

Appendix D. Transition from Pilot to the FNAL.GOV Realm (User Information)

The production realm FNAL.GOV was launched on May 10, 2001. We are now transitioning to this realm from PILOT.FNAL.GOV. We expect the transition phase to end before October 31, 2001. In this appendix, we discuss issues that users need to be aware of.



The information in this chapter assumes that UNIX/Linux machines have the Fermi Kerberos product installed, and Windows systems use WRQ.

D.1 When did you Get a Principal?

D.1.1 Users who started in the Pilot Program (before 5/10/01)

Everyone who had a pilot realm principal before May 10, 2001 has had their principal, password (including expiration date) and CRYPTOCARD key replicated in the production realm.

You don't need to do anything differently until any of the Kerberized machines you use migrates to the FNAL.GOV realm. However, we recommend that you complete a couple of preparatory tasks:

- If your pilot realm password is near expiration, then your password for the production realm is, too. Go ahead and change your password on each realm.
- Wherever you have a `$HOME/.k5login` file (described in section Appendix : *The .k5login File*), be sure both your principals are in it. (If those are the only two principals listed, you don't need this file at all.)

D.1.2 Users Starting After Production Realm Launched (after 5/10/01)

Principals created after May 10, 2001 have been issued in either FNAL.GOV alone, or in both realms if requested.

You can run `kinit [<yourFNALprincipal>]` on a machine with any version of the Fermi kerberos product as long as `krb5conf` is `v1_0` or newer. To check on a UPS system, run `ups list krb5conf` and see what's current. If a current instance is listed in more than one database, run `echo $PRODUCTS` to see which database is listed first.

Users with Production Realm Principal Only

If have only a FNAL.GOV principal, you can freely access machines in the FNAL.GOV realm, of course. In addition, if you get initial credentials in FNAL.GOV on one machine, you can use them to log onto a target host in the pilot realm if and only if one of the following conditions hold:

- There's a `$HOME/.k5login` file on the target host that lists your FNAL.GOV principal
- The target host has Fermi kerberos v1_2 or later and krb5conf v1_3 or later, and there is no `$HOME/.k5login` file.

D.2 Introduction to the Dual-Realm Environment

D.2.1 The Relationship between the Realms

Trust between the two realms is two-way and transparent. While a Kerberized machine is configured to have a default realm¹, it may still recognize and honor credentials issued for another realm. In addition to the trust relationship, this just requires and that the client be listed in the `.k5login` file. As long as a machine recognizes both realms and recognizes your principal, it doesn't matter which realm your principal is in, you may freely access Kerberized resources on that machine.

D.2.2 About the Fermi Kerberos Versions

Fermi kerberos v1_2 is the first version of the software that knows about both realms. Versions prior to v1_2 only recognize PILOT.FNAL.GOV. A machine which runs Fermi kerberos v1_2 (or later) and krb5conf v1_0 (or later, preferably v1_3 or later) can recognize principals and credentials in both realms, and may have either the pilot or the production realm as its default realm. If you must access some machines with PILOT.FNAL.GOV as the default realm and others with FNAL.GOV, it is easiest if all the machines run these recent product versions.

D.2.3 Password Issues

Whatever your Kerberos password for the PILOT.FNAL.GOV realm was at 1:00 p.m. on Thursday, May 10, 2001, that became your Kerberos password in the FNAL.GOV realm . It will expire (or did expire!) on the same date as your pilot realm password. After May 10, password changes in one realm are not reflected in the other; you must change each separately.

1. To determine a machine's default realm, see section

If your password has only a short time left until expiration in the pilot realm, you might be required to change it before you have begun using it in the production realm. If so, log in to a pilot node which knows about both realms (i.e., which runs Fermi kerberos v1_2 and krb5conf v1_0, or later versions) then enter:

```
% kpasswd [yourprincipal]@FNAL.GOV
```

to change your password in the production realm.

D.3 Accessing Systems in the Pilot and Production Realms

D.3.1 Systems Running kerberos v1_2 and krb5conf v1_0 (or later versions)

For systems running kerberos v1_2 and krb5conf v1_0 (or later versions), you can freely access multiple machines without worrying about which realm each uses as a default, and which principal you're using (many users have a principal in each realm). You don't need a `$HOME/.k5login` file, but if you create one on a machine, include both your principals in it (see section ?? for information on the `.k5login` file).

You may authenticate as either *yourprincipal@FNAL.GOV* or *yourprincipal@PILOT.FNAL.GOV* and you will have normal access. From that system, you should have normal access to any other system which also recognizes both realms.



Note that if you have credentials existing in one realm, and you start a new session and run **kinit** (with no principal argument), you will get credentials in the same realm by default, regardless of the machine's default realm. If you want credentials for a different realm, do one of the following:

- provide a principal argument (including the realm part) with **kinit**
- run **kdestroy** before **kinit**

D.3.2 Other Configurations

If the machine runs a version of krb5conf v1_0 or greater and any version of kerberos, then you can **kinit** under either principal, if you have both. You can connect to such a machine from an FNAL.GOV-only host with your FNAL.GOV principal, if one of the following is true:

- the target host's `.k5login` file includes your FNAL.GOV principal
- the target host runs kerberos v1_2 or later and krb5conf v1_3 or later.

