

Kerberos Authentication

This document contains the following sections:

- [Introduction](#)
- [Authentication Overview](#)
- [Kerberos for Macintosh](#)
- [Kerberos for Windows](#)
- [WebISO Authentication](#)

For information related to this topic refer to:

- [Security: General Practices](#)
(<http://www.cmu.edu/computing/doc/security/general/index.html>)
- [Information Security Office](#) (<http://www.cmu.edu/computing/security/>)

Last Updated: 0711/08

Introduction

Many users are under the misconception that by using their password to log on to a service, they are securing information that is sent over to the server. Unfortunately, this is typically not the case. Even if you do not keep confidential or important information online, you should still be concerned with network security.

You may not care if someone reads your email, but you probably would be alarmed if your account was used to send email for the purpose of organizing a crime. Additionally, someone with your password may be able to make your account unusable to you. For these and other reasons, it's a good idea to protect your password and to practice secure networking.

Last Updated: 06/02/06

Kerberos and Authentication Management Software

To provide the best-available protection for your account information and data, Carnegie Mellon uses Kerberos authentication management software. The Kerberos authentication management software is implemented in conjunction with applications that use Kerberos for authentication (e.g., Oracle Calendar) to ensure that your password is protected. These authenticated applications also use encryption to protect your e-mail and files from being read by people who intercept your traffic.

While your password identifies you to a server, most applications do not use Kerberos to manage the authentication process. This results in your password being sent over the network in the clear. Furthermore, most applications also transmit your data (e-mail, files, etc.) in the clear as well. This leaves your account open to being eavesdropped by users who know how to "snoop" network traffic.

What is Kerberos?

Kerberos is an authentication service developed at MIT for open network computing environments. When you log in through authentication management software (e.g., Kerberos for Windows or Mac), the application uses your user ID and password to create a ticket that is then matched against a private ticket on the server to which you are authenticating. Your user ID and password are secure since they are never sent over the network.

Kerberos Tickets

Kerberos "tickets" are encrypted protocol messages used to identify you to kerberized network utilities. Once you have logged in, Kerberos grants you these tickets so that you do not need to login again every time you communicate with the server. Kerberos uses two types of tickets in its process of authentication: TGTs (Ticket Granting Tickets) and Service Tickets.

How Authentication Management Software Works With Kerberos

Kerberos for Windows or Mac works as a "ticket agent" between the applications that use Kerberos for authentication and the servers that they access.

Once you login through these software packages, Kerberos is given an initial TGT (Ticket Granting Ticket). When you start an application such as Oracle Calendar, it uses the TGT to retrieve service tickets that are then used by the application. This is why you don't need to login every time you start an application that uses Kerberos.

If you start an application that uses Kerberos authentication but you have NOT already logged in through Kerberos for Windows or Mac (or if your tickets have expired), the Leash/Kerberos login dialog box is displayed. Simply enter your userID and password to authenticate.

Using Authentication Management Software Correctly

When used properly, Kerberos provides the best-possible security for your Andrew password and data. However, if you use them improperly, other users may gain access to your account, e-mail and files!

When an application does not use Kerberos for authentication, the software asks you for your userID and password every time you start the application. Likewise, when you exit the application, you are no longer authenticated. At this point, if another user starts the application, they can login with their userID and password and access their data, not yours.

With Kerberos for Windows or Mac, you could potentially login once in the morning and not have to login again all day regardless of how many times you exited and restarted the applications that use this authentication management software. However, if you exit an application (e.g., Oracle Calendar) and another user starts the application, they will not be asked for their userID and password. Instead, Kerberos **will use your tickets** to authenticate to the server, and that user will have access to your data!

