whether you want a static IP address or if you want to use DHCP.

Chapter 17: The Kerberos Configuration File:

krb5.conf

In this chapter we describe the Kerberos configuration file `krb5.conf`.

A `krb5.conf` file must exist in the `/etc` directory on each UNIX node that is running Kerberos. We provide a template for this file in the **krb5conf** product in KITS (under `ftp://ftp.fnal.gov/products/krb5conf/`).

If you install Fermi **kerberos** from KITS using UPS/UPD or RPM for Linux, the **krb5conf** product (and file) gets installed automatically for you. If you obtain Kerberos from another source, you must obtain this file yourself, edit it as necessary, and copy it into the `/etc` directory of your machine.

You may need to update your `krb5.conf` file from time to time as the template in KITS gets updated. New versions are announced on the *kerberos-users@fnal.gov* mailing list.

If you need to change a setting in `krb5.conf` but cannot or don't want to change the file in `/etc`, you can copy `/etc/krb5.conf` to a new file and edit this copy. Then set the environment variable `$KRB5_CONFIG` to the full name of your copy. Your copy will be honored by client programs such as **kinit** or **rlogin**, but not by programs that need a trusted configuration file, e.g., **ksu** and the service daemons.

17.1 What does `krb5.conf` Control?

The file consists of several stanzas, each of which controls certain aspects of the installation:

- `[libdefaults]` sets defaults for Kerberos on your system, e.g., default realm, default ticket lifetime
- `[realms]` tells where to find the KDCs for each realm
- `[instancemapping]` maps client principal properly (for things like cron jobs which require a special principal)
- `[domain_realm]` maps domains to realms
- `[logging]` tells Kerberos where and how to log errors

- [appdefaults] lists default settings for outgoing Kerberized network connection applications and for incoming portal mode connections

In section 17.4 *krb5.conf.template (krb5conf v1_5)* we list the template `krb5.conf` file (current as of November '01) with annotations.

17.2 Reinstall krb5conf Using UPD

To reinstall **krb5conf** and thus update your `/etc/krb5.conf` file using UPS/UPD, log in as *root* (or any login id with permissions to write in `/etc`), and run:

```
% upd install krb5conf -G -c
```

Then on all nodes in the cluster (including the original node), run the command:

```
% ups installAsRoot krb5conf
```

Or instead of the **ups installAsRoot** command, after running **upd install**, you may manually set the `SOURCE_FILE` environmental variable to point to the `krb5.conf.template` script:

```
% SOURCE_FILE=/path/to/krb5/ups/krb5.conf.template
```

and then invoke the `install` script

```
% /path/to/krb5/ups/install
```

17.3 Obtain krb5conf without Using UPD

If you're not running **UPS/UPD**, go to

```
ftp://ftp.fnal.gov/products/krb5conf/vx_y/NULL/krb5c  
onf_vx_y_NULL.tar (where x_y is 1_5 as of September 2001).
```

Download and untar the file. Look at the top of the `installAsRoot` script for instructions on how to install it without **UPS**. If you're not running **AFS**, check to be sure that the `installAsRoot` script changes the following line in `/etc/krb5.conf` to "false":

```
krb5_run_aklog = false
```

17.4 krb5.conf.template (krb5conf v1_5)

For reference, we provide the `krb5.conf.template` file contents for version `v1_5`, with some explanations inserted. If you install the **krb5conf** product using UPD, the necessary name substitutions will be made as part of the installation; otherwise, you need to edit this file manually.

[libdefaults]

This section sets defaults for Kerberos on your system.

```
ticket_lifetime = 1560
```

There are some implementations of Kerberos that read the above number as seconds, and is equivalent to 26 hours. In MIT-derived code (which Fermi's is), it's read as minutes.

```
default_realm = xMYREALMx
```

The UPD installation process changes `xMYREALMx` to `FNAL.GOV`. (In Kerberos transactions, this `default_realm` is assumed when you mention any principal without its “@REALM” part.)

```
checksum_type = 1
```

```
ccache_type = 2
```

```
default_tgs_etypes = des-cbc-crc
```

```
default_tkt_etypes = des-cbc-crc
```

[realms]

This section lists the realms, and for each the KDCs, admin server (master KDC), the `default_domain` for converting between Kerberos v4 and Kerberos v5 service names, and principal-to-account name matching info.

If and when we cross-authenticate with some other site, each host that wants to initiate connections *to* the other site will have to list that site's realm information here. (We think it won't be necessary for accepting connections *from* that site.)

```
PILOT.FNAL.GOV = {
```

```
    kdc = krb-pilot-1.fnal.gov:88
```

```
    kdc = krb-pilot-3.fnal.gov:88
```

```
    kdc = krb-pilot-4.fnal.gov:88
```

```
    kdc = krb-pilot-5.fnal.gov:88
```

```
    admin_server = krb-pilot-admin.fnal.gov
```

```
    default_domain = fnal.gov
```

```
    auth_to_local = RULE:[1:$1@$0](.*@FNAL\.GOV)s/@.*//
```

This RULE line allows authentication for `username@FNAL.GOV` and `username@PILOT.FNAL.GOV` no matter which is the host's default realm.

```
    auth_to_local = DEFAULT
```

The `auth_to_local` lines provide rules for matching an authenticated principal name to a (local) UNIX name; they are used only if there is no `.k5login` file in the user's UNIX home directory. The value `DEFAULT` is equivalent to having no `auth_to_local`.

```

}
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
    default_domain = fnal.gov
    auth_to_local = RULE:[1:$1@$0](.*@PILOT\.FNAL\.GOV)s/@.*//
    auth_to_local = DEFAULT
}
WIN.FNAL.GOV = {
    kdc = newpckits.fnal.gov:88
    admin_server = newpckits.fnal.gov
    default_domain = fnal.gov
}

