

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, NT4, XP¹) 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 v10.0.0**.

As of January 2005, WRQ v12 is available. This chapter has not been updated, but you can find the software under \\Pseekits\WRQ.

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 W2k), XP, NT4, 95 or 98, you need to install two **WRQ® Reflection** software products, **Reflection Kerberos Manager** which runs the **Kerberos Manager** on your PC, and **Reflection X** 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 (except on XP).
- Installing the recommended components of the **WRQ® Reflection v12.0.0** 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.

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

- After installing this software you will still log into your PC the same way as before (e.g., for the W2k Kerberized domain, use your W2k Kerberos password). You will need to provide your FNAL realm 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, or (as of version 10.0.0) to access **ssh**-only nodes.
- 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 v12.0.0

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, XP and Win 2000. It may work on Windows ME, 98 and 95 as well, but has not been tested.

The **WRQ® Reflection** v12.0.0 installation script is located at `\\PSeeKits\WRQ\Reflection_12\Install_WRQ.bat`. Read the `README.txt` file.

There is a helpful discussion in the *wrq-users@fnal.gov* list with the subject "Configuring WRQ Reflection X 12.0", that took place in late March 2005. Many useful tips!

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 12.0
Do you want to continue [Y,N]?y
Installing WRQ Reflection
Wait for the installation window to disappear, then
Press any key to continue ...
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
(If you're upgrading, you'll get a different message here "you already have
a saved copy of the services file...")
Install of Reflection X 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 Configuration for Addressless Tickets

If you plan to use Reflection from off-site through a local area router with NAT (for information about NAT, see section 6.5 *Network Address Translation*), you'll need to configure your system to get addressless tickets. To do so,

- 1) Start WRQ Reflection Kerberos Manager
- 2) Pull down Configuration > Configure Realms
- 3) Select FNAL.GOV
- 4) Click on Properties
- 5) Choose Realm Defaults
- 6) Clear the IP address in the Ticket Address box
- 7) OK
- 8) OK

Now when you authenticate (see section 4.6 *Logging In Through WRQ® Reflection Software from Windows*), you'll get an addressless ticket.

Your IP address will appear in the Realm properties, even if you successfully get an addressless ticket. Reflection puts it there in case you want to reset to getting an addressed ticket. To verify that you've gotten an addressless ticket, first get one, then right click on it, and click on properties. The resulting box will have the address cleared if it's addressless.

What if you get the message the message "Kerberos Ticket forwarding failed." and you're sure you checked "Forwardable Ticket" in the configuration? Here are a couple of possible reasons:

- 1) You actually have an addressed ticket and are going through a NAT router. To check, right click on the ticket, chose properties and check that the ticket is addressless. If it isn't, clear the address from: Kerberos Manager -> Configuration -> Configure Realms -> FNAL.GOV -> Properties -> Realm Defaults, then reauthenticate.
- 2) Some versions of the software on the host will not accept forwarded tickets. This is sensitive to:
 - a) defaults and program versions on the host

- b) which one of the WRQ programs you are using: WRQ Reflection for UNIX and Digital (WRQ's terminal emulator) or WRQ Reflection X Manager (pop an xterm).
- c) the protocol you are using on your end: Kerberized Telnet, OPENssh, etc.

If you use the X manager with OPENSSSH to pop an xterm, make sure you've set ssh to tunnel. This gets through (not around, through) all the problems with NAT, routers etc. You might also try going to a different machine!

19.4 Time Synchronization

Kerberos requires a time sync within five minutes, each machine to its local time zone. Version 10.0.0 of the **WRQ® Reflection** software includes time sync software (versions 9.0.0 and 7.0.2 also did; version 8.0.0 did not).

19.4.1 WRQ® Reflection 10.0.0

- Navigate to **START > PROGRAMS > REFLECTION > UTILITIES > REFLECTION TIMESYNC** to open the **Reflection TimeSync** application.
- Make sure the *Synchronize* tab is selected.
- Under **Time 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.
- 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).
- Again under **Time synchronization**, click **Synchronize Now** to set the system clock and check the time server setting.
- Click **OK**.