To avoid the risk of someone gaining access to your account and private data, consider the following guidelines when using Kerberos-enabled applications (e.g., Oracle Calendar):

- If you need to leave the machine unattended for any period of time during which someone else could gain access to the machine, you should logoff (or destroy tickets) through Kerberos for Windows or Mac to prevent others from gaining access to your password and your data.
- If you are going to allow someone else to use your machine temporarily to run a Kerberos-enabled application, you must logoff through Kerberos for Windows or Mac. If you do not, the Kerberos-enabled application will use your Kerberos logon when the application is started.

Last Updated: 06/02/06

WebISO Authentication

WebISO is a different type of authentication method used by Computing Services. WebISO allows Carnegie Mellon web services to securely verify the identity of Carnegie Mellon users to allow access to a web page. For more information on WebISO, please visit: <http://www.cmu.edu/computing/webiso/> (<http://www.cmu.edu/computing/webiso/>)

Last Updated: 06/02/06

Using Kerberos for Windows: Network Identity Manager

Network Identity Manager is a utility that allows programs to use Kerberos authentication on Windows machines.

Please read the following pages to learn more about Network Identity Manager:

- [System Tray and Menu](#)
- [Log in / Log out & View Credentials](#)
- [Change Your Password](#)
- [Exit](#)

For more information:

Network Identity Manager is installed with an extensive online help file. If you need information that is not included in this document, please refer to the online help. To access their Help, right-click on the Application icon in the system tray and select Help Contents.

Last Updated: 07/11/08

The System Tray Icon

By default, the Network Identity Manager automatically starts when your computer does. When it is running, an Application icon appears in the system tray near your system clock. The icon display will vary depending on whether you are logged in or not. The following describes the status indicators for the icon.

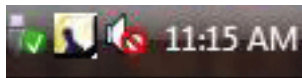
Notification Icons



There are no managed credentials for any identity.



There are valid credentials for all the identities.



Some of the credentials will expire in the next few minutes. This icon will be displayed even if automatic renewals are enabled. In this case, the credentials in question may be renewed before they expire and the icon will change to reflect this.



Some of the managed credentials have expired.



A warning message is waiting to be displayed. Click the icon to view the warning message.

Display the Menu

To display the menu right-click on the Applications icon in the system tray. Use the menu to obtain new credentials, destroy credentials, renew credentials and change your password. The menu items are explained in the following sections.



Andrew Windows Computers

As an Andrew Windows machine, your tickets are handled slightly differently. Your Windows Logon session is authenticated using Kerberos. When you log in to your machine, your Windows tickets are automatically imported into the Kerberos application. You will not be prompted to login a second time.



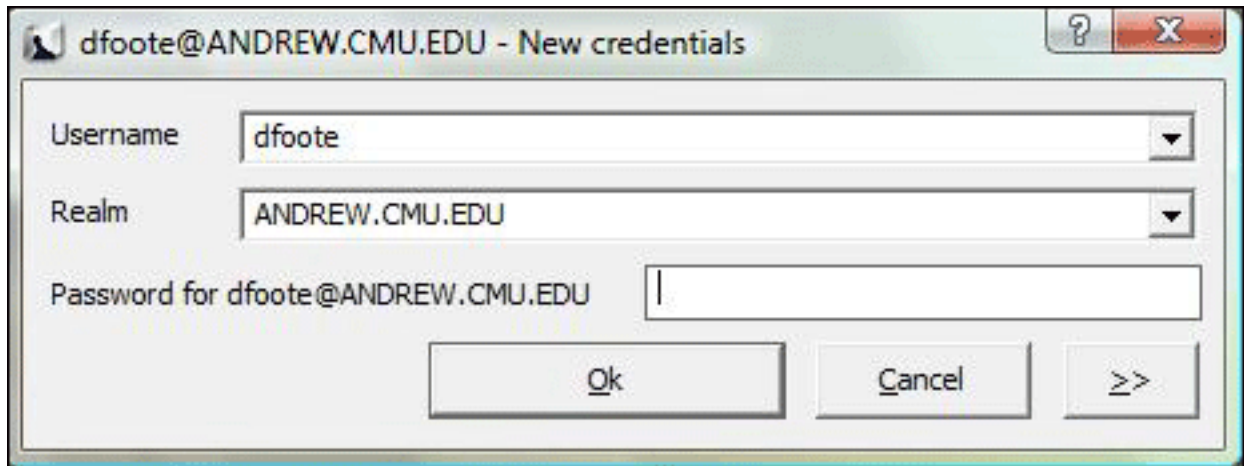
If your computer is part of the Andrew domain, the Import Tickets Credentials will be active on the menu. This option destroys your existing tickets and imports (or pulls over) Kerberos credentials from your Windows logon session to be used with other authenticated applications. Because it is pulling the information from your Windows session, the Import option does not require you to login again. If you elect to Obtain new credentials, you will be asked to type your Andrew userID and password.