```

[instancemapping]

This deals with the instance portion of a principal (see *principal* in the *Glossary*). The lines that follow instruct Kerberos to strip a trailing `/cron/*` or `/cms/*` portion of the client principal when generating a Kerberos v4 ticket for the service called `afs`.

```

afs = {
    cron/* = ""
    cms/* = ""
}

```

[domain_realm]

In this section the domains get mapped to the realms. (This determines the realm in which you need to get a service ticket to log into a Kerberized host in a particular domain.) For individual machines in a domain that need to be mapped to a different realm than the domain as a whole, list each machine separately, mapped to the correct realm. Make your changes in the lower part of this section as noted below.

```

.fnal.gov = PILOT.FNAL.GOV
.minos-soudan.org = FNAL.GOV
xMYNODEx = xMYREALMx

```

The first and third items above are not needed if you use DNS.

```

fsus01.fnal.gov = xMYREALMx
fsus03.fnal.gov = xMYREALMx

```

```
fsus04.fnal.gov = xMYREALMx
```

The previous three are individual AFS server nodes that happen not to have Kerberos V5 at all (yet). To make **aklog** work without spurious error messages, it has to believe that the AFS servers are in the same realm as the host itself.

```
c243580-a.wheaton1.il.home.com = FNAL.GOV
```

```
# The whole "top half" is replaced during "ups installAsRoot
krb5conf", so:
```

```
# It would probably be a bad idea to change anything on or above
this line
```

```
# If you need to add any .domains or hosts, put them here
```

```
[domain_realm]
```

```
.ts.infn.it = PILOT.FNAL.GOV
```

```
.pi.infn.it = PILOT.FNAL.GOV
```

```
.physics.lsa.umich.edu = PILOT.FNAL.GOV
```

```
.phys.ttu.edu = PILOT.FNAL.GOV
```

```
mojo.lunet.edu = FNAL.GOV
```

```
[logging]
```

This section tells Kerberos where and how to log errors; through syslog or directly to file.

```
default = SYSLOG:ERR:AUTH
```

```
[appdefaults]
```

This section lists default application settings (ticket attributes, login parameters, etc.). All of these defaults (or nearly all) can be overridden by a command-line flag. The `krb5.conf` file just sets the defaults for the host. The ftp client does not look for defaults here.

```
default_lifetime = 7d
```

```
retain_ccache = false
```

`retain_ccache` determines whether tickets in a user's ticket cache on a particular host get saved (`true`) or destroyed (`false`) when the user closes his session on that host.

```
autologin = true
```

```
forward = false
```

`forward` should in most cases be set to `true`, in order to forward tickets obtained as "forwardable" to remote hosts by default.

```
renewable = true
```

```
encrypt = true
```

```
krb5_aklog_path = /usr/krb5/bin/aklog
```

The initial list is for common settings. These values are used by all the applications except when an overriding value is listed for a particular application; see below.

```
telnet = {  
}
```

Telnet uses the common settings; no overrides.

```
rcp = {  
    forward = false  
    encrypt = false  
    allow_fallback = true  
}
```

Whereas rcp sets two overrides (the first of which is unnecessary) and one additional parameter.

```
rsh = {  
    allow_fallback = true  
}  
rlogin = {  
    allow_fallback = false  
}  
  
login = {  
    forwardable = true  
    krb5_run_aklog = true  
    krb5_get_tickets = true  
    krb4_get_tickets = false  
    krb4_convert = false  
}
```

`login` is invoked by `telnetd` (not `telnet`) and `sshd` (not `ssh`), and may be invoked by the OS for a local (console) login. CRYPTOCard logins use these settings.

```
kinit = {  
    forwardable = true  
    krb5_run_aklog = true  
}
```

```
pam = {  
    forwardable = true  
}
```

```
rshd = {  
    krb5_run_aklog = true  
}
```

```
ftpd = {
```

```
krb5_run_aklog = true
default_lifetime = 6h
```

The ticket lifetime here is only invoked for CRYPTOCARD FTP access.

```
}
```


Chapter 18: Additional UNIX Sysadmin

Information for Off-Site Installations

In this chapter, we discuss some miscellaneous issues that sysadmins of off-site Kerberos installations should be aware of. Also see Chapter 6: *Logging In from Off-Site*.

18.1 root access to /usr

The binaries for the **kerberos** product go into `/usr/krb5`, so you don't need access to `/usr/local`. As long as you have *root* access to `/usr`, you can install the product.

18.2 Obtaining the krb5.conf File

We recommend that you use the most recent **UPS** tar file for `krb5.conf` from `ftp://ftp.fnal.gov/products/krb5conf/` (as of this writing, December 4, this would be `ftp://ftp.fnal.gov/products/krb5conf/v1_5/NULL/krb5conf_v1_5_NULL.tar`). The `krb5.conf` template is updated from time to time. These updates are announced on the *kerberos-announce* mailing list.

If you're not running **UPS**, untar it and look at the top of the `installAsRoot` script for instructions on how to install it without **UPS**. If you're not running **AFS**, check to be sure that the `installAsRoot` script changes the line in `/etc/krb5.conf` to:

```
krb5_run_aklog = false
```

The `krb5.conf.template` file from the `krb5conf` product now has lines containing `xMYREALMx` and `xMYNODEx` which have to be edited if doing a manual installation. To join the `FNAL.GOV` production realm, change `xMYREALMx` to `FNAL.GOV` and `xMYNODEx` to the fully-qualified name of host.