19.4.2 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.

19.5 Configuring WRQ® Reflection Kerberos Manager v12.0.

- 1) Bring up your Kerberos Manager: Start -> Programs -> WRQ Reflection -> Utilities -> Kerberos Manager
- 2) Then Configuration -> Configure Realms
- 3) If the Realm list does **not** say: FNAL.GOV, then add it. The KDC host is `krb-fnal-1.fnal.gov`. Click OK.
- 4) Highlight FNAL.GOV -> Properties
- 5) Choose the KDC tab: Add to your KDC list any missing from `krb-fnal-1.fnal.gov` through `krb-fnal-5.fnal.gov`.
- 6) Kadmin server should be: `krb-fnal-admin.fnal.gov`
- 7) Hosts tab: `krb-fnal-1.fnal.gov` through `krb-fnal-5.fnal.gov`
- 8) Realm Defaults tab: Ticket Lifetime, anything greater than 26 hours will give you 26 hours, the realm maximum. Ticket renew time, enter anything greater than 7 days. Pre-Authentication: choose "Encrypted timestamp". Check "Forwardable ticket". For addressless tickets, clear "Ticket Address".
- 9) Encryption tab: the default of RSA_MD5 in both boxes is fine.
- 10) Click OK

Back in the Configuration box:

- 11) User Defaults tab: Default realm = FNAL.GOV. Default storage, chose "File". Click OK.

Back at WRQ Reflection Kerberos Manager:

- 12) Authenticate (Chose 26 hours, Forwardable, 7 days (should be set at or greater than these already). Click OK.
- 13) It should ask for your kerberos password. Type it in and a krbtgt/FNAL.GOV@FNAL.GOV ticket should appear in the text box. Right click on it, chose "Properties". Check the flags (Initial, Renewable, Forwardable, Pre-Auth should be set but greyed out). Check the expiration times. For addressless tickets, check that the Addresses text box is empty.

19.6 Configuring WRQ® Reflection X

This section has purposely not been updated for v10.0.0 and following; we encourage you to use the automated install, in which case you don't need to configure the software manually. You DO need to configure individual X connections; see section ???

For version 9 and below:

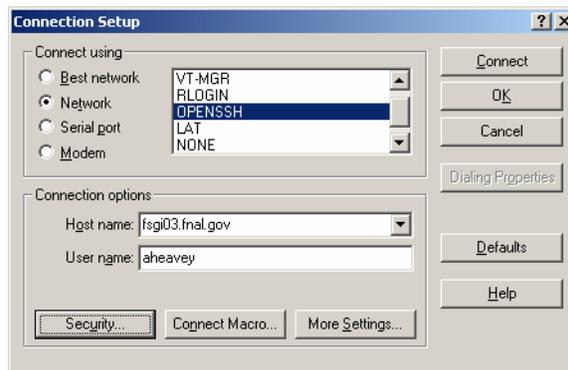
- 1) Invoke the **Reflection X Client Manager** using the **START** menu. You will be prompted to run the **Reflection X Performance Tuner**. Click **YES** to run these tests to optimize performance before using the X client manager.
- 2) The **Reflection X Client Manager** next prompts you to **SELECT 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.

19.7 Configuring WRQ® Reflection OpenSSH Connections

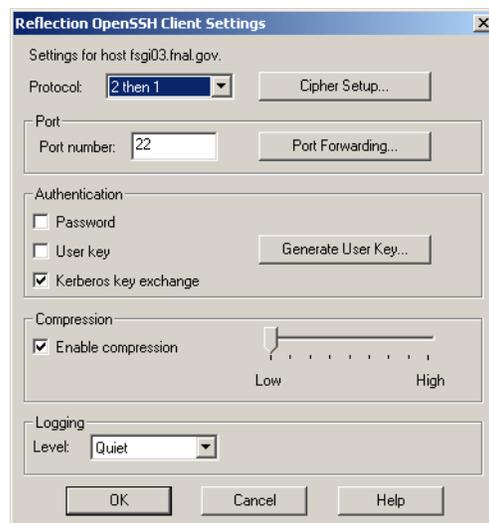
You can define an OpenSSH configuration (profile) specific to each host you need to access, and save each one to a file. To run OpenSSH to a particular host, you just run its corresponding profile (see section 4.6 *Logging In Through WRQ® Reflection Software from Windows*).