Get Tickets (Log In)

Follow this procedure to login to Kerberos.

1. Right-click on the **Application** icon in your system tray to display the Leash menu. Select **Obtain Credentials**.

The New Credentials dialog box is displayed.



2. Enter your **Andrew UserID** in the Username field and your **Andrew Password**.
3. Click **OK**.
If you entered a valid user ID and password, the Application icon is made active. If you didn't enter valid user information, an error displays. Click OK and complete the login again.

Destroy Credentials (Log Out)

It is very important to Destroy credentials at the end of a session to avoid account misuse. If you do not destroy the credentials, someone else could potentially gain access to your account or data. Note that quitting the authenticated application does NOT destroy credentials!

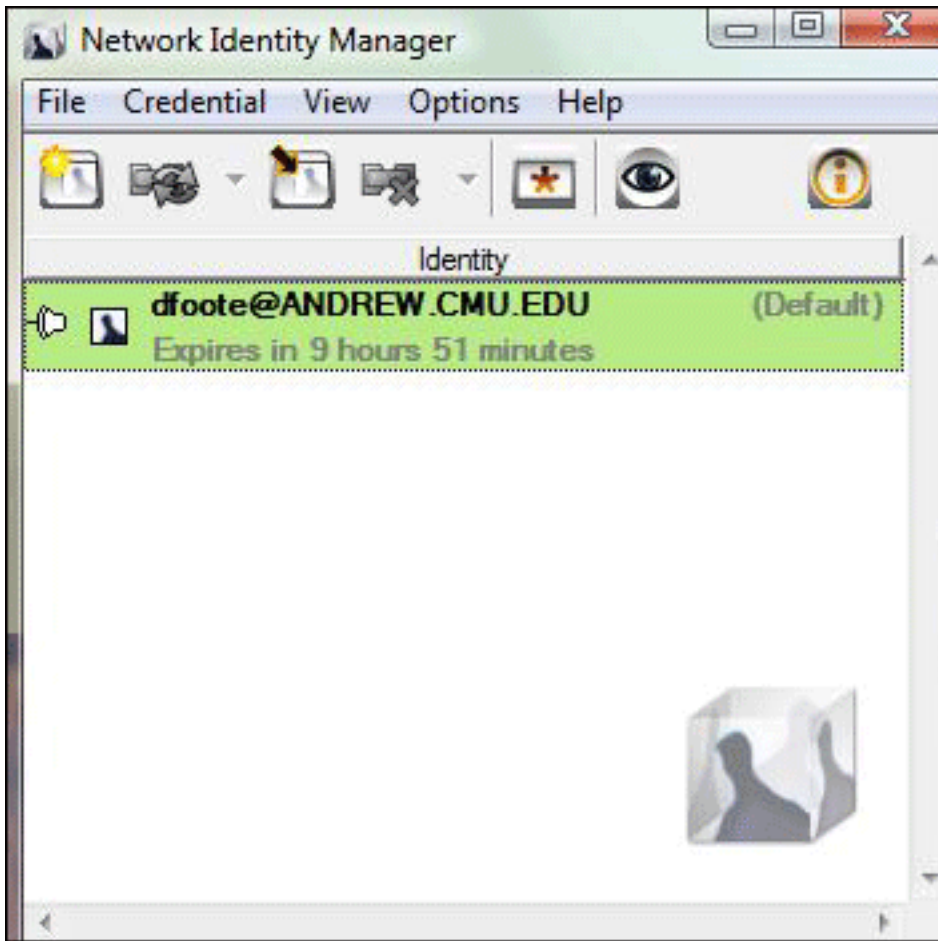
Follow these instructions to destroy Kerberos tickets (log out).