18.3 When your Node is in a Different Domain

If your machine is part of a different domain than `.fnal.gov`, you need to inform applications (e.g., **rsh**, **rlogin**, **telnet**, **FTP**) that it is part of the `FNAL.GOV` strengthened realm. There are two ways to do this:

The First Way:

In the `[domain_realm]` section of the `/etc/krb5.conf` file on the systems from which you'll be logging on, add lines of the form:

```
<domain> = FNAL.GOV
```

with and without the leading dot, e.g.,

```
.myuniv.edu = FNAL.GOV
```

```
myuniv.edu = FNAL.GOV
```

(You only need to add the domain without the leading dot if the undotted form is the name of some host, which is sometimes the case.) This tells applications that any node in this domain should be assumed to be in the `FNAL.GOV` realm. Otherwise the host's realm is taken to be the hostname's domain portion converted to upper case.

Since the **krb5conf** product can be updated independently of each new release of the Fermi **kerberos** product, you can send mail to *nightwatch@fnal.gov* to request that your domain be added to the template.

The Second Way:

Whenever you run one of the network connection applications (except **FTP**), just add **-k FNAL.GOV** to the command line, e.g.,:

```
% telnet -x -k FNAL.GOV mynode.myuniv.edu
```

18.4 Connecting from One Off-Site Domain to Another

This concerns connections between two Kerberized machines in the `FNAL.GOV` strengthened realm where neither is in the `fnal.gov` domain and they are in different domains from each other, e.g., *mynode.myuniv.edu* and *yournode.youruniv.edu*. In order for one of these Kerberized machines to connect directly to the other via **telnet** or **FTP**, the `/etc/krb5.conf` file

on each must contain the `[domain_realm]` mapping for both off-site domains. This does not concern portal mode where the client machine is unstrengthened.

Chapter 19: Installing and Configuring WRQ®

Reflection on a Windows System

In this chapter we describe how to install and configure the **WRQ® Reflection** software on your Windows system (Windows 2000, NT4¹) in order to authenticate to Kerberos from your Windows desktop, access Kerberized machines, and optionally encrypt your data transmissions. This has been updated for **WRQ® Reflection v9.0.0**.

19.1 Getting Ready

First, verify that you have administrator privileges on the PC. Next, you need to obtain a Kerberos principal and initial password for the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal*.

For PCs running Windows Windows 2000 (also called Win2k), NT4, 95 or 98, you need to install two **WRQ® Reflection** software products, **Reflection Kerberos Manager v9.0.0** which runs the **Kerberos Manager** on your PC, and **Reflection X v9.0.0** which is a terminal emulation package similar to **Hummingbird eXceed**, but with Kerberos authentication added.



- Notes: You need a license for the **WRQ® Reflection** software; contact your group's PC administrator or your local W2k/NT server administrator to request one.
- You do not need to remove previous versions of the software before installing these components.
- Installing the recommended components of the **WRQ® Reflection v9.0.0** product will consume about 65 MB of disk space.
- It is possible to run **WRQ® Reflection** with other terminal emulation products, however the Computing Division may not support combined installs.
- After installing this software you will still log into your PC the same way as before (e.g., for the FNAL NT domain, use your FNAL NT domain userid and password; for the W2k Kerberized domain, use your W2k Kerberos password). You will need to provide your FNAL realm

1. The procedures are expected to work also on Windows ME, 98 and 95, although these operating systems have not been tested.

principal and Kerberos password only when you run the **Kerberos Manager** or attempt to connect to a Kerberized node over the network from your PC.



- You can configure the **Reflection** software to access nonKerberized nodes, however it doesn't provide access to **ssh**-only nodes. For that you'll need to install **ssh** software on your PC. See the *Ssh Programs for Windows* page for suggestions (http://www.fnal.gov/www/docs/strongauth/html/ssh_programs.html).
- The **Reflection X** portion of the software must be installed before the **Security Components** portion; the automated install takes care of this.

Subscribe to the *wrq-users@fnal.gov* mailing list to receive announcements about this product, to benefit from other users' experiences and to share your own, or to ask questions.

19.2 Automated Installation of WRQ® Reflection v9.0.0

A script is available that performs an automated installation of both portions of the **WRQ® Reflection** software: **Reflection X**, and **Reflection Security Components**. It has been successfully tested on NT4 and Win 2000. It may work on Windows ME, 98 and 95 as well, but has not been tested.

The **WRQ® Reflection** v9.0.0 installation script is located at `\\PCKits\WRQ\Reflection_9.0\Automated Install\Install_WRQ.bat`. We reproduce it here:

Read the `README.txt` file,

```
Instructions to install WRQ Reflection X and Security Components using
the automated script.
```

```
This script has been tested on Windows NT 4.0 and 2000, use it on
Windows 9x or ME at your own risk!
```

- ```
1) Ensure that one of the following two conditions exists:
 a) the \\pckits\WRQ area is mapped to a drive letter (even if this area
 appears in your network listing, the installation will only work
 if the area is MAPPED TO A DRIVE LETTER)
or
 b) the Automated_Install directory is copied to a local drive.

2) To launch the install, double click on Install_WRQ.bat and follow
the prompts in the Command Prompt window that opens.

3) Note that if your program files folder is not "C:\Program Files"
the automated install will stop after installing the Reflection X
product and give you instructions on how to install and configure
the Security Components.
```

Run the `Install_WRQ.bat` file by double-clicking on it. You will need to respond to a series of questions, reproduced here. Answer each with a “y” for “yes”, as shown. A series of windows will appear and provide status information.

```
This will install WRQ Reflection 9.0 with Security Components 9.0
Do you want to continue [Y,N]?y
Installing WRQ Reflection
Wait for the installation window to disappear, then
Press any key to continue ...
Installing WRQ Security Components.
Wait for the installation window to disappear, then
Press any key to continue ...
Do you wish to install the default FNAL realms[Y,N]?y
Writing the realm defaults into the Registry
Do you wish to update your services file[Y,N]?y
Install of Reflection X and Security Components has completed.
ECHO is off.
Please reboot!
Press any key to continue ...
```

Reboot as instructed. The **Reflection** products will appear in your **START** menu under **PROGRAMS**. The **Kerberos Manager** configuration should reflect the FNAL production realm when done.

