

Chapter 4: Accessing Kerberized Machines

(Fermilab-Supported Methods)

In this chapter we discuss accessing systems in the FNAL.GOV realm from UNIX and Windows machines using the methods recommended and supported by the Fermilab Computing Division. We cover logging in at the console, connecting over the network, and using CRYPTOCards with portal mode.



Very important note: Any time you're about to enter your Kerberos password, first verify that you're using the host's directly-connected keyboard! On rare, necessary occasions you may transmit your password over an encrypted network connection, but this is not to be done on a regular basis. See Chapter 11: *Encrypted vs. Unencrypted Connections* for information.

4.1 Logging In at the Console of a Kerberized UNIX Machine

4.1.1 Using Standard UNIX Login Program



If your desktop machine is running the standard login program, log in at the console normally, entering your standard UNIX password (note that if your machine runs AFS, your UNIX and AFS passwords may be the same). The standard login program does not accept your **kerberos** password. You need to run **kinit** after logging in to obtain your credentials. The credentials should then get forwarded to other strengthened machines normally. The **kerberos** login program is not installed by default with the **kerberos** product.

4.1.2 Using Kerberos Login Program

If your desktop machine is configured to use the **kerberos** login program¹, you can authenticate to Kerberos at login by entering your Kerberos password at the password prompt. You do not need to run **kinit** after login. (You can still login using your UNIX password, then run **kinit** to get Kerberos

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

tickets, if you wish.) An advantage to using the **kerberos** login program is that it checks the `/etc/krb5.conf` file in which you or your system administrator can set defaults for Kerberized applications.

4.1.3 If you don't have a principal yet...



Note that if you have an account and a standard UNIX password on a machine (in the `passwd` file or NIS map) but no principal or Kerberos password, you can still log in at the console. (From any terminal other than the console, the Kerberized machine looks for existing Kerberos credentials, and responds in portal mode if none are found; you have no option to enter your UNIX password.) However, once logged in, you cannot make outbound connections from there since Kerberized services are unavailable to you.

You can use `ssh` to log into machines running mixed mode Kerberos, as described in section 4.1.4 *Machines Running Mixed Mode Kerberos*.

4.1.4 Machines Running Mixed Mode Kerberos

Machines that are Kerberized in mixed-mode allow logins via `ssh` for users who don't yet have a Kerberos principal. This is in addition to allowing login via Kerberized services or CRYPTOCARD. Mixed-mode machines are not allowed on-site.

4.2 Connecting from One Kerberized Machine to Another

Make sure you have forwardable credentials on your desktop machine, then run the Kerberized version of the connection program you want to use (**ssh**, **slogin**, **telnet**, **rsh**, **rlogin**, **rcp**, **scp** or **ftp**) to connect and forward your credentials to the target machine. Forwarding is described in section 9.2.4 *Forwarding Tickets*. The Kerberized features of these programs are described in Chapter 13: *Network Programs Available on Kerberized Machines*.



Do not run **kinit** over the network to authenticate on the remote machine. As of Kerberos v1_5, **kinit** is equipped with a warning that appears if the userid issuing the command doesn't own the console device. It is designed to help users avoid typing their password inadvertently over the network.

Assuming your credentials get forwarded to the target machine, you should be automatically recognized and authenticated there; you should not be prompted for your Kerberos password.

A few notes:

- If the usernames on the machines differ, use the `-l` `<login_name_on_target_host>` option; e.g., `ssh -l <login_name_on_target_host>`.
- If ticket forwarding has been set “off” for your system, and you want to connect to a Kerberized machine with ticket forwarding turned on, use the appropriate option, e.g., `-f` or `-F` for **telnet**, **rsh**, and **rlogin** (`-F` marks them reforwardable whereas `-f` does not).
- If ticket forwarding has been set “on” for your system, and you want to connect to a Kerberized machine with ticket forwarding turned off, use the appropriate option (e.g., `-N` for **telnet**, **rsh**, **rlogin**, and **rep**, or `-k` for Kerberized **ssh**). Forwarding is described in section 9.2.4 *Forwarding Tickets*.



Warning! If your on-site Kerberized system accepts a reusable login password over the network (even on an encrypted connection), this is a violation of the Fermilab Policy on Computing (see <http://www.fnal.gov/cd/main/cpolicy.html>).