19.7.1 For Kerberized Host

- 1) To configure the **Reflection OpenSSH** client to access a remote Kerberized system, first open **START > PROGRAMS > REFLECTION > HOST - UNIX AND DIGITAL**.
- 2) 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 **OPENSSH** is highlighted in the scroll box:



- 3) Fill in the **HOST NAME** of your target Kerberos system
- 4) **Very important!!!** Click **SECURITY**.



- 5) The default **PROTOCOL** and **PORT NUMBERS** are fine. Change **AUTHENTICATION** to **KERBEROS KEY EXCHANGE**. **COMPRESSION** and **LOGGING LEVEL** settings are optional. Click **OK**.

6) Back on the **CONNECTION SETUP** window, click **CONNECT**.

19.7.2 For nonKerberized Host

Follow the same procedure as in section 19.7.1 *For Kerberized Host*, but on the **REFLECTION OPENSHELL CLIENT SETTINGS** window, choose the **AUTHENTICATION** method appropriately for the target system.

19.7.3 Create a Template Configuration

To create a template **OpenSSH** profile, first create and save a model profile for any Kerberized or nonKerberized host, as appropriate, as described in the preceding sections. 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, add the desired host name, and save it to a different file with a host-specific name.

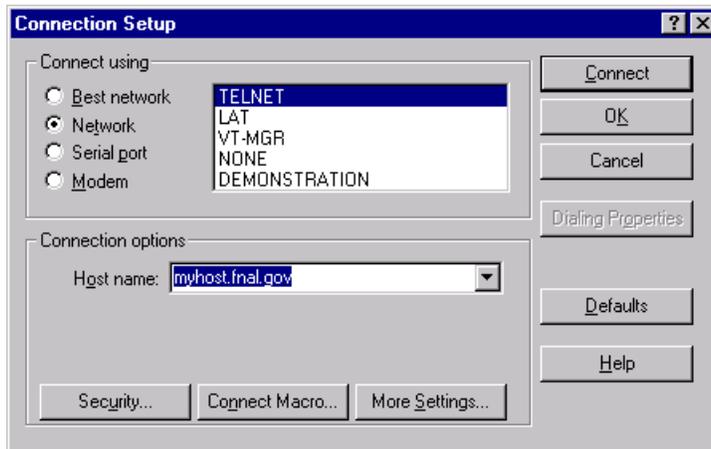
19.8 Configuring WRQ® Reflection telnet Connections

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 4.6 *Logging In Through WRQ® Reflection Software from Windows*).

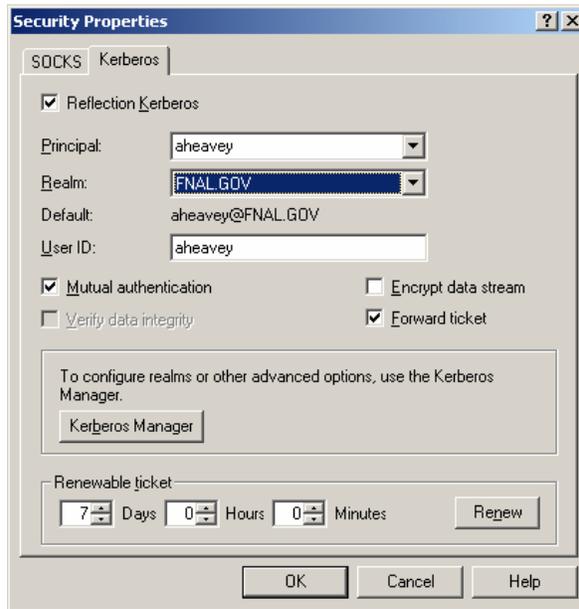
19.8.1 For Kerberized Host

- 1) To configure the **Reflection telnet** client to access a remote Kerberos system, first open **START > PROGRAMS > REFLECTION > HOST - UNIX AND DIGITAL**.
- 2) 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:

Fill in the **HOST NAME** of your target Kerberos system



3) **Very important!!!** Click **SECURITY**.