## 19.3 Time Synchronization

---

Kerberos requires a time sync within five minutes, each machine to its local time zone. Version 9.0.0 of the **WRQ® Reflection** software includes time sync software (version 7.0.2 also did; version 8.0.0 did not).

### 19.3.1 WRQ® Reflection 9.0.0

- Navigate to **START > PROGRAMS > REFLECTION > UTILITIES > REFLECTION TIMESYNC** to open the **Reflection TimeSync** application.
- Make sure the *Synchronize* tab is selected.
- Under **Time synchronization**, check `Automatically synchronize time:` and check `Once at system startup`, or if you don't restart your machine frequently, the other option is better (the default 1000 mSec accuracy is fine).
- Under **Time Servers** enter the IP addresses of the default primary and secondary time servers. Use the Fermilab core router 131.225.8.200 as primary and 131.225.17.200 as secondary. Check `NTP` for both.
- Again under **Time synchronization**, click `Synchronize Now` to set the system clock and check the time server setting.
- Click **OK**.

## 19.3.2 WRQ® Reflection 8.0.0

### Windows 2000 Host

If you first want to see what your Time service is set to on your Win2K machine, pull up the command prompt, and query the setting by issuing:

```
% net time /querysnTP
```

To synchronize the time, issue the following command:

```
% net time /setsntp:131.225.xx.200
```

where **131.225.xx.200** is the IP address of your network gateway at Fermilab. Stop and restart the network time service, by running:

```
% net stop "windows time"
```

```
% net start "windows time"
```

### Windows NT Host

To synchronize the time on an NT machine, we recommend the MicroSoft utility TIMESERV. This is part of the Windows NT resource kit, and called Timeserv.exe. The servers are configured to look at the gateway given in the IP request.

## 19.3.3 WRQ® Reflection 7.0.2

If you had installed **Reflection Signature v7.0.2** and you haven't removed it, you can navigate to **START > PROGRAMS > REFLECTION > TIMESYNC** to open the **Reflection TimeSync** application. Then follow the instructions under section 19.3.1 *WRQ® Reflection 9.0.0*.

## 19.4 Configuring WRQ® Reflection Kerberos Manager v9.0.0

---

In this section we assume you've just installed **WRQ®** for the first time via the automated install script. Most of the configuration is done for you. Your software should recognize the FNAL.GOV realm, and your principal should be set up.

- 1) Navigate to **START > PROGRAMS > REFLECTION > UTILITIES > KERBEROS MANAGER** to open the **Reflection Kerberos Manager** application. Pull down the **CONFIGURATION > CONFIGURE REALMS...**

menu, make sure the *Configuration* tab is selected. Highlight the `FNAL.GOV` realm and click the *User Defaults* tab.

- 2) On the **USER DEFAULTS** screen, the default realm should show `FNAL.GOV`. Set the default ticket lifetime to 23 hours (or less)<sup>1</sup>. Click **OK**.
- 3) Your default principal profile, `<your_principal_name>@FNAL.GOV`, should be created and configured properly by the automated install. If you wish to store your Kerberos credentials in memory rather than in a file<sup>2</sup>, you'll have to create a new principal profile. To do so, continue with the next step. To use the existing profile, skip to step 7.
- 4) To create a new profile, on the **REFLECTION KERBEROS MANAGER** window, select **CREDENTIALS > NEW PRINCIPAL PROFILE...** On the **ENTER PRINCIPAL** screen, check that your principal name is correct and that the **REALM** shows `FNAL.GOV`; they should be filled in by default. Click **OK**.
- 5) On the **CREATE NEW PRINCIPAL** screen, you can leave the **CREDENTIALS STORAGE** name as given. For **STORAGE MEDIA**, you can accept the **FILE** default, or you can choose **MEMORY** for higher security. Click **CREATE**. Your newly created profile is automatically set as the default profile (notice the blue check next to it).
- 6) Remove your original profile. First make sure it is no longer set as the default profile. (Select the new one and click **SET AS DEFAULT PROFILE** if necessary.) Select your original profile and click **CREDENTIALS > REMOVE PRINCIPAL PROFILE**. Click **YES** at the confirmation prompt.
- 7) To go ahead and authenticate, click **CREDENTIALS > AUTHENTICATE...** and enter your Kerberos password when prompted. You should see a ticket-granting ticket `krbtgt/FNAL.GOV@FNAL.GOV`. If you receive an error message instead, check that the above steps were followed correctly and that you typed the right password. Also check the **TIME SYNC** (see section 19.3 *Time Synchronization*). If you

---

1. If you leave it as zero, then when you authenticate, the default lifetime is set to 8 hours. It's easier to set it to the right value once in the configuration rather than to set it each time you authenticate.

2. Storing your credentials in memory causes your credentials to be destroyed when the **REFLECTION KERBEROS MANAGER** and all Kerberized applications are closed. If you choose to store them in a file (the default), we recommend that you also check **CLEAR ALL TICKETS ON SHUTDOWN** under the **CONFIGURATION** menu. **CLEAR ALL TICKETS ON SHUTDOWN** causes all tickets on the PC to be cleared when you close the last application that was using Kerberos authentication. See also the application's Help for "Storing Your Principal Profiles and Credentials".

continue to receive an error message, send the exact error message text to [nightwatch@fnal.gov](mailto:nightwatch@fnal.gov).