D.3.3 CRYPTOCARD Logins

We remind you that your account name on each machine to which you want to login via CRYPTOCARD must match your principal name. CRYPTOCARDS issued before May 10, 2001 13:00 are configured differently than those issued after that date and time.

Issue date before 5/10/01 13:00

Assuming that your principal name in both realms is the same (it should be), you should be able to use your CRYPTOCARD to log into a machine with either realm as its default. It will authenticate you to the default realm of the machine.

Note that your CRYPTOCARD challenge sequence will be out of sync in the production realm with respect to the pilot realm, so you may have to manually enter a challenge into your card the first time you do a portal login to a production realm host. In fact, every time you alternate realms with your CRYPTOCARD, you may need to resynchronize it with the realm's KDC. Since you probably don't want to bother keying in a challenge to your CRYPTOCARD very often, it is best to pick only machines in one realm or the other for all your CRYPTOCARD logins, then use your Kerberos ticket to log in from there to any hosts you need to use in the other realm.

In the case of FTP, the realm with which your CRYPTOCARD is synchronized must match the one to which the target machine would map its own hostname (in the `[domain_realm]` section of `krb5.conf` or DNS). This is generally the same as the machine's default realm, but a sufficiently deranged configuration could make it different, and thus make FTP fail.

Issue date after 5/10/01 13:00

CRYPTOCARDS issued after this date are valid for login only to a machine in the realm for which the CRYPTOCARD was initialized. Pick only machines in the proper realm for all your CRYPTOCARD logins, then use your Kerberos ticket to log in from there to any hosts you need to use which are in the other realm.

D.3.4 A Tricky Issue - Expired Credentials

Say your Kerberos tickets expire, and you want to type `kinit` to get new ones. Be aware that you still have a credential cache (with expired credentials) from your previous authentication (unless your `/tmp` has been cleared, you've removed the credential file manually, or you've run `kdestroy`). `kinit` will assume you want to authenticate as the same principal that credential cache belongs to unless (a) you list a different principal on the `kinit` command line, or (b) you issue the `kdestroy` command before

running **kinit**. In the case of (b), the machine's default realm is taken as the realm in which to authenticate, unless you specify your principal in the other realm on the command line.

D.4 WRQ® Reflection Issues

D.4.1 Add FNAL.GOV to Configuration

A registry update file has been created to set up the definitions for the FNAL.GOV realm for the **WRQ®** Kerberos Manager v7.0. It will add the realm definition for FNAL.GOV, update the admin servers for both FNAL.GOV and PILOT.FNAL.GOV, add the new KDCs for FNAL.GOV and PILOT.FNAL.GOV, and change the default realm for the machine to FNAL.GOV.

To apply the update, go to **NETWORK NEIGHBORHOOD**, find **Pckits**, and execute the registry export file:

```
\\pckits\WRQ\FNAL.GOV.reg
```

After applying the registry update, open the **Kerberos Manager** and, under the **CREDENTIALS** menu, create a **NEW PRINCIPAL PROFILE...** for yourself in the production FNAL.GOV realm. Note that you can keep principal profiles defined in both realms.

Please note that this update is NOT valid for the v8.0 Kerberos Manager.

If you don't have access to `\\Pckits`, you can perform the configuration by hand. Follow the instructions in section 19.4 *Configuring WRQ® Reflection Kerberos Manager v9.0.0* under step (2).

D.4.2 Change Password Before Logging In via WRQ®

This note applies only to principals that were initially created in the PILOT.FNAL.GOV realm¹. Your FNAL.GOV realm password won't work with the current **WRQ®** software until you change the password at least one time in that realm after May 10, '01. If you changed your initial FNAL.GOV password before that date, CHANGE IT AGAIN! You'll probably have to log in on a UNIX system to change the password. After this, you can change your password again from **WRQ®** if you like.

D.5 Finding out which Hosts have Migrated

The list of machines in the pilot realm was inserted into DNS (domain name server) as explicit records on May 10, 2001 and those that change their default realm to FNAL.GOV are being deleted from the list as their administrators

1. This may also apply to Windows 95 users whose principals are in FNAL.GOV only.

report in. If your client software doesn't check in DNS for host-to-realm information but you need to know, look for a `txt` record belonging to `_kerberos.<hostname>`. For example, run `dig` or `nslookup`:

dig

```
% dig _kerberos.cdfsga.fnal.gov txt
```

This has several lines of output, one of which gives the realm:

```
;; ANSWER SECTION:
_kerberos.cdfsga.fnal.gov.      21600    TXT      PILOT.FNAL.GOV
```

Hosts without their own explicit listing default to the listing for the parent DNS domain, e.g.,:

```
% dig _kerberos.fnal.gov txt
```

```
...
;; ANSWER SECTION:
_kerberos.fnal.gov.           21600    TXT      FNAL.GOV
```

nslookup

```
% nslookup -q=txt _kerberos.<host>.fnal.gov. | grep kerberos
```

If the host is part of the PILOT realm, you should see the response:

```
_kerberos.<host>.fnal.gov text = "PILOT.FNAL.GOV"
```