4) Select the *Kerberos* tab. Check *Reflection Kerberos*.

Principal: Select your FNAL principal name from the pull-down list.

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`. Seven days is provided as a default. (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.

- 5) 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**.)
- 6) 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**.
- 7) 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.
- 8) 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.

19.8.2 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 19.8.1 *For Kerberized Host*, but make sure the host name is a nonKerberized node, and eliminate step (3) which sets the Kerberos security.

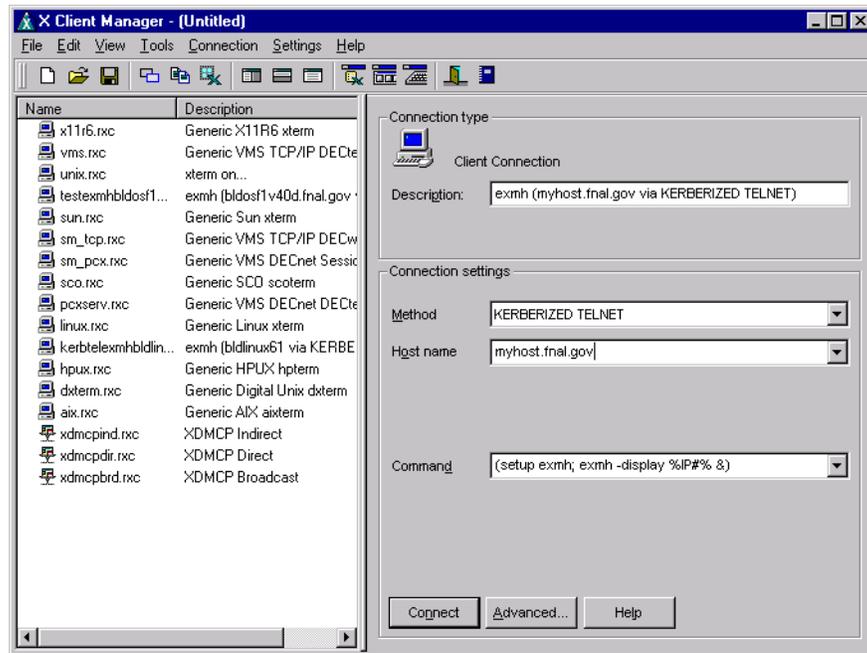
19.8.3 Create a Template Configuration

Follow the procedure described in section 19.7.3 *Create a Template Configuration*.

19.9 Configure X Connection to Host

Here we describe how to create a profile to use for making an X connection to a host.

- 1) Use **START > PROGRAMS > REFLECTION > REFLECTION X** to start the **Reflection X Client Manager**.
- 2) On the left side, click Client Templates, then Client Startup. Choose the startup template that corresponds to the target OS. This puts the appropriate command in the Command field on the right hand side.



- 3) 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.)
- 4) Enter a description in the Description field, and your username on the host in the User Name field.
- 5) On the right hand side, under **CONNECTION SETTINGS** pull down **METHOD**, and scroll down and select **KERBERIZED TELNET** or **OPENSSH**, depending on what service is installed on the target machine.

If you select Kerberized Telnet:

- 1) Click the Advanced button.
 - a) Check the “Show host response” box (it’s helpful in case the connection fails).
 - b) Click Configure Kerberos, and make sure Reflection Kerberos, Mutual Authentication, and Forward Ticket are all checked. Click OK (twice).
- 2) For either Kerberized Telnet or Openssh, click the Settings button at the bottom of the window.
 - a) Under Category on the left of the X Settings window, click Security.
 - b) On the right, click Host Based security for “Security Mode”, and Refuse Connection for “If client cannot be authorized”.