4.3 Connecting via Kerberized SSH



Any machines that are sited at FNAL and that wish to use `ssh` are required to use Kerberized `ssh` (available from `ftp://ftp.fnal.gov/KITS/` as `ssh v1_2_27g` or higher). Non-Kerberized `ssh` is not permitted on these machines. With both **kerberos** and Kerberized `ssh` installed on your machine, make sure you have a Kerberos ticket, then run the Kerberized version of the connection program you want to use (e.g., **ssh**, **slogin**, or **scp**) to connect to a remote Kerberized host. The Kerberized options for these programs are described in Chapter 13: *Network Programs Available on Kerberized Machines*. You do not get prompted for your Kerberos password during login.

Ssh encrypts the connection by default, typically (check your configuration). You can always use the `-c <cipher>` option to ensure encryption.

4.4 Connecting from a NonKerberized Machine: Portal Mode

4.4.1 About Portal Mode

If your local desktop computer does not run Kerberos software and is not configured for the FNAL.GOV realm, then you can't authenticate to FNAL.GOV locally on this computer. You can work on the desktop with no problem, but in order to connect over the network to Kerberized UNIX hosts, you must authenticate to FNAL.GOV first.

Kerberized machines in the FNAL.GOV realm are configured to require entry of a single-use password whenever they receive a login request coming from an unKerberized computer over the network. (The password gets transmitted over the network, and it could get intercepted. That's why it must be valid for only one login.) The target computer is said to respond in *portal mode* in this case. It is acting as a secure gateway into the strengthened realm.

How do you get a single-use password that Kerberos will recognize and honor? The FNAL.GOV realm at Fermilab is setup to use CRYPTOCards to provide these single-use passwords.

Once you've logged on successfully through the portal, the KDC "knows who you are", and the machine obtains your Kerberos credentials for you. You are not required to provide your Kerberos password when making further network connections to other machines in the FNAL.GOV realm. If you need to reauthenticate, run the command `new-portal-ticket`. This provides a portal mode prompt.

4.4.2 About CRYPTOCard

Fermilab has implemented portal mode using CRYPTOCard technology. A CRYPTOCard is a calculator-style, battery-powered device used for generating a single-use password.



To read more about what a CRYPTOCard is and how it works, see Chapter 5: *Using your CRYPTOCard*. To request one fill out the online form *Request Form for Computing Username and Primary Accounts* at

http://www.fnal.gov/cd/forms/acctreq_form.html. When you get your CRYPTOCARD, go back to Chapter 5: *Using your CRYPTOCARD* for information on how to use it and take care of it.



Two notes:

- No special hardware or software is required on the nonKerberized machine for CRYPTOCARD use.
- The CRYPTOCARD login code assumes that the user's login name and principal match. If yours don't match, you won't be able to log in using this method.

4.4.3 Programs for Initiating CRYPTOCARD Login

To log on to a machine in the FNAL.GOV realm from your nonKerberized machine, run any of the following commands:

```
% ssh <host>
% slogin <host>
% telnet <host>
% ftp <host>
```

as usual (the standard, nonKerberized version of the program, as the Kerberized version is not available on nonKerberized machines).

Two notes regarding the use of **ssh** and **slogin** with CRYPTOCARD:

- The Kerberos login program supports **ssh** only when no command argument is given, i.e., when it is effectively equivalent to **slogin**. (Fundamentally, **slogin** is the only **ssh** program supported.)
- The Kerberized sshd on the remote host prompts for an **ssh** password before displaying the CRYPTOCARD challenge. Just press Return for the **ssh** password, don't enter any characters.

After you issue the network command, the remote host will prompt you to provide a non-reusable password rather than your Kerberos password:

```
Press ENTER and compare this challenge to the one on your
display: [12345678]
Enter the displayed response:
```

Use your CRYPTOCARD to provide this password, as described in section 5.5 *Log in Using CRYPTOCARD (the First Time)*, or section 5.6 *Log in Using CRYPTOCARD (Subsequently)*.



Notes:

- Never type your Kerberos password over a CRYPTOCARD **telnet** session! The connection is not encrypted.
- You may type your password infrequently over an encrypted CRYPTOCARD **ssh/slogin** session.

- **rsh**, **rlogin**, **rcp** and **scp** are not available for portal mode.