1. Right-click on the **Application icon** in the system tray. The menu is displayed.
2. Select **Destroy**.
3. The Application icon is now inactive and your credentials have been destroyed.

View Credentials

Follow these steps to view the Kerberos credentials:

1. Right-click on the **Application icon** in your system tray.
Note: If you are not logged in, you will have to select Obtain New Credentials and log in.
2. Select **Show Network Identity Manager** window. A window is displayed listing your active credentials.



Change Your Password

Follow this procedure to change your password.

1. Right-click on the **Application Icon** in your system tray to display the menu.
2. Click on **Change Password**.

The Change Password window is displayed.

The screenshot shows a dialog box titled "dfoote@ANDREW.CMU.EDU - Changing password". It has a standard Windows-style title bar with a question mark icon and a close button. The dialog contains the following elements:

- Username:** A text box containing "dfoote" with a dropdown arrow on the right.
- Realm:** A text box containing "ANDREW.CMU.EDU" with a dropdown arrow on the right.
- Changing Kerberos v5 Password:** A section header above three password input fields.
- Current Password:** An empty text box.
- New Password:** An empty text box.
- New Password again:** An empty text box.
- Buttons:** Three buttons at the bottom: "Ok", "Cancel", and a right-pointing arrow "≥>".

3. Enter your **Andrew UserID** in the Username field and current password in that field.
4. Enter your new password in the **New Password** field and then enter it once again in the **New Password again** field.
5. Click **OK**.

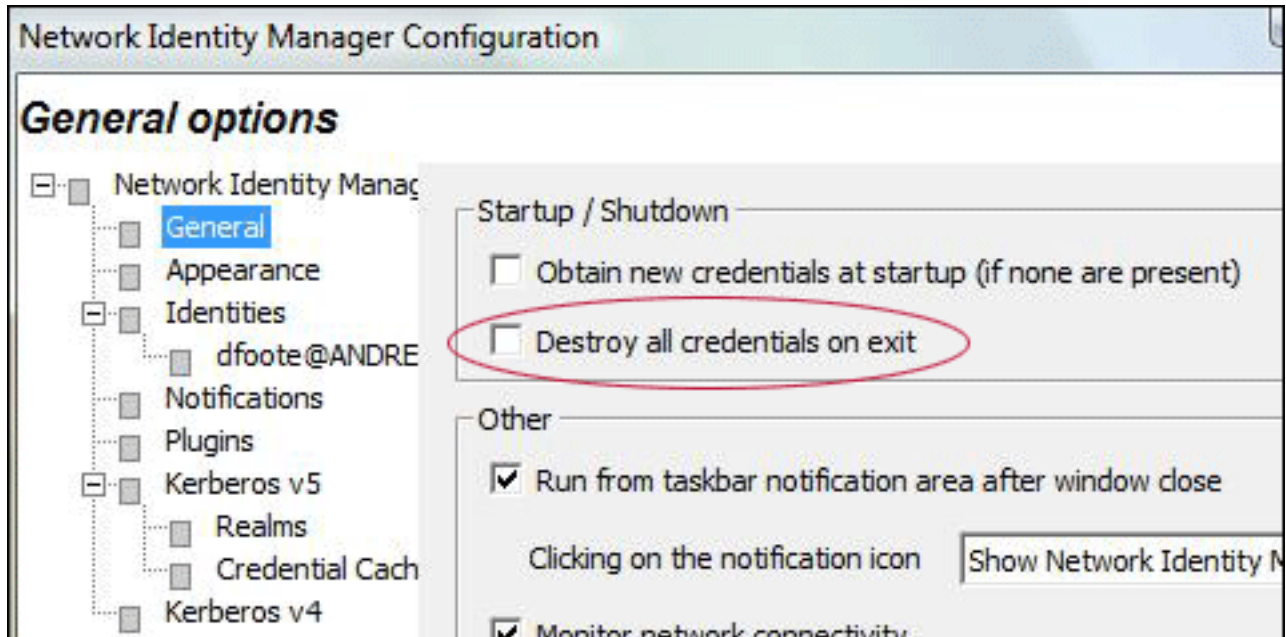
Note: For important information on choosing a more secure password, see [Managing Your Account and Password](http://www.cmu.edu/computing/doc/accounts/passwords/index.html) (<http://www.cmu.edu/computing/doc/accounts/passwords/index.html>).

