Leash User Documentation

Release 2.6.4

Copyright 2004 by the Massachusetts Institute of Technology

What Is Leash and When To Use It?

Leash is a graphical system-tray tool designed to manage for Kerberos tickets on Microsoft Windows. Leash is used to obtain Kerberos tickets, change your Kerberos password, and obtain Andrew File System (AFS) tokens.

Leash combines the functionality of several command line tools a user would use to manage Kerberos functions: kinit, klist, kdestroy, ms2mit, akog, and passwd or kpasswd. Leash combines all of these functions into one user interface and supports auto-renewal or user notification when tickets are approaching expiration.

There are many ways to execute Leash. In addition to clicking on a Leash shortcut, you can start Leash from the Windows command Prompt or Run... option. Command-line options may be specified. If you run Leash with the options -i or -kinit, it will display the ticket initialization dialog and exit; -m or –ms2mit or –import will import tickets from the Microsoft Windows logon session (if available) and exit; -d or -destroy will destroy all existing tickets and exit; -r or –renew will renew existing Kerberos tickets (if possible) and exit; -a or –autoinit will display the ticket initialization dialog if you have no Kerberos tickets.

You may create a shortcut to Leash within your Windows Startup folder (Start Menu->Programs->Startup). A shortcut to "Leash32.exe –autoinit" ensures that Kerberos tickets are available for the use of Kerberized applications throughout your Windows logon session.

If Leash is not executed before using a Kerberized application, the application may prompt you for your password. Some applications, like lpr, never prompt you for a password. These applications simply terminate with a message indicating that you are not authenticated. Before these applications can successfully be used a separate program, such as Leash or kinit, must be used to first authenticate you using Kerberos.

Leash does not perform a logon in the sense of the Windows Logon Service. A logon service would do more than manage Kerberos tickets. A logon service would authenticate you to the local machine, validate access to your local file system and performs additional set-up tasks. These are beyond the scope of Leash. Leash simply allows you to manage Kerberos tickets on behalf of compatible applications and to change your Kerberos password.

Leash Screen Display (Kerberometer and Dash Notification)

The window title contains the name "Leash" followed by the current date and time. Below the title are a menu bar; a tool bar (optional); a tree view; and a status bar (optional).
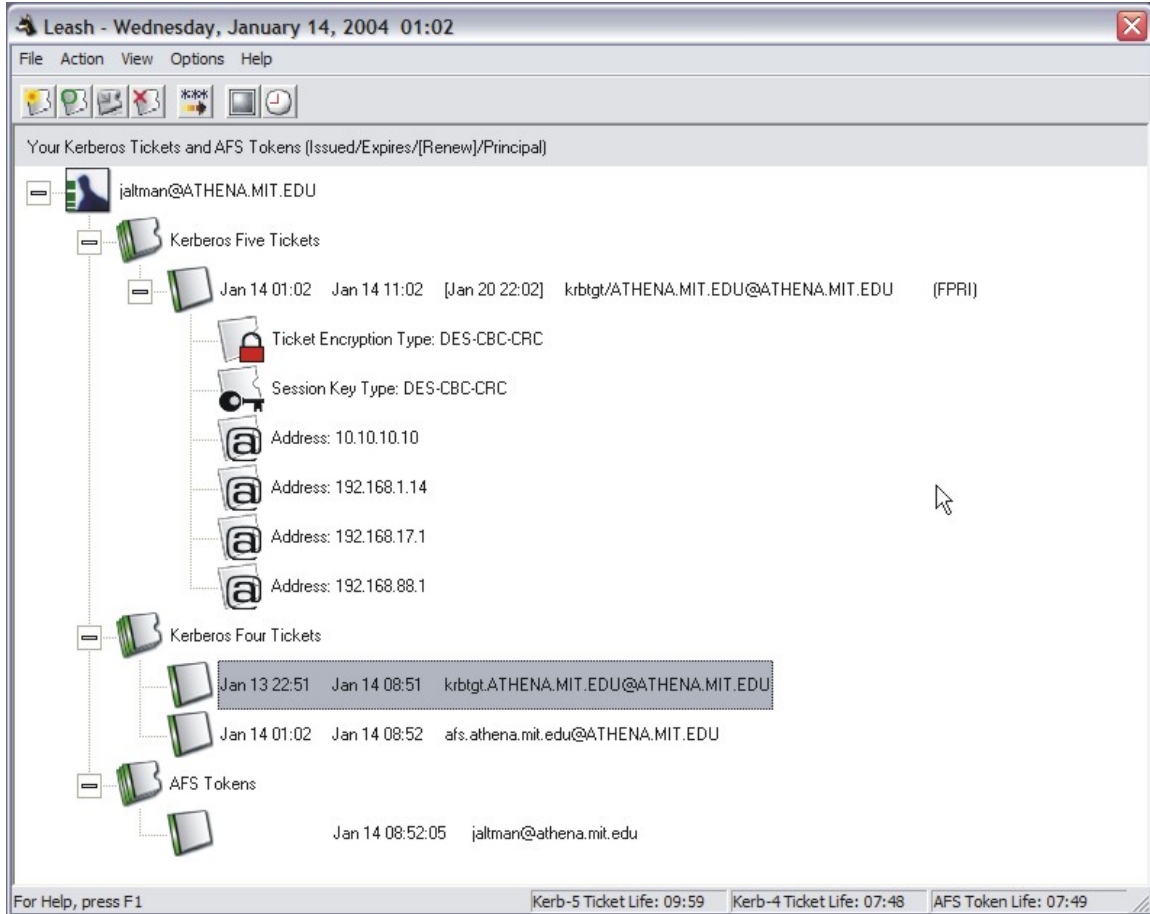
The root of the Leash tree view shows the active user principal name (user@REALM). This entry appears with a "+" icon and a Kerberos icon to its left. Click on this plus icon of a line to expand the branch, displaying a "-" icon. Click on the minus sign to close the branch.

Below user principal, the tree contains ticket categories. Below each ticket category are the current tickets belonging to the group. Each ticket entry contains the current ticket status, the time it was issued, the time it will expire, and the service principal and flags. For Kerberos 5 tickets, encryption types and network address information are listed below each ticket.

The tree updates once per minute. If you need an immediate update of your ticket status, you can either click in the window or the press the Update Display button on the toolbar.

On the right of the status bar is a display of the remaining time of your tickets (both Kerberos 4 and Kerberos 5, as some programs obtain only Kerberos 4 tickets, these are not necessarily the same) in hours, minutes, and seconds. This used to be known as the **Kerberometer**.