4.4.4 Portal Mode FTP when you can't see the Challenge

If you're doing portal mode **FTP** with a client that does not show you the output text from the server (e.g., **FTP** under **emacs** or from a variety of Windows **FTP** clients), it won't display the challenge string. In this case, go ahead and use your **CRYPTO**card anyway, and enter the response as your password. This works if your card is in sync with the KDC, which should generally be the case.

If you're using the **WRQ**® **FTP** client with standard (nonKerberos) security, select **VIEW > COMMAND WINDOW** to see the **CRYPTO**Card challenge.

If the **FTP** login is unsuccessful, you need to synchronize your card. To do so, start a **telnet** connection, and type the displayed challenge into your **CRYPTO**Card. Then disconnect the **telnet** session **BEFORE** you enter the response so that you save it for your **FTP** session! Otherwise the response will get used and you'll be out of sync again.

4.5 Logging into a UNIX Account that's not your own

If you wish to log into an account for which your login id is different from your principal name (e.g., a group account), your principal must be listed in either the `.k5login` or the `.k5users` file (**ksu** only) of the target account. See section 9.3.1 *The .k5login File*.

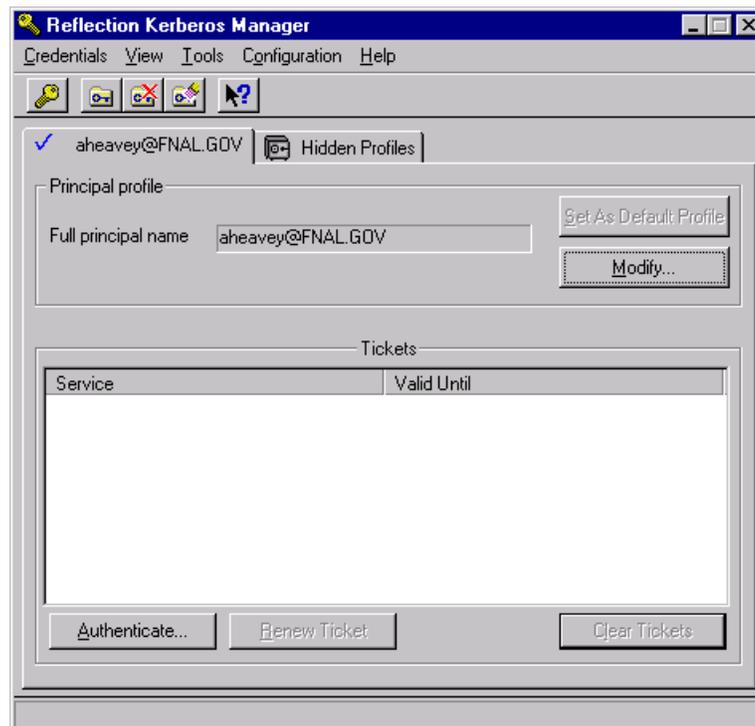
First log in to your own account on a Kerberized machine and obtain credentials as usual, then connect to the target account after you're authenticated. If the target account is on a different machine, simply connect to that machine using one of the Kerberized connection utilities, and use the `-l <login_name>` option where `<login_name>` is the target account name. If the account is on the same machine, use `ksu <login_name>`.

4.6 Logging In Through WRQ® Reflection Software from Windows

4.6.1 Authenticate Locally via the Kerberos Manager

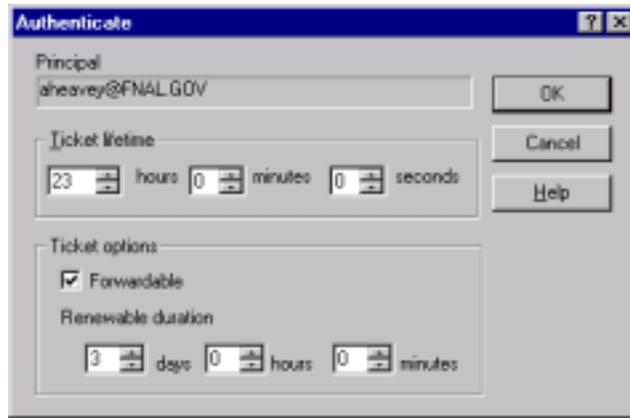
The **Reflection Kerberos Manager** program authenticates you to Kerberos and supports ticket forwarding. This means it obtains an initial Kerberos ticket for the principal on the tab chosen¹, and you, as that principal, can freely connect to Kerberized machines without needing to type your Kerberos password again.