- 8) If you haven't changed your initial Kerberos password (which expires 30 days after it is created), you can change it now. Back on the **REFLECTION KERBEROS MANAGER** window, from the **TOOLS** menu select **CHANGE PASSWORD...** and change it. See section 3.2.2 *Choosing a Kerberos Password* for information on choosing passwords.
- 9) You may want to create a shortcut for the **Reflection Kerberos Manager** application in your **PROGRAMS > STARTUP** folder to start the application automatically each time you log into Windows.
- 10) Proceed with the configuration of **Reflection X**, below.

## 19.5 Configuring WRQ® Reflection X

---

- 1) Invoke the **Reflection X Client Manager** using the **START** menu. You will be prompted to run the **Reflection X Performance Tuner**. Click **YES** to run these tests to optimize performance before using the X client manager.
- 2) The **Reflection X Client Manager** next prompts you to **SELECT XDMCP HOST**. Click **NO** if you don't use XDMCP (X Display Manager Control Protocol) to start clients.
- 3) Now you have the option to let the client wizard create **Reflection X** client files for you. If you say yes, follow the wizard's instructions.
- 4) At the bottom of the **Reflection X Client Manager** window, click **Never close client starter connection** under the **ADVANCED** button. Also select **KERBERIZED TELNET** as the method.
- 5) If you logged on as **Administrator**, log off and log back on with your normal userid.
- 6) You may want to create a shortcut for the **Reflection X Client Manager** application in your **PROGRAMS > STARTUP** folder to start the application automatically each time you log into Windows. If so, we recommend that you specify "Run: Minimized" in the shortcut properties.

## 19.6 Configuring WRQ® Reflection telnet Connections

---

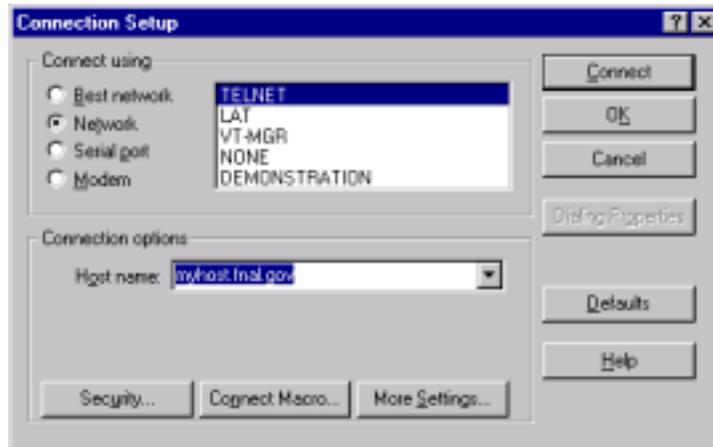
You can define a telnet configuration (profile) specific to each host you need to access, and save each one to a file. To run telnet to a particular host, you just run its corresponding profile (see section 4.7 *Logging In Through WRQ® Reflection Software from Windows*).

### 19.6.1 For Kerberized Host

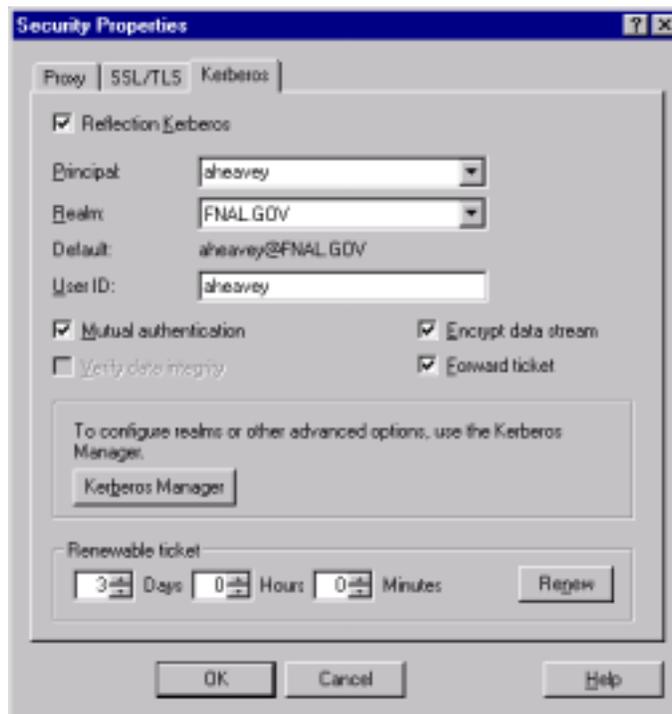
- 1) To configure the **Reflection telnet** client to access a remote Kerberos system, first open **START > PROGRAMS > REFLECTION > HOST - UNIX AND DIGITAL**.

To configure your profile, start from the **UNTITLED - REFLECTION FOR UNIX AND DIGITAL** window. Pull down the **CONNECTION > CONNECTION SETUP...** menu, click the **NETWORK** radio button in the **CONNECT USING** area, and make sure **TELNET** is highlighted in the scroll box:

- 2) Fill in the **HOST NAME** of your target Kerberos system.



- 3) Click **SECURITY**.



Select the *Kerberos* tab. Check *Reflection Kerberos*.  
Principal: Enter your FNAL principal name.

Realm: Assuming the target host is in the FNAL.GOV realm and FNAL.GOV is the default realm set in **Kerberos Manager**, select either (default) or FNAL.GOV.

User ID: If your user id on the target host doesn't match your principal, fill in the user ID.

Mutual authentication should be checked by default; leave it checked.

Check just `Forward ticket`, or check both that and `Encrypt data stream`. If you have forwardable tickets and choose `Forward tickets`, then you can make further connections to other Kerberized machines without having to type your Kerberos password over the net, so you may not need an encrypted connection. (Whenever you authenticate via the **Kerberos Manager**, you will need to check **FORWARDABLE** in order to obtain tickets that can be forwarded by this telnet connection.) Conversely, if you don't forward tickets, then you must make sure not to do anything that involves typing your Kerberos password over the net, even if you check `Encrypt data stream`.

