# Network Identity Manager User Documentation

MIT Kerberos for Windows Release 3.0.0

Copyright 2005 by the Massachusetts Institute of Technology

## What Is the Network Identity Manager and When To Use It?

Network Identity Manager (NetIdMgr) is a graphical system-tray tool designed to manage Kerberos identities on Microsoft Windows. NetIdMgr is used to obtain Kerberos tickets (aka credentials), change the Kerberos password, and obtain Andrew File System (AFS) tokens for one or more AFS cells[*].

NetIdMgr 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. NetIdMgr combines all of these functions into one user interface and supports automatic renewal or user notification when credentials are approaching expiration.

There are many ways to execute NetIdMgr. In addition to clicking on a Network Identity Manager shortcut, you can start NetIdMgr from the Windows command Prompt or Run... option. Command-line options may be specified. If you run NetIdMgr 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 NetIdMgr within your Windows Startup folder (Start Menu->Programs->Startup). A shortcut to "NetIdMgr.exe –-autoinit" ensures that Kerberos tickets are available for the use of Kerberized applications throughout your Windows logon session.

If NetIdMgr 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 NetIdMgr or kinit, must be used to obtain credentials.

NetIdMgr 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 NetIdMgr. NetIdMgr simply allows you to manage Kerberos identities on behalf of compatible applications and to change your Kerberos password.

---

[*] An optional OpenAFS plug-in is required.

## Network Identity Manager Screen Display

The window title contains the name "Network Identity Manager".  Below the title are a menu bar; a tool bar; and a tree view.
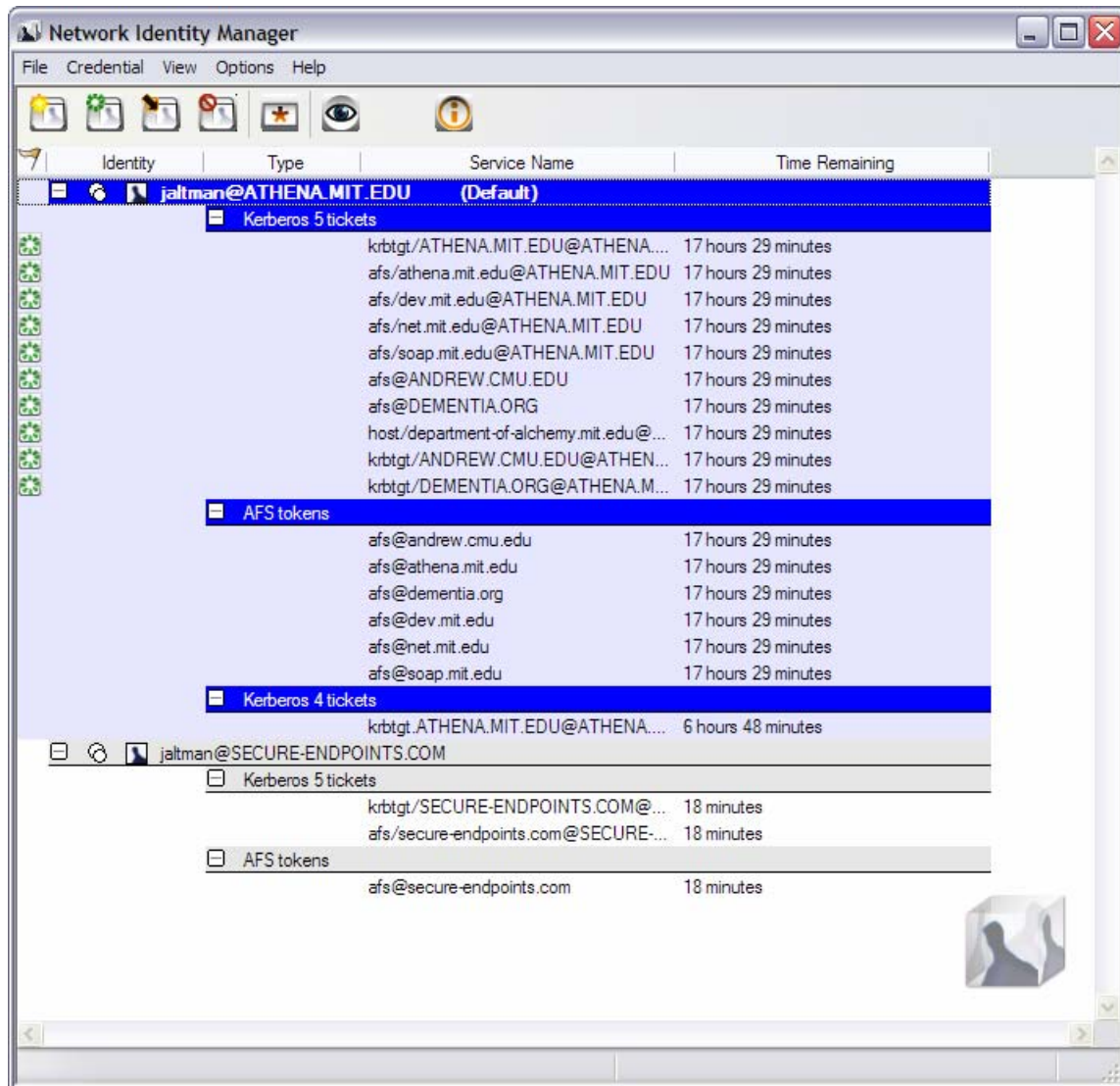


In its default configuration, the NetIdMgr tree view displays a list of user identity names (aka Kerberos principals, user@REALM).  Each entry appears with a ⊞ or ⊟ button, a ◌ or ⬠ button and an Identity icon ▮ to its left.  Click on the ⊞ button of an identity to expand the branch, displaying a ⊟ button.  Click on the ⊟ button to hide the branch.

Below each user identity, the tree contains credential categories.  Below each credential category are the current credentials (tickets or tokens) belonging to the group.  Each credential entry contains the current credential status, the service name and time remaining before expiration.

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.

To the right of each credential may be an icon representing one of the following states:

| | | |
|---|---|---|
| None | = | credentials are valid |
| | = | credentials are valid and renewable |
| | = | credentials are valid and the initial expiration warning has been issued |
| | = | credentials are valid and the final expiration warning has been issued |
| | = | credentials are invalid or expired |

At 15 minutes[*] before expiration renewable credentials will be renewed automatically.
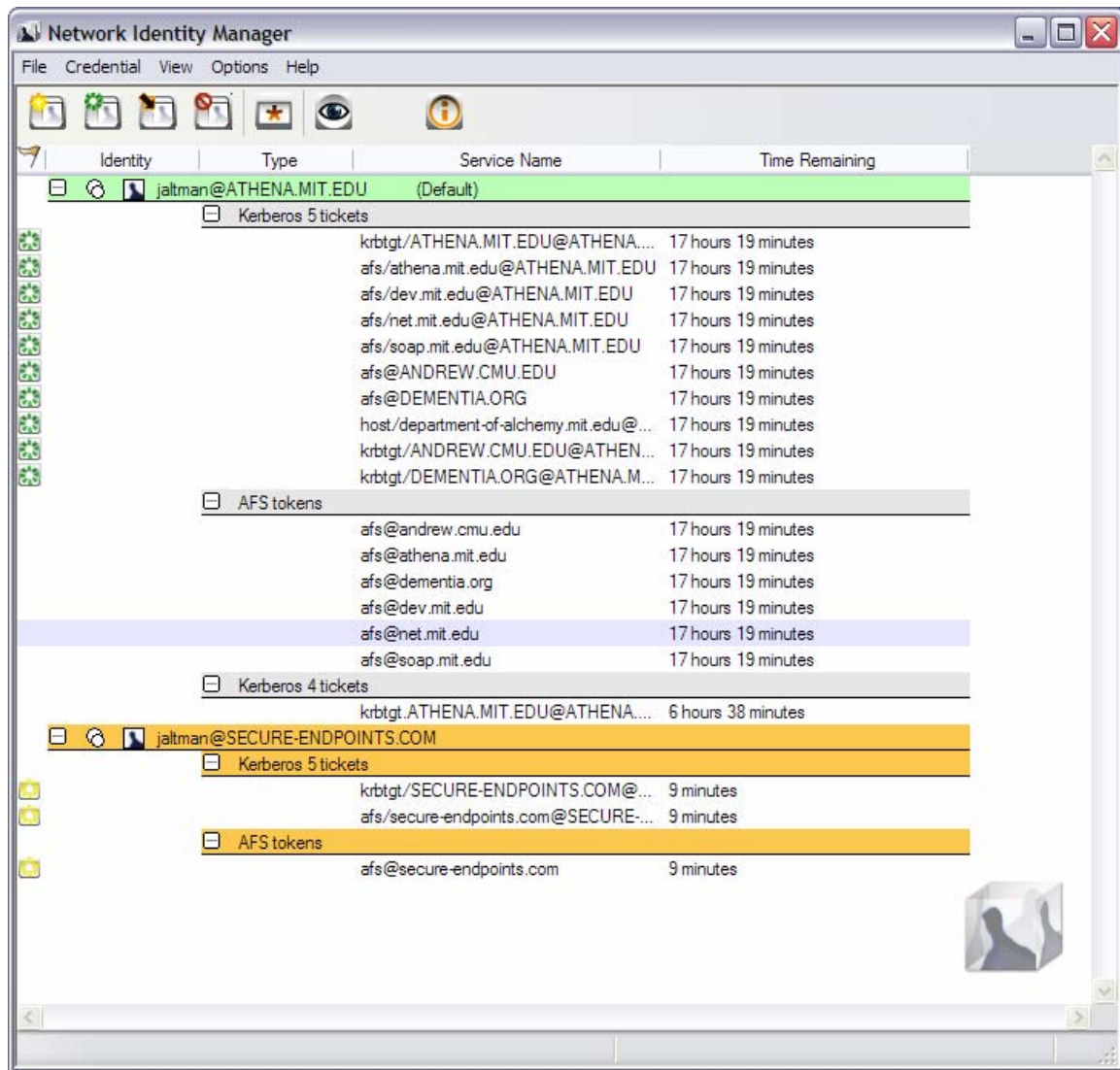


At 10 minutes and 5 minutes[+] before your credentials expire, a balloon tip is displayed to warn that your credentials will soon expire and to provide you the opportunity to obtain new ones.