Navigate to **START > PROGRAMS > REFLECTION > UTILITIES > KERBEROS MANAGER** to open the **Reflection Kerberos Manager** application.



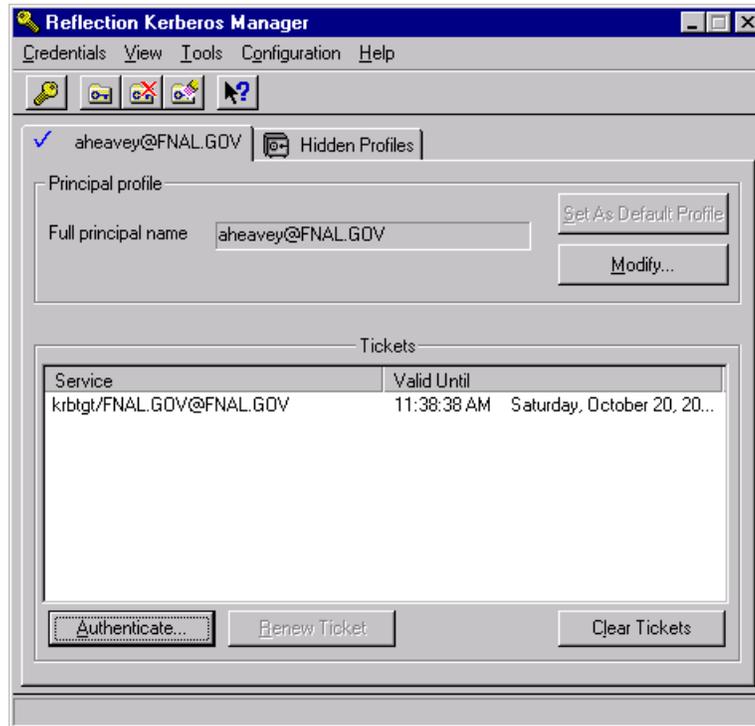
Choose your principal that corresponds to the default realm of the target machine. Click **AUTHENTICATE**.

1. You may have one for PILOT.FNAL.GOV and for FNAL.GOV.



- Verify or change **TICKET LIFETIME** (if you give a value greater than the KDC limit of 23 hours, the renewable lifetime will be set to 23 hours)
- Check **FORWARDABLE** in order to forward your ticket to target host (besides forwarding your Kerberos ticket, it's necessary in order for an AFS token to be automatically generated when you connect to a system running AFS)
- To set your ticket as renewable, enter a non-zero time for **RENEWABLE DURATION** (if you give a value greater than the KDC limit of seven days, the renewable lifetime will be set to seven days). The AFS token you get will have a lifetime equal to the Kerberos ticket's renewable duration.

Click **OK**, and provide your Kerberos password at the prompt. Back on the **KERBEROS MANAGER** window, you should see the new ticket-granting ticket (TGT) `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. If you continue to receive an error message, send the exact error message text to `nightwatch@fnal.gov` together with the date and time of the error and the IP address of your system.



Once you run **Reflection Kerberos Manager** and authenticate, you do not need to keep the application active; you can exit and continue to log in to Kerberized machines. The authentication is valid for the lifetime of the ticket.



When you have finished your session and disconnected from all Kerberized machines, it's important to prevent another user at your machine from using your tickets. Bring up the application again and clear your tickets by clicking **CLEAR TICKETS** on the **REFLECTION KERBEROS MANAGER** window. You can automate this by clicking **CLEAR ALL TICKETS ON SHUTDOWN** on the **CONFIGURATION** menu.