To request a renewable ticket (maximum lifetime at Fermilab defined as seven days), enter a non-zero lifetime value under `Renewable ticket`. (Whenever you authenticate via the **Kerberos Manager**, you will need to specify a non-zero **RENEWABLE LIFETIME** in order to get tickets that can be renewed. The lesser of the two renewable lifetimes value is used.)

Click **OK** to return to the **CONNECTION SETUP** window.

4) If you want to connect immediately, click **CONNECT**. (If you haven't already run **Kerberos Manager** to obtain a ticket-granting ticket, you'll be prompted for your Kerberos password and then logged in. If you don't want to connect now, just click **OK**.)

5) Optional: From the **REFLECTION FOR UNIX AND DIGITAL** window you can go to the **SETUP** menu and choose to configure a number of nonessential but useful features in the areas of terminal emulation, keyboard mapping, mouse mapping, display, and so on.

If you will be logging onto several different hosts, it is particularly useful to set each `Window Title` to the host name (use `&h`). For instructions, in the **SETUP > DISPLAY... > OPTIONS** dialog box, click on the ? (upper right corner, as usual), then on **WINDOW TITLE > DETAILS**.

6) Run **FILE > SAVE AS** to save the host-specific settings in a file that you name. The system prompts you to save the file in the **PROGRAMS\REFLECTIONS** folder.

7) To start a telnet session to the host for which the profile was created, navigate to **START > PROGRAMS > REFLECTION > HOST - UNIX AND DIGITAL**. Pull down the **FILE** menu, select **OPEN**, and double-click the configuration file name. If you haven't yet authenticated, you will need

to provide your Kerberos password. It does not go over the net when typed at this point.

## 19.6.2 For nonKerberized Host

For connections allowing weak (standard) authentication, you don't need to worry about the **Kerberos Manager** since credentials aren't an issue. To configure a standard **telnet** profile, follow the same steps as in section 19.6.1 *For Kerberized Host*, but make sure the host name is a nonKerberized node, and eliminate step (3) which sets the Kerberos security.

## 19.6.3 Create a Template Configuration

To create a template **telnet** profile, first create and save a model profile for any Kerberized or nonKerberized host, as appropriate, as described in section 19.6.1 or 19.6.2. Pull up that profile, use it to log on to the host, and exit out. Select **CONNECTION > CONNECTION SETUP...** Remove the host name from the configuration and save it as a template file (choose an appropriate filename). To use the template to create a host-specific profile, bring up the template (it should appear in the **Reflections** folder), add the desired host name, and save it to a different file with a host-specific name.

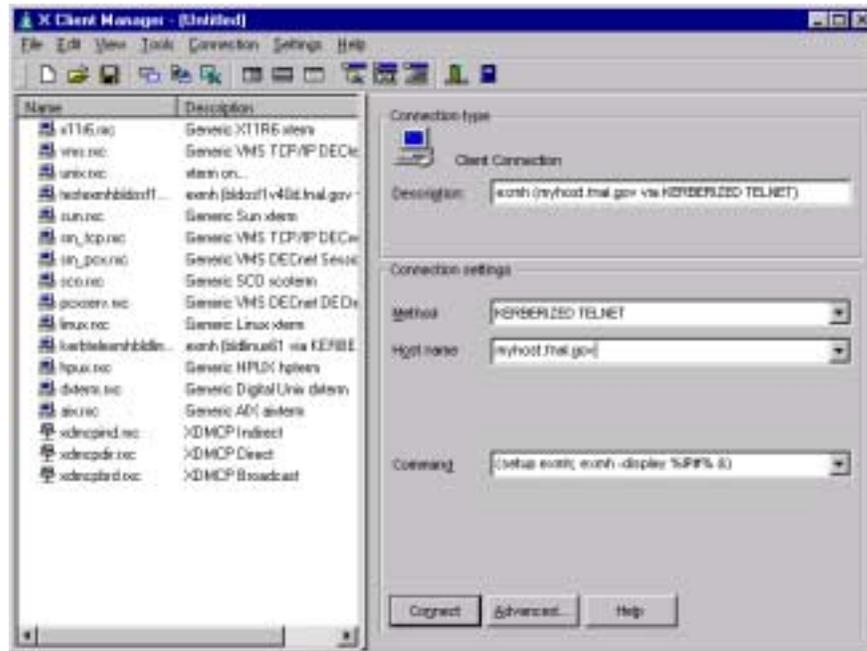
## 19.6.4 Connect to Host with X Application Startup



Here we describe how to create a profile to use for connecting to a host and starting a generic X application. (This procedure is somewhat dependent on the target OS.) **Be aware that this method provides unencrypted connections only, so use this only for applications that don't require Kerberos authentication.**

The easiest way to create a profile is to use the X client wizard. Go to **START > PROGRAMS > REFLECTION > WIZARDS > X CLIENTWIZARD** and follow the instructions. To do it manually, follow the instructions that follow here.

- 1) Use **START > PROGRAMS > REFLECTION > REFLECTION X** to start the **Reflection X Client Manager** if it isn't already running.
- 2) Use **FILE > NEW...** to open the **NEW CONNECTION** dialog, and select **Client Connection** and click **OK**; *or* (in "Split Window Vertically" view) highlight an existing connection in the left pane of the **X CLIENT MANAGER** window to use as a template.