- c) Edit the host access security file: scroll to the bottom and add the fully-qualified host name for the target machine if it's not there yet. Save it and exit.
 - d) Ideally you should set Security Mode back to User-based security, but you may have connection problems on some hosts. If you leave it as Host-based security, you're more likely to connect successfully, but the CD security scans may pick you up and ask you to close your session (you can answer No, but you risk being blocked!).
- 3) 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.)
 - 4) Choose **FILE > SAVE** or **FILE > SAVE AS...** to permanently save the settings.

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.

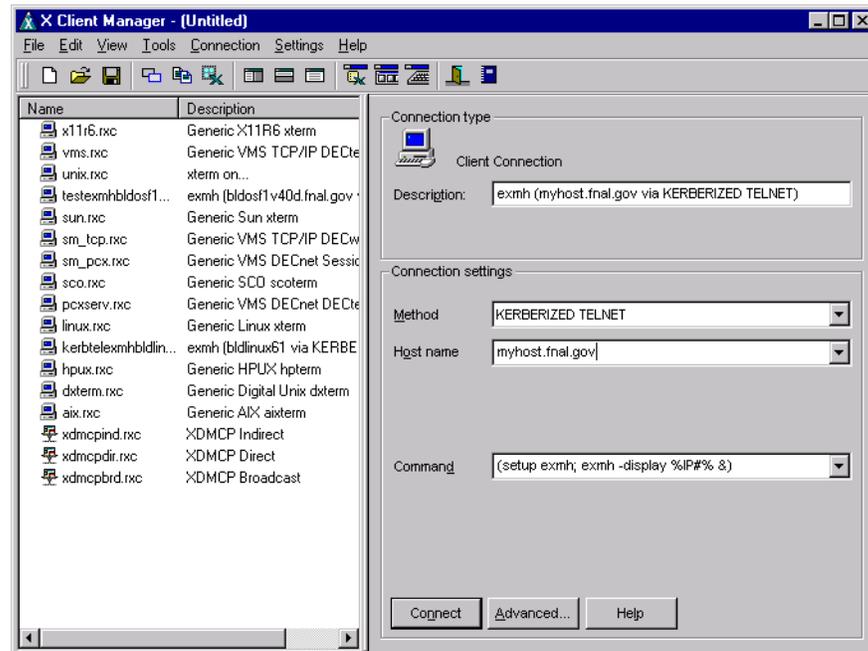
19.9.1 Connect to Host with X Application Startup

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 **exmh** 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

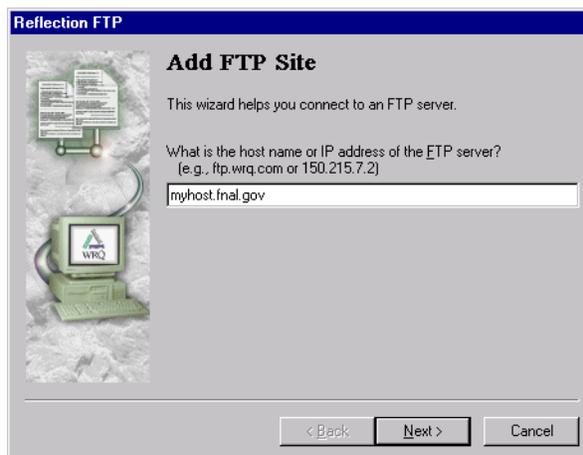
- To debug the dialog between the **X Client Manager** and the remote host, select **CONNECTION > HOST RESPONSE** before clicking the **CONNECT** button.
- The remote host's prompt character(s) must be recognized by the **X Client Manager** for the connection script to work correctly. Add the correct 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.

19.10 Configuring WRQ® Reflection FTP Connections

19.10.1 Create a Profile for 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 or IP address 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 19.8 *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.

Check Forward tickets. Version 10.0.0 is the first version of Reflection's FTP client for which this option is available!

- 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 [2] in section 19.5 *Configuring WRQ® Reflection Kerberos Manager v12.0.*) must be set to the default realm of the target FTP host.



19.10.2 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 19.10.1 *Create a Profile for 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).

19.10.3 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**.