

Novell Kerberos Login Method for NMASTM

1.0

www.novell.com

QUICK START

Installing and Configuring the Kerberos Login Method for NMASTM

The Kerberos Login method for Novell Modular Authentication Services™ (NMASTM) enables a user to authenticate to eDirectory™ using Kerberos tickets.

This method assumes that you already have a Kerberos KDC running on the network. If you do not have one, you must install and configure a Kerberos KDC (MIT, Microsoft AD, or Heimdal KDC) for this method to work.

The Kerberos Login Method for NMASTM contains the following components:

- ♦ **NMASTM Kerberos Login Server Method (LSM):** Installed on the eDirectory server that has the NMASTM Server already installed.
- ♦ **Novell Kerberos LDAP Extensions:** Installed on all the servers that are used for administering the Kerberos Login Method for NMASTM.
- ♦ **iManager Plug-in for NMASTM Kerberos:** Lets you manage the Kerberos objects and attributes.
- ♦ **NMASTM Kerberos Login Client Method (LCM):** Installed along with the Novell Client™ and NMASTM client on the Windows* workstations. This must be installed on each Windows workstation that will use the Kerberos Login Method for NMASTM.

INSTALLING AND CONFIGURING THE KERBEROS LOGIN METHOD FOR NMASTM

Information for installing and configuring the Kerberos Login Method for NMASTM is provided here. For additional information, including how to create and authorize login sequences, refer to the NMASTM Administration Guide at the *Novell Documentation Web site* (<http://www.novell.com/documentation/lg/nmas23/index.html>).

Prerequisites

You must meet the following prerequisites for installing the Kerberos Login Method for NMASTM:

SERVER MACHINE (FOR INSTALLING NMASTM KERBEROS LSM)

- ♦ One of the following operating systems:

Novell®

- ♦ NetWare® 6 Support Pack 3 or NetWare 6.5 Support Pack 1
- ♦ Red Hat* Linux* 7 or later
- ♦ Red Hat Advanced Server 2.1
- ♦ Solaris* 7, 8, or 9 on Sun* SPARC*
- ♦ SUSE® Linux Enterprise Server 8.1
- ♦ Windows 2000 with Service Pack 3 or 4
- ♦ Windows 2003
- ♦ eDirectory 8.7.1 or 8.7.3
- ♦ NMAS Server 2.2.0 or later

IMANAGER

- ♦ iManager 2.0.1 or later

CLIENT MACHINE (FOR INSTALLING NMAS KERBEROS LCM)

- ♦ Windows* 98 SE, NT 4, 2000, or XP
- ♦ Novell Client™ 4.83 or later
- ♦ NMAS Client 2.1 or later

KDC

- ♦ A Kerberos KDC (MIT, Microsoft AD, or Heimdal KDC) available on the network

For Microsoft AD, you must have the Kerberos tools installed. These tools are part of the Windows installation and can be installed from the \support\tools\setup.exe of the Windows installation CD.

Time Synchronization

You must synchronize the time on the NMAS client machine, the NMAS server machine, and the KDC machine for this method to work. For information on synchronizing network time, refer to *eDirectory 8.7.3 Administration Guide* (<http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/a2iiies.html>).

Installing the Kerberos Login Method for NMAS Components

You must complete the following tasks in the sequence given below to make the Login Method available for use:

- 1 "Installing the NMAS Kerberos LSM" on page 3
- 2 "Installing the Kerberos LDAP Extensions" on page 5

- 3 "Installing the iManager Plug-In for NMAS Kerberos" on page 8
- 4 "Installing the NMAS Kerberos LCM" on page 9

Configuring the Kerberos Login Method for NMAS Components

- 1 "Creating a Service Principal for eDirectory" on page 10
- 2 "Extracting the Key of the Service Principal for eDirectory" on page 11
- 3 "Configuring the Kerberos Login Method for NMAS" on page 12
- 4 "Creating a Login Sequence" on page 15

INSTALLING THE NMAS KERBEROS LSM

You can use one of the following to install the NMAS Kerberos LSM:

- ♦ **The Login Method Installer**

This installer (`methodinstaller.exe`) is a standalone utility that runs on Windows and can be used to locally or remotely install NMAS Login Methods into eDirectory on all supported platforms.