Exit

Follow these steps to exit the Network Identity Manager application:

1. **Right-click** on the Application icon in your system tray.
2. Select **Exit** from the menu.

Depending on how your Kerberos options are configured, your credentials may or may not be destroyed when you exit the program. To set this option, click the Network Identity Manager icon in your system tray and select **Option > General**.



If the "Destroy all credentials on exit" option is NOT selected, when you exit the program, your tickets are NOT destroyed. Do not mistake the absence of the Application icon in your system tray as an indication that your tickets have been destroyed.

Note: Normally, you will not exit out of the Network Identity Manager program completely. If, however, you do exit, your Application icon will be removed from the system tray. To restore the icon, you must launch the Network Identity Manager by selecting **Start > All Programs > Kerberos for Windows** and then selecting Network Identity Manager).

Using Kerberos for Mac

Kerberos for Mac is a utility that allows programs to use Kerberos authentication on machines running Mac OS X 10.4 or higher. Kerberos for Mac manages your kerberos authentication status.

Please read the following pages to learn more about Kerberos for Mac:

- [The Dock Area](#)
- [Tickets \(Log in / Log out\)](#)
- [Change Password](#)
- [Synchronize Clock](#)

Last Updated: 6/27/08

Using the Dock Area

The Kerberos for Mac installation automatically adds the Kerberos icon to the Dock area for the active user (the user who is logged in at the time of installation). By running the program in your Dock area, your tickets will be automatically renewed for up to 7 days. If you close the Kerberos application, your tickets will expire after 25 hours.

Note: If you were not the active user when Kerberos for Mac was installed, the Kerberos icon will NOT display in your Dock area. In this case, launch the Kerberos for Mac utility (Applications > Utilities > Kerberos for Mac) and add the utility to your Dock area.



Logged in icon
(active tickets)

- When Kerberos for Mac is running and you have tickets, the Key Ring icon appears in the Dock area. The time left on your active tickets displays at the bottom of the icon.



Logged out icon
(no tickets)

- When you do NOT have active tickets, the time remaining does not display.