Each ticket is described and represented by an icon of a little ticket. The color of the ticket changes based on its viability:

green = normal
yellow = tickets are within 15 minutes of expiration
red = tickets have expired, or you have no tickets
gray = these tickets are not available to you

At 15, 10, and 5 minutes before your Kerberos tickets expire, a screen pops up to warn that your Kerberos tickets will expire soon and to give you the opportunity to renew them. This used to be known as **Dash-style notification**.

Andrew File System (AFS) tokens information is displayed only on machines that have either OpenAFS for Windows http://www.openafs.org or Transarc AFS 3.6 for Windows.

Leash Command Line Options

When Leash is executed from the command line one of the following command line options may be specified:

-kinit, **-i** performs a Kerberos ticket initialization (and exits)
-ms2mit, **-import**, **-m** imports credentials from the Windows Logon Session (and exits)
-**renew, -r** renews credentials (and exits)
-destroy, -d destroys credentials (and exits)
-autoinit, **-a** performs ticket initialization only if the credential cache is empty

Leash Commands

File:

File | Action | View | Options | Help
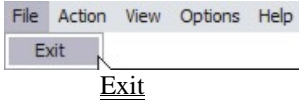
Exit

Exit

<u>Exit Command</u>
From the File menu, you can use this command to exit the Leash program.

<u>Important Note...</u>
Exiting the Leash program will **not** destroy your current Kerberos tickets. Unless you have selected this in the options menu, you need to use the destroy tickets command.

Action:

File | Action | View | Options | Help

Get Ticket(s)/Token(s)	Ctrl+T
Renew Ticket(s)/Token(s)	Ctrl+R
Import Ticket(s)/Token(s)	Ctrl+I
Destroy Ticket(s)/Token(s)	Ctrl+D
Change Password...	
Reset Window Size/Pos	
Synchronize Time	
Update Display	F5
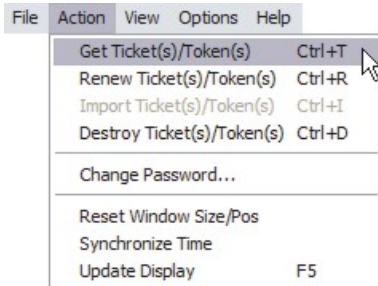
<u>Get Ticket(s)/Token(s) Command, Ctrl+T</u>
This command is found under the Action menu; it is also the first button (from the left) in the toolbar. Use this command to obtain new Kerberos tickets (and perhaps AFS tokens).
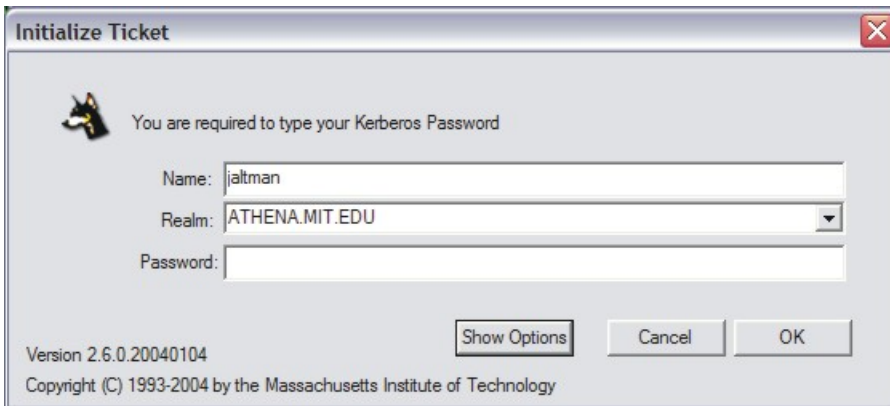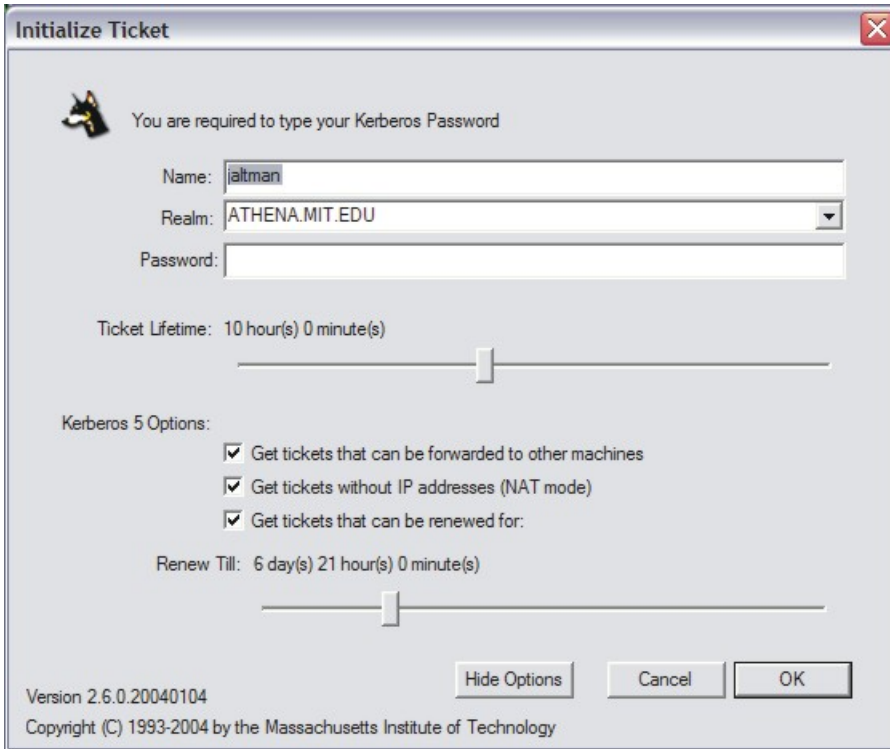
When you select this command, Leash displays a dialog requesting your Username, Kerberos Realm, and Password; if these are correct, Leash will obtain tickets for you. You may optionally specify a ticket lifetime and various Kerberos 5 ticket options: ticket forwarding, addressless tickets, and renewable ticket times.

Renew Ticket(s)/Token(s) Command, Ctrl+R
This command is found on the Action menu; it is also the second button (from the left) in the toolbar. Use this command to renew the Kerberos tickets (and perhaps AFS tokens) on your local machine without requiring the use of a password. If your existing tickets cannot be renewed the ticket initialization dialog will be displayed allowing you to request new tickets.

Note: This command is only available if your existing Kerberos tickets are renewable.