- 3) On the right hand side, under **CONNECTION SETTINGS** pull down **METHOD**, and scroll down and select **KERBERIZED TELNET**.
- 4) Enter the **HOST NAME** or select it from the pull down list. (The pull down list is generated from the replies to the **XDMCP** broadcast plus any systems you have used recently.)
- 5) Enter the following **COMMAND** for execution on the remote host:
 

```
(setup <Xprogram>; <Xprogram> -display %IP## &)
```

 where **<Xprogram>** is some X application, for example **xcmh** or **xemacs**. The special string **IP#** substitutes the IP address and display number of the local display (i.e., the PC). Make sure that your UNIX login files don't reset this variable to a different display. Other special strings are documented in the **Reflection X** help file under "Command Line Macro Syntax".
- 6) Click the **CONNECT** button to establish the connection and run the remote command. (If you haven't already run **Kerberos Manager** to obtain a ticket-granting ticket, you'll be prompted for your Kerberos password. It's OK to enter it at this stage.)
- 7) Choose **FILE > SAVE** or **FILE > SAVE AS...** to permanently save the settings.

Other remote client commands and variations are left as an exercise for the reader(!).

## Troubleshooting

- To debug the dialog between the **X Client Manager** and the remote host, select **CONNECTION > HOST RESPONSE** before clicking the **CONNECT** button.
- The remote host's prompt character(s) must be recognized by the **X Client Manager** for the connection script to work correctly. Add the correct character(s) if they're not already in the list(s) by selecting **ADVANCED....**

There is extensive on-line help for other problems or applications.

## 19.7 Configuring WRQ® Reflection FTP Connections

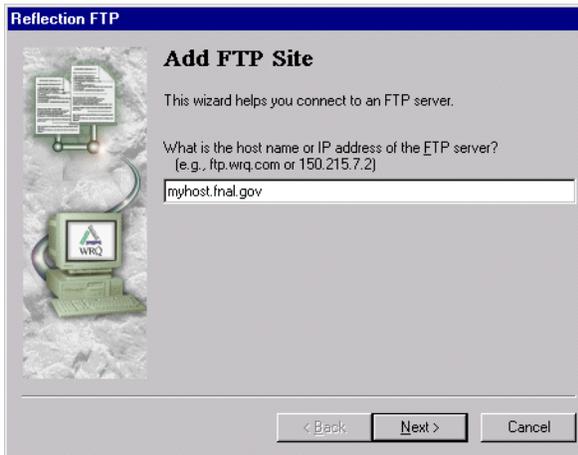
---

### 19.7.1 Create a Profile to FTP to Kerberized Host

- 1) Navigate to **START > PROGRAMS > REFLECTION > FTP CLIENT**.
- 2) Click **NEW** in the **CONNECT TO FTP CLIENT** screen. This brings you to the FTP wizard. On the **ADD FTP SITE** screen, fill in the name of the Kerberized host and click **NEXT >**.



- 3) In the **LOGIN INFORMATION** box, click the **USER** radio button and



click **ADVANCED...** to get to the **<HOST> PROPERTIES** screen.

- 4) With the **GENERAL** tab selected, click **SECURITY** to get to the **SECURITY PROPERTIES** screen. Select the *Kerberos* tab. The screen is similar to the **SECURITY** screen for configuring telnet connections in section 19.6 *Configuring WRQ® Reflection telnet Connections*.

Check Reflection Kerberos.

For a target host in the FNAL.GOV realm, enter your FNAL.GOV principal name and select either (default) or FNAL.GOV for the realm.

If your user id on the target host doesn't match your principal, fill in the user ID.

Mutual authentication and Verify data integrity should be checked by default; leave them checked.

You may check Encrypt data stream, but it usually isn't necessary.

Forward tickets is not an available option for FTP.

- 5) Click **OK** twice to return to the **LOGIN INFORMATION** screen. Click **NEXT >**.



- 6) In the **FTP USER LOGIN** screen, your username should be filled in. **Don't check** Save my password as encrypted text. Click **NEXT >**.

- 7) On the **CONNECT** screen, verify the name of the **FTP** host, choose whether you want to connect immediately, then click **FINISH**. Note that in order to connect, the default realm set in **USER PREFERENCES** (see number [3] in section 19.4 *Configuring WRQ® Reflection Kerberos Manager v9.0.0*) must be set to the default realm of the target FTP host.

## 19.7.2 Connect to nonKerberized Host

For connections allowing weak (standard) authentication, you don't need to worry about the **Kerberos Manager** since credentials aren't an issue. To configure a standard **FTP** connection profile, follow the same steps as in section 19.7.1 *Create a Profile to FTP to Kerberized Host*, but make sure the host name is a nonKerberized node, and don't bother with **ADVANCED...** in step (3). Instead, click **NEXT >** and continue from step (6).

## 19.7.3 Edit an FTP Setup

- 1) Open **START > PROGRAMS > REFLECTION > FTP CLIENT**.
- 2) In the **CONNECT TO FTP SITE** screen, select a configuration file and click **PROPERTIES**.

# Chapter 20: Installing and Configuring the Windows AFS Client

In this chapter we describe how to install and configure the **Windows AFS Client** software on your Windows system (Win2K or NT4) in order to transfer files between a Windows desktop and AFS space.

## 20.1 Download and Install AFS Client

---

- 1) Verify that you have administrator privileges on your Windows machine.
- 2) In your **NETWORK NEIGHBORHOOD**, navigate to  
\\PCKits\DesktopTools\PC\_Tools\Apps\AFS 3.6.2.
- 3) Run the \\PCKits\DesktopTools\PC\_Tools\Apps\AFS 3.6.2\Setup.exe program. Accept the license agreement and accept all the default settings. Before finishing, the InstallShield gives you an option to have it reboot your system. Click **No, I will restart my computer later**. Then click **FINISH**.