- ♦ **The `nmasinst` utility** (Linux/Solaris)

This utility lets you remotely install NMAS Login Methods into eDirectory from a Linux/Solaris machine. If eDirectory is already installed on the Linux/Solaris machine, the `nmasinst` utility is located in the `/usr/bin` directory.

Installing Using the Login Method Installer

- 1 Double-click `methodinstaller.exe` from the `extracted_folder\NMAS_Kerberos_Method_10`, where `extracted_folder` is the folder where you extracted the `NMAS_Kerberos_Method_10.zip` file.
- 2 Read the Welcome screen, then click Next.
- 3 From the Available Login Methods list, select Kerberos and then click Next.
- 4 Specify the following eDirectory login information:
 - ♦ **User Name:** The name of the administrator or the user with administrator-equivalent rights.
For example, `admin`.
 - ♦ **Password:** The password of the user
 - ♦ **Context:** The context of the user
This must be in the format `ou=sales,o=org`.
 - ♦ **Server:** The domain name or the IP address of the server

- 5 Click Next.
- 6 (Conditional) If your LDAP server requires confidentiality, accept the server's certificate for establishing a secure SSL connection or provide a certificate of your own, and then click Next.
- 7 Read the license agreement, then click Accept > Next.

Review the Login Method information. You can change the name of the Login Method. The method name will be used as the Login Method Object name in eDirectory.
- 8 Click Next.
- 9 Review the Module list, then click Next.
- 10 If you want to create a login sequence that will use the Kerberos Login Method for NMAS, select Create Login Sequence and accept the default name or provide a different name for the login sequence.

If you do not want to create a login sequence, ensure Create Login Sequence is not selected.

NOTE: For the Kerberos Login Method for NMAS to work, you must create a Login Sequence.
- 11 Click Next.
- 12 Review the list of methods that have been successfully installed, then click Finish.

Installing Using the `nmasinst` Utility

IMPORTANT: Before you install a Login Method using the `nmasinst` utility on Linux/Solaris, you must first install NMAS.

For additional information, see the *NMAS Installation Guide* (<http://www.novell.com/documentation/lg/nmas23/index.html>).

- 1 Run the `nmasinst` utility on the server:

```
nmasinst -addmethod admin.context treename config.txt [-h  
hostname[:port]]
```

- ♦ `admin.context`: The admin name and context.
- ♦ `treename`: The name of the eDirectory tree where you are installing the Login Method.
- ♦ `config.txt`: The path to the `config.txt` file of the Login Method you want to install. The `config.txt` for this method is available at `extracted_folder/NMAS_Kerberos_Method_10/Novell/Kerberos`, where `extracted_folder` is the directory where you extracted the `NMAS_Kerberos_Method_10.zip` file.
- ♦ `hostname`: The name or IP address of the server on which this Login Method is to be configured.
- ♦ `port`: The server port.

For example, `nmasinst -addmethod admin.org mytree extracted_folder/NMAS_Kerberos_Method_10/Novell/Kerberos/config.txt`

NOTE: If the Login Method already exists, `nmasinst` will update it.

INSTALLING THE KERBEROS LDAP EXTENSIONS

Kerberos LDAP Extensions provide the functionality to manage Kerberos keys.

PREREQUISITE

Before installing the Kerberos LDAP Extensions on NetWare or Windows, you must install the LDAP libraries for C. For more information, refer to <http://developer.novell.com/ndk/cldap.htm> (<http://developer.novell.com/ndk/cldap.htm>).

Based on where the Kerberos LDAP Extensions must be installed, complete one of the following procedures:

- ♦ “Installing the Kerberos LDAP Extensions on NetWare” on page 5
- ♦ “Installing the Kerberos LDAP Extensions on Windows” on page 6
- ♦ “Installing the Kerberos LDAP Extensions on Linux/Solaris” on page 7

Installing the Kerberos LDAP Extensions on NetWare

The Kerberos LDAP Extensions can be installed from a Windows machine to a remote NetWare machine. You must map the SYS: volume on the NetWare machine to a drive on the Windows machine that you are installing the Kerberos LDAP Extensions from.

- 1 Double-click `Krbldapext_Install.exe` at `extracted_folder\NMAS_Kerberos_Method_10\Novell\Kerberos\Kerberos_Ldap_Extensions\NetWare`, where `extracted_folder` is the directory where you extracted the `NMAS_Kerberos_Method_10.zip` file.
- 2 Read the Welcome screen, then click Next.
- 3 Browse to select the drive that is mapped to the SYS volume of the NetWare machine.