Display the Kerberos Menu

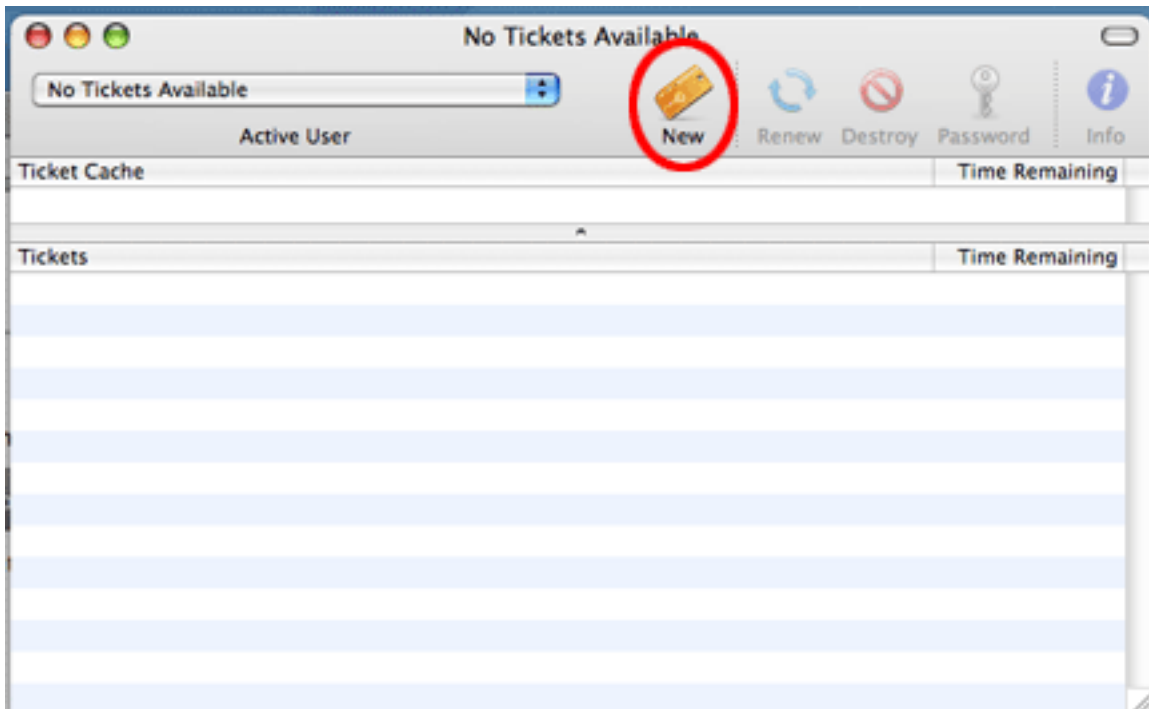
1. **Click and hold** the **Kerberos icon** in the Dock area.
2. The Kerberos menu displays with the following options:
 - **Get tickets:** Use this option to "get" authentication tickets (log in).
 - **Renew tickets:** Select this option to extend the ticket life of your existing tickets.
 - **Change password:** This option is not activated at Carnegie Mellon.
 - **Keep in Dock/Remove from Dock:** Toggles the Kerberos icon on and off in the Dock area.
 - **Open at Login:** Select this option to automatically start the Kerberos for Mac utility when you log into your machine.
 - **Show in Finder:** Use this option to open the application folder containing Kerberos for Mac.
 - **Hide:** Hides the Kerberos window.
 - **Quit:** Exits the Kerberos for Mac utility but does NOT destroy tickets. The "time remaining" in the Key Ring icon is no longer displayed.

Last Updated: 6/27/08

Get Tickets (Log In)

Follow this procedure to login to Kerberos for Mac 10.4 (Tiger) or 10.5 (Leopard):

1. Click on the **Kerberos** icon in the Dock area. The following window displays.



Click **New**.