4.6.2 Run a telnet Session to Kerberized Host

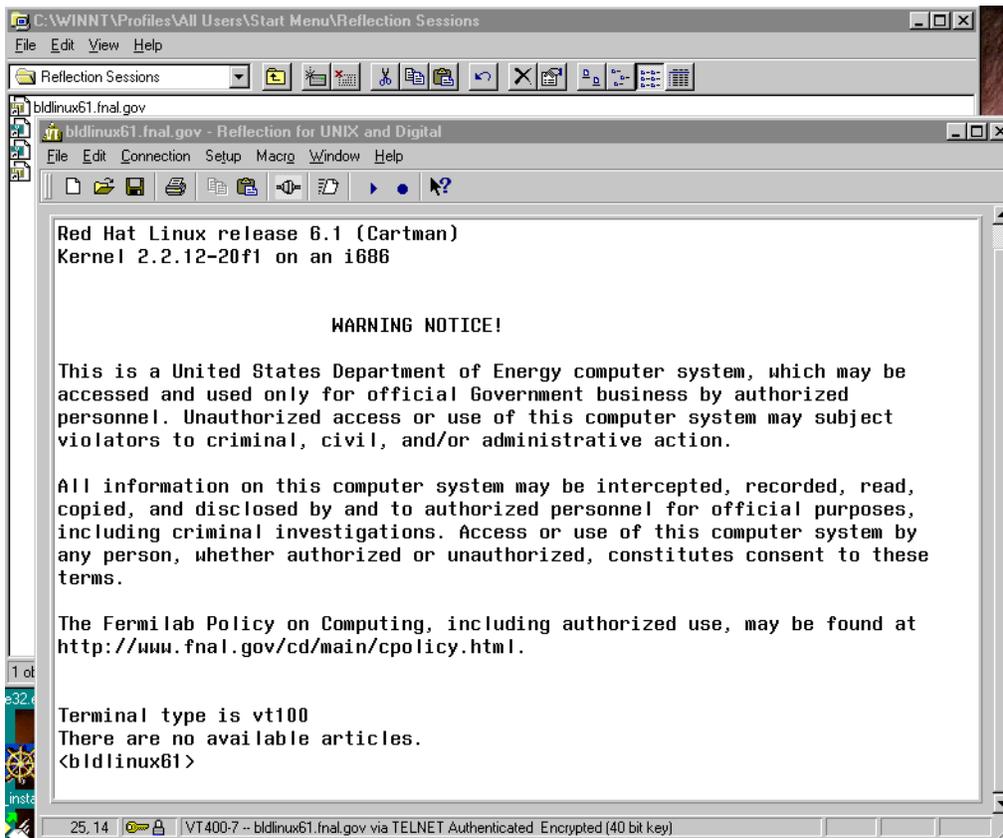
To use the **WRQ® Reflection telnet** client to access machines in the strengthened realm, you first need to set (and save) a separate **telnet** configuration for each host with ticket forwarding set. The configuration procedure is outlined in section 19.6 *Configuring WRQ® Reflection telnet Connections*.



To run an Xwindows session, see section 10.1.2 *Windows NT4/98/95*.

Start the **Reflection Kerberos Manager** first to authenticate, as explained in section 4.6.1 *Authenticate Locally via the Kerberos Manager*. The easiest way to start a session is to make a short cut for your telnet configuration file, and just double-click on it. Otherwise, to start your session:

- Navigate to **START > PROGRAMS > REFLECTION > HOST - UNIX AND DIGITAL**.
- On the **REFLECTION FOR UNIX AND DIGITAL** window, select **FILE > OPEN**.
- Double click on the file in your **REFLECTION** folder corresponding to the host to which you want to connect. (If you haven't already authenticated you will be prompted to provide your Kerberos password.) It will bring up a VT window and log you in:



Assuming that you have authenticated with a forwardable ticket, and that your telnet configuration file specifies `Forward ticket`, then you have credentials on the host (including AFS token if needed).

If you authenticate with the **Kerberos Manager** and get a nonforwardable ticket, and then start a telnet session with forwarding enabled, you'll get another password prompt from **WRQ®** so that it can obtain a forwardable ticket for you.