Import Ticket(s)/Token(s) Command, Ctrl+I
This command is found on the Action menu; it is also the third button (from the left) in the toolbar. Use this command to import Kerberos tickets from your Windows Logon Session. Importing tickets will result

in the destruction of existing tickets. Leash will confirm the operation if necessary.

Note: This command is only available if your Windows Logon Session is authenticated using Kerberos.

Destroy Ticket(s)/Token(s) Command, Ctrl+D

This command is found on the Action menu; it is also the fourth button (from the left) in the toolbar. Use this command to destroy all of the Kerberos tickets (and perhaps AFS tokens) on your local machine. Leash confirms your intentions before completing the request. Tickets for individual services may not be destroyed by the Leash application.

Once tickets are destroyed, you must Get or Import new tickets before Kerberized applications can once again access network services.

Change Password Command

This command is found on the Action menu; it is also the fifth button (from the left) in the toolbar. This command changes your Kerberos password.

Note: This command will not change your local machine password unless your Windows Logon Session is authenticated using Kerberos.

How To Choose a Password...
Your passwords are the keys to many computers, from a bank machine to a multiuser mainframe to a server on a network. Your password helps to prove that you are who you say you are, and ensures your privacy.
Compromised passwords are the means by which most unauthorized (and unscrupulous) people gain access to a system. Someone logging on under your name has access not only to your computer files, but to most of the facilities of the computer system. Since tampering can have far-reaching and serious consequences, it's important to take to heart the following guidelines for choosing a password.

Do choose:
*   Something easy for you to remember with at least six characters.
*   Something obscure. For instance, you might deliberately misspell a term or use an odd character in an otherwise familiar term, such as "phnybon" instead of "funnybone." Or use a combination of two unrelated words or a combination of letters and numbers.
*   A combination of letters and numbers, or a phrase like "many colors" and then use only the consonants "mnYc0l0rz."
*   An acronym for your favorite saying, for example, "L!isn!" (Live! It's Saturday Night!)

Don't choose:
*   Your name in any form - first, middle, last, maiden, spelled backwards, nickname or initials.
*   Your userid or your userid spelled backwards.
*   Part of your userid or name.
*   Any common name, such as Joe.
*   The name of a close relative, friend, or pet.
*   Your phone or office number, address, birthday, or anniversary.
*   Your license-plate number, your social-security number, or any all numeral password.
*   Names from popular culture, e.g., spock, sleepy.
*   Any word in a dictionary.
*   Passwords of fewer than four characters.

Mum's the Word
Never tell anyone your password -- not even your system administrator or account manager -- and don't write it down. Make sure you have chosen a password that you can remember. And, finally, change your password at regular intervals

Reprinted from i/s, Vol. 4, No. 9,
May 1989. Revised March 1993.
Copyright C 1993 MIT Information Systems

Before You Begin...
Remember that *passwords are case-sensitive,* and note whether your keyboard has Caps Lock on. Leash is not programmed to inform you about the state of your Caps Lock key.

How To Use Change Password...
1.   In Leash, click on the Change Password button (the one that has "***" and an arrow), type your username in the first field of the dialogue box.
2.   Type your *current* password in the Old Password field.
3.   Type your *new* password in the New Password field.
4.   Retype your *new* password in the New Password (again) field to verify it
5.   Press Enter or click OK.
        The program checks the username and password you entered and notifies you if either is invalid.

If you have entered the new password twice with consistent spellings, Leash replaces your old password with the new, *if it is a strong password.* If Kerberos determines the password is weak, a message notifies you, and you need to repeat steps 1 through 4 with a strong password, as described by the "How To Choose a Password" guidelines above.

How Change Password Works...
When you type into the password fields of the dialog box characters are replaced with bullets. The program accepts only printable characters for new passwords, i.e., characters between ASCII codes 0x20 and 0x7E.

When you have entered the new password twice consistently, the program attempts to change the password via a dialogue with the Kerberos administrative server. Some Kerberos sites, including MIT's Athena environment, check the password's strength before allowing the change to take place and notifies you if it determines that the password is weak.

Reset Window Size/Pos Option
When you select this from the Options menu, the Leash window moves to its default size and position, near the upper left corner of the screen.

Synchronize Time
This command is found on the Action menu; it is also the sixth button (from the left) in the toolbar. When you select this command, Leash synchronizes the local machine time with the time server specified in the Leash Properties dialog.

Note: Kerberos authentication protocol requires loosely synchronized time between computers. The local machine clock and the Kerberos server clock need to be within five minutes of each other for Kerberos to function properly. This function can also be performed with the clock icon on the toolbar and has no keyboard equivalent.

Update Display Command, F5
Use this command (in the Actions menu, or the black rectangular icon) to update the display of your current Kerberos tickets. You can also perform this function by clicking in the main Leash window.

Why Use It...
Although most end users will likely find this Leash feature irrelevant, application developers and support staff may occasionally find it to be useful. For example, you may want an immediate status check of Kerberos tickets if you have just used command-line kinit or kdestroy and want to check that they have functioned successfully.

How It Works...
While Leash automatically checks the status of your Kerberos tickets every 30 seconds, the Update Display command forces an immediate status check.

View:
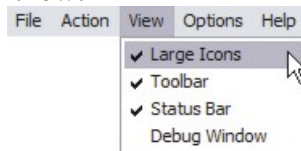
Large Icons
When this option is checked on the View menu, the icons and fonts in the main window (such as the picture of Kerberos) will be about twice as big as the minimal icon and font size. Naturally, smaller icons allow many more tickets to fit into a nonscrolling window. The default setting of Leash is Large Icons.
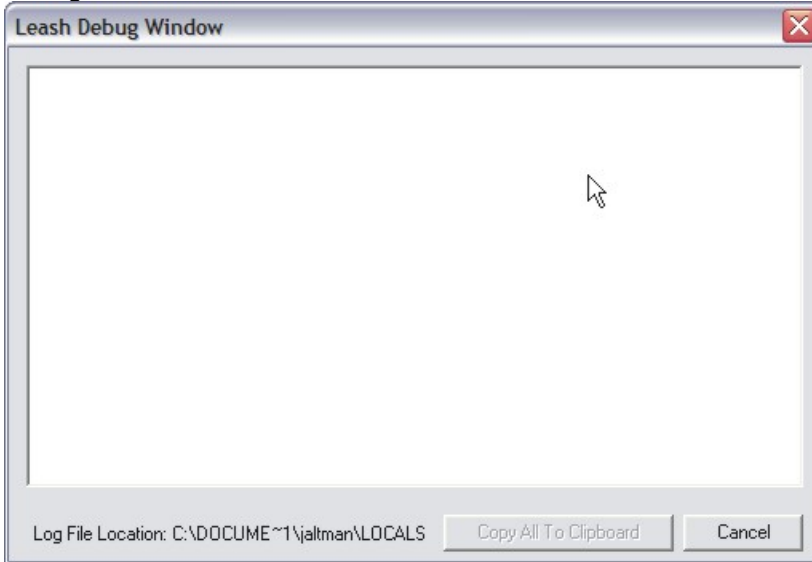
Toolbar
By default, this option on the View menu is selected. When it is checked, the toolbar containing icons for commonly used commands is visible. Otherwise, Leash hides it.