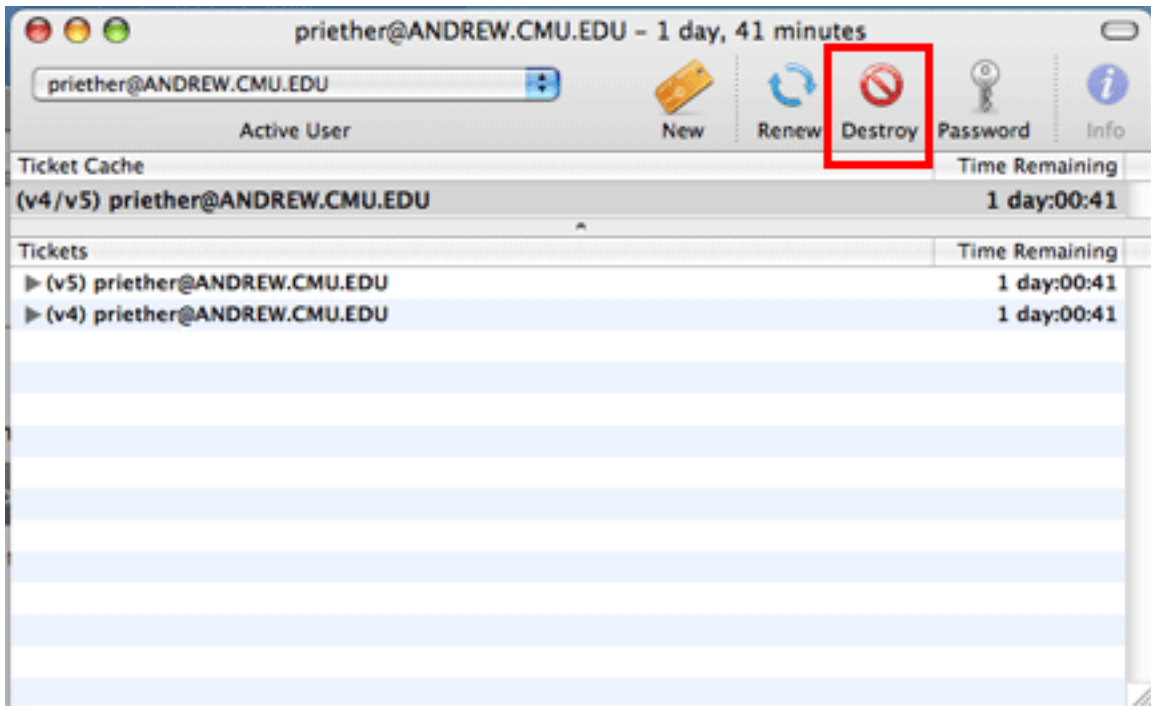
2. The Kerberos login screen displays. Enter your **Andrew userID** (if needed) and your **password** and click **OK**.
If you entered a valid user ID and password, the "time remaining" will display on the Key Ring icon in the Dock area.

Destroy Tickets (Log Out)

It is very important to Destroy Tickets through Kerberos at the end of a session to avoid account misuse. If you do not destroy the tickets that Kerberos is managing for you, someone else could potentially gain access to your account or data. Quitting the authenticated application (e.g., Oracle Calendar) does NOT destroy tickets!

Follow this procedure to destroy Kerberos tickets (log out).

1. Click on the **Kerberos** icon in the Dock area.
2. From the Kerberos window, click **Destroy**.




Last Updated: 6/27/08

Change Your Password


Follow this procedure to change your password.

1. Click on the **Kerberos** icon in the Dock area.
2. Click **Password**. The Change Password Window is displayed.

Kerberos Change Password

 Please change the Kerberos password for "[redacted]@ANDREW.CMU.EDU"

Old Password:

New Password: 

Verify New Password:

3. Enter your current password in the **Old Password** field.
4. Enter your new password in the **New Password** field and then enter it once again in the **Verify Password** field.
5. Click **OK**.

Note: For important information on choosing a more secure password, see [Managing Your Account and Password \(http://www.cmu.edu/computing/doc/accounts/passwords/index.html\)](http://www.cmu.edu/computing/doc/accounts/passwords/index.html).

Last Updated: 6/27/08

Synchronize the Clock

For Kerberos to work properly, your system clock must be synchronized with the server clock that you are connecting to. If for some reason your clock is not in synch with the Kerberos server time, you may receive an error message stating that your system clock needs to be set or synchronized with the network server. If you are running Mac OS X 10.4 or higher, follow these steps to synchronize your machine clock to the server.

1. Click the **Apple menu** and select **System Preferences**.
2. From the System Preferences window, select **Date & Time** under the System area.
3. Select the **Date & Time** tab.
4. Verify that the **Set date & time automatically** option is selected and type **ntp.net.cmu.edu** in the drop-down field.
5. Close the Date & Time window.

Last Updated:6/27/08