## 20.2 Reset your Path

---

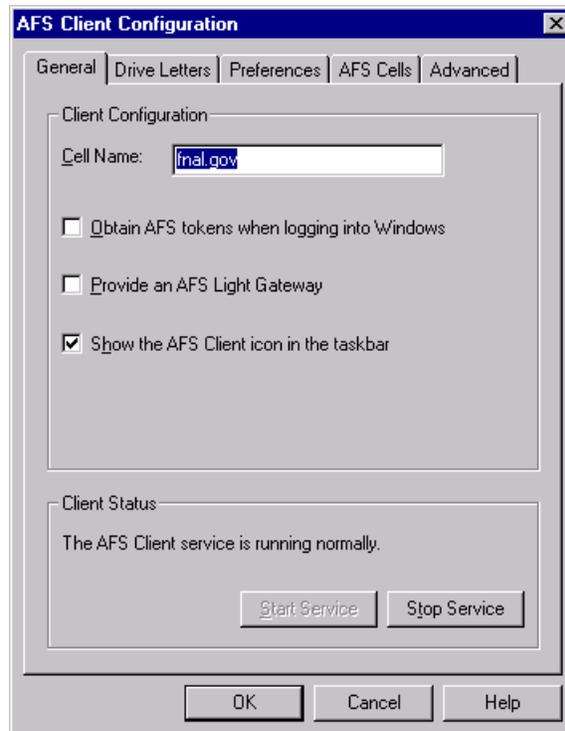
Next, you need to change your Windows NT path. Navigate to **START > SETTINGS > CONTROL PANEL > SYSTEM**. On the **SYSTEM PROPERTIES** window, bring up the **ENVIRONMENT** tab. This displays all the system variables, including `Path`. Scroll down to `Path` and select it. Notice that its value is displayed near the bottom of the window:



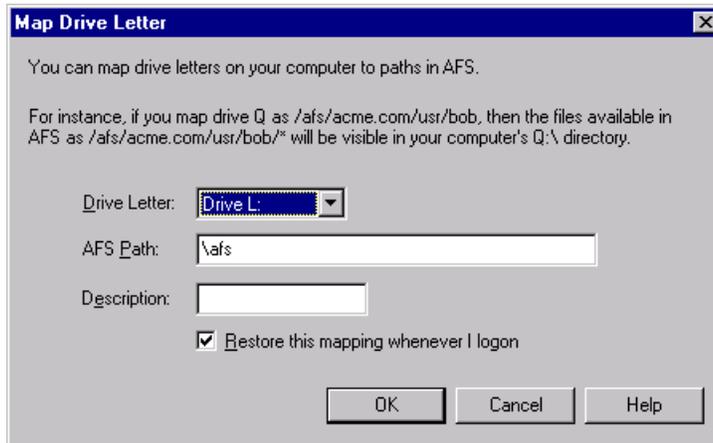
## 20.3 Configure AFS Client

---

- 1) After you log in again, you'll get a message stating that the AFS Client cannot be used because it is not yet configured. Click **OK**.
- 2) Go back to the **CONTROL PANEL**, and double-click on the **AFS CLIENT CONFIGURATION**. Select the **General** tab.



- 3) For the Cell Name, replace (unknown) with `fnal.gov`. Make sure Show the AFS Client icon in the taskbar is checked. Click **OK**.
- 4) A caution window pops up stating that The AFS client service is not running... and asks Do you want to start the service now? Click **YES**.
- 5) Next you will map one or more branches of AFS space to drive letters on your machine. Select the **Drive Letters** tab. Click **ADD...** to get to the **MAP DRIVE LETTER** window:



6) In the **DRIVE LETTER** box, the first unused letter is displayed. Choose any letter in the dropdown list. In **AFS PATH**, type in the directory in AFS space that you want to map to the drive (e.g., your home directory). Provide a short description; this will identify the drive on your **WINDOWS EXPLORER** or **MY COMPUTER** windows. If convenient, make sure **Restore this mapping whenever I logon** is checked. If you leave it unchecked, you'll need to map this volume manually each time you need it. Click **OK**.

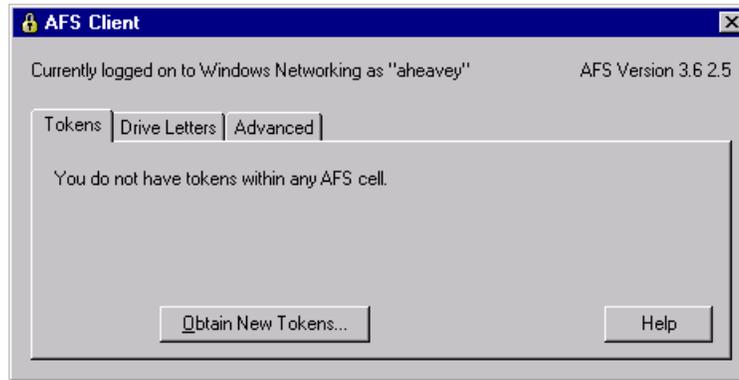
7) Repeat the previous two steps for other AFS directories that you want to map.

You do not need to alter any information under the other tabs.

## 20.4 Authenticate to AFS and Use the AFS Client

---

Authenticate to AFS space either by clicking on the AFS icon (the lock symbol) on your task bar, or by navigating to **START > PROGRAMS > IBM AFS > CLIENT > AUTHENTICATION**. The icon on the task bar shows a red X when you have no token (🔒). This X disappears when you obtain a token (🔑). On the **AFS CLIENT** window, click **OBTAIN NEW TOKENS...**



You will be prompted for your AFS password. (Currently this method does not require Kerberos authentication.)

Now you're ready to copy/paste/edit files on the AFS volumes in the same manner as for other drives. In the **MY COMPUTER** image below, they appear as the drives G:, H:, I: and J:, labelled: <description> on 'Www-56964-afs' (<drive letter>:).