---

[*] The actual time is configurable. 15 minutes is the default time. Automatic renewal may be disabled.
[+] The actual times are configurable. 10 minutes and 5 minutes are the default times, Expiration warnings may be disabled.
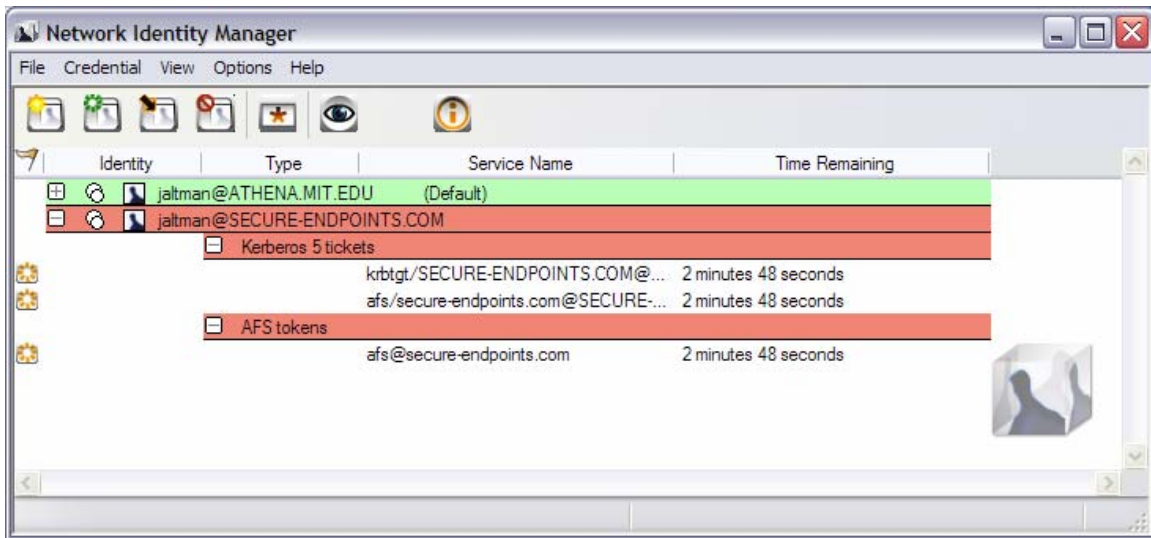
Credentials that are not renewed will expire.



Andrew File System (AFS) token information is available only on machines that have installed OpenAFS for Windows[#] and that have installed the required plug-in[%].

The Network Identity Manager manages multiple identities.   Most applications do not know how to request a specific identity or how to search for the appropriate credentials cache.  Instead these applications assume that the identity to be used is stored within the default credentials cache.  NetIdMgr allows one identity to be specified as the **default identity**.
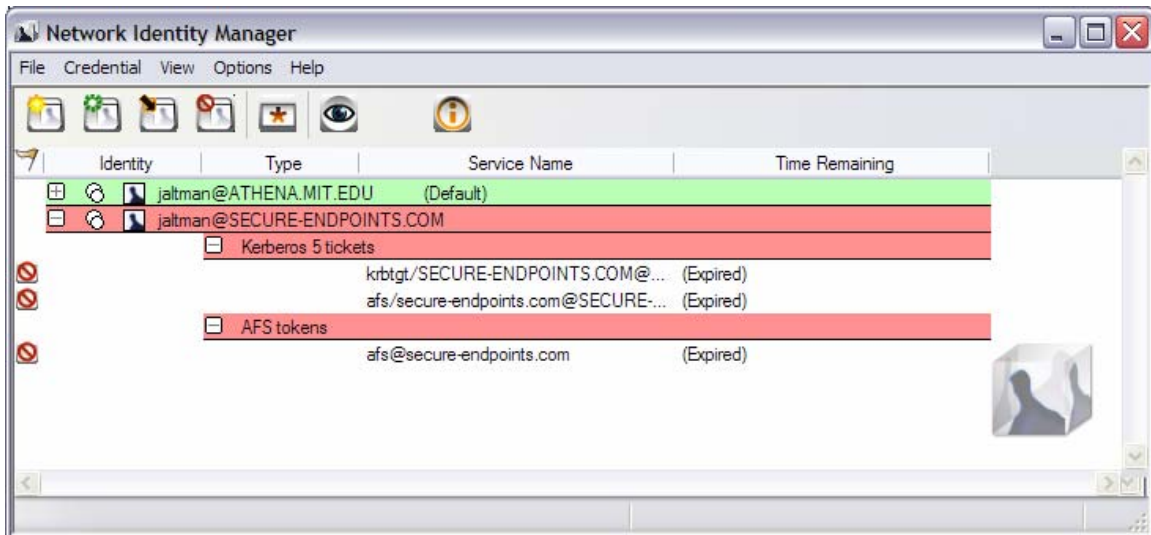
The push pin buttons are used to choose whether an identity should be displayed even when there are no credentials.  ⊘ indicates that the identity will be displayed without credentials.  ⌐ indicates that the identity will not be displayed without credentials.  The buttons act as a toggle between the two states.

---

[#] http://www.openafs.org
[%] Until such time as the OpenAFS Credential Manager plug-in is integrated into OpenAFS for Windows, it can be obtained from Secure Endpoints Inc. at no charge.  http://www.secure-endpoints.com

## Network Identity Manager Command Line Options

When NetIdMgr 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

## Network Identity Manager Commands

### File:

| | |
|---|---|
| Properties ... | |
| Exit | CTRL+X |

Exit

Properties…
From the File menu, will display the Properties dialog for the currently selected item whether it be an Identity or a Credential.



An Identity Property dialog
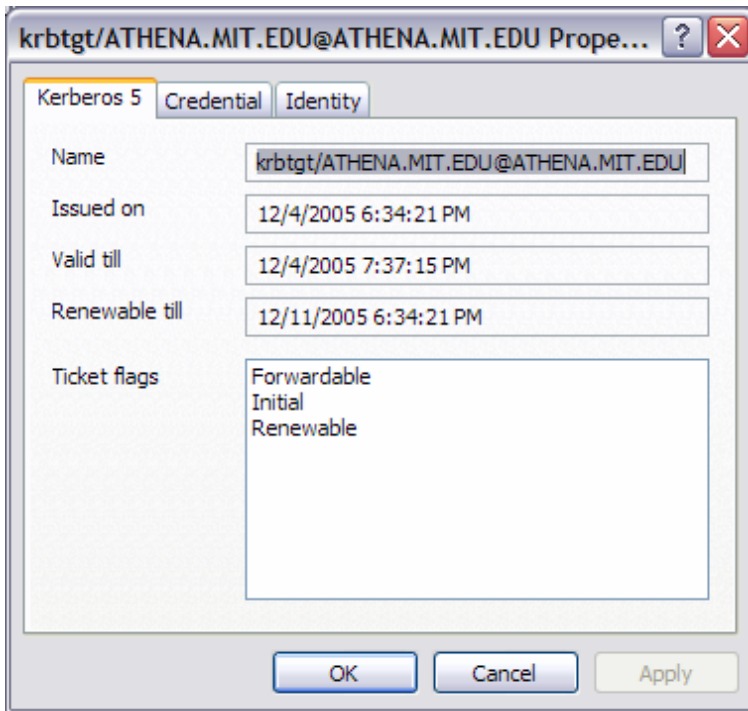
A Kerberos 5 Ticket Property dialog
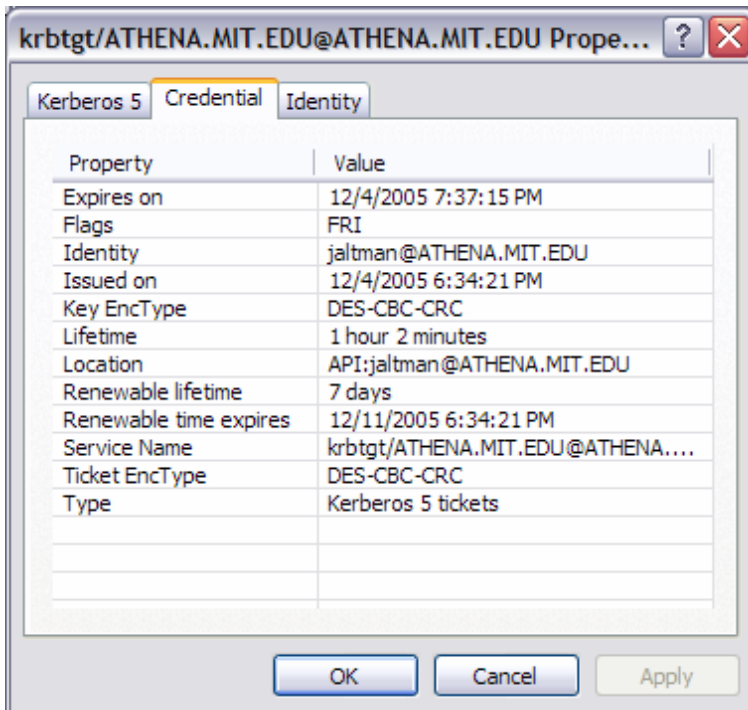

Associated credential properties

The properties dialog can also be displayed by pressing the ⬛ button on the Identity header or by double clicking a credential.

Exit Command
From the File menu, you can use this command to exit the Network Identity Manager.

Important Note...
Exiting the Network Identity Manager will **not** destroy your current credentials. Unless you have chosen to delete credentials on exit from the General Configuration page, you need to use the destroy credentials command.

## Credential:
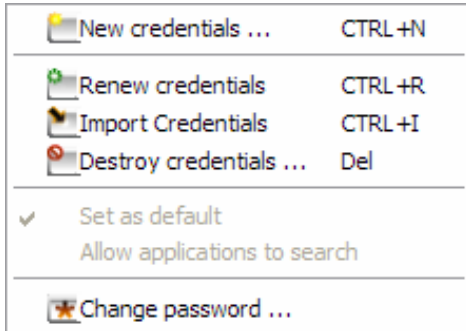


New Credentials Command, Ctrl+N

This command is found under the Credentials menu; it is also the first button (from the left) in the toolbar. Use this command to obtain new credentials.
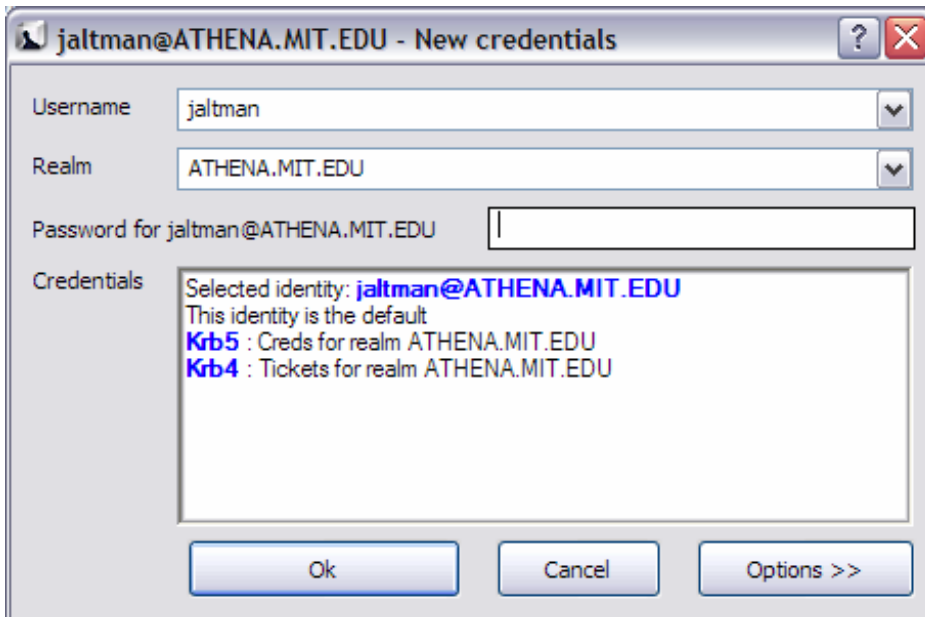


When you select this command, NetIdMgr displays a dialog requesting your Username, Kerberos Realm, and Password; if these are correct, NetIdMgr will obtain tickets for you.   You may optionally specify options for each of the credential types.
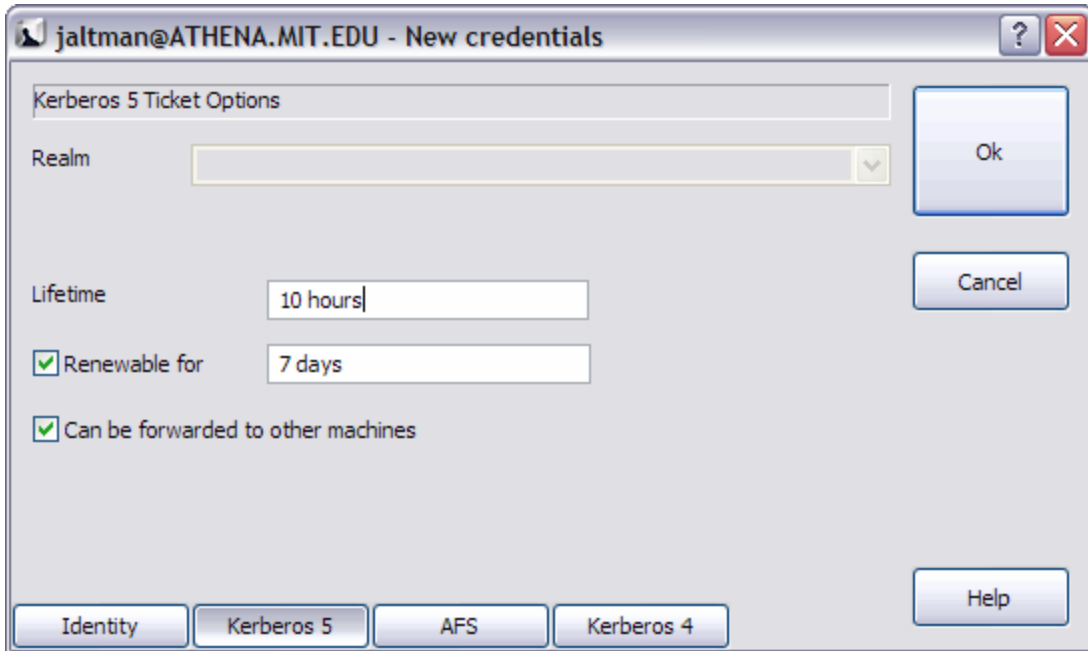
Kerberos 5 options include the ability to select the ticket lifetime as well as renew and forwarding. The Kerberos 5 ticket granting ticket represents the selected identity. As such, obtaining Kerberos 5 tickets is mandatory.

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 **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**, NetIdMgr 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.
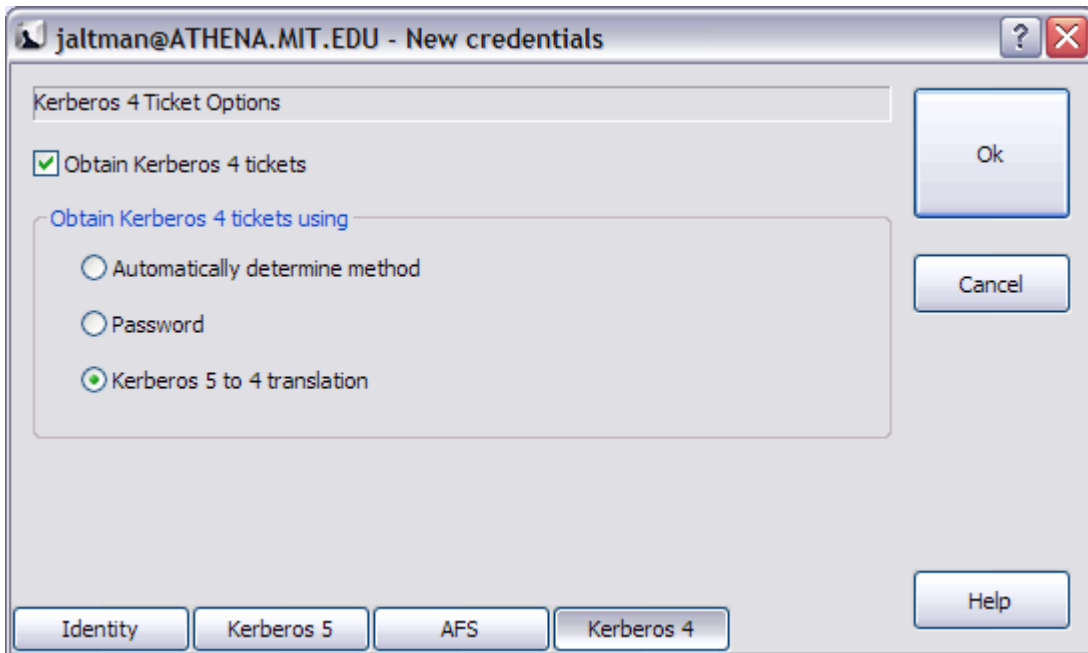
If available, obtaining Kerberos 4 tickets is optional.  They may only be obtained for a single identity.
Kerberos 4 tickets may be obtained via use of a Kerberos 5 to 4 translation service or by a separate
password based request.  Selecting "Automatically determine method" will first try the translation service
and if that fails, the password based request will be attempted.
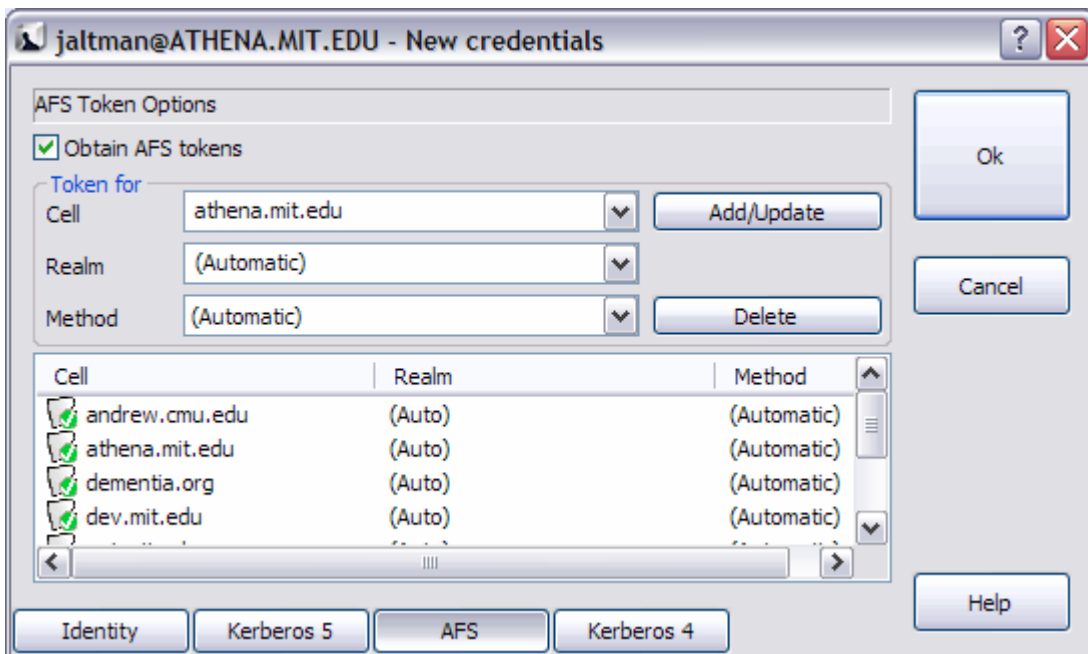


If available, obtaining AFS tokens is optional.  A single identity may be used to obtain tokens for multiple
AFS cells.  The Add/Update and Delete buttons are used to manage the list of AFS cells.   If the Kerberos
realm associated with the AFS cell cannot be automatically determined, it may be entered manually.  The
method of AFS token acquisition is one of: "Automatic", "Kerberos 5", "Krb524" or "Kerberos 4".
Kerberos 5 based tokens should be used when possible.   If not, the next best choice is the 524 translation

service.  As a last resort, a Kerberos 4 ticket request can be used directly.  In most cases, using "Automatic" will just work.
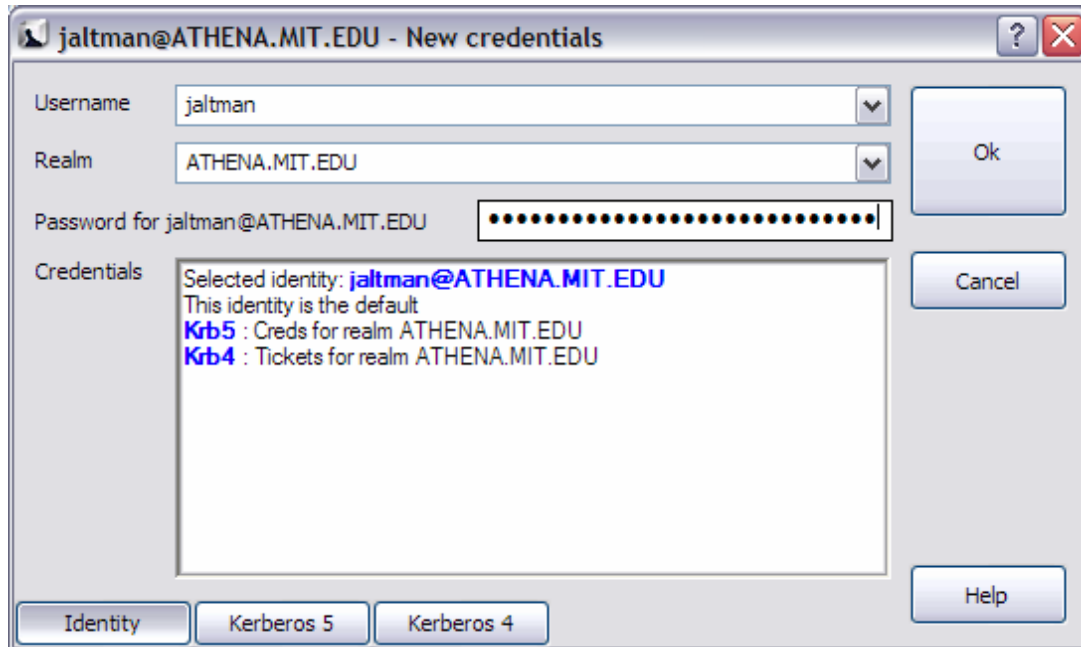


After entering the correct password for the selected identity, press the Ok button to obtain the specified credentials.

### Renew Credentials Command, Ctrl+R
This command is found on the Credential menu; it is also the second button  (from the left) in the toolbar.  Use this command to renew the selected credentials, Kerberos tickets (and perhaps AFS tokens), on your local machine without requiring the use of a password.

### Import Credentials Command, Ctrl+I
This command is found on the Credential menu; it is also the third button  (from the left) in the toolbar.  Use this command to import the Windows Logon Session Identity.  Importing tickets will not result in the destruction of existing tickets.

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

### Destroy Credentials Command, Del
This command is found on the Credential menu; it is also the fourth button  (from the left) in the toolbar.  Use this command to destroy the selected credentials, Kerberos tickets (and perhaps AFS tokens), on your local machine.

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

### Change Password Command

This command is found on the Credential 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.

How To Use Change Password...
1.    Type your username in the first field of the dialogue box.
2.    Type your *current* password in the Current 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, Network Identity Manager 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.

## View:
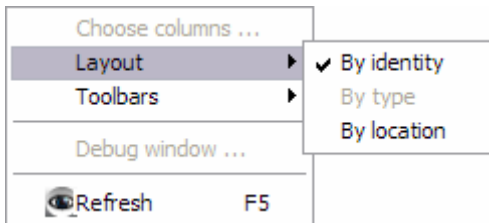


Choose Columns
This feature is not available in the current release.

Layout By Location
The By Location Layout provides an alternate view of your credentials based not upon the Identity name but instead on their storage location.
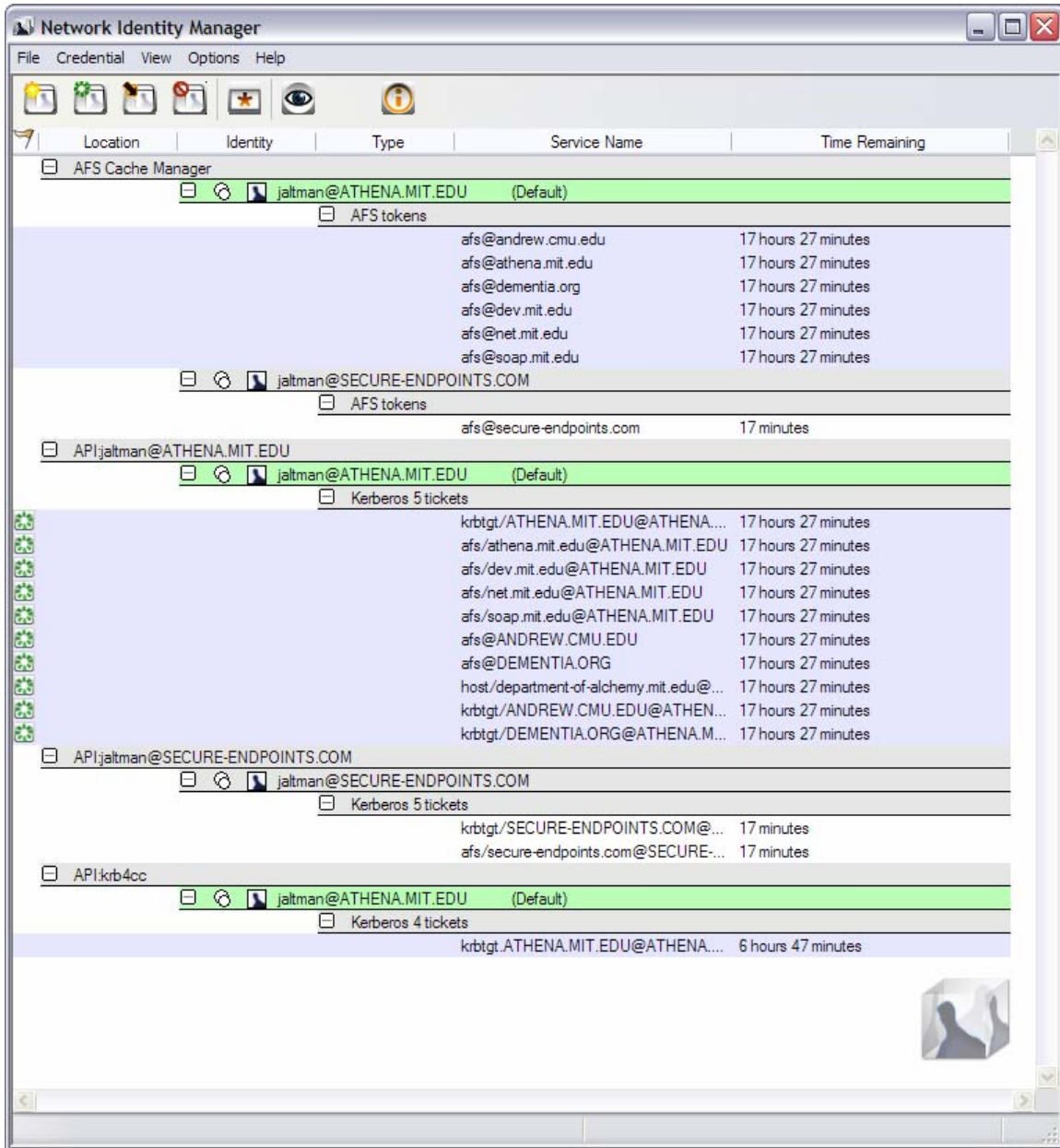
## Toolbars
There is only one toolbar available in the current release.

## Debug Window
The debug window functionality is not available in the current release.

## Refresh Command, F5

Use this command (in the View menu and the toolbar ) to update the display of your current Credentials.

## Why Use It...
Although most end users will likely find this feature irrelevant, application developers and support staff may occasionally find it to be useful. For example, you may want an immediate status check of available

credentials if you have just used command-line <u>kinit</u> or <u>kdestroy</u> and want to check that they have functioned successfully.

<u>How It Works...</u>
While NetIdMgr automatically checks the status of your credentials every minute, the Update Display command forces an immediate status check.

## Options:

General ...
Identities ...
Notifications ...
Plugins ...
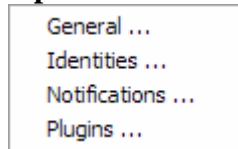
<u>General Options</u>
The General options dialog, accessed via the Options menu, allows you to configure operational properties specific to the NetIdMgr application.
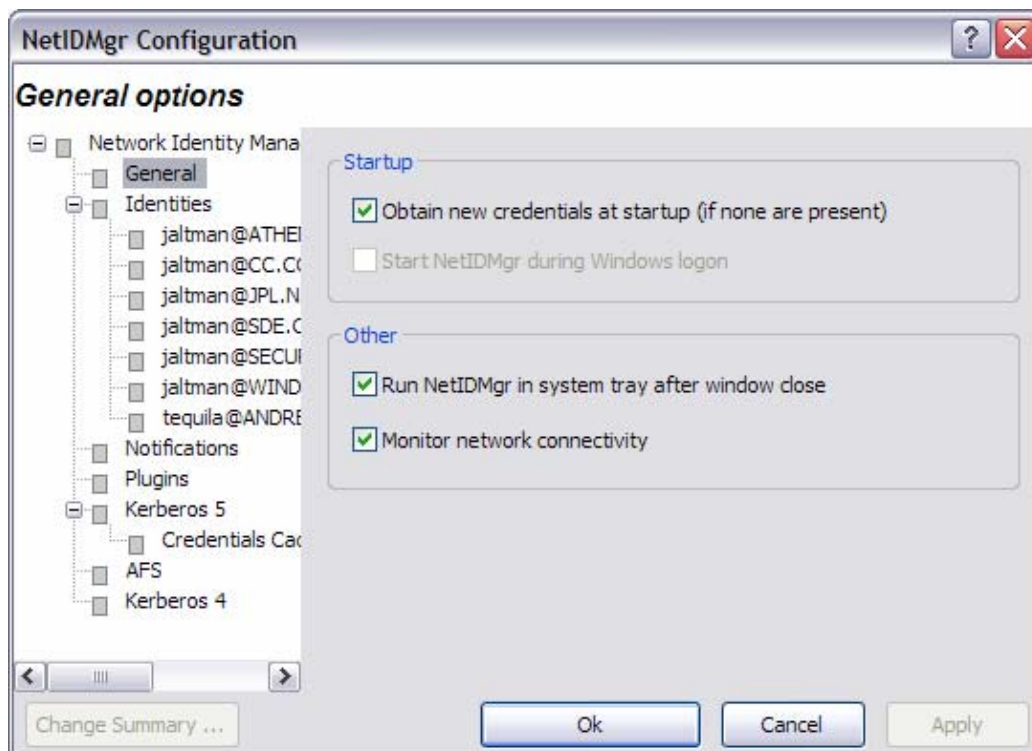


The **Obtain new credentials at startup (if none are present)** checkbox will determine whether or not NetIdMgr will display the New Credentials dialog at startup when no valid credentials exist.

The **Start NetIDMgr during Windows logon** feature is not available in this release.  It will determine whether or not NetIdMgr is automatically run by Windows immediately after logging in.

The **Run NetIdMgr in system tray after window close** checkbox determines the behavior of the window close button.  When checked, NetIdMgr will close the window but will continue running and can be accessed from the system tray.  When unchecked, NetIdMgr will behave as if File->Exit was selected from the menu.

<u>Identities Options</u>

Identity Options fall into two broad categories:  global settings used as default values for Identities and Identity specific values that override the defaults.

<u>Global Identity Settings</u>
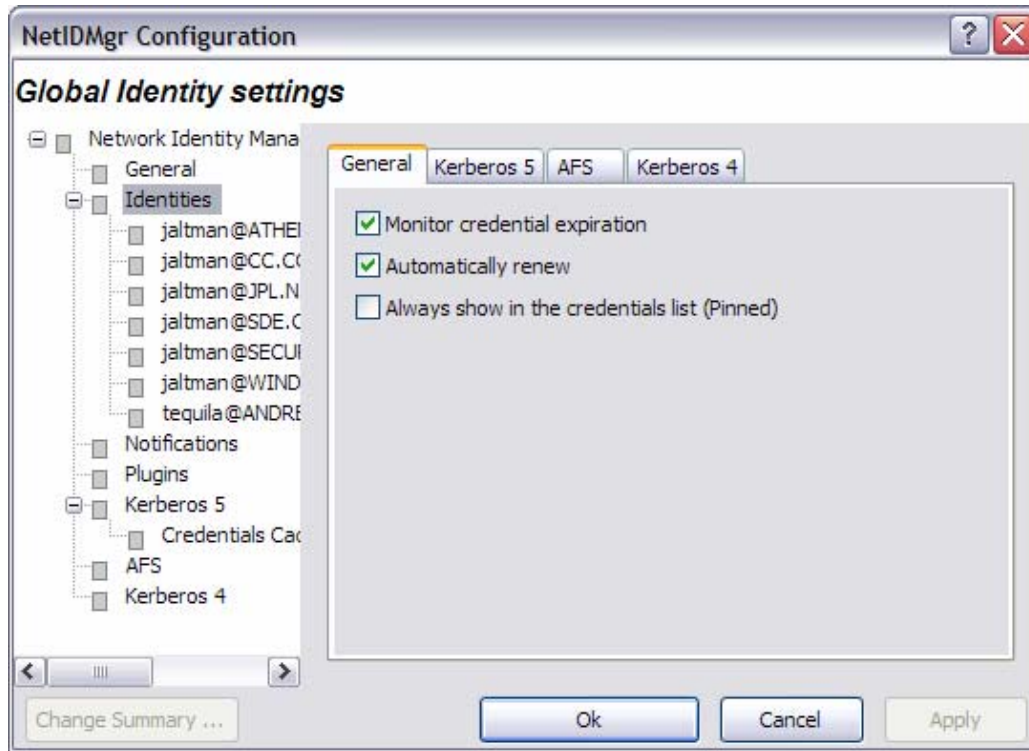


There are three general settings that can be used to set global defaults.

The **Monitor credential expiration** setting determines whether or not NetIdMgr should monitor the credential lifetimes and issue expiration notifications.   This value is used as the default for all new identities.

The **Automatically renew** setting determines if *renewable* credentials are automatically renewed prior to expiration.  This value is used as the default for all new identities.

The **Always show in the credentials list (Pinned)** setting determines whether new identities are always pinned within the credentials list.  A pinned identity will always be displayed regardless of whether or not there are credentials associated with it.
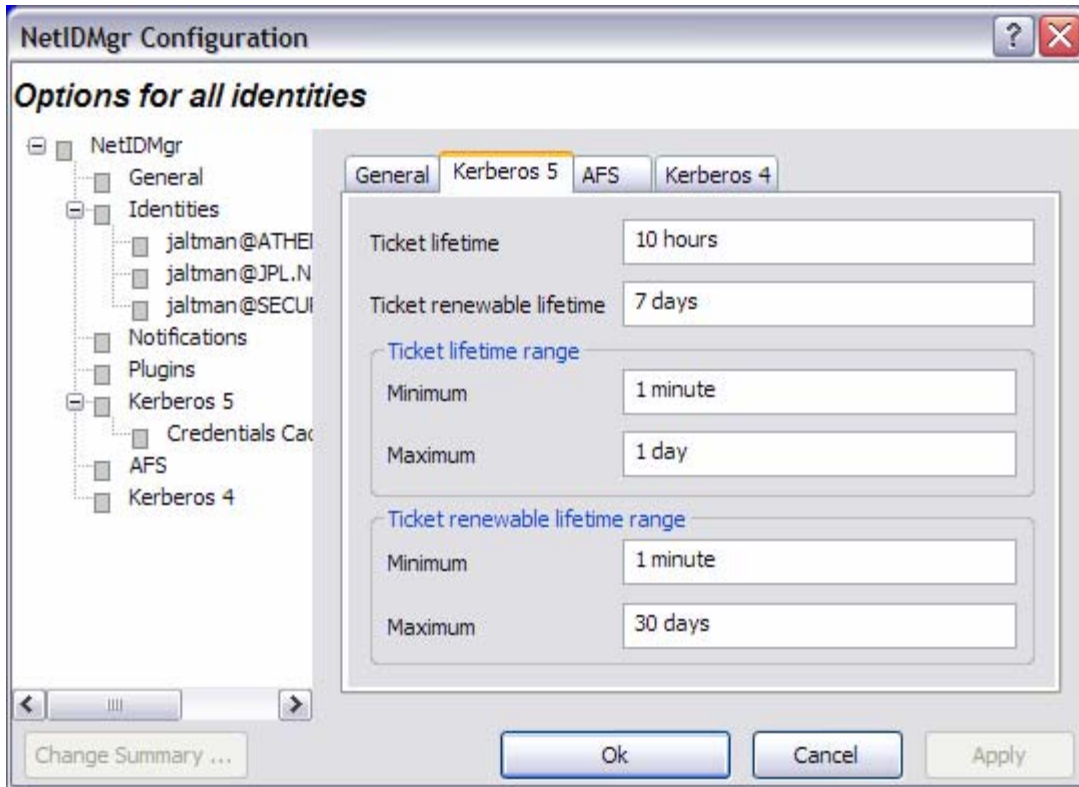
The global Kerberos 5 settings define default credential lifetimes and minimum and maximum values for use in constructing the slider controls used to set the lifetimes.

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 NetIdMgr 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.
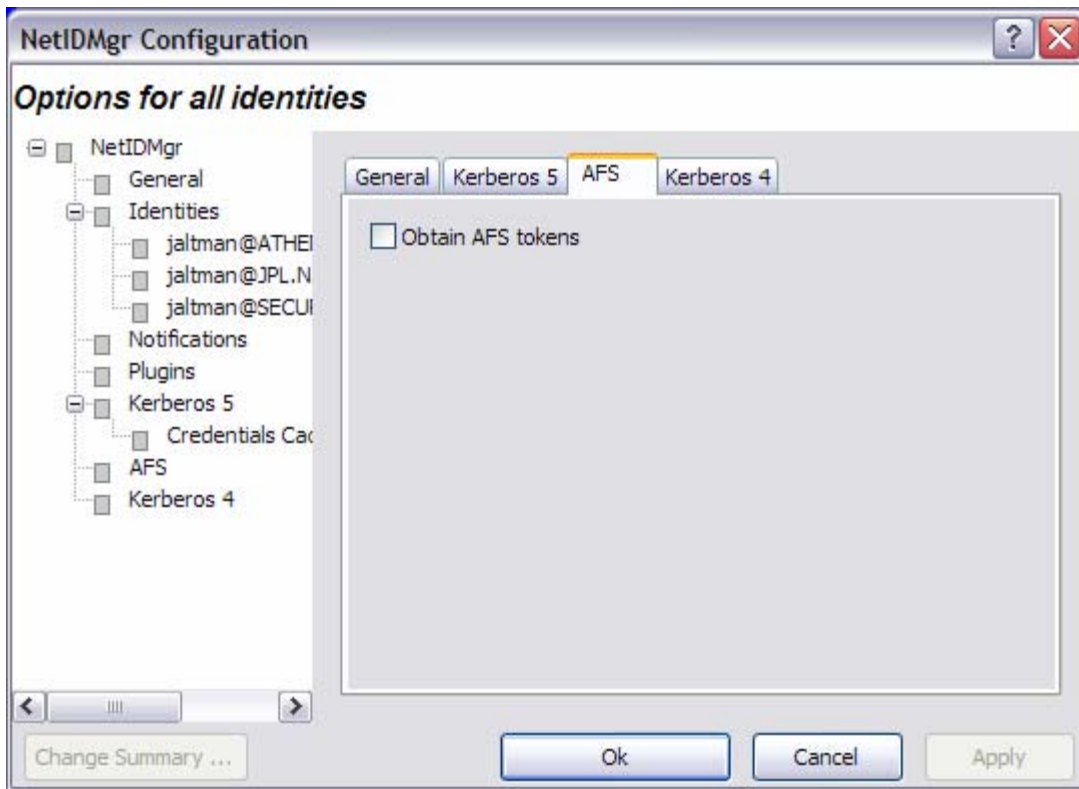
When the **Obtain AFS tokens** button is checked, NetIdMgr will attempt to retrieve AFS tokens when ticket initialization, renewal, or importation is performed.   If you do not frequently access AFS cells, it is suggested that this button be unchecked.
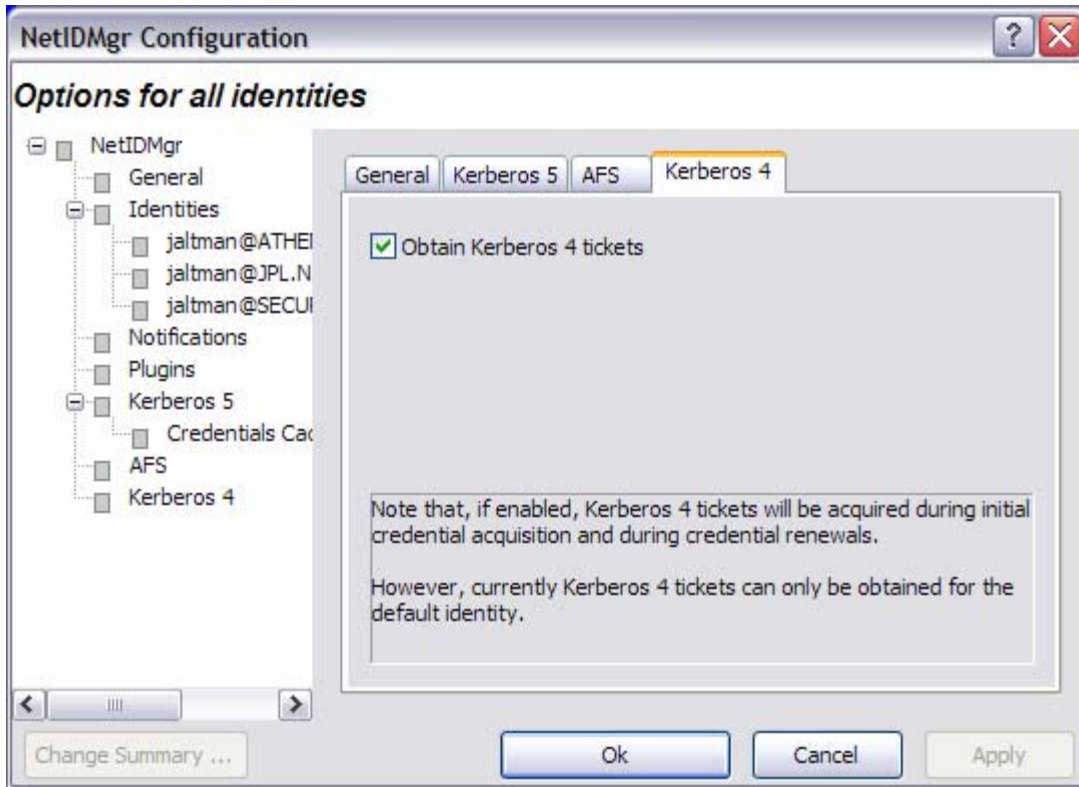
When the **Obtain Kerberos 4 credentials** button is checked, NetIdMgr will attempt to retrieve Kerberos 4 credentials when ticket initialization, renewal, or importation is performed.  Kerberos realms are increasingly configured to support only Kerberos 5 (e.g., Windows Active Directory Domains.)  If the realms you use do not support Kerberos 4 it is suggested that this button be unchecked.

Be aware that only the default identity can obtain Kerberos 4 credentials.   This limitation is due to the inability of Kerberos 4 applications on Microsoft Windows to specify a credentials cache.

Identity Specific Options

Each Identity knows to the Network Identity Manager is provided its own set of tabbed pages that can be used to override the default values specified on the Global Identity Settings pages.   There are two distinctions.
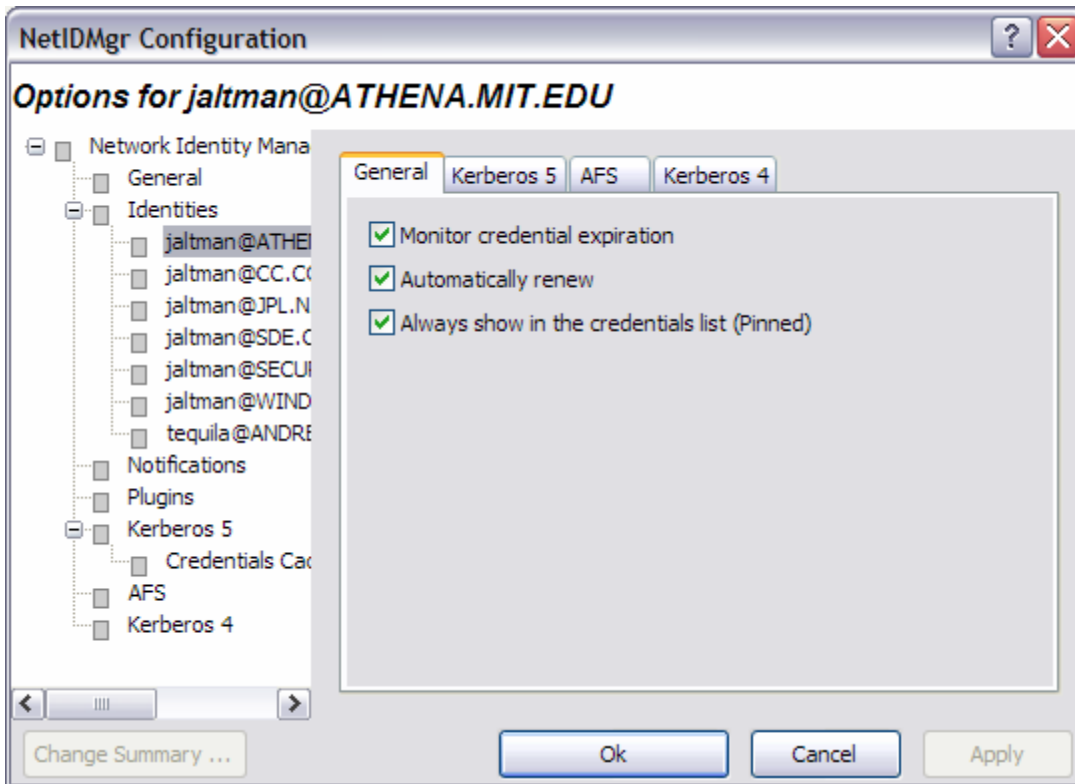
The General page contains a **Remove Identity** button that can be used to delete this Identity from the Network Identity Manager.
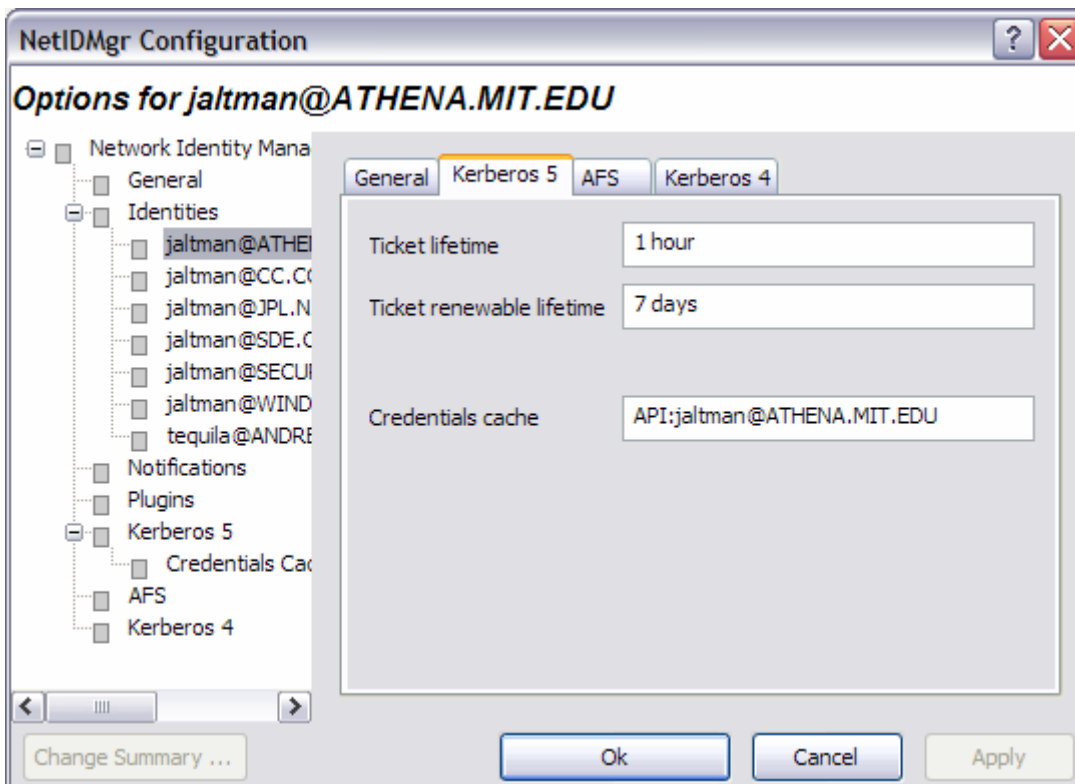
The Kerberos 5 page displays the name of the credential cache currently associated with the Identity.

Notifications Options
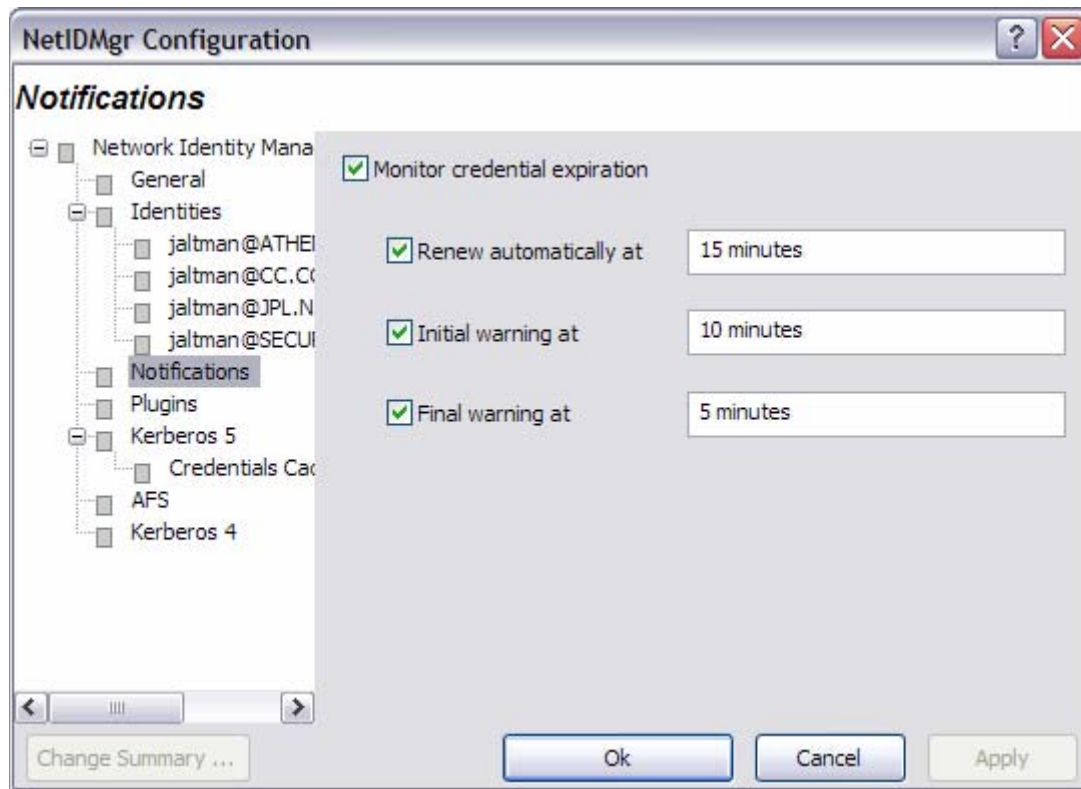


The **Renew automatically at** check box determines whether or not renewable tickets will be renewed by NetIdMgr when they reach the specified time remaining.

The **Initial warning at** check box determines whether or not a warning will be issued when the specified time remaining is reached.

The **Final warning at** check box determines whether or not a warning will be issued when the specified time remaining is reached.

Notifications are performed in two ways. First, icons are displayed next to the affected credentials in the flags column of the display. Second, a balloon tip is displayed off of the NetIdMgr system tray icon.

Plugins and Modules
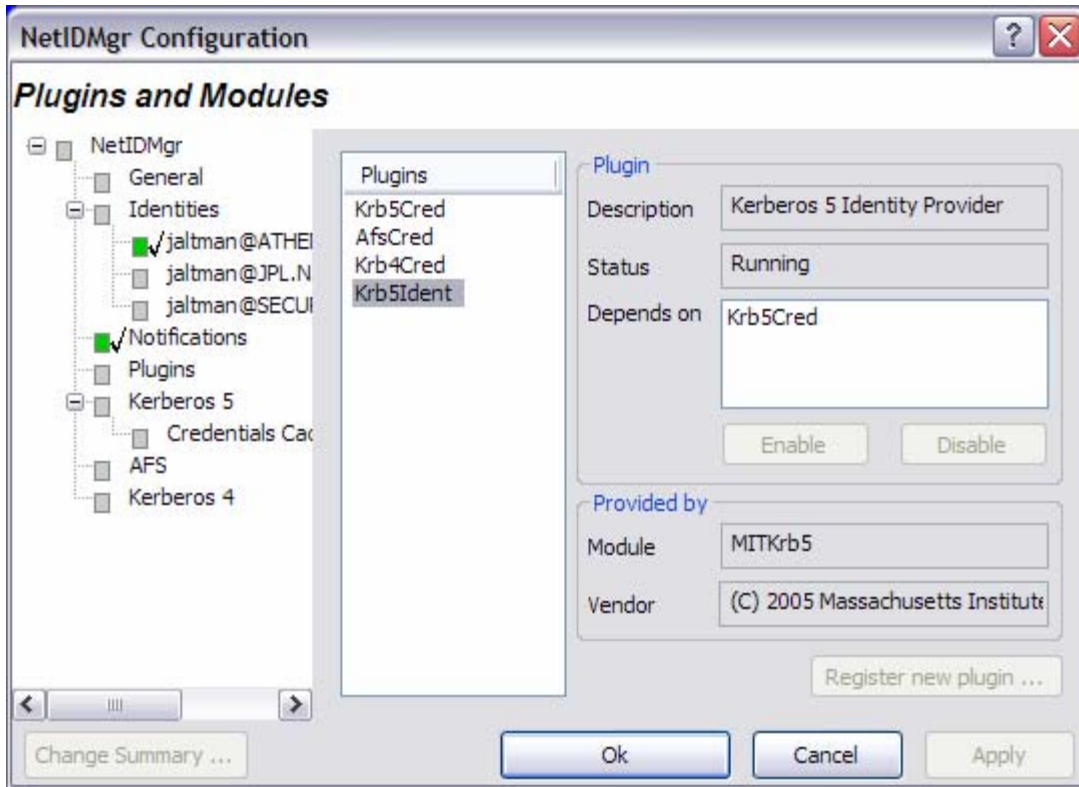
The Plug-ins and Modules page provides status information on the currently loaded plugins and modules include a description of their purpose; whether or not it was loaded properly; which other modules are required; and what organization developed it.

In a future release, the use of plug-ins determined at run time by manually enabling or disabling them.

Kerberos 5 Configuration
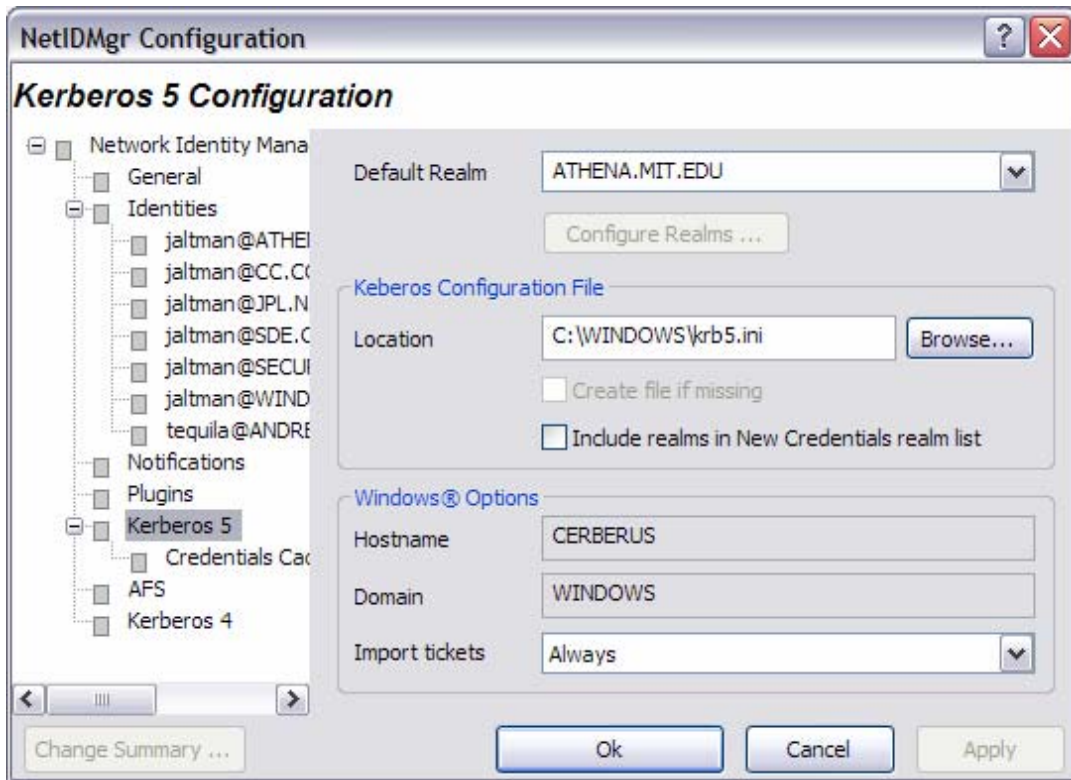
In the **Default Realm** field, select a Kerberos realm from the dropdown list.

The **Kerberos 5 Configuration** tab allows you to specify the location of the Kerberos 5 configuration file. The **Configuration File** field specifies the path to the Kerberos 5 configuration file, krb5.ini.

The Kerberos libraries depend on configuration files for their proper operation. When **Create file if missing** is checked, NetIdMgr 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**. [This functionality is not available in this release.]

The Kerberos 5 configuration file frequently contains lists of realms and associated Kerberos server location information. If you wish this list to be used to populate the realm list in the **Obtain New Credentials** dialog, check the **Include realms in New Credentials realm list** box.

The field labeled **Host Name** displays the name of your local machine. The **Domain Name** field displays the domain to which your local machine currently belongs.

The **Import Tickets** listbox allows you to configure how NetIdMgr interacts with the Microsoft Kerberos Authentication Provider. NetIdMgr 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 **Only when the Principal matches** means import tickets from the MSLSA only if the MSLSA Kerberos principal belongs to the Default Realm.
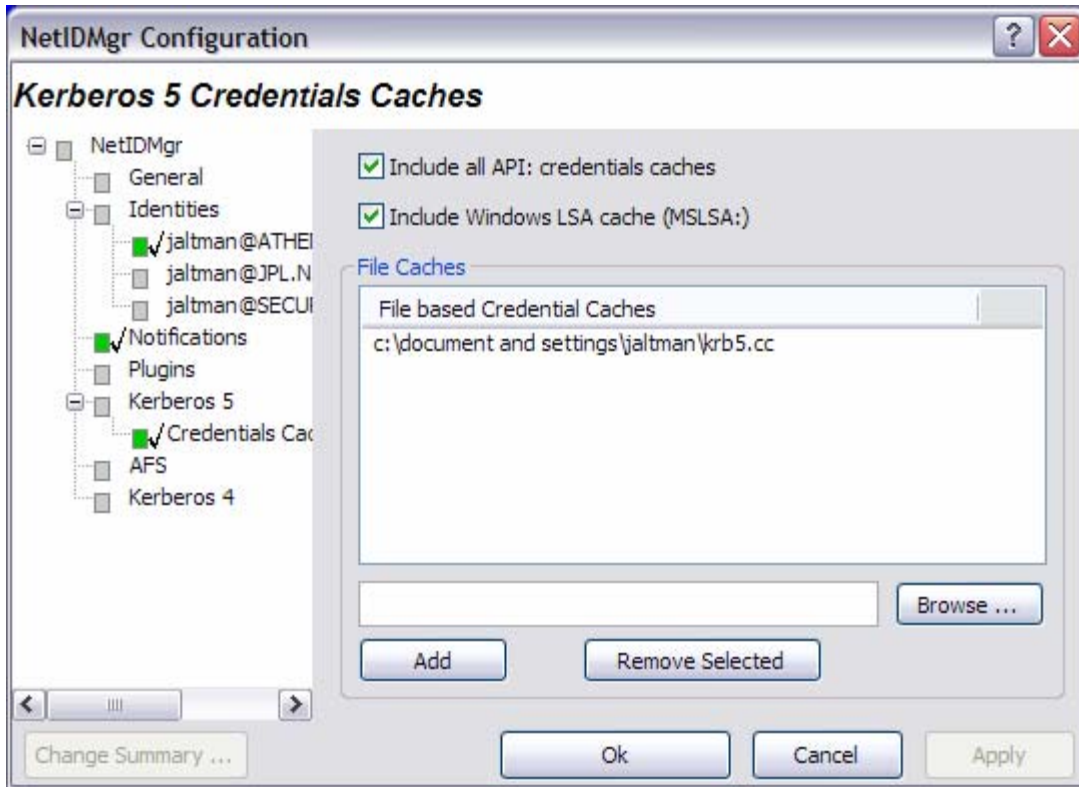
The **Kerberos 5 Credentials Caches** page determines the contents of which credential caches types are displayed within the Network Identity Manager. The **Include all API: credential caches** check box determines whether or not CCAPI caches are included. CCAPI caches are the most frequently used with MIT Kerberos for Windows. The **Include Windows LSA cache (MSLSA:)** check box determines whether or not the Windows Logon Session Identity is displayed within NetIdMgr.

The Network Identity Manager can also display the contents of FILE: credential caches. Each FILE: credential cache must be manually added to the list.

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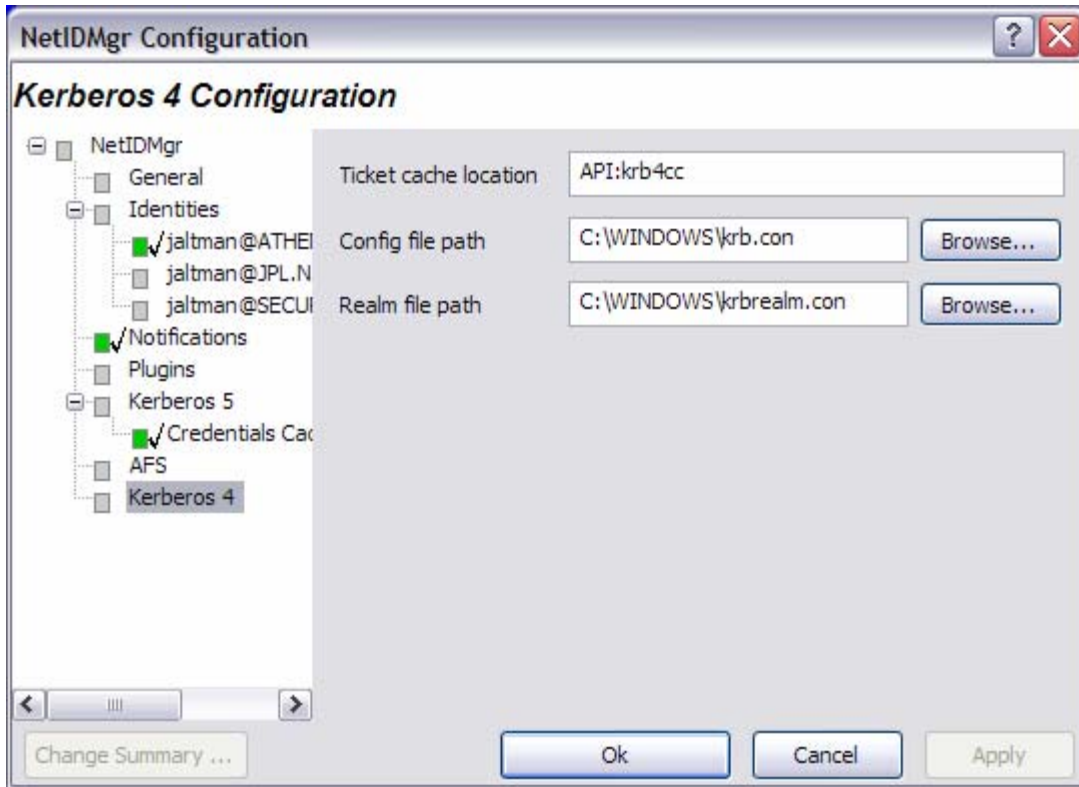
Here, you can specify the name of the in-memory cache used to store the Kerberos 4 tickets. The format of the name is "API:" followed by the cache name. Disk caches are not supported by Kerberos for Windows.

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.

## Help:
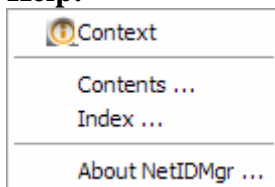


About Network Identity Manager

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 NetIdMgr may require.

**About Network Identity Manager**

NetIDMgr 1.0.0.0

OK

(C) 2005 Massachusetts Institute of Technology

Official build.  Please send bug reports to kfw-bugs@MIT.EDU

Loaded modules

| Name | Path |
|------|------|
| WSHELP32.dll | C:\Program Files\MIT\Kerberos\bin\WSHELP32 |
| rasadhlp.dll | C:\WINDOWS\system32\rasadhlp.dll |
| wshtcpip.dll | C:\WINDOWS\System32\wshtcpip.dll |
| hnetcfg.dll | C:\WINDOWS\system32\hnetcfg.dll |
| dnssd.dll | c:\program files\bonjour\dnssd.dll |
| mdnsNSP.dll | C:\Program Files\Bonjour\mdnsNSP.dll |
| SETUPAPI.dll | C:\WINDOWS\system32\SETUPAPI.dll |
| wshbth.dll | C:\WINDOWS\system32\wshbth.dll |
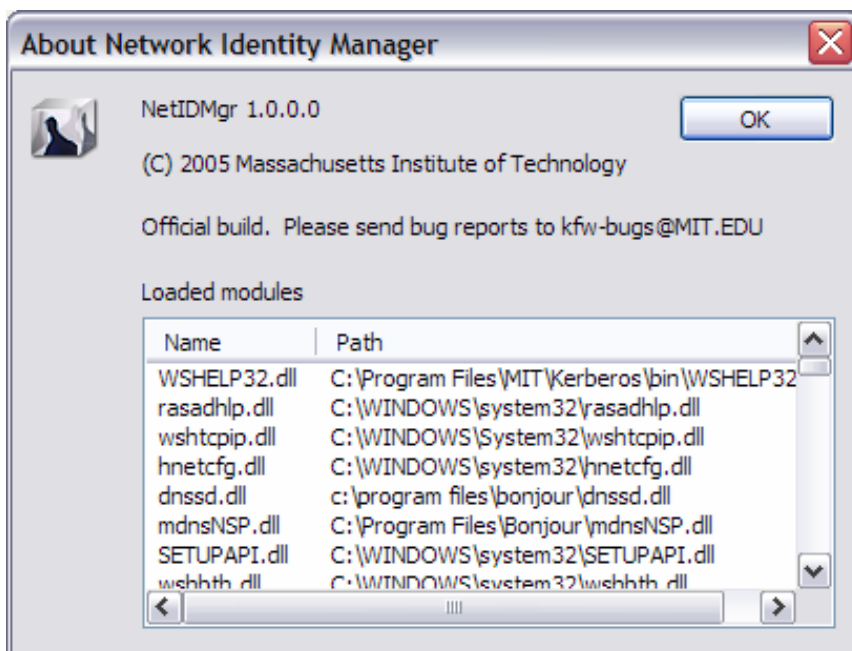
The About dialog provides access to the Network Identity Manager version number; the applicable copyright statement; the e-mail address to which bug reports should be sent; and a list of all of the modules loaded by the application.

## System Tray

While NetIdMgr is running the ![icon] icon will be displayed in the system tray.  Clicking on the icon with the first mouse button will open or close the Network Identity Manager display window.  Clicking with the second mouse button will display a menu of commands.

     ![icon]   = all credentials are valid

     ![icon]   = some credentials are about to expire

     ![icon]   = some credentials are expired

### System Tray menu
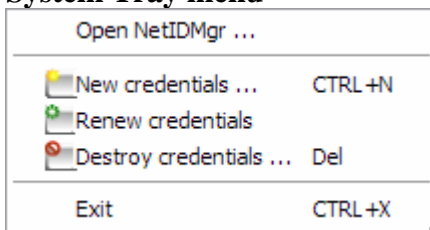


Open NetIdMgr …
The Open NetIdMgr … command will restore the Network Identity Manager Ticket Display window.  If the window is already open this option will appear as "Close NetIdMgr …".

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

Exit
You can use this command to exit the Network Identity Manager.

Important Note...
Exiting NetIdMgr will **not** destroy your current Kerberos tickets.

## Toolbar

The Network Identity Manager 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

## Copyrights

### Network Identity Manager 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 1992-2005 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 1992-2005 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

Copyright (C) 1989-2005 by the Massachusetts Institute of Technology

**Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.**

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Export of the documentation is not restricted.

## 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 <u>authorization form</u>** from the web page http://web.mit.edu/kerberos/.

## Important notice regarding Kerberos 4 support

In the past few years, several developments have shown the inadequacy of the security of version 4 of the Kerberos protocol. These developments have led the MIT Kerberos Team to begin the process of ending support for version 4 of the Kerberos protocol. The plan involves the eventual removal of Kerberos 4 support from the MIT implementation of Kerberos.

The Data Encryption Standard (DES) has reached the end of its useful life. DES is the only encryption algorithm supported by Kerberos 4, and the increasingly obvious inadequacy of DES motivates the retirement of the Kerberos 4 protocol. The National Institute of Standards and Technology (NIST), which had previously certified DES as a US government encryption standard, has officially announced[1] the withdrawal of the Federal Information Processing Standards (FIPS) for DES.

NIST's action reflects the long-held opinion of the cryptographic community that DES has too small a key space to be secure. Breaking DES encryption by an exhaustive search of its key space is within the means of some individuals, many companies, and all major governments. Consequently, DES cannot be considered secure for any long-term keys, particularly the ticket-granting key that is central to Kerberos.

Serious protocol flaws[2] have been found in Kerberos 4. These flaws permit attacks which require far less effort than an exhaustive search of the DES key space. These flaws make Kerberos 4 cross-realm authentication an unacceptable security risk and raise serious questions about the security of the entire Kerberos 4 protocol.

The known insecurity of DES, combined with the recently discovered protocol flaws, make it extremely inadvisable to rely on the security of version 4 of the Kerberos protocol. These factors motivate the MIT Kerberos Team to remove support for Kerberos version 4 from the MIT implementation of Kerberos.

The process of ending Kerberos 4 support began with release 1.3 of MIT Kerberos 5. In release 1.3, the default run-time configuration of the KDC disables support for version 4 of the Kerberos protocol. Release 1.4 of MIT Kerberos continues to include Kerberos 4 support (also disabled in the KDC with the default run-time configuration), but we intend to completely remove Kerberos 4 support from some future release of MIT Kerberos, possibly as early as the 1.5 release of MIT Kerberos.

The MIT Kerberos Team has ended active development of Kerberos 4, except for the eventual removal of all Kerberos 4 functionality. We will continue to provide critical security fixes for Kerberos 4, but routine bug fixes and feature enhancements are at an end. We recommend that any sites which have not already done so begin a migration to Kerberos 5. Kerberos 5 provides significant advantages over Kerberos 4, including support for strong encryption, extensibility, improved cross-vendor interoperability, and ongoing development and enhancement.

If you have questions or issues regarding migration to Kerberos 5, we recommend discussing them on the kerberos@mit.edu mailing list.

## References

[1] National Institute of Standards and Technology. Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 43-3, Data Encryption Standard (DES); FIPS 74,Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation. Federal Register 05-9945, 70 FR 28907-28908, 19 May 2005. DOCID:fr19my05-45

[2] Tom Yu, Sam Hartman, and Ken Raeburn. The Perils ofUnauthenticated Encryption: Kerberos Version 4. In Proceedings of the Network and Distributed Systems Security Symposium. The Internet Society, February 2004.   http://web.mit.edu/tlyu/papers/krb4peril-ndss04.pdf