Status Bar
The Status Bar is on by default; turning it off causes the bar at the bottom of the Leash window (with the time remaining on any tickets that you might have) to disappear.

Debug Window

When this item (found under the View menu) is checked, the Leash Debug Window appears. From this window, commands that Leash issues to the Kerberos server are visible. Here, you can see exactly what Leash is doing. This action is useful if you are having a problem with Leash and want to see more exactly what is going on, or if you are writing Kerberized applications dependent on Kerberos tickets or the actions of Leash.

Note: Debugging is only supported by Kerberos 4 and AFS. Kerberos 5 protocol operations cannot be debugged using Leash.

Options:
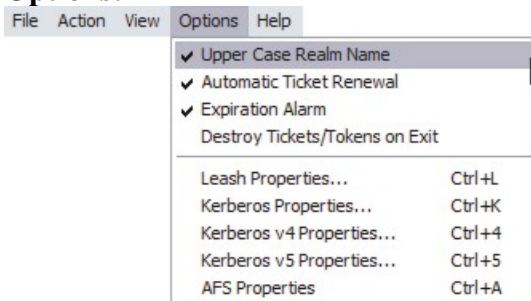
Upper Case Realm Name
The default for this (accessible from the Options menu) is on; when this option is selected, the Kerberos realm name that you type (such as ATHENA.MIT.EDU) is converted to upper case regardless of how you type it.

<ins>Automatic Ticket Renewal</ins>
When **Automatic Ticket Renewal** is on, whenever tickets are near expiration (within 15 minutes) Leash will attempt to extend the ticket lifetime either via ticket renewal or ticket importation. If these attempts fail, Leash will display the ticket initialization dialog. In this way, Leash ensures that there are always valid Kerberos tickets.

<ins>Expiration Alarm</ins>
Leash will always pop up windows with warnings that your tickets are about to expire, beginning 15 minutes before the time of expiration and continuing every 5 minutes. However, when this option is selected under the Options menu, a bell will ring as well.

When you view your tickets and tokens, those shown in yellow are due to expire in less than 15 minutes; those in green have 15 minutes or greater. (A red ticket is one you have but is expired; gray tickets are not available to you at the current time, because Leash or your machine is missing a requisite module or piece of functionality.)

<ins>Destroy Tickets/Tokens on Exit</ins>
If this option is selected under the Options menu, Leash destroys your tickets and tokens when you shut down Leash; otherwise, the tickets remain. This option is turned off by default.

<ins>Leash Properties Dialog, Ctrl+L</ins>
The Leash Properties dialog, located on the Options menu, allows you to configure operational properties specific to the Leash application which are not accessible directly via the Options menu.
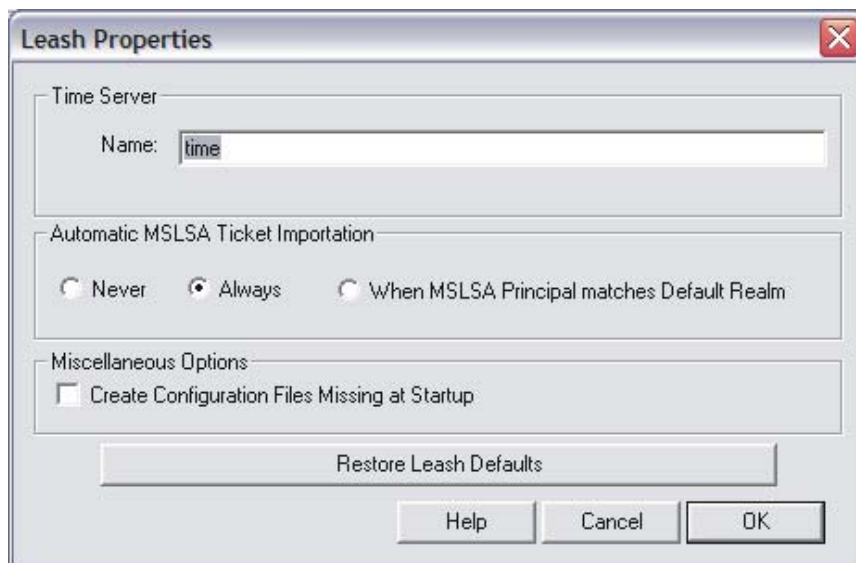
Here you can set a time server from which Leash will obtain the correct time. Leash needs the correct time because of the time dependencies in Kerberos tickets. When you specify a time server, Leash tries to get the time from that server when you next run the Synchronize Time command. The default value for the time server is "time". If access to a time server were to fail, Leash would notify you, and revert to the server "time". Whichever server succeeds, Leash would tell you where it found the time. See the Synchronize Time command for more information.

The **Automatic MSLSA Ticket Importation** radio buttons allow you to configure how Leash interacts with the Microsoft Kerberos Authentication Provider. Leash will automatically import Kerberos Tickets from the Microsoft LSA at startup depending upon the selected option and whether or not the Kerberos Authentication Provider was used for Windows Logon authorization. **Never** means do not import tickets from the MSLSA; **Always** means do import tickets from the MSLSA; and **When MSLSA Principal**

matches Default Realm means import tickets from the MSLSA only if the Kerberos principal belongs to the Kerberos Realm specified within the <u>Kerberos Properties Dialog.</u>

The Kerberos libraries depend on configuration files for their proper operation. When **Create Missing Configuration Files** is checked, Leash will construct replacements for missing configuration files upon startup. This is performed by extracting Kerberos configuration information from the local Windows registry and the Domain Name System. The contents of the created file may then be edited using the **Kerberos Properties Dialog**.

The **Restore Leash Defaults** button is used to restore user configurable Leash settings to the defaults as configured either by the local machine system administrator or by the Kerberos for Windows distribution.

<u>Kerberos Properties Dialog, Ctrl+K</u>
When you select this from the Options menu, Leash will display a tabbed window. The box within this window has four tabs: Default Realm Configuration; Ticket Lifetime and Other Initialization Options; Realm/Server Mapping; and DNS/Realm Mapping.

Default Realm Configuration
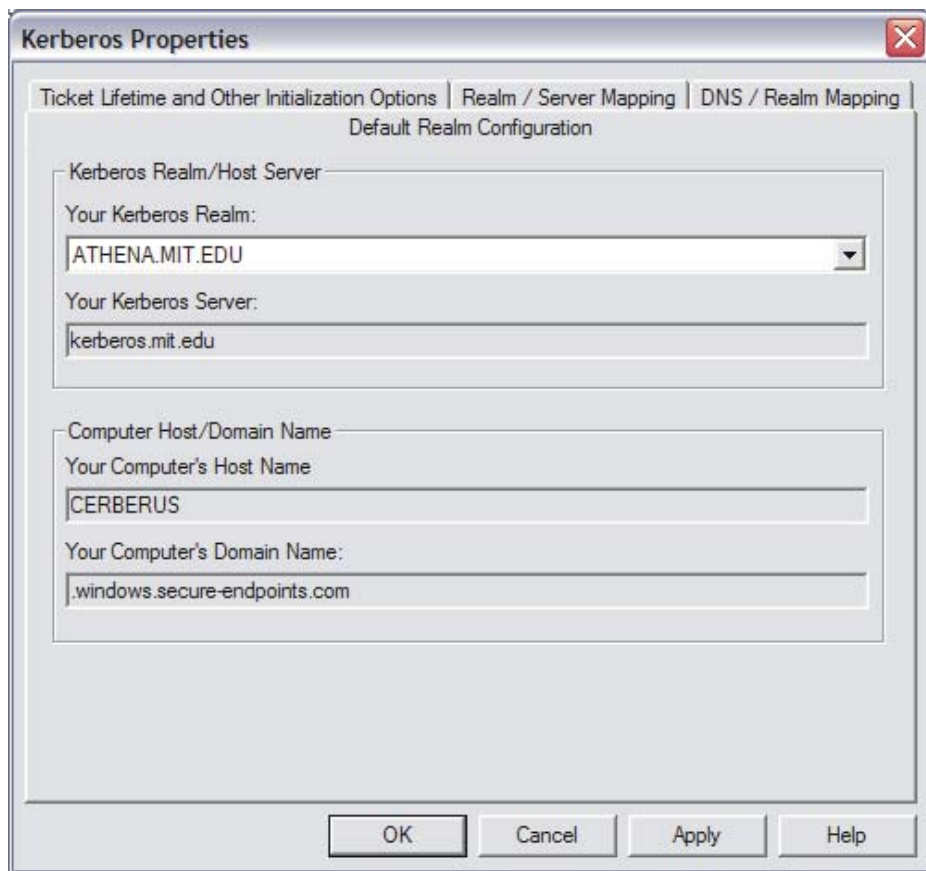
There are two groups, the **Kerberos Realm/Host Server** and the **Computer Host/Domain Name**.

Kerberos Realm/Host Server: In the **Your Kerberos Realm** field, select a Kerberos realm from the dropdown list. The list is editable using the Realm/Server Mapping tab, below.   Leash automatically fills in your Kerberos server with the first server in the "Servers Hosting a KDC" list on the Realm/Server Mappings tab.

Computer Host/Domain Name: The field labeled **Your Computer's Host Name** displays the name of your local machine. The **Your Computer's Domain Name** field displays the domain to which your local machine currently belongs.

*Ticket Lifetime and Other Initialization Options*

There are two expiration times associated with Kerberos tickets. The first specifies the length of the time period during which the tickets are valid for use. The second specifies the length of the renewable lifetime. Valid Kerberos tickets may have their valid use lifetime repeatedly extended up until the renewable lifetime expires. The settings on this page are used to configure default lifetime values for Leash to use when requesting Kerberos tickets from the Kerberos server (key distribution center). The Kerberos server may issue tickets with shorter lifetimes than were requested.

The minimum and maximum values are used by the ticket initialization dialog box when constructing the Lifetime and Renewable Lifetime sliders. These sliders can be used to modify the requested ticket lifetimes when Kerberos tickets are initialized.

When the **Request Kerberos 4 credentials** button is checked, Leash will attempt to retrieve Kerberos 4 credentials when ticket initialization, renewal, or importation is performed. Leash will attempt a Kerberos 5 to Kerberos 4 conversion and if that fails an initial Kerberos 4 ticket request will be generated. Kerberos realms are increasingly configured to support on Kerberos 5. If the realms you use do not support Kerberos 4 it is suggested that this button be unchecked.

When the **Preserve Ticket Initialization Options** button is checked, changes to the Lifetime, Renewable Lifetime, and Kerberos 5 ticket properties on the Ticket Initialization Dialog will be saved as the new default values for the current user.

Realm/Server Mapping
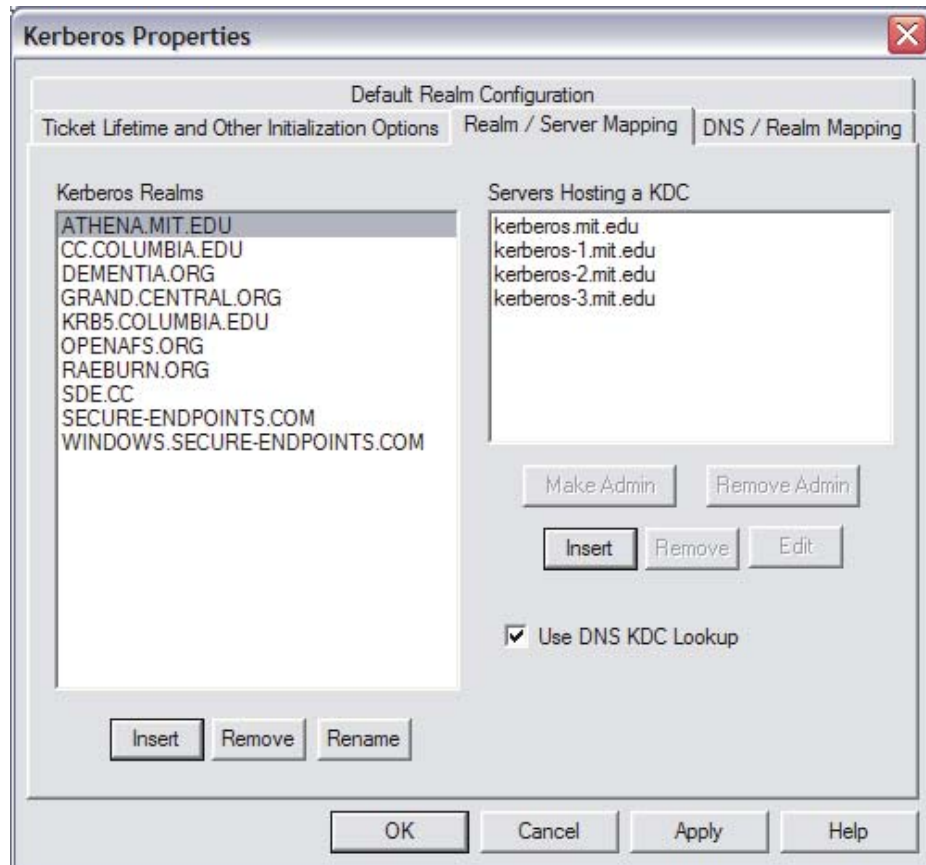
The **Kerberos Realms** list box is used to add, remove or rename realms from the local Kerberos configuration files. To add a new realm, click on the Insert button beneath the Kerberos Realms list box. In the dialog, type the name of the new realm and click OK. However, for the realm to be inserted, it needs one or more servers. Immediately after you enter the new realm name, you will be prompted for the names of one Kerberos server in that realm. If you do not enter a server name, Leash will not insert the realm.

To add servers to an existing realm, select the realm from the Kerberos Realms list box and click the Insert button under Servers Hosting a KDC list box. You will be prompted for the name of the new server. You can also remove servers, and designate either one or none as the administrative server. (The administrative server is the preferred server for performing password changes.)

By clicking and dragging on the server that you want to move, you can change their order; this is important because the server listed at the top appears in this window under the **Default Realm Configuration** tab as the value for **Your Kerberos Server**.

The **Use DNS KDC Lookup** checkbox is used to specify whether or not Kerberos should utilize the domain name service to attempt to find Kerberos Servers when the existing listed servers are not available.

DNS/Realm Mapping
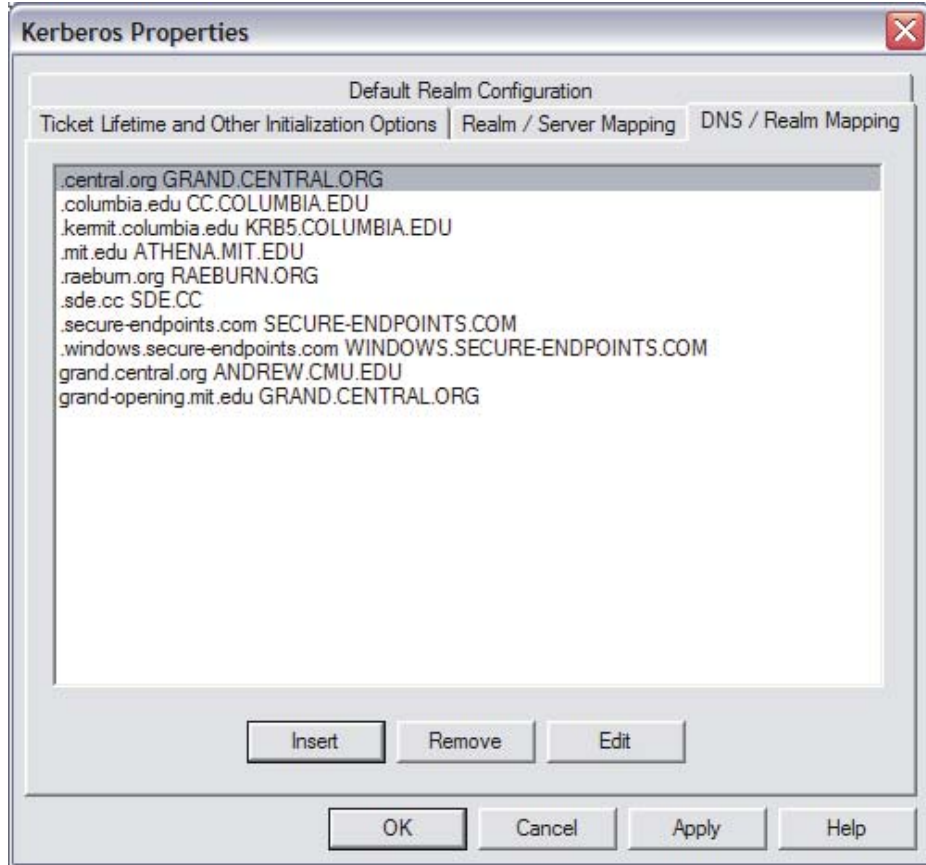
Each entry here consists of two portions: the domain name (such as .mit.edu) or hostname (such as dialup.athena.mit.edu) followed by a space and the Kerberos realm (such as ATHENA.MIT.EDU) which is used by that domain or machine. You can insert new entries, edit existing ones, or delete old entries.

Kerberos v4 Properties Dialog, Ctrl+4

The Kerberos v4 Properties dialog is accessible from the Options menu.
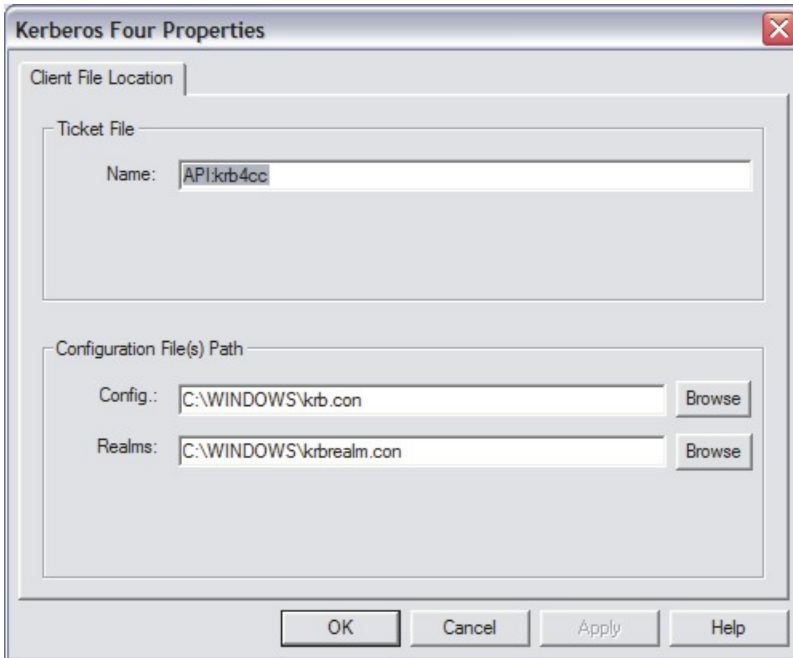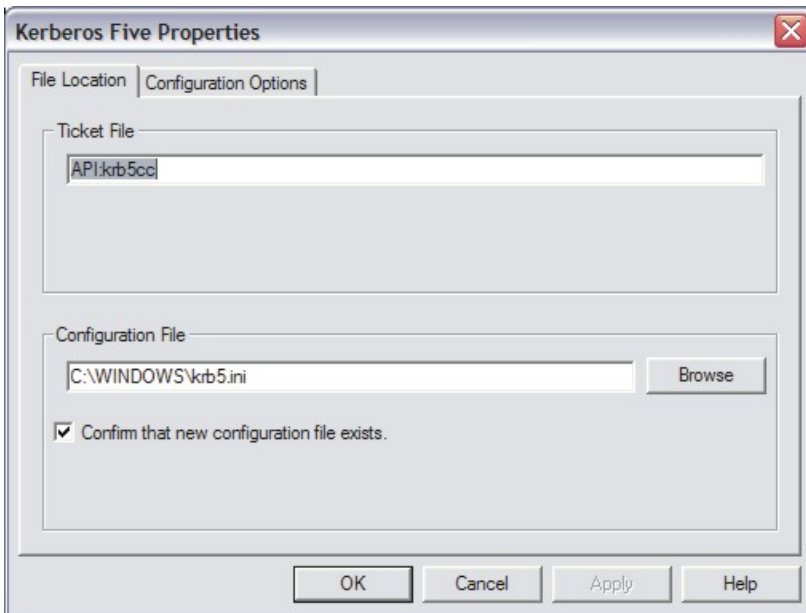

Here, you can specify the name of the in-memory cache used to store the Kerberos 4 tickets. The format of the name is "API:" followed by the cache name. Disk caches are not supported by Kerberos for Windows.

The paths to the Kerberos 4 configuration files: krb.con and krbrealm.con may be changed from this dialog if necessary. The default is to store the configuration files in the Windows directory.

Kerberos v5 Properties Dialog, Ctrl+5

The Kerberos v5 Properties dialog is accessible from the Options menu. This dialog has two tabs: **File Location** and **Configuration Options**.

The **File Location** tab allows you to specify the location of the Kerberos 5 ticket cache and configuration file. The **Ticket File** field specifies the name of the in-memory cache (Ticket File) used to store the Kerberos 5 tickets. The format of the name is "API:" followed by the cache name. Disk caches are not supported by Kerberos for Windows. The **Configuration File** field specifies the path to the Kerberos 5 configuration file, krb5.ini. If **Confirm that new configuration file exists** is checked when the configuration file location is changed, then Leash will not accept values which are not pre-existing Kerberos 5 configuration files.
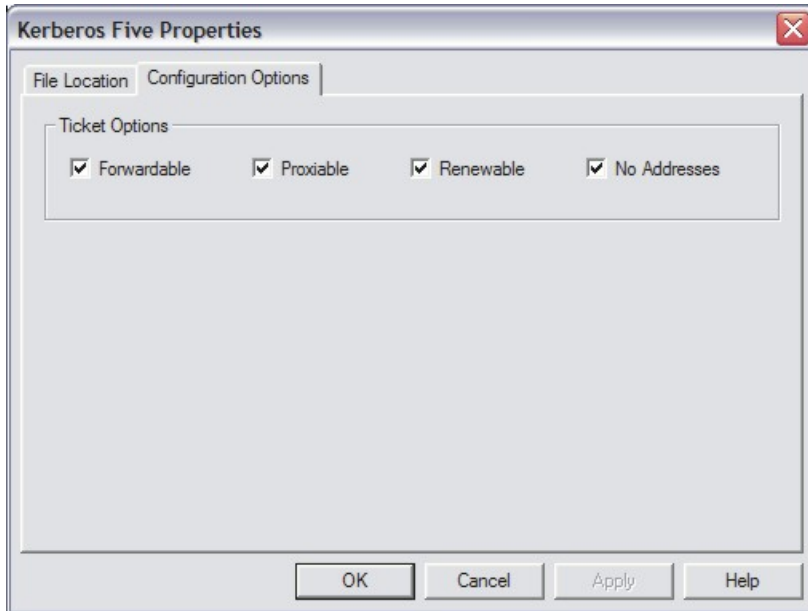
On the **Configuration Options** page, you provide default attribute values to be used when requesting Kerberos 5 tickets from the Kerberos server.

When **Forwardable** tickets are received from the Kerberos Server, these tickets can be forwarded to a remote host when you connect via telnet, ssh, ftp, rlogin, or similar applications. When tickets are forwarded, there is no need to obtain Kerberos tickets again to access Kerberized services on the remote host.

When **Proxiable** tickets are received from the Kerberos Server, these tickets can be passed onto Kerberized services which can in turn act on your behalf.

When **Renewable** tickets are received from the Kerberos Server, the ticket lifetimes may be renewed without prompting the user for her password. This allows Kerberos tickets to be issued with short lifetimes allowing compromised accounts to be disabled on short notice without requiring the user to enter a password every few hours. When combined with **Automatic Ticket Renewal** (Option menu), Leash can maintain valid tickets for a week, a month, or longer by automatically renewing tickets prior to their expiration. The ability to renew tickets without a password is limited by the ticket's renewable lifetime as issued by the Kerberos Server.

Traditionally, Kerberos tickets have included a list of network addresses within the tickets. This address list restricts the use of the tickets to the computers which are assigned those addresses. The use of address lists has become a headache for many users of Kerberos on network connections which use either Network Address Translation (Cable/DSL routers) or Network Address Hiding (VPN) capabilities. On these networks the address of the client machine appears to be different to the network service than it does to the client. The result is the Kerberos ticket is deemed to be invalid by the service even though it has not been stolen. When **No Addresses** is checked, Kerberos will not insert an address list into the Kerberos tickets.

For Kerberized services which do not require address lists, this will enable Kerberos to be used across NAT and VPN based connections.

Note 1: As of Kerberos 5 release 1.3, the library default is to disable the use of address lists. Leash will detect the setting from the Kerberos 5 configuration and check the **No Addresses** box. If you attempt to re-enable address lists while the library is configured to disable them , Leash will warn you that the Kerberos 5 configuration file must be altered.

Note 2: Distributed Computing Environment (DCE) servers require the use of address lists.

AFS Properties Dialog, Ctrl+A
The **AFS Properties** dialog can be found on the Options menu when AFS is available.
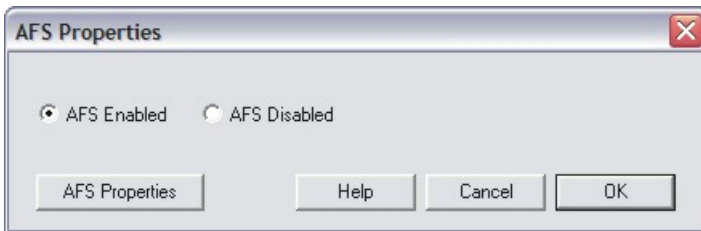

There is a radio button pair to enable or disable the retrieval and display of AFS tokens. There is also an AFS Properties button to bring up the AFS Client Configuration program in order to alter settings for Client Properties, Cell Hosts, and Submounts.

Help:
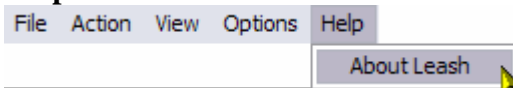
About Leash
When you access this window from the Help menu, you see a Module list, three radio buttons, and a Properties button. Modules are executables and dll files that Leash may require.
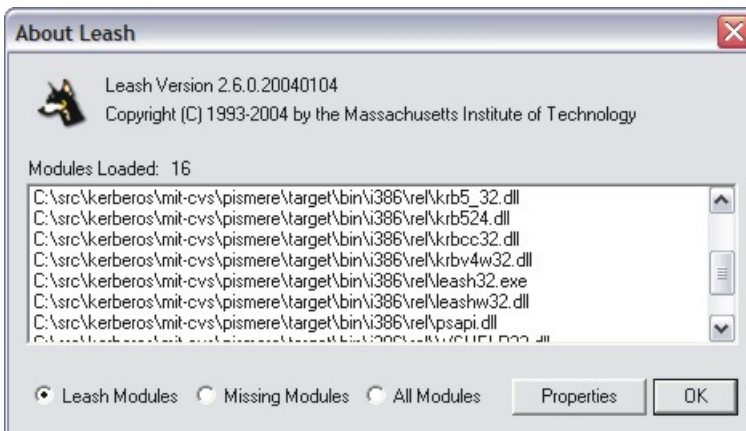
The radio buttons let you choose to view a list of:

- Leash Modules - displays the modules that Leash currently has loaded for its own use;

- All Modules - displays Leash modules as well as those loaded by the OS;

- Missing Modules - displays modules that Leash needs for complete functionality but that are not found. (Leash can still function with some modules missing.). This is useful if part of Leash is missing; you can find which files are needed to restore full functionality.

If you select a module and click on the Properties button, Leash displays the properties of the selected module - both the general properties and those of this particular version.

System Tray

While Leash is running one of the following icons will be displayed in the system tray based upon the current state of your Kerberos tickets. Clicking on the icon with the first mouse button will open or close the Leash display window. Clicking with the second mouse button will display a menu of commands.

Green: tickets are valid and have a lifetime of greater than 20 minutes
Grey: no tickets are present
Orange: tickets are valid and about to expire
Red: tickets have expired

System Tray menu

Open Leash Window
The Open Leash Window command will restore the Leash Ticket Display window. If the window is already open this option will appear as "Close Leash Window".

Get Ticket(s)/Token(s)
Renew Ticket(s)/Token(s)
Import Tickets
Destroy Ticket(s)/Token(s)
Change Password
The **Leash Commands: Actions** section of this document describes these commands

Automatic Ticket Renewal
Expiration Alarm
The **Leash Commands: Options** section of this document describes these commands.

Exit
You can use this command to exit the Leash program.

Important Note...
Exiting the Leash program will **not** destroy your current Kerberos tickets. Unless you have selected this in the options menu, you need to use the destroy tickets command.

Toolbar

The Leash Toolbar contains buttons which act as shortcuts to the most frequently used Actions found on the Menubar. From left to right:
1. Get Tickets
2. Renew Tickets
3. Import Tickets
4. Destroy Tickets
5. Change Password
6. Update Display
7. Synchronize Time

Copyrights

Leash Copyright

This software is being provided to you, the LICENSEE, by the Massachusetts Institute of Technology (M.I.T) under the following license. By obtaining, using and/or copying this software, you agree that you have read, understood, and will comply with these terms and conditions:

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software and documentation, including modifications that you make for internal use or for distribution:

Copyright 1992-2004 by the Massachusetts Institute of Technology. All rights reserved.

THIS SOFTWARE IS PROVIDED "AS IS", AND M.I.T. MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, M.I.T. MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

The name of the Massachusetts Institute of Technology or M.I.T. may NOT be used in advertising or publicity pertaining to distribution of the software. Title to copyright in this software and any associated documentation shall at all times remain with M.I.T., and USER agrees to preserve same.

Project Athena, Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira, OLC, X Window System, and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.

Kerberos Copyright

This software is being provided to you, the LICENSEE, by the Massachusetts Institute of Technology (M.I.T.) under the following license. By obtaining, using and/or copying this software, you agree that you have read, understood, and will comply with these terms and conditions:

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software and documentation, including modifications that you make for internal use or for distribution:

Copyright 1992-2004 by the Massachusetts Institute of Technology. All rights reserved.

THIS SOFTWARE IS PROVIDED "AS IS", AND M.I.T. MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, M.I.T. MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

The name of the Massachusetts Institute of Technology or M.I.T. may NOT be used in advertising or publicity pertaining to distribution of the software. Title to copyright in this software and any associated documentation shall at all times remain with M.I.T., and USER agrees to preserve same.

Project Athena, Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira, OLC, X Window System, and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.

Kerberos Export Restrictions and Source Code Access

Reporting Bugs and Requesting Assistance

If you find bugs, please mail them to kfw-bugs@MIT.EDU.

kerberos@MIT.EDU is a mailing list set up for discussing Kerberos issues. It is gatewayed to the Usenet newsgroup 'comp.protocols.kerberos'. If you prefer to read it via mail, send a request to kerberos-request@MIT.EDU to get added or subscribe via the web page:

http://mailman.mit.edu/mailman/listinfo/kerberos

Obtaining Kerberos for Windows Source Code and SDK

To retrieve the source code distribution or software development kit for Kerberos for Windows follow the link to **Download: Souces and binaries from MIT via authorization form** from the web page http://web.mit.edu/kerberos/.