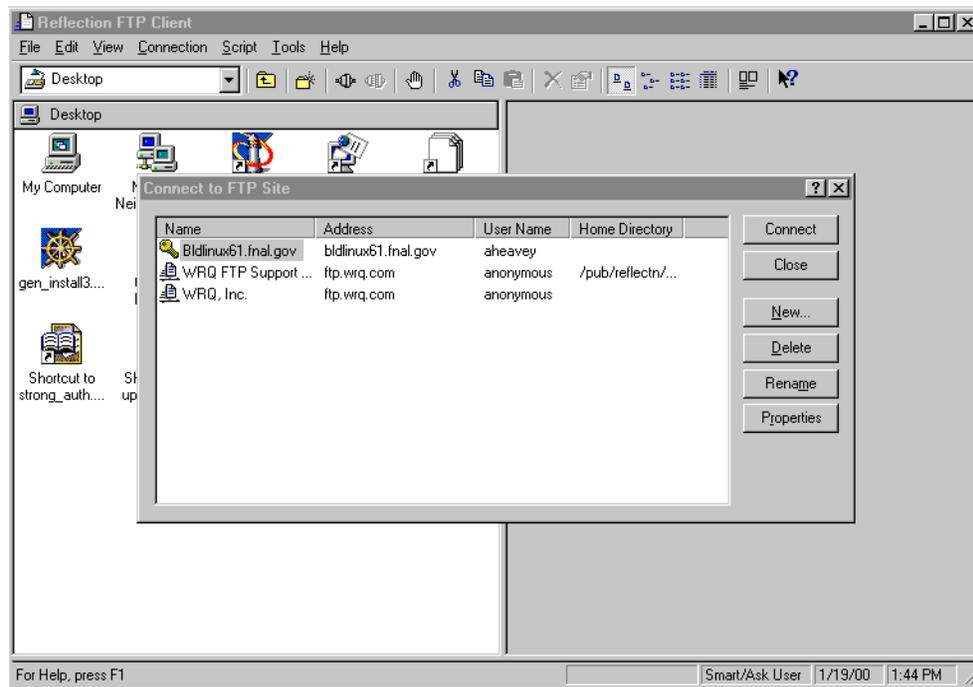


If you did not have your ticket forwarded, then to obtain credentials on the host (and to obtain an AFS token if AFS runs on the host) you will need to run **kinit** (see section 9.2.1 *Obtaining Tickets (Authenticating to Kerberos)*) and enter your password again after you log in. **Don't do this on a regular basis!** Before you enter your password, glance at the bottom of the VT window and verify that it says "Encrypted" and shows a locked lock icon (as shown on the above image). If it doesn't, *log out and verify your configuration* (under **CONNECTION>SECURITY**, check Reflection Kerberos and check Encrypt data stream)! **Always make sure the data stream is encrypted before entering your password!**

4.6.3 Run an FTP Session to Kerberized Host

Configuration of **FTP** sessions is covered in section 19.7 *Configuring WRQ® Reflection FTP Connections*. Make sure that the default realm for **REFLECTION** is set to the default realm of the target host (see number [3] in section 19.4 *Configuring WRQ® Reflection Kerberos Manager v9.0.0*).

To use the **Reflection FTP** client to access a Kerberos system: open **START > PROGRAMS > REFLECTION > FTP CLIENT**:



and double-click the file corresponding to the host you want to access.



WRQ® Reflection FTP does not forward ticket to remote host or obtain an AFS token for you on the host. This does not pose problems on non-AFS machines, but you can't get access to AFS volumes. For transferring files to AFS space, you have two options:

- 1) Install and use the Windows AFS client, as described in sections Chapter 20: *Installing and Configuring the Windows AFS Client* and 4.7 *Windows AFS Client for File Transfers to AFS Space*.
- 2) Configure the WRQ® FTP client with standard (nonKerberos) security and use a CRYPTOCARD (this has also been tested with NT and Windows 2000 command line FTP, and FTP client in **FrontPage2000**).
 - Select **VIEW > COMMAND WINDOW** to see the CRYPTOCARD challenge.
 - Connect to host, generate a response on your CRYPTOCARD, and enter it at the password prompt.

4.7 Windows AFS Client for File Transfers to AFS Space

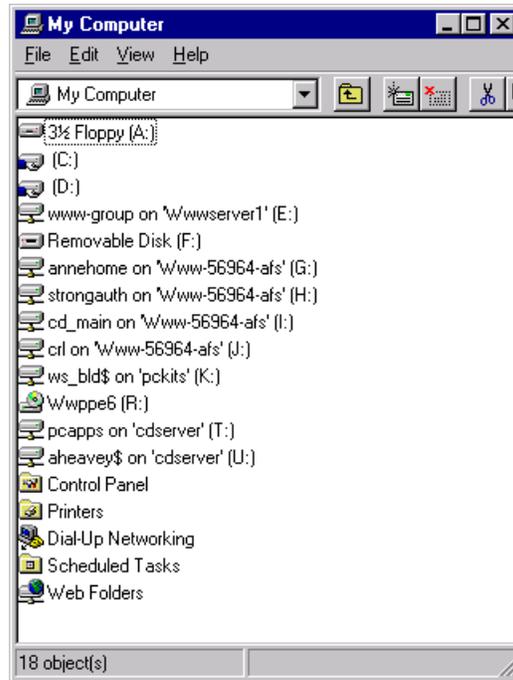


Due to the inability of the Kerberized FTP clients for Windows, including WRQ®'s, to forward Kerberos tickets (and thus generate AFS tokens on the remote host), we recommend that you bypass FTP entirely and install the Windows AFS client for file transfers to and from AFS space. Installation and configuration is described in the document *Installing IBM AFS Client 3.6 for Windows NT/2000/XP* at http://www-oss.fnal.gov/csi/afs_windows/.