To map a drive, in Windows Explorer, click Tools > Map Network Drive, select the drive on the Windows machine that is to be mapped, and then specify the SYS: volume on the remote NetWare machine as `\\NetWare_machine\sys:` (where `NetWare_machine` is the hostname or the IP address of the remote NetWare machine).

- 4 Click Next to specify the following LDAP authentication information:
 - ♦ Bind FDN: The FDN of the administrator or the user with administrator-equivalent rights
This must be in the format `cn=admin,o=org`.
 - ♦ Bind FDN Password: The password of the Bind FDN

- ◆ LDAP Server: The hostname or IP address of the LDAP Server
- ◆ LDAP Server port (optional): The port that the LDAP server is running on
If you do not specify the LDAP server port but specify the trusted root certificate, the default port 636 is used.
- ◆ Trusted Root Certificate (optional): The trusted root certificate filename for SSL bind
If you do not specify the LDAP server port and the trusted root certificate, the default port 389 is used.

For more information, refer to **"Exporting the Trusted Root Certificates"** on page 16.

- 5 Click Next to install the Kerberos LDAP Extensions.
- 6 Click Finish to complete the installation.

IMPORTANT: You must manually refresh the LDAP server for the installation changes to take effect. For more information, refer to the *eDirectory 8.7.3 Administration Guide* (<http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/agqbavu.html#agqbavu>).

Installing the Kerberos LDAP Extensions on Windows

- 1 Double-click Krbldapx_Install.exe at *extracted_folder*\NMA_S_Kerberos_Method_10\Novell\Kerberos\Kerberos_Ldap_Extensions\Windows, where *extracted_folder* is the directory where you extracted the NMA_S_Kerberos_Method_10.zip file.
- 2 Read the Welcome screen, then click Next to specify the following LDAP authentication information:
 - ◆ Bind FDN: The FDN of the administrator or the user with administrator-equivalent rights
This must be in the format cn=admin,o=org.
 - ◆ Bind FDN Password: The password of the Bind FDN
 - ◆ LDAP Server: The hostname or IP address of the LDAP Server
If it is not specified, the name of the local host that Krbldapext_Install.exe is invoked from is used as the default.
 - ◆ LDAP Server port (optional): The port that the LDAP server is running on
If you do not specify the LDAP server port but specify the trusted root certificate, the default port 636 is used.
 - ◆ Trusted Root Certificate (optional): The trusted root certificate filename for SSL bind
If you do not specify the LDAP server port and the trusted root certificate, the default port 389 is used.

For more information, refer to **"Exporting the Trusted Root Certificates"** on page 16.

3 Click Next to install the Kerberos LDAP Extensions.

4 Click Finish to complete the installation.

IMPORTANT: You must manually refresh the LDAP server for the installation changes to take effect. For more information, refer to the *eDirectory 8.7.3 Administration Guide* (<http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/agqbavu.html#agqbavu>).

Installing the Kerberos LDAP Extensions on Linux/Solaris

1 Log in as *root* or root-equivalent user on the machine where you want to install the Kerberos LDAP Extensions for NMAS.

2 Extract the files from the tar file:

- ♦ On Linux: *extracted_folder*/NMAS_Kerberos_Method_10/Novell/Kerberos/Kerberos_Ldap_Extensions/Linux/Linux_ldapx_install.tar.gz
- ♦ On Solaris: *extracted_folder*/NMAS_Kerberos_Method_10/Novell/Kerberos/Kerberos_Ldap_Extensions/Solaris/Solaris_ldapx_install.tar.gz

where *extracted_folder* is the directory where you extracted the NMAS_Kerberos_Method_10.zip file.

3 Execute the *krbldapx_install* script by entering:

```
krbldapx_install -i -D bind_fdn [-w bind_fdn_password]  
[-h ldap_server] [-p port] [-e trusted_root_file]
```

where

- ♦ *bind_fdn* is the FDN of the administrator or the user with administrator-equivalent rights. This must be in the format *cn=admin,o=org*.
- ♦ *bind_fdn_password* is the password of the *bind_fdn*.
- ♦ *ldap_server* is the hostname or IP address of the LDAP server.
- ♦ *port* is the port that the LDAP server is running on.
- ♦ *trusted_root_file* is the trusted root certificate filename for the SSL bind.

For more information on exporting the trusted root certificate, refer to “Exporