

Network Identity Manager User Documentation

MIT Kerberos for Windows Release 3.2

Copyright 2004-2007 by the Massachusetts Institute of Technology

Copyright 2006-2007 by Secure Endpoints Inc.

WHAT IS NETWORK IDENTITY MANAGER?	3
HOW TO START NETWORK IDENTITY MANAGER	4
OBTAINING CREDENTIALS	4
NETWORK IDENTITY MANAGER APPLICATION WINDOW	5
NETWORK IDENTITY MANAGER COMMAND LINE OPTIONS.....	10
NETWORK IDENTITY MANAGER COMMAND REFERENCE.....	10
FILE:.....	10
<i>Properties</i>	10
<i>Exit Command</i>	12
CREDENTIAL:	12
<i>New Credentials Command, Ctrl+N</i>	12
<i>Renew Credentials Command, Ctrl+R</i>	15
<i>Import Credentials Command, Ctrl+I</i>	16
<i>Destroy Credentials Command, Del</i>	16
<i>Change Password Command</i>	16
VIEW:	18
<i>Advanced Command, F7</i>	18
<i>View Columns</i>	18
<i>Layout</i>	19
<i>Layout By Identity</i>	19
<i>Layout By Type</i>	20
<i>Layout By Location</i>	21
<i>Custom</i>	21
<i>Refresh Command, F5</i>	21
OPTIONS:	22
<i>General Options</i>	22
<i>Appearance Options</i>	23
<i>Identities Options</i>	23
<i>Notifications Options</i>	31
<i>Plug-ins and Modules</i>	32
<i>Kerberos v5 Configuration</i>	33
<i>Kerberos v4 Configuration</i>	35
<i>AFS Configuration</i>	35
HELP:	36
<i>About Network Identity Manager</i>	36
WINDOWS TASKBAR NOTIFICATION AREA	36
TASKBAR NOTIFICATION AREA MENU	37
<i>Show Network Identity Manager window</i>	37
<i>New Credentials</i>	37
<i>Renew</i>	37

<i>Destroy</i>	37
<i>Destroy Ticket(s)/Token(s)</i>	<i>Error! Bookmark not defined.</i>
<i>Change Password</i>	37
<i>Exit</i>	37
TOOLBAR	37
COPYRIGHTS	38
NETWORK IDENTITY MANAGER COPYRIGHT	38
KERBEROS COPYRIGHT	38
KERBEROS EXPORT RESTRICTIONS AND SOURCE CODE ACCESS.....	39
REPORTING BUGS AND REQUESTING ASSISTANCE	39
OBTAINING KERBEROS FOR WINDOWS SOURCE CODE AND SDK	39
IMPORTANT NOTICE REGARDING KERBEROS V4 SUPPORT	40
REFERENCES	40

What Is Network Identity Manager?



Network Identity Manager (NetIdMgr) is a graphical tool designed to simplify the management of network identities and their credentials which are used by network authentication protocols while providing secure access to network services. When NetIdMgr is used with Kerberos v5 each network identity is a unique Kerberos principal name and the credentials are Kerberos v5 tickets. Kerberos v5 tickets can be used by NetIdMgr to obtain Andrew File System (AFS) tokens^{*}, and X.509 public key certificates⁺.

When you log into Microsoft Windows with a domain account, your account name and the Windows Domain name when combined form a Kerberos principal name. As an example, “WINDOWS\user” is actually a short form representation of user@WINDOWS.DOMAIN. Microsoft Windows uses Kerberos-based network identities for all domain-based network authentications.

Since Microsoft Windows already provides a network identity, why do you need NetIdMgr? Here are some examples:

1. Your only network identity is your Windows Domain account but you have third-party applications that rely on MIT Kerberos for authentication for access to remote files, e-mail, web data, or other services. In this scenario, NetIdMgr will automatically import your Windows Domain credentials into a form that can be used by applications that rely on MIT Kerberos.
2. You do not have a Windows Domain account but you must obtain network credentials in order to securely access a network service. In this scenario, NetIdMgr can be used to obtain new credentials for network identities and can automatically renew them before they expire.
3. You have Kerberos credentials for a network identity and you have third-party applications that require an alternative form of network credential, such as an AFS token or a X.509 certificate, which can be obtained via a Kerberos authentication. In this scenario, NetIdMgr can automatically use your existing credentials to obtain and renew the additional network credentials types.
4. You have a Windows Domain account but you need to authenticate to a service belonging to a Kerberos realm outside the Windows Domain. In this scenario, NetIdMgr can be used to manage multiple network identities, the Windows Domain identity as well as the additional Kerberos identity required for the external network services.
5. You have multiple network identities within the same Kerberos realm which are used for different roles. For example, an unprivileged user identity and a privileged identity that is only meant to be used for system administration. In this scenario, NetIdMgr can be used to obtain credentials for all of your identities and automatically renew them as necessary.

NetIdMgr's automated credential acquisition and renewal makes it an invaluable tool necessary when providing users with a Single Sign-on experience.

NetIdMgr is most commonly configured as a StartUp item and remains running with an icon in the Taskbar Notification Area until you logout. While running, NetIdMgr automatically renews your credentials, notifies you of pending expirations and prompts you when a Kerberized application requires credentials that have not already been obtained.

When configured to do so, NetIdMgr will prompt you immediately after it starts to obtain Kerberos credentials. This is often referred to as logging on to Kerberos. 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

^{*} A OpenAFS plug-in is distributed with OpenAFS for Windows release 1.5.9 and above.

⁺ A Kerberized X.509 Certificate Authority plug-in is available from <http://www.secure-endpoints.com>

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.

How to Start Network Identity Manager

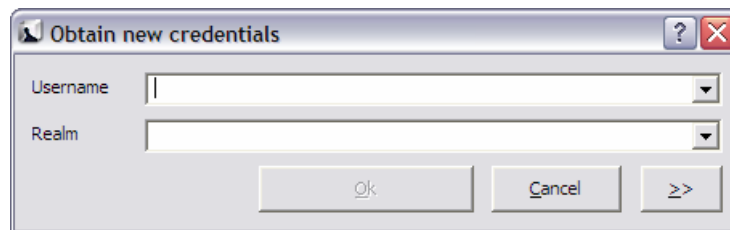
There are many ways to start Network Identity Manager.. In addition to clicking on a Network Identity Manager shortcut, you can start NetIdMgr from the Windows command Prompt or Start Menu Run... option. NetIdMgr supports a number of command-line options which may be specified.

- If you run NetIdMgr with the options `-i` or `--kinit`, it will display the obtain new credentials dialog and exit;
- `-m` or `--ms2mit` or `--import` will import tickets from the current 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.
- `-z` or `-exit` will signal a previously started instance of NetIdMgr to exit.

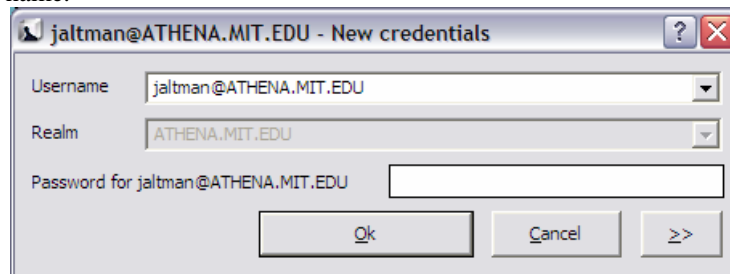
You may create a shortcut to NetIdMgr within your Windows Startup folder (Start Menu->Programs->Startup) if one has not been created for you by the MIT Kerberos for Windows installation package. A shortcut to "NetIdMgr.exe --autoinit" ensures that Kerberos tickets are available for the use of Kerberized applications throughout your Windows logon session.

Obtaining Credentials

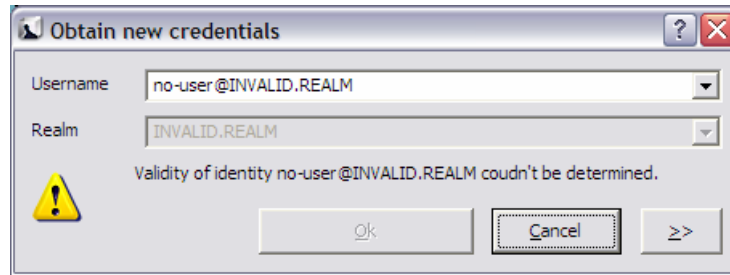
When Network Identity Manager starts, if it is configured to **obtain new credentials at startup (if none are present)** and no credentials are present, the Obtain New Credentials dialog will be displayed.



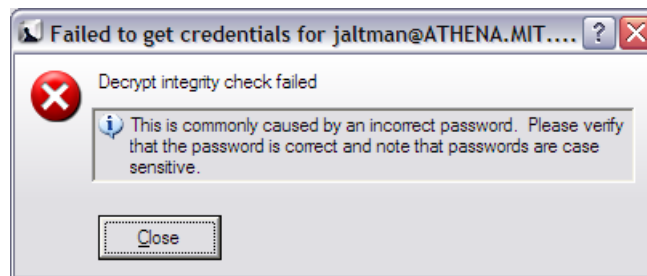
This dialog prompts you for the Username and Realm. The Username field can be used to enter the entire Kerberos principal name.



If the entered name can be verified, you will be prompted to enter your password. If the entered name cannot be validated, you will be presented an error message.



If the password is successfully entered, your credentials will be obtained. If not, you will be presented with a balloon in the notification area of the Windows Task Bar. Clicking on the balloon will provide you additional information regarding the error condition. For example:

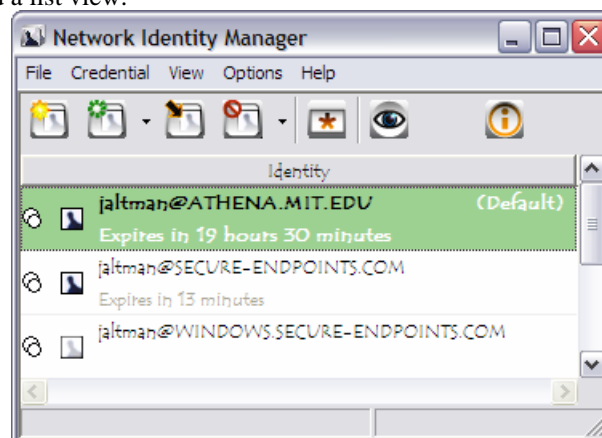





For additional information on the Obtain New Credentials dialog, see the section on the **Credential->New Credentials ...** menu item later in this document.

Network Identity Manager Application Window



The Network Identity Manager application window when open displays the current status of your network identities and provides you the tools necessary to obtain new credentials, renew existing credentials, destroy credentials, change your password, configure the behavior of your network identities, and access the on-line help. There are two primary views of network identity status: basic and advanced.

In the basic view, the window title contains the name “Network Identity Manager”. Below the title are a menu bar; a tool bar; and a list view.



The NetIdMgr basic view displays a list of network identity names (aka Kerberos principals, user@REALM). Each entry appears with a push-pin  or  button and an Identity icon  to its left. Below the identity name is the remaining lifetime of the identity's credentials.

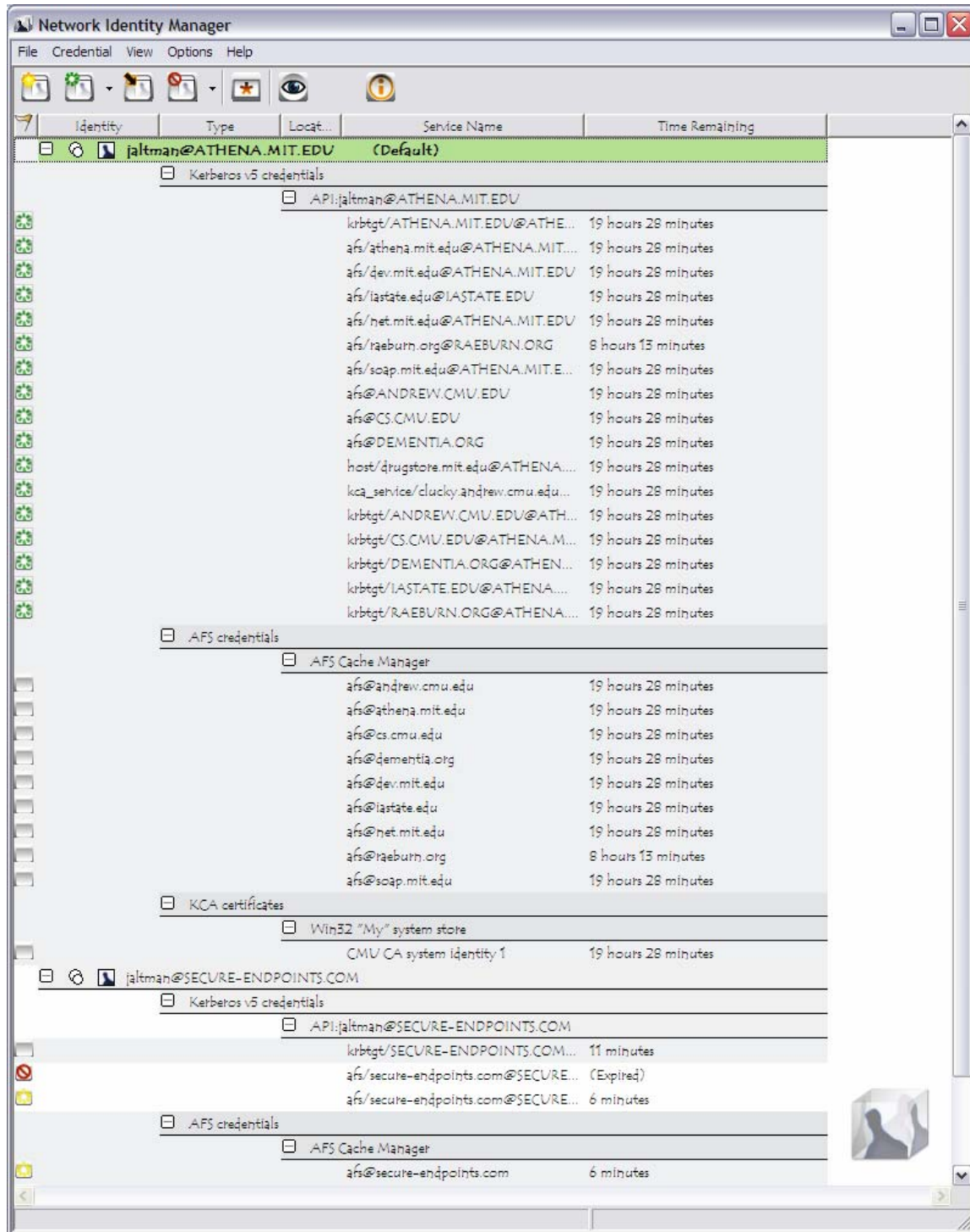
The Network Identity Manager manages multiple identities. Most applications do not know how to request a specific identity or how to search for the appropriate credentials cache. Instead these applications assume that the identity to be used is stored within the default credentials cache. NetIdMgr allows 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.

In the above image, there are three identities listed. [jaltman@ATHENA.MIT.EDU](#) is the default identity and it has valid credentials that will expire in 19 hours and 30 minutes. The [jaltman@SECURE-ENDPOINTS.COM](#) identity has valid credentials that will expire in 13 minutes. The [jaltman@WINDOWS.SECURE-ENDPOINTS.COM](#) identity has no credentials but is listed because it is pinned to the display. Other configured identities may exist but they neither have credentials nor are they pinned.

The fact that [jaltman@ATHENA.MIT.EDU](#) is green indicates that its credentials are renewable.

In the advanced view, 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 advanced view displays a list of network 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.

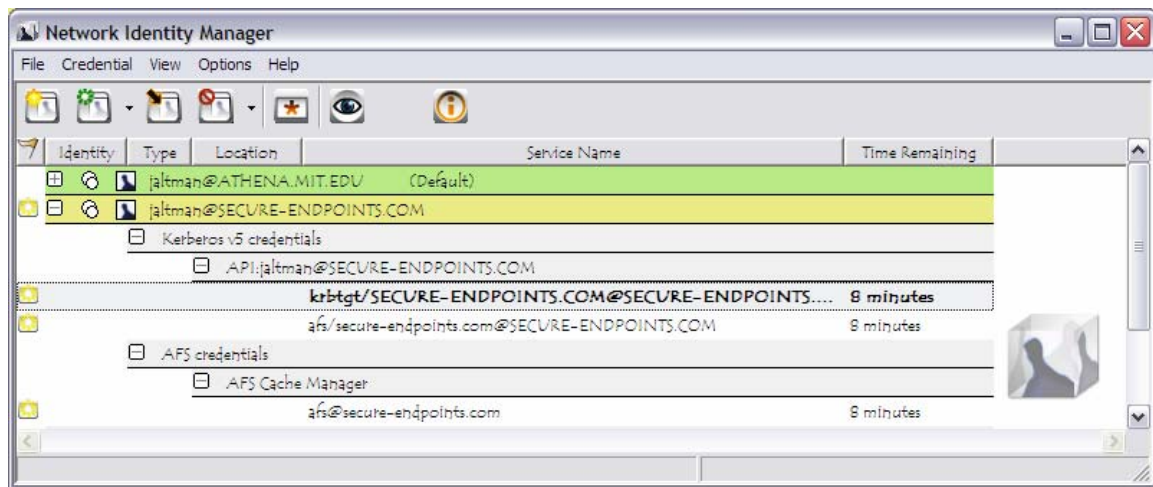
Below each network identity, the tree contains credential categories. Below each credential category are the active credential locations and the current credentials belonging to the category. Each credential entry contains the current credential status, the service name and time remaining before expiration.

The tree updates once per minute. If you need an immediate update of your ticket status, you can press the Update Display button on the toolbar or the F5 key.

To the right of each credential is a flag 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

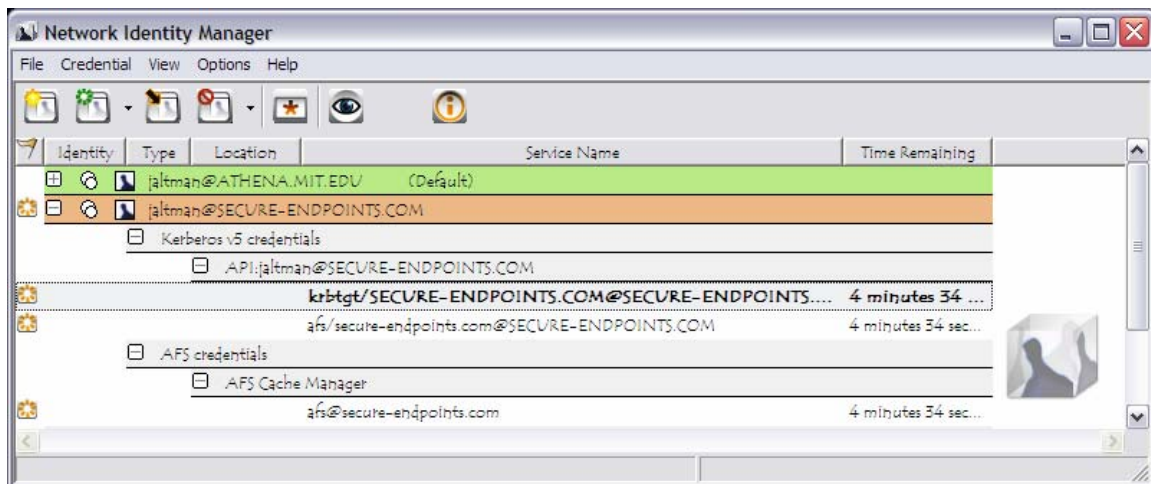
Attempts to renew renewable credentials are performed at half-life intervals and 15 minutes* before expiration.



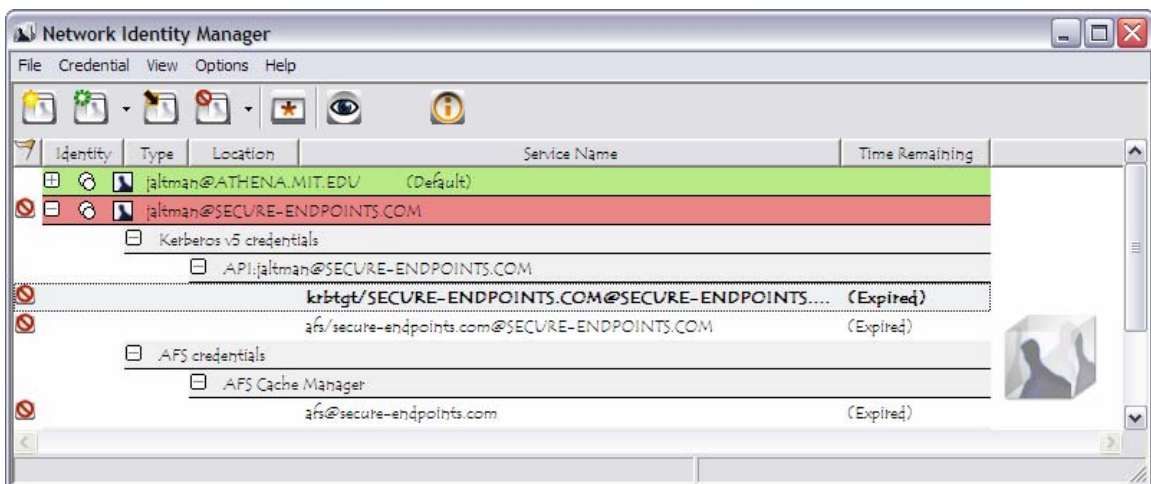
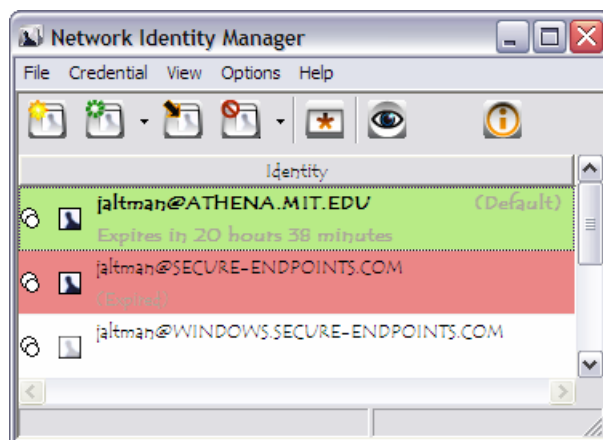
At 10 minutes and 5 minutes+ before your credentials expire, a balloon tip is displayed to warn that your credentials will soon expire and to provide you the opportunity to obtain new ones.

* The actual time is configurable. 15 minutes is the default time. Automatic renewal may be disabled by using the Notifications Options page.

+ The actual times are configurable. 10 minutes and 5 minutes are the default times, Expiration warnings may be disabled by using the Notifications Options page.



Credentials that can not be renewed will expire.



Andrew File System (AFS) token management is available only on machines that have installed OpenAFS for Windows[#]. KCA certificates management is available only on machines that have installed the Secure Endpoints Inc. KCA plug-in[†].

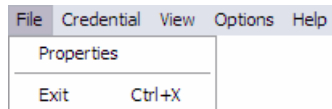
Network Identity Manager Command Line Options

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
--exit, -x closes any copy of netidmgr currently running in the same Windows Logon Session

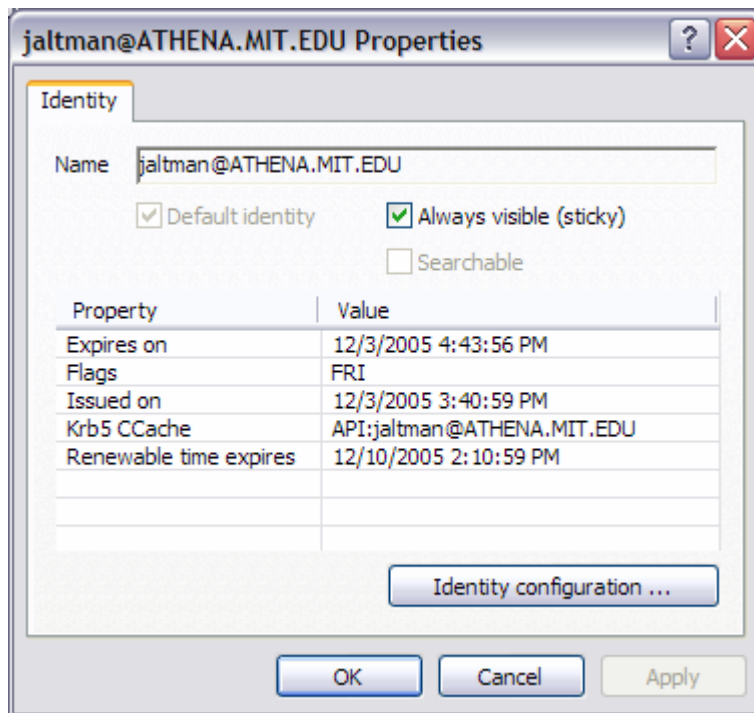
Network Identity Manager Command Reference

File:



Properties...

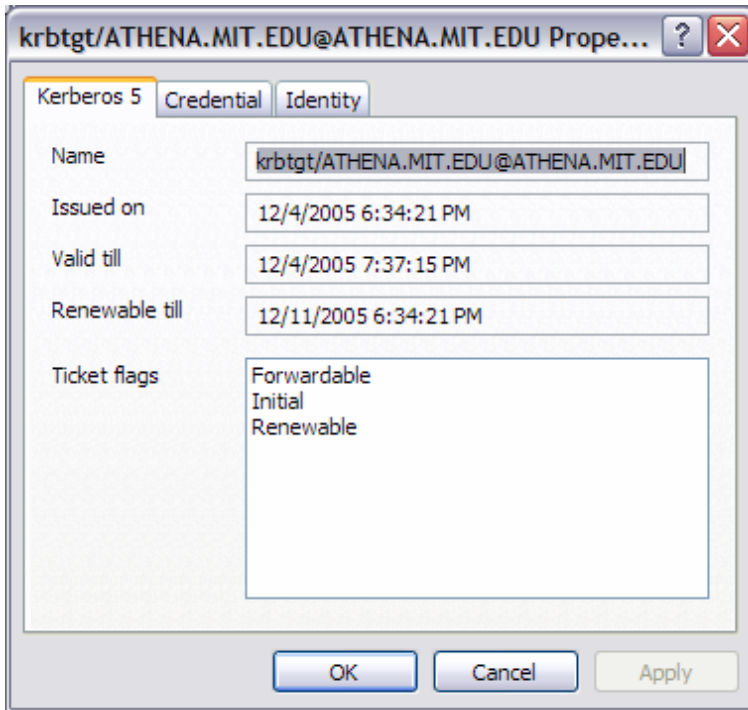
From the File menu, will display the Properties dialog for the currently selected item whether it be an Identity or a Credential.



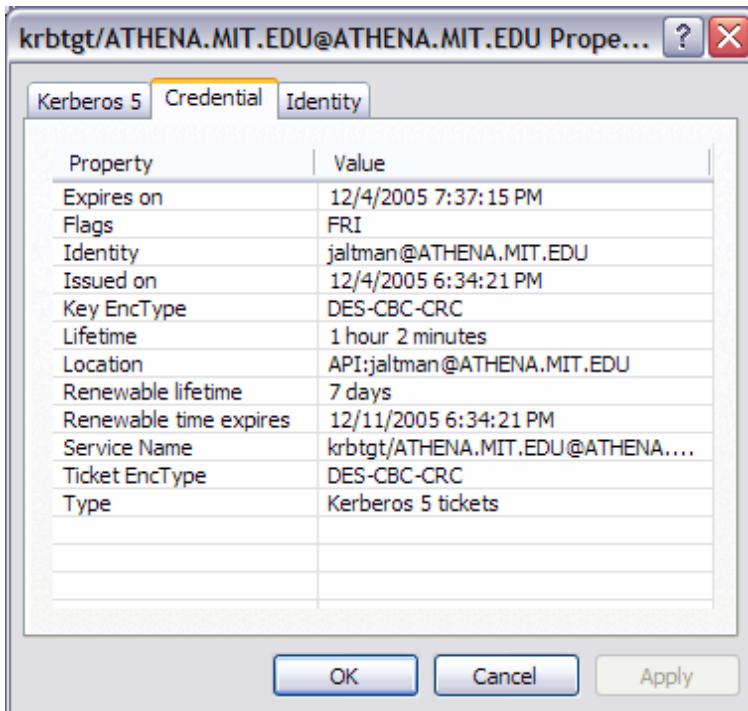
An Identity Property dialog

[#] OpenAFS for Windows 1.5.9 or higher is required. <http://www.openafs.org>


[†] The Kerberized Certificate Authority plug-in can be downloaded from <http://www.secure-endpoints.com/>.



A Kerberos v5 Ticket Property dialog



Associated credential properties

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

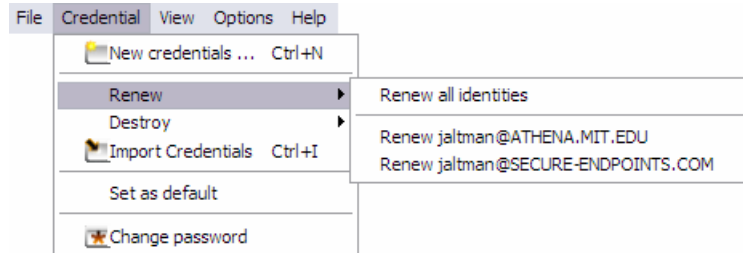
Exit Command

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


Important Note...

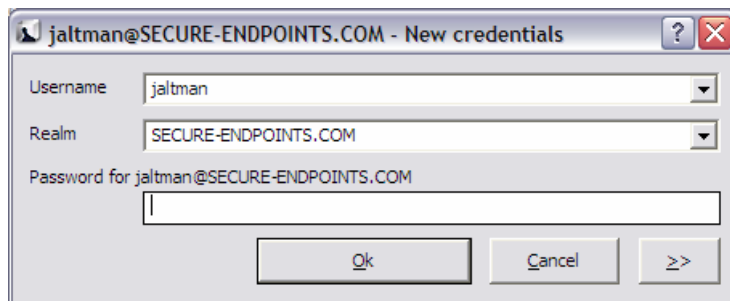
Exiting the Network Identity Manager will **not** destroy your current credentials. Unless you have chosen to delete credentials on exit from the General Configuration page, you need to use the destroy credentials command.

Credential:



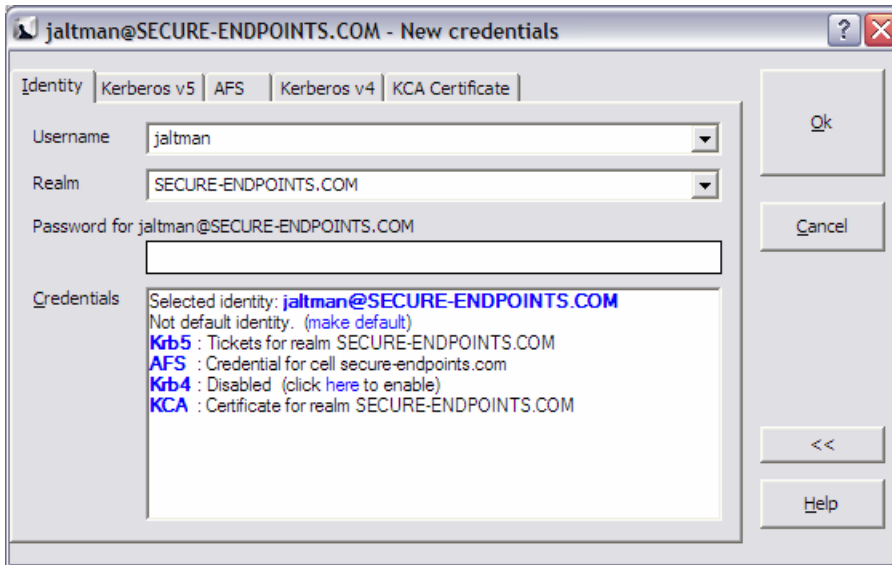
New Credentials Command, Ctrl+N

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.

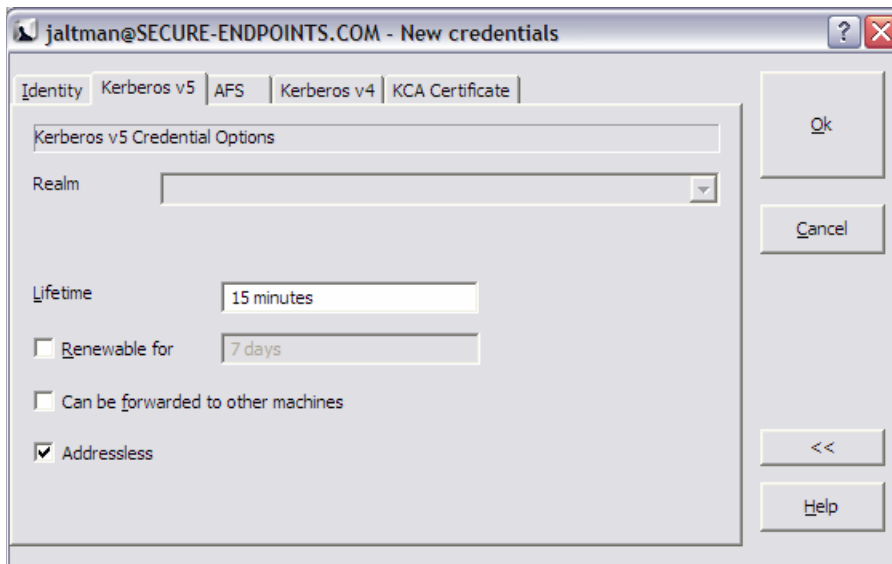


When you select this command, NetIdMgr displays a dialog requesting your Username, Kerberos Realm, and Password; if these are correct, NetIdMgr will obtain tickets using either a known configuration for the entered identity (Username@Realm) or the default identity configuration if the identity has not been previously used.

If you wish to alter the configuration for the entered identity, activate the Advanced view by pressing the ">>" button.



In the Advanced view, a credentials browser window displayed along with tabs for each credential type that can be obtained for this identity. The credentials browser summarizes the state of the identity and which credentials will be obtained as part of a successful authentication.



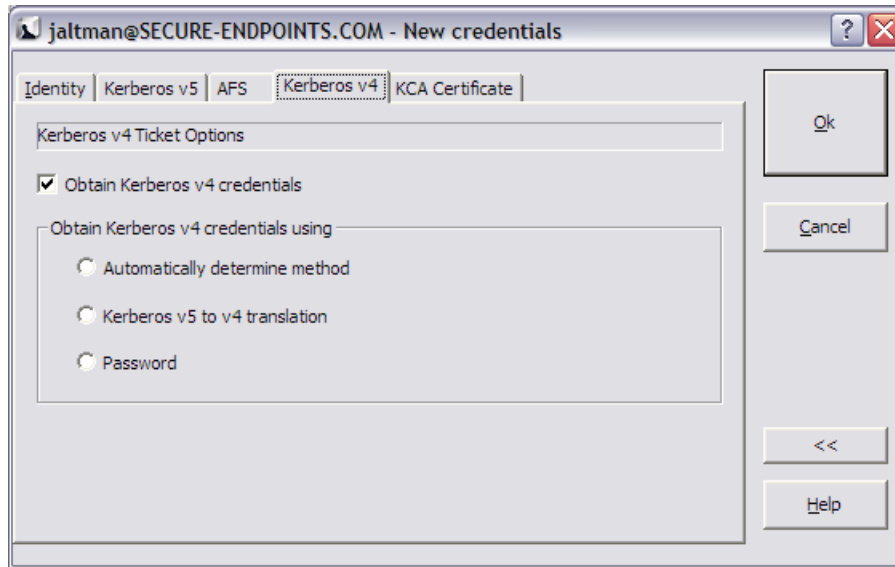
Kerberos v5 options include the ability to select the ticket lifetime as well as renew and forwarding. The Kerberos v5 ticket granting ticket represents the selected identity. As such, obtaining a Kerberos v5 ticket is mandatory.

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. **Forwardable** tickets are often required when authenticating to a remote host using ssh or ftp when the remote host requires the ability to authenticate to a remote file system such as AFS.

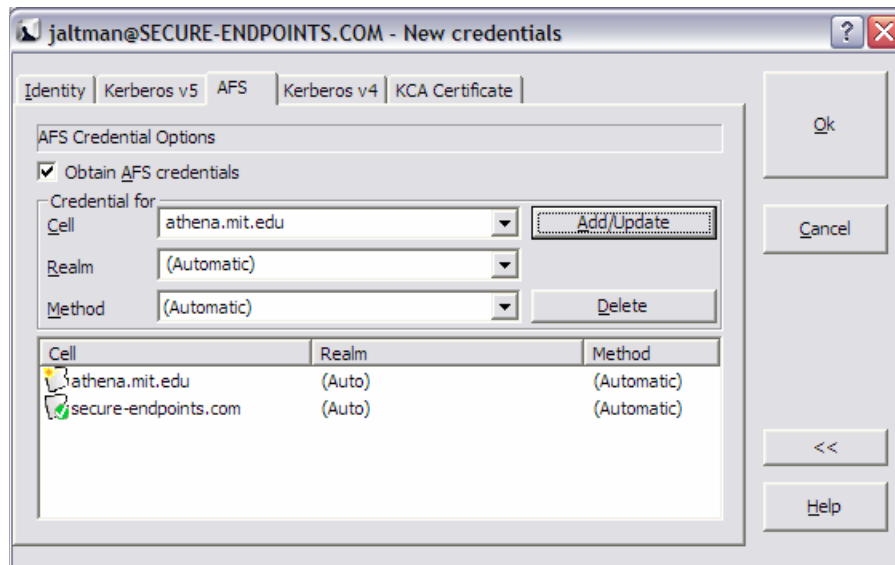
When **Renewable** tickets are received from the Kerberos Server, the ticket lifetimes may be renewed without prompting the user for her password. This allows Kerberos tickets to be issued with short lifetimes allowing compromised accounts to be disabled on short notice without requiring the user to 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.

When **Addressless** is selected, the tickets do not contain IP address information. This enables the tickets to be used from behind Network Address Translators which are frequently found in Cable and DSL Modems.

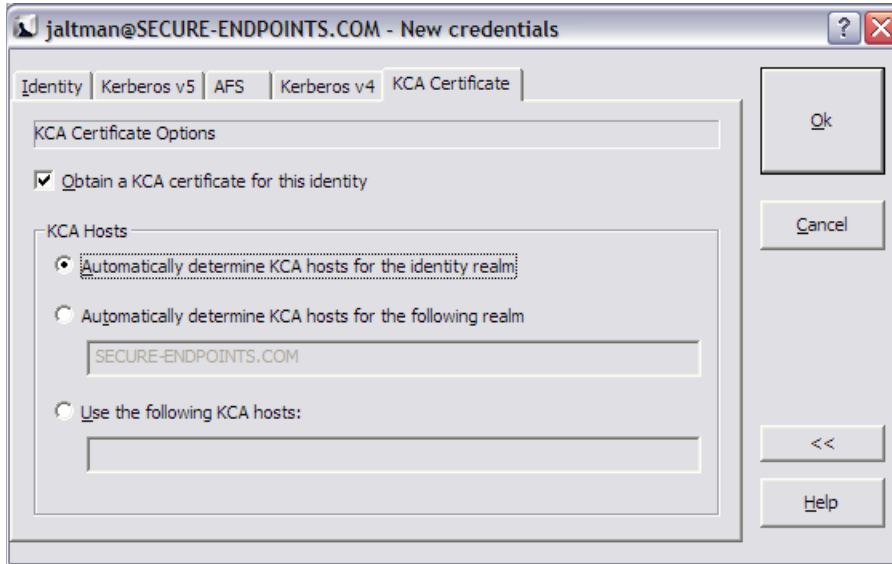


Obtaining Kerberos v4 tickets is optional and may not be available on all systems. When available, Kerberos v4 tickets may only be obtained for the default identity. Kerberos v4 tickets may be obtained via use of a Kerberos v5 to v4 translation service or by a separate password based request. Selecting “Automatically determine method” will first try the translation service and if that fails, the password based request will be attempted. Automatic renewal of Kerberos v4 tickets can only occur if the translation service is used.

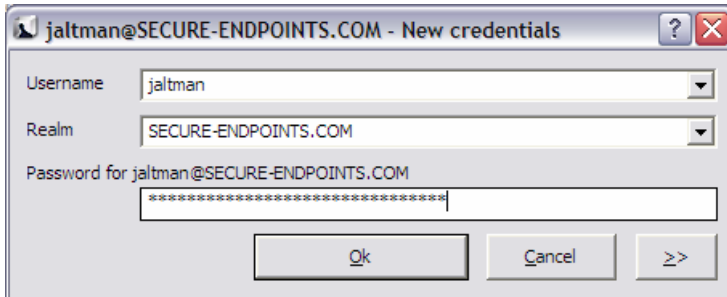


Obtaining AFS tokens is only available on systems with an appropriate version of OpenAFS for Windows installed. An identity may be used to obtain tokens for multiple AFS cells. The Add/Update and Delete

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 v5”, “Kerberos v5 to v4” or “Kerberos v4”. Kerberos v5 based tokens should be used when possible. If not, the next best choice is the Kerberos v5 to v4 translation service. As a last resort, a Kerberos v4 ticket request can be used directly. In most cases, using “Automatic” will just work.




A Kerberized Certificate Authority certificate is an X.509 certificate that can be used with web browsers to authenticate the user as the Kerberos identity even though Kerberos authentication is not used authentication to the web server. The KCA certificate can be obtained from servers in the identity realm or from servers in an alternate realm. As of the KCA 1.1 plug-in, only one KCA certificate can be obtained for a given identity. Obtaining KCA certificates is only available on systems with a KCA plug-in installed.




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 credentials either for all identities or the specified identity on the menu. Individual credentials can be renewed by selecting them in the Advanced View and using the right-mouse context menu Renew option. If the selected identity cannot be renewed without a password, a dialog will be displayed providing an opportunity to obtain new credentials.

Import Credentials Command, Ctrl+I

This command is found on the Credential menu; it is also the third button 


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

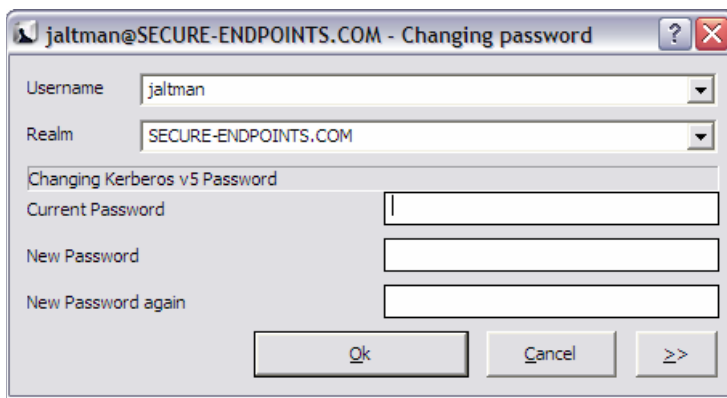
Destroy Credentials Command, Del

This command is found on the Credential menu; it is also the fourth button 

Once credentials are destroyed, you must Obtain 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 



Note: This command will not change your local machine password unless you login to your computer using a Windows Domain account or otherwise authenticate using an MIT Kerberos identity.

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

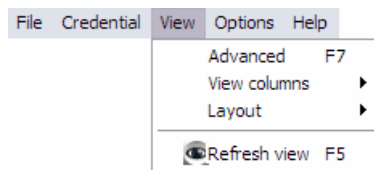
password is weak, a message notifies you, and you need to repeat steps 1 through 4 with a strong password, as described by the "How To Choose a Password" guidelines above.

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.

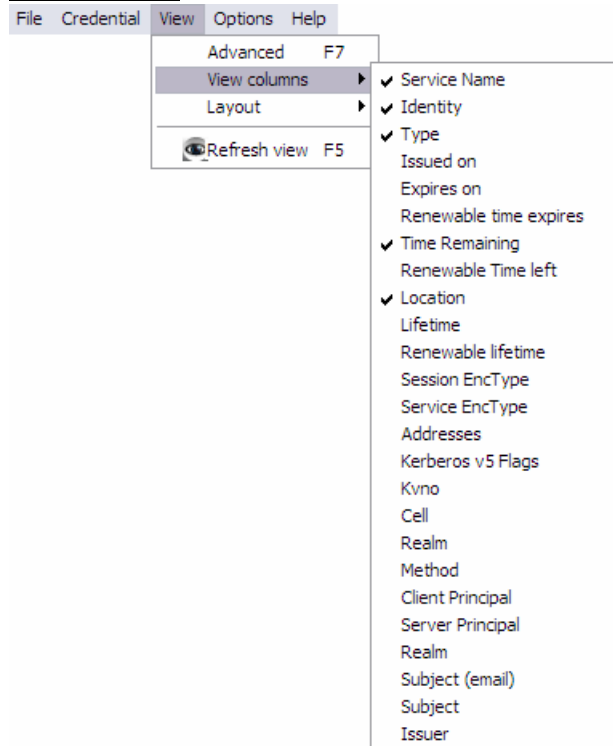
View:



Advanced Command, F7

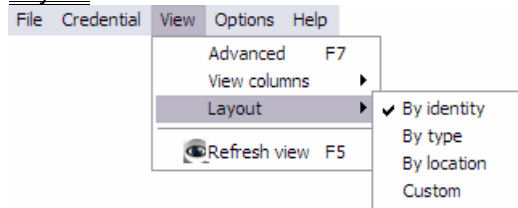
Use this command to toggle between the Basic and Advanced view modes for the Network Identity Manager Application Window.

View Columns



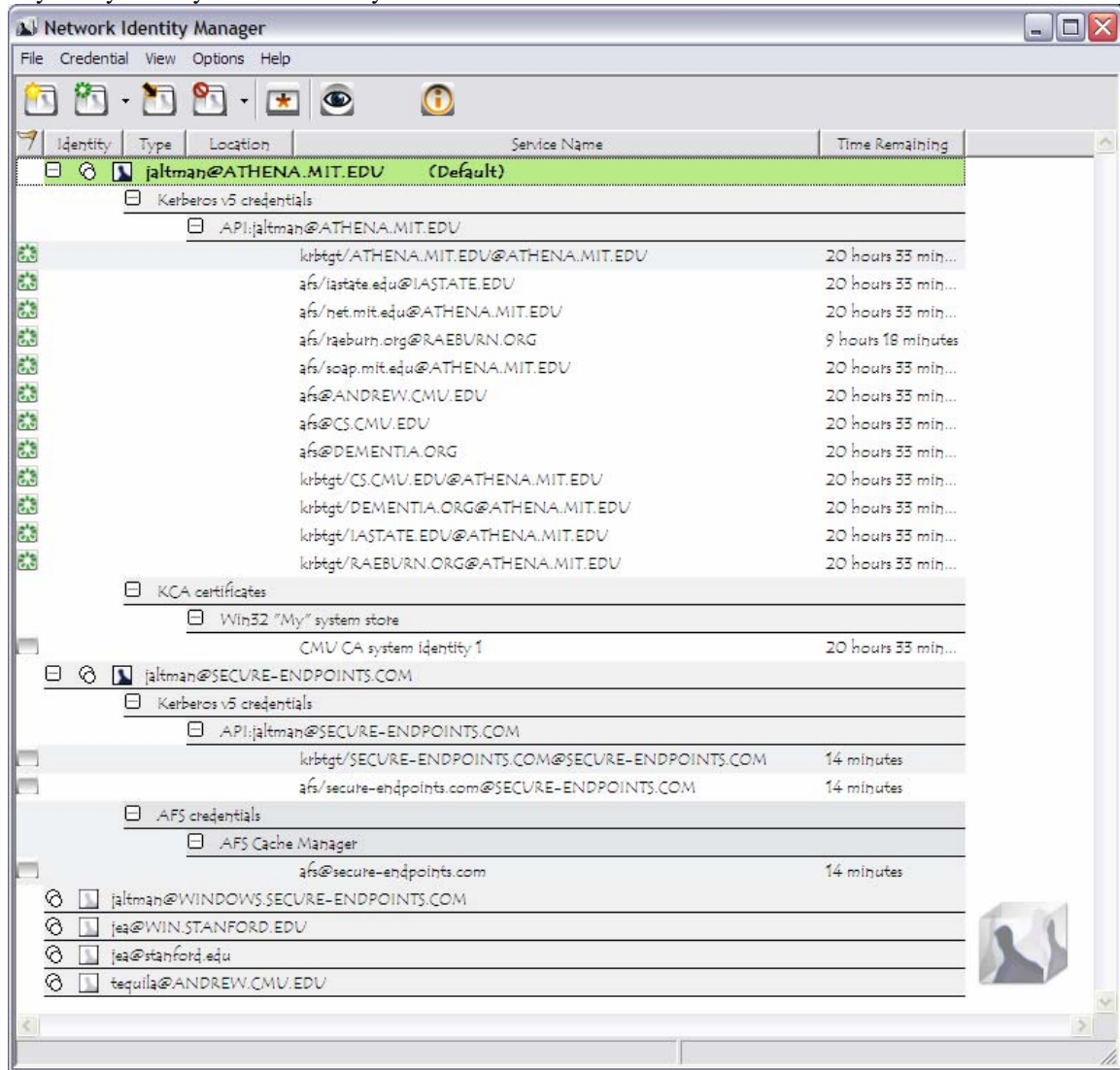
By default only the Service Name, Identity, Credential Type, Time Remaining and Location are displayed. Using the View->View Columns menu you can select a variety of other credential properties to display in the NetIdMgr window. After displaying the columns, you can re-organize them by dragging the column headers into the desired location. The selected configuration will be preserved.

Layout



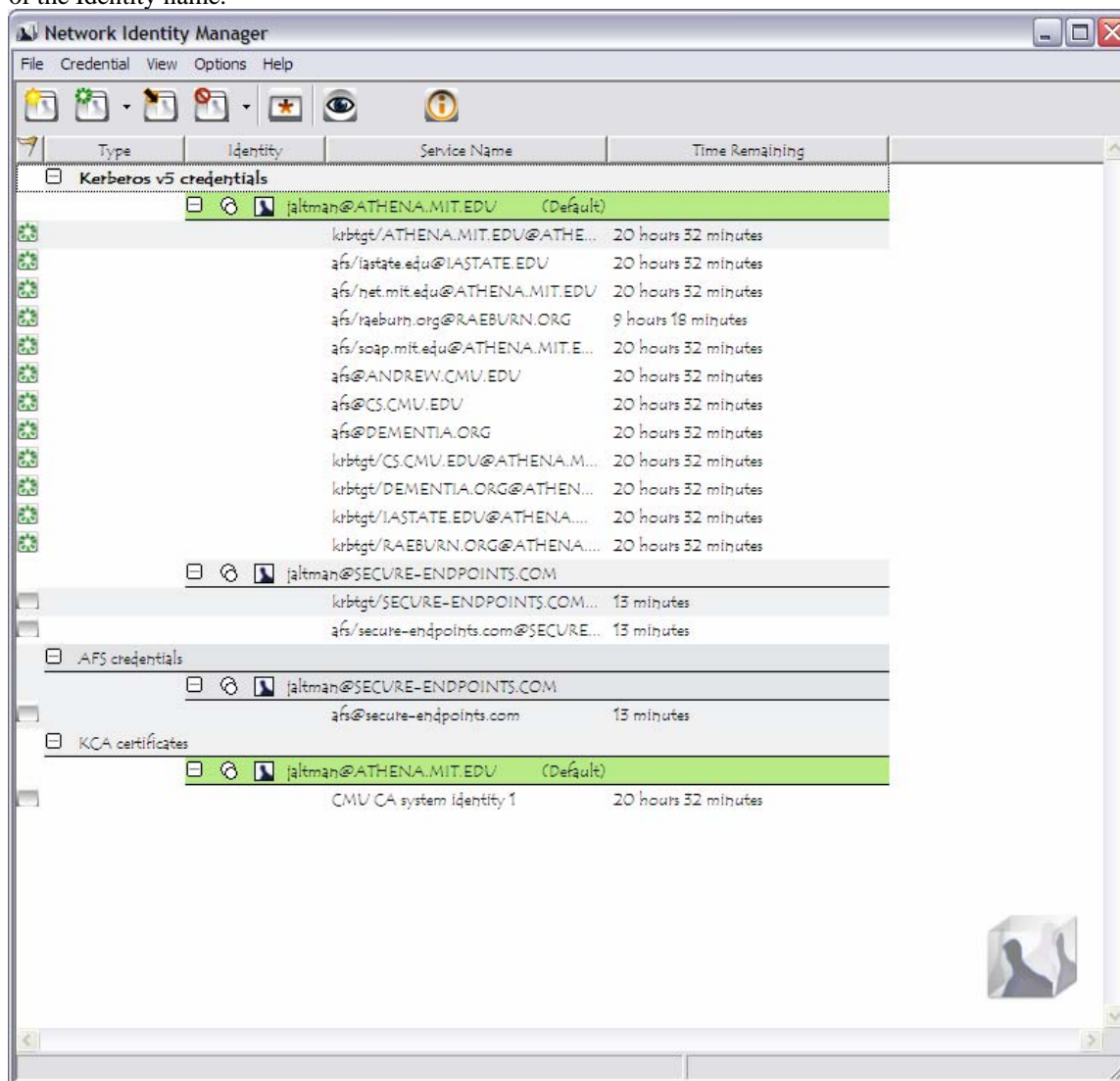
Layout By Identity

Layout By Identity is the default layout.



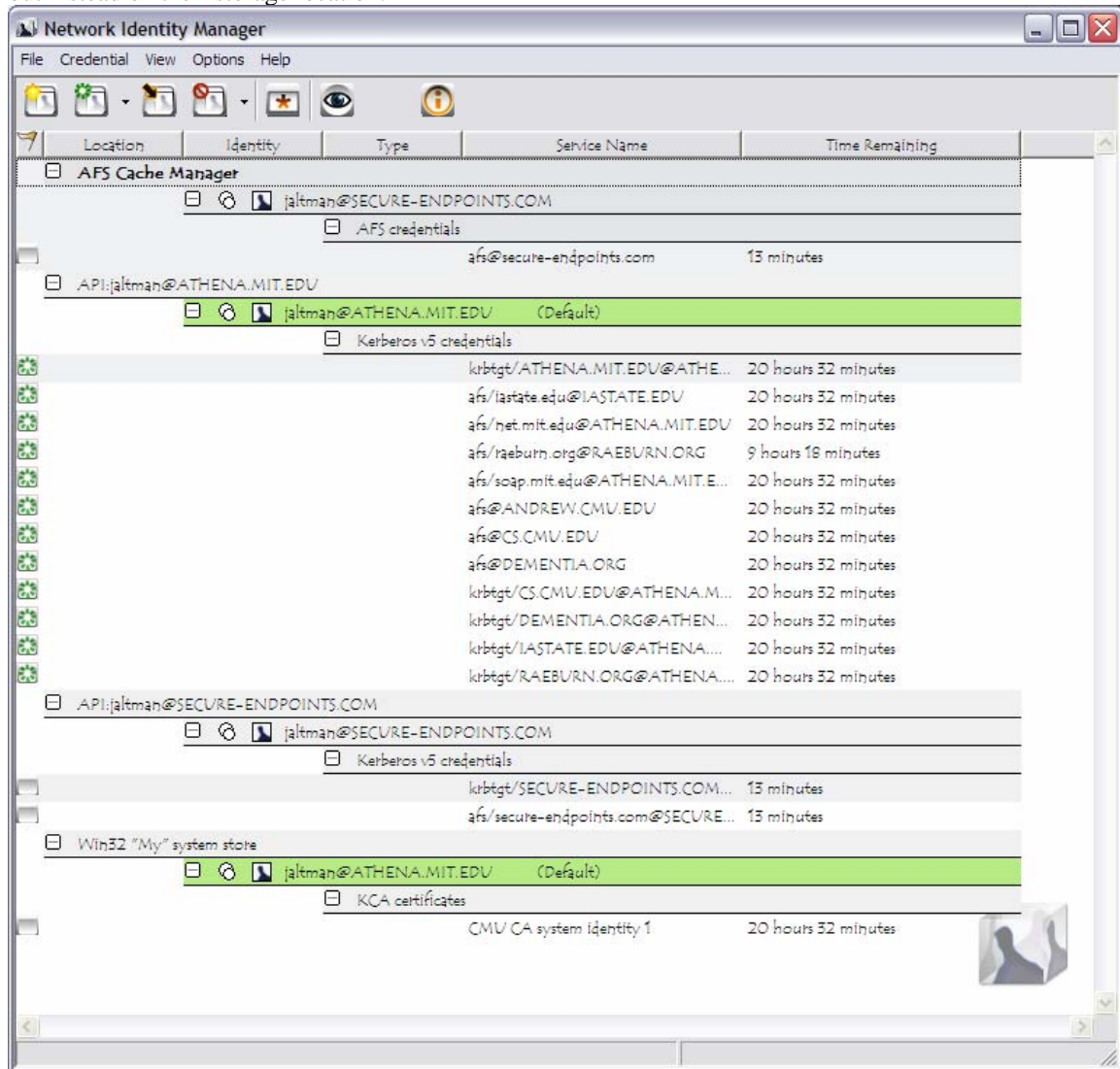
Layout By Type

Layout By Type provides an alternative view of your credentials ordered by the type of credential instead of the Identity name.



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.



Custom

Custom views can be obtained by clicking on the column headers to produce an ordering of your choice.

Refresh Command, F5

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

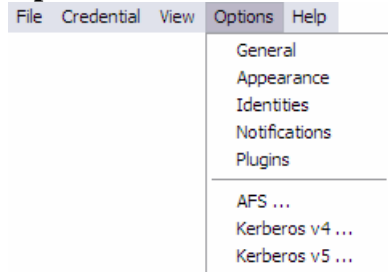
Why Use It...

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 `kinit` or `kdestroy` and want to check that they have functioned successfully.

How It Works...

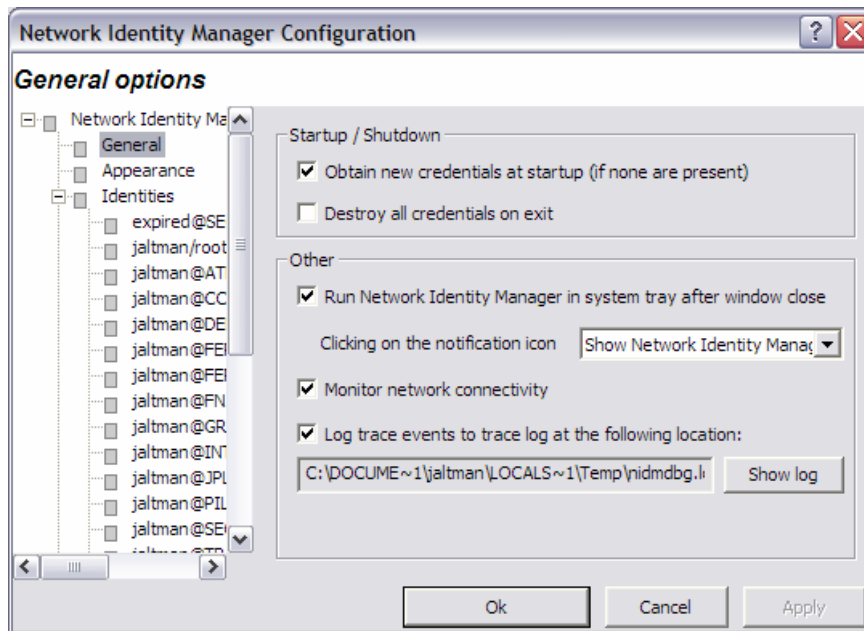
While NetIdMgr automatically checks the status of your credentials every minute, the Update Display command forces an immediate status check.

Options:



General Options


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 **Destroy all credentials on exit** option can be used to empty all of the credential caches when the NetIdMgr is terminated.

The **Run NetIdMgr in taskbar notification area 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 taskbar notification area. When unchecked, NetIdMgr will behave as if File->Exit was selected from the menu.

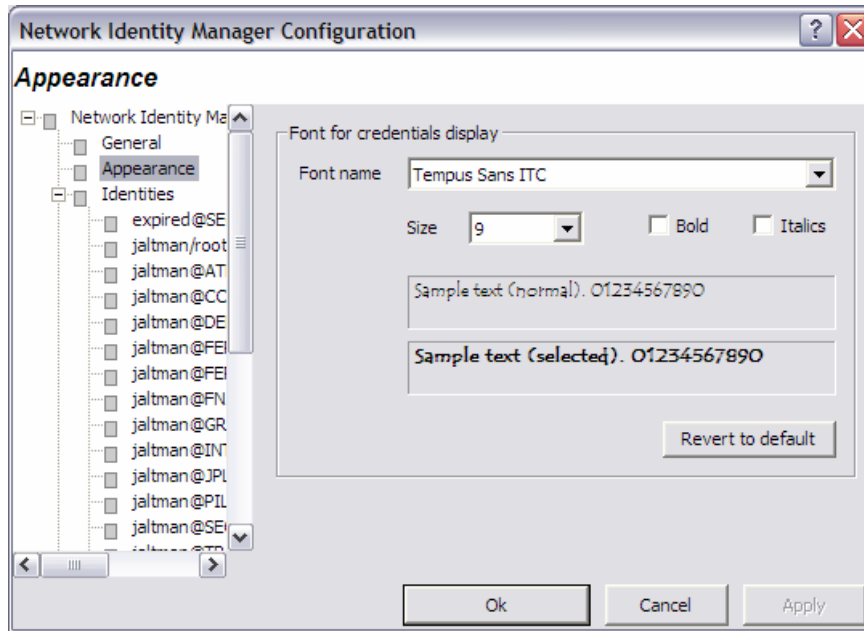
Clicking on the notification icon can be configured to either *Show Network Identity Manager* or *Obtain New Credentials*. This option controls which menu item on the notification icon menu is the default action.

The **Monitor network connectivity** option determines whether or not NetIdMgr monitors the configuration of IP addresses on the machine. When IP addresses are added or removed and this feature is activated, the NetIdMgr will probe the identity management servers (e.g., Kerberos Key Distribution Centers) to determine if they are reachable and if so will automatically obtain credentials.

The **Log trace events to trace log at the following location** option is used to activate a log file that can be used to help debug the behavior of NetIdMgr and its plug-ins. Press the **Show log** button to view the log file in Windows Notepad.

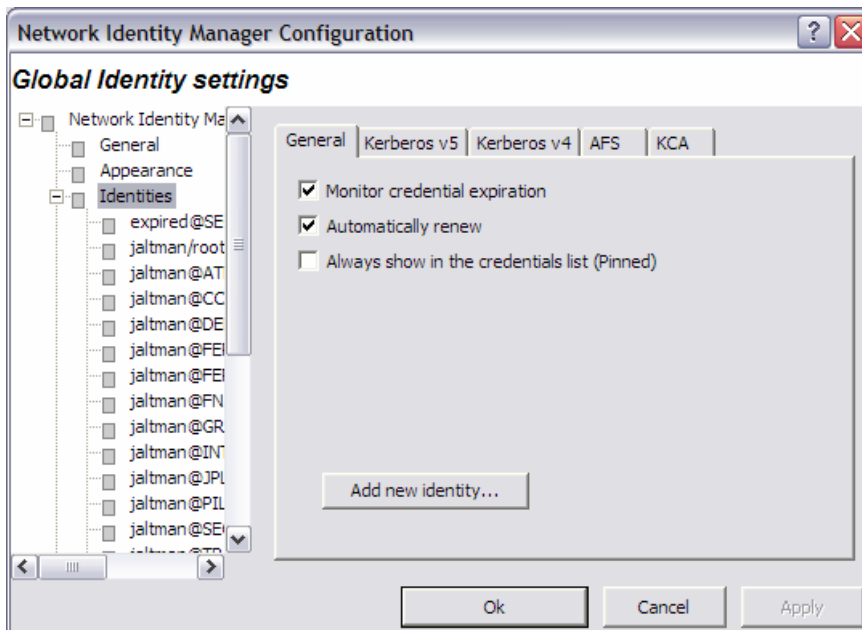
Appearance Options

The Appearance Options page can be used to select an alternate typeface to be used when displaying credentials in the NetIdMgr.



Identities Options

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

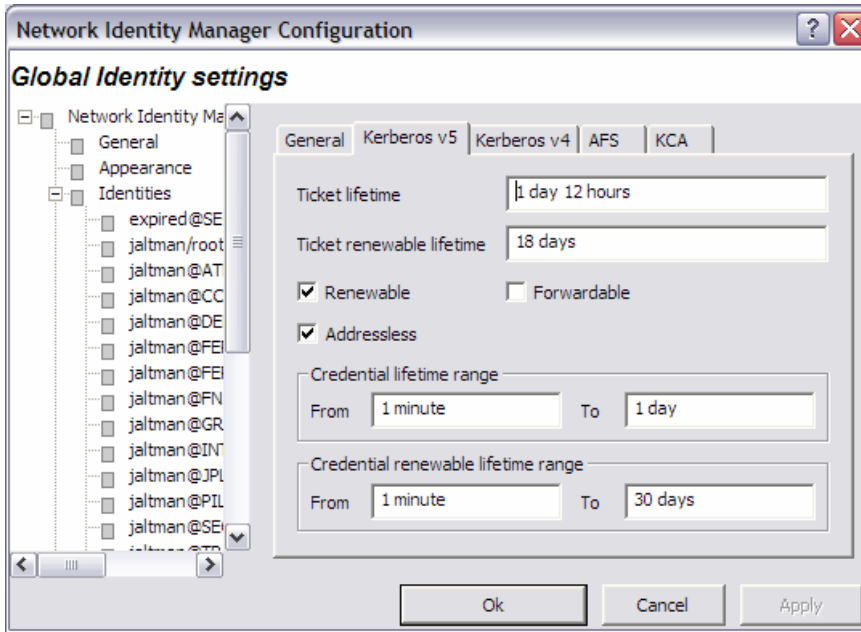
Global Identity Settings

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 v5 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.

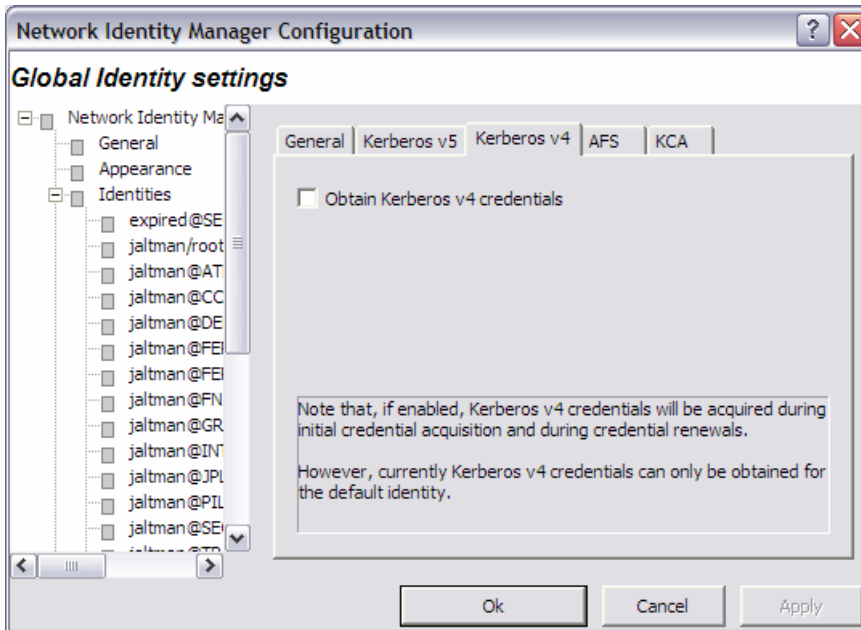
The **Renewable**, **Forwardable**, and **Addressless** options determine whether or not new identities default to obtaining Kerberos v5 tickets with these options.

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. **Forwardable** tickets are often required when authenticating to a remote host using ssh or ftp when the remote host requires the ability to authenticate to a remote file system such as AFS.

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.

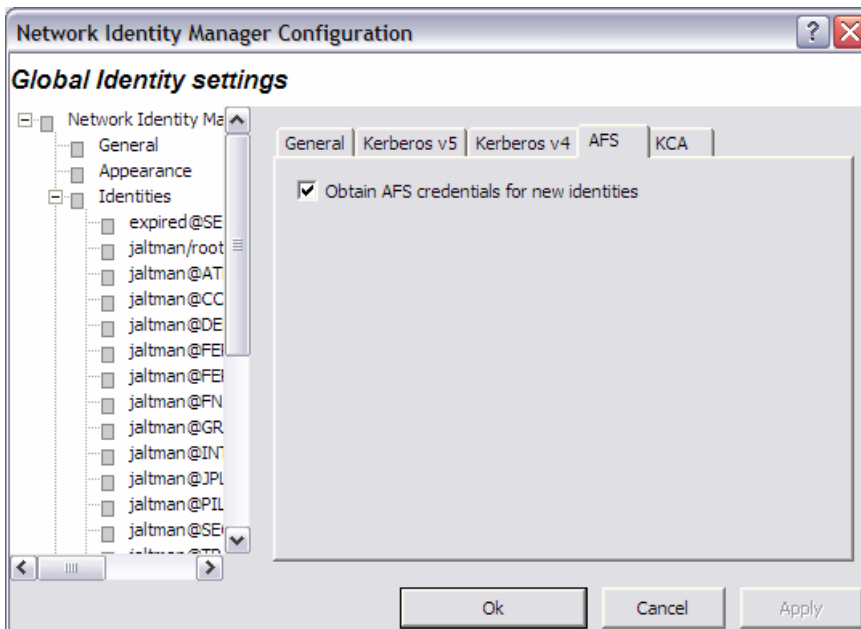
When **Addressless** is selected, the tickets do not contain IP address information. This enables the tickets to be used from behind Network Address Translators which are frequently found in Cable and DSL Modems.

The minimum and maximum ranges 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.

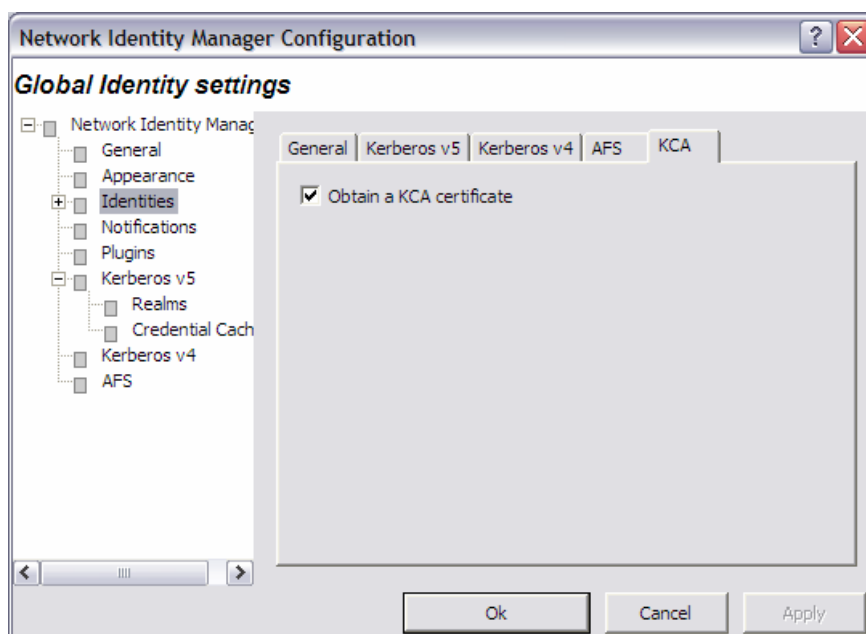


When the **Obtain Kerberos v4 credentials** button is checked, NetIdMgr will attempt to retrieve Kerberos v4 credentials when ticket initialization, renewal, or importation is performed. Kerberos realms are increasingly configured to support only Kerberos v5 (e.g., Windows Active Directory Domains.) If the realms you use do not support Kerberos v4 it is suggested that this button be unchecked.

Be aware that only the default identity can obtain Kerberos v4 credentials. This limitation is due to the inability of Kerberos v4 applications on Microsoft Windows to specify a credentials cache.



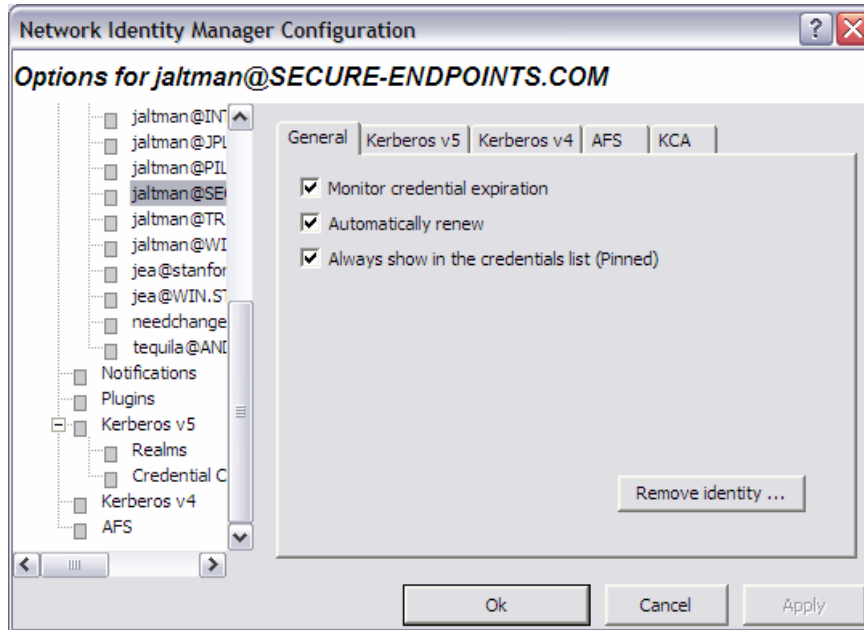
When the **Obtain AFS tokens** button is checked, NetIdMgr will attempt to retrieve AFS tokens when ticket initialization, renewal, or importation is performed. If you do not frequently access AFS cells, it is suggested that this button be unchecked.



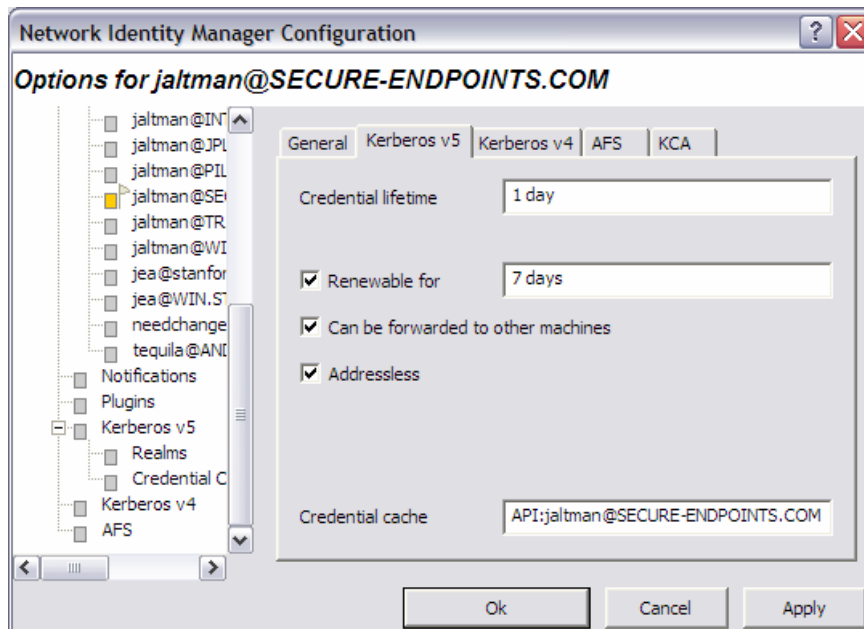
When the **Obtain a KCA certificate** button is checked, NetIdMgr will attempt to obtain a KCA certificate when ticket initialization, renewal, or importation is performed. Most Kerberos realms do not support KCA certificates, it is suggested that this button be unchecked.

Identity Specific Options

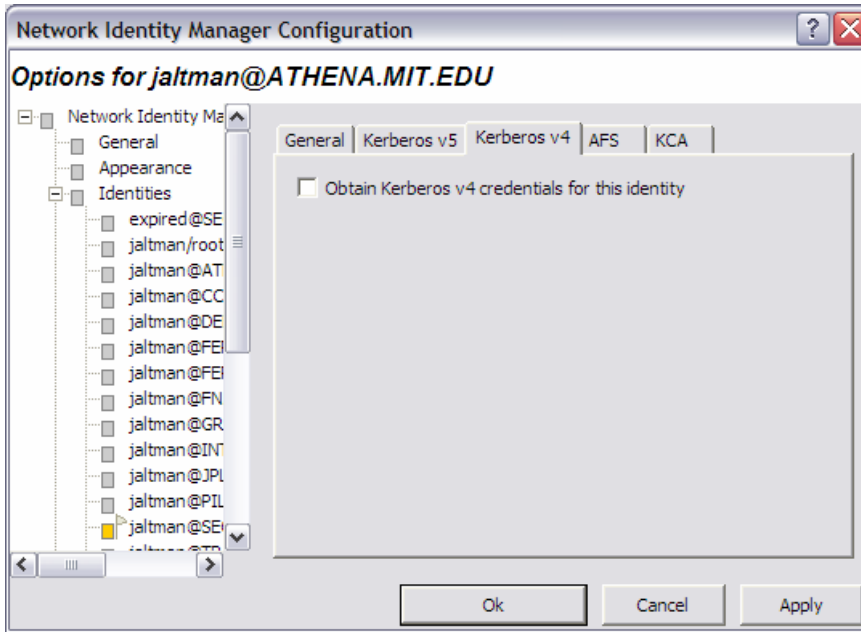
Each Identity known to the Network Identity Manager is provided its own set of tabbed pages that can be used to override the default values specified on the Global Identity Settings pages. There are two distinctions.



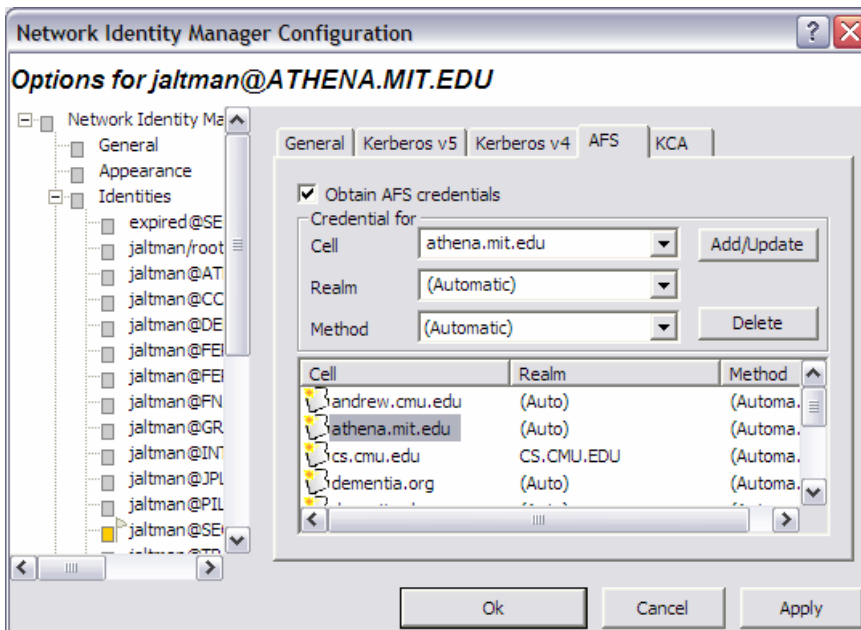
The General page contains a **Remove Identity** button that can be used to delete this Identity from the Network Identity Manager.



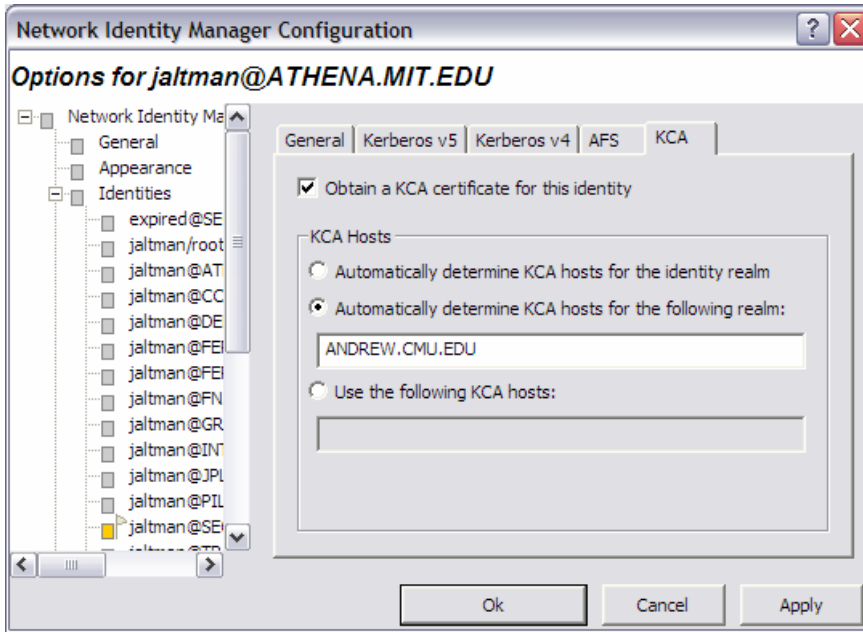
The Kerberos v5 page displays the name of the credential cache currently associated with the Identity.



The Kerberos v4 page is optional and may not appear on all systems. Only one identity can obtain Kerberos v4 credentials at a time.

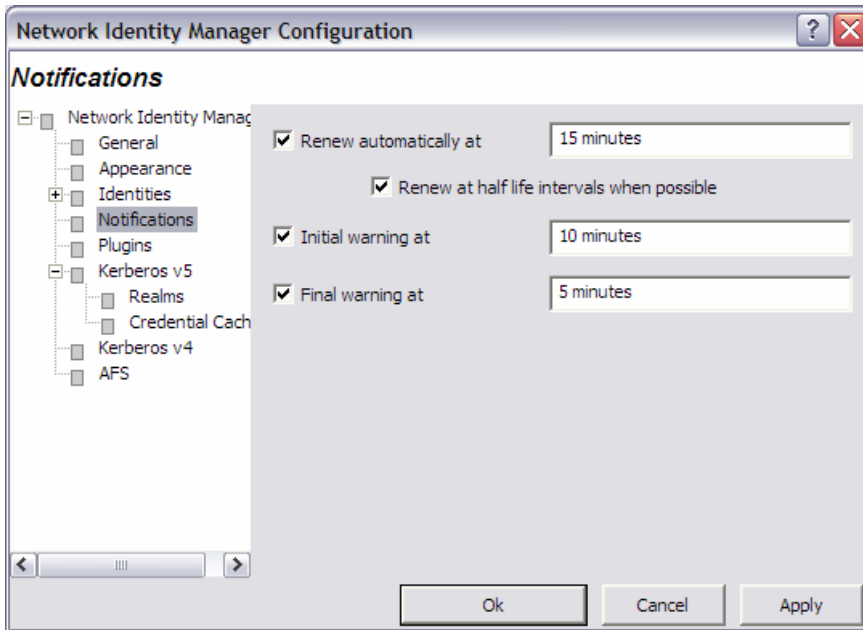


The AFS page is optional and may not appear on all systems. A single identity may be used to obtain tokens for multiple AFS cells. The Add/Update and Delete buttons are used to manage the list of AFS cells. If the Kerberos realm associated with the AFS cell cannot be automatically determined, it may be entered manually. The method of AFS token acquisition is one of: “Automatic”, “Kerberos v5”, “Kerberos v5 to v4” or “Kerberos v4”. Kerberos v5 based tokens should be used when possible. If not, the next best choice is the Kerberos v5 to v4 translation service. As a last resort, a Kerberos v4 ticket request can be used directly. In most cases, using “Automatic” will just work.



A Kerberized Certificate Authority certificate is an X.509 certificate that can be used with web browsers to authenticate the user as the Kerberos identity even though Kerberos authentication is not used authentication to the web server. The KCA certificate can be obtained from servers in the identity realm or from servers in an alternate realm. As of the KCA 1.1 plug-in, only one KCA certificate can be obtained for a given identity. Obtaining KCA certificates is only available on systems with a KCA plug-in installed.

Notifications Options



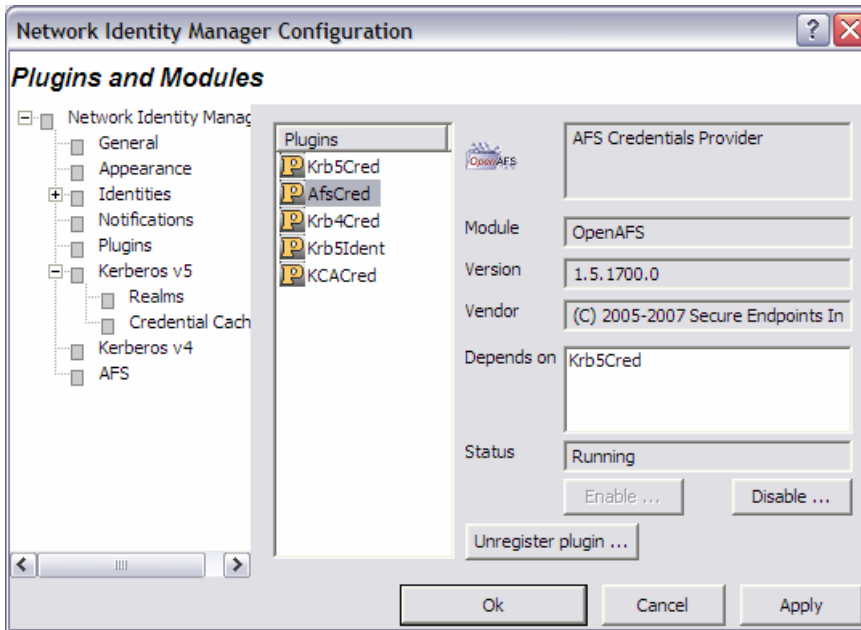
The **Renew automatically at** check box determines whether or not renewable tickets will be renewed by NetIdMgr when they reach the specified time remaining.

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.

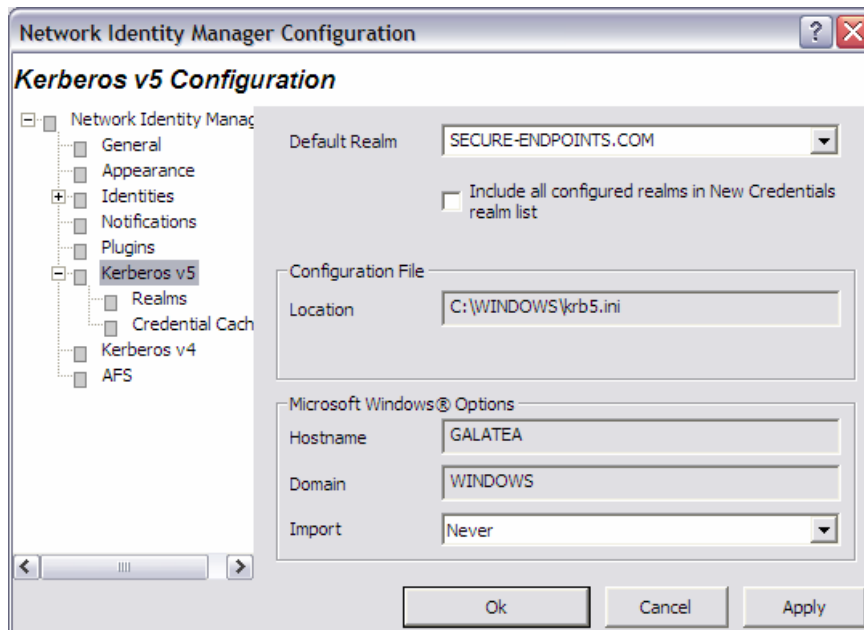
Notifications are performed in two ways. First, icons are displayed next to the affected credentials in the flags column of the display. Second, a balloon tip is displayed off of the NetIdMgr taskbar notification area icon.

Plug-ins and Modules



The Plug-ins and Modules page provides status information on the currently loaded plug-ins 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.

Kerberos v5 Configuration



The **Kerberos v5 Configuration** tab allows you to alter the behavior of the Kerberos v5 identity provider.

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

The **Include all configured realms in New Credentials realm list** determines whether all of the realms declared in the Kerberos v5 Configuration file are included in the realms list of the **Obtain New Credentials** dialog. If disabled, only the realms previously used to obtain credentials are displayed.

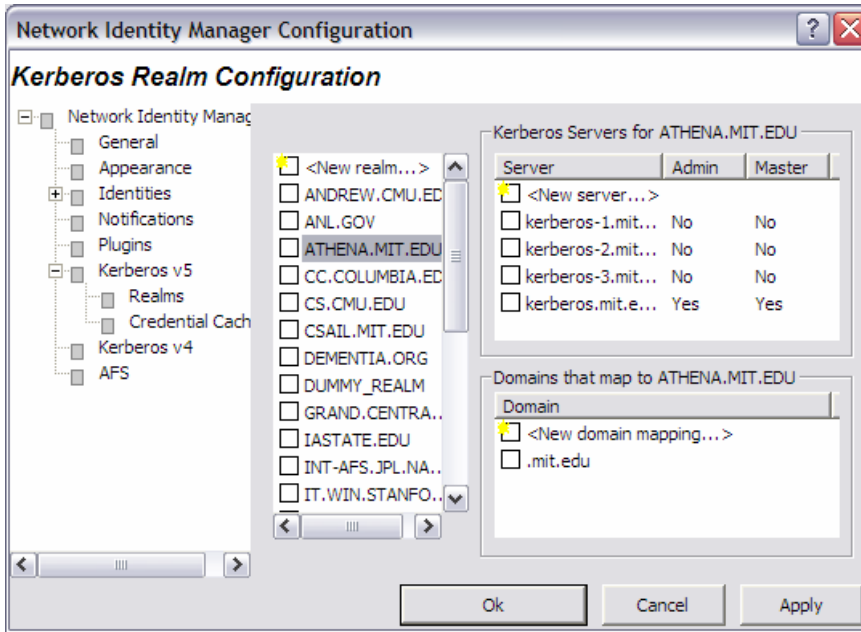
The **Configuration File** field displays the path to the Kerberos v5 configuration file, krb5.ini.

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.

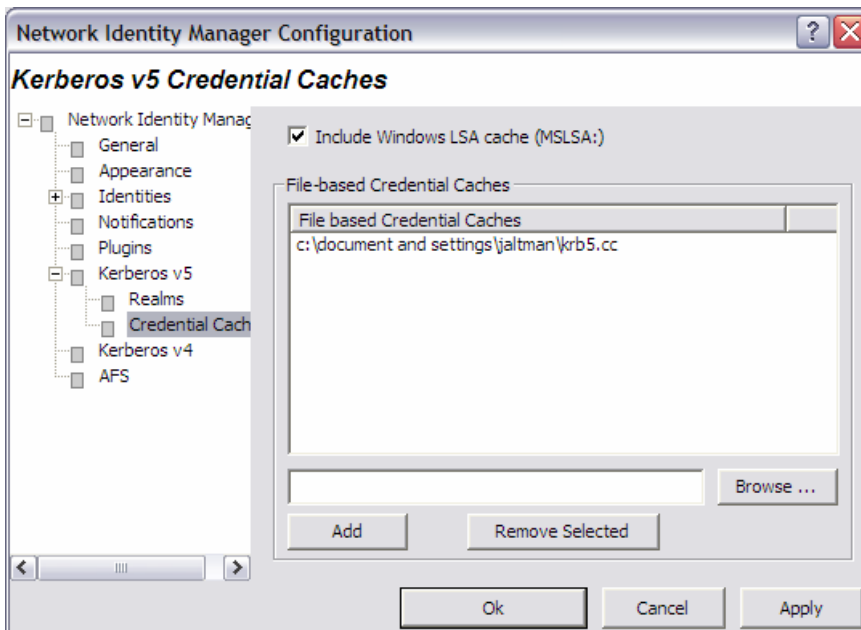
The **Import Tickets** listbox allows you to configure how NetIdMgr interacts with the Microsoft Kerberos Authentication Provider. NetIdMgr will automatically import Kerberos Tickets from the Microsoft LSA at startup depending upon the selected option and whether or not the Kerberos Authentication Provider 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.

When the Windows Logon identity is imported and is configured as the default identity, the MIT credential cache will be used in preference to the MSLSA credential cache.



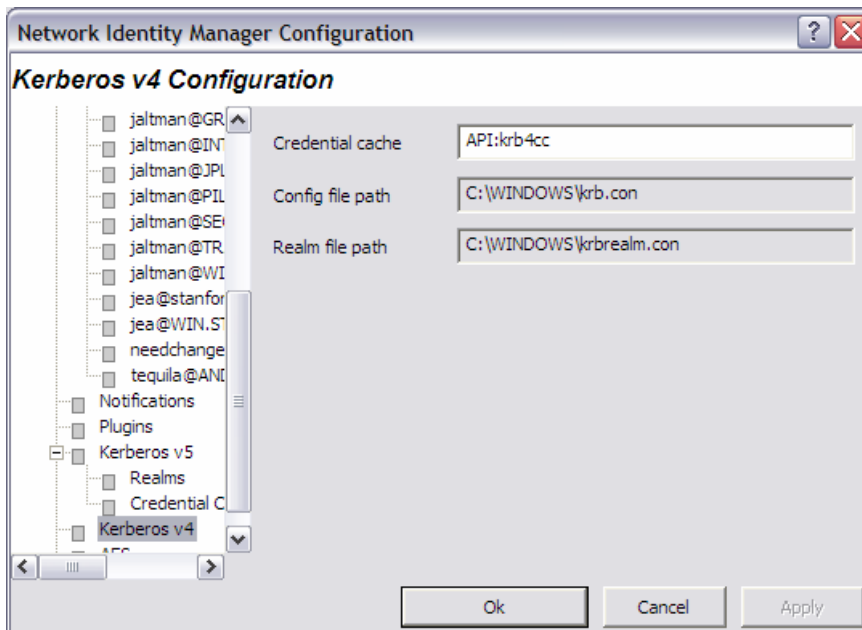
The Kerberos Realm Configuration dialog can be used to manage the contents of the [Realms] and [Domain_Realm] sections of the Kerberos v5 configuration file.



The **Kerberos v5 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.

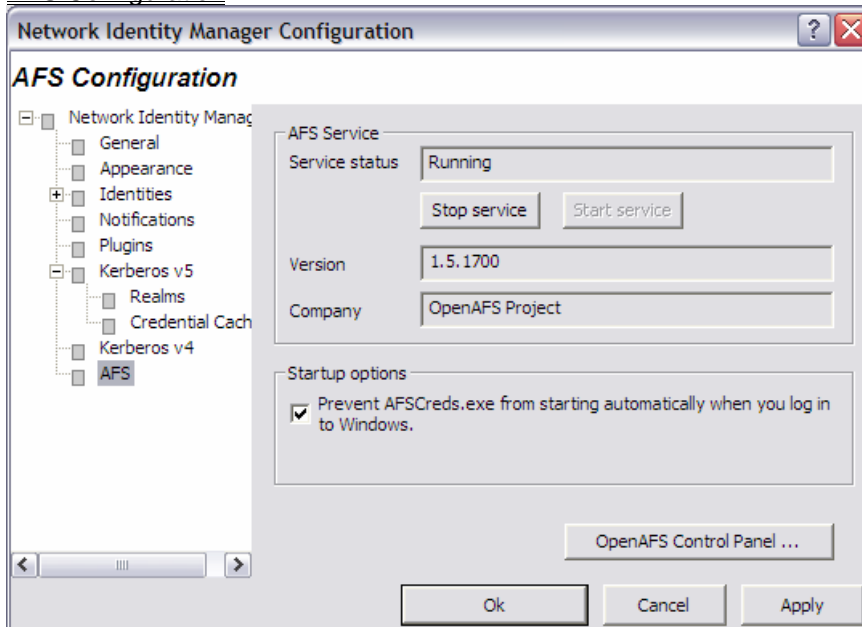
Kerberos v4 Configuration



Here, you can specify the name of the in-memory cache used to store the Kerberos v4 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 v4 configuration files: krb.conf and krbrealm.conf may be viewed from this dialog. The default is to store the configuration files in the Windows directory.

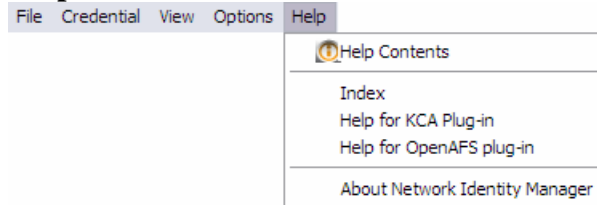
AFS Configuration



The AFS Configuration page is optional and may not appear on all systems. The AFS page can be used to stop and start the AFS Client Service, view the AFS version number and distribution source, and access the AFS Control Panel.

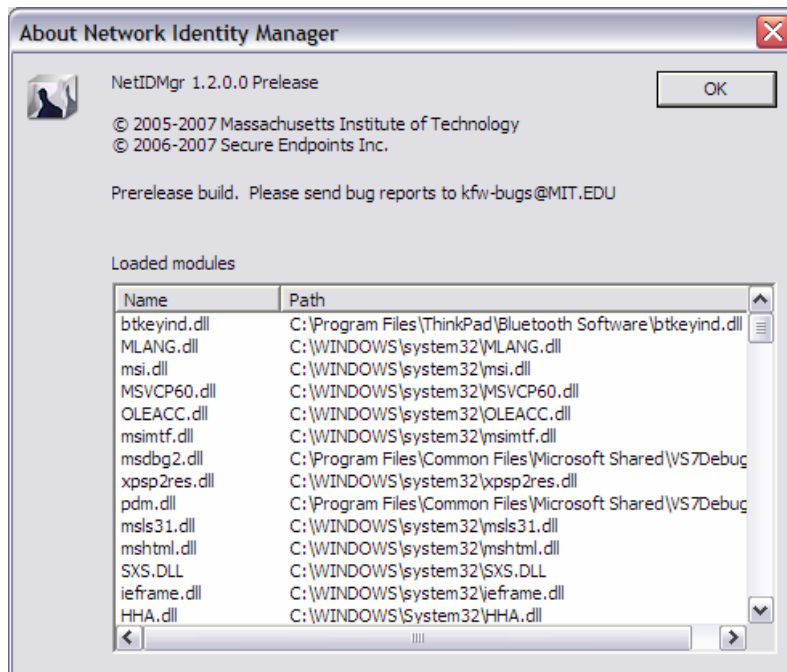
The **Prevent AFSCreds.exe from starting automatically everytime you log in to Windows** feature will disable the use of the AFS Notification Icon application known as afscreds.exe. This feature is required until such time as the NetIdMgr replaces afscreds.exe in the OpenAFS distribution.

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.





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.

Windows Taskbar Notification Area

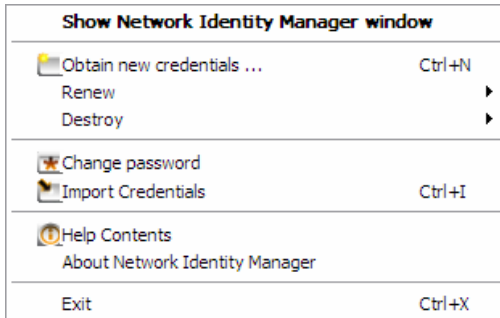
While NetIdMgr is running the  icon will be displayed in the taskbar notification area. Clicking on the icon with the first mouse button will open or close the Network Identity Manager application window or open the Obtain New Credentials dialog based upon the current configuration. The behavior can be adjusted from the Options->General page. Clicking with the second mouse button will display a menu of commands.

 = all credentials are valid

 = some credentials are about to expire

 = some credentials are expired

Taskbar notification area menu



Show Network Identity Manager window

The Show Network Identity Manager window command will restore the Network Identity Manager application window. If the window is already open this option will appear as “Close Network Identity Manager window”.

Obtain new credentials ...

Renew

Destroy

Import Credentials

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 unless the **Destroy all credentials on exit** option is configured. See the Options->General page.

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 1992-2006 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.

Copyright 2006-2007 by Secure Endpoints Inc. All rights reserved.

THIS SOFTWARE IS PROVIDED "AS IS", AND SECURE ENDPOINTS INC. MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, SECURE ENDPOINTS INC. 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.

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 1992-2007 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.

Copyright 2006-2007 by Secure Endpoints Inc. All rights reserved.

THIS SOFTWARE IS PROVIDED "AS IS", AND SECURE ENDPOINTS INC. MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, SECURE ENDPOINTS INC. 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.

Kerberos Export Restrictions and Source Code Access

Copyright (C) 1989-2007 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: Sources and binaries from MIT via authorization form** from the web page <http://web.mit.edu/kerberos/>.

Important notice regarding Kerberos v4 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 v4 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 v4, and the increasingly obvious inadequacy of DES motivates the retirement of the Kerberos v4 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 v4. These flaws permit attacks which require far less effort than an exhaustive search of the DES key space. These flaws make Kerberos v4 cross-realm authentication an unacceptable security risk and raise serious questions about the security of the entire Kerberos v4 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 v4 support began with release 1.3 of MIT Kerberos v5. 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 v4 support (also disabled in the KDC with the default run-time configuration), but we intend to completely remove Kerberos v4 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 v4, except for the eventual removal of all Kerberos v4 functionality. We will continue to provide critical security fixes for Kerberos v4, 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 v5. Kerberos v5 provides significant advantages over Kerberos v4, 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 v5, 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 of Unauthenticated 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>