4.7.1 How does AFS Appear on your Desktop?

The AFS client should be installed and configured such that at login the drive mapping is restored and the AFS client service restarts¹. Your AFS drive(s) appear automatically in **MY COMPUTER**, **WINDOWS NT EXPLORER**, etc. In the image below, the drives G:, H:, I: and J:, labelled: <description> on 'Www-56964-afs' (<drive letter>:), are all AFS volumes:

1. If the AFS Client Service does not start up automatically when machine is booted, click on the AFS icon on your task bar (the lock symbol; it will appear with a red X at this stage ). Select the **Advanced** tab, and click **START SERVICE**. Also, if not remapped automatically at login, the AFS drive(s) must get mapped in the same way as any other drive.



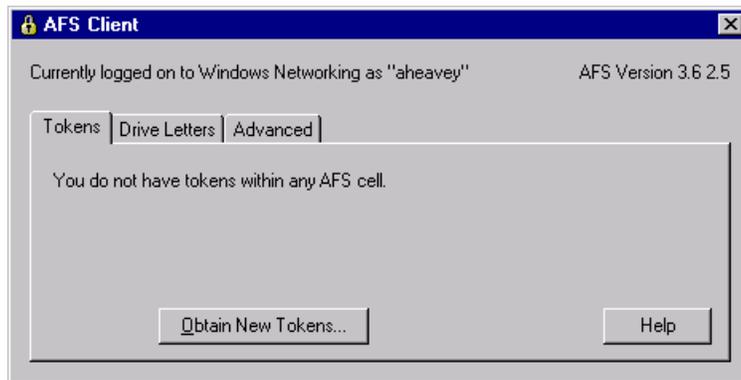
To use most AFS volumes, you must first authenticate to AFS. The exception is a public AFS volume (for which access is allowed for `system:anyuser`); this does not require a token¹.

The AFS icon in your task bar is a lock symbol. It displays a red X (🔒) before you authenticate to AFS, and the X goes away (🔓) after you authenticate to AFS and obtain a valid token.

4.7.2 Authenticate to AFS

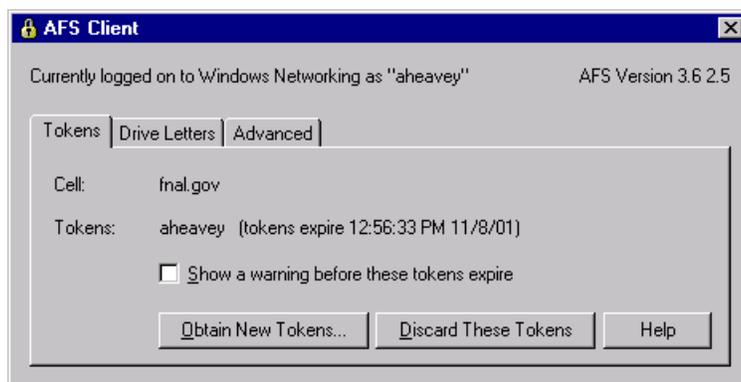
- 1) Make sure the AFS Client Service is running.
- 2) Authenticate to AFS space either by clicking on the AFS icon (the lock symbol with X: 🔒) on your task bar, or by navigating to **START > PROGRAMS > IBM AFS > CLIENT > AUTHENTICATION**. On the **AFS CLIENT** window, select the **TOKENS** tab. Click **OBTAIN NEW TOKENS...**

1. If the AFS Client Service is not running, the AFS mapped drives display a red X and are unusable. The Xes go away when the service is restarted.



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

3) The token expiration date/time then appears on the window:



Your token is valid for six days, unless the AFS service is stopped before then. Every time you reboot, the service is halted and restarted, and thus the token is destroyed. 'Now you're ready to copy/paste/edit files on the AFS volumes in the same manner as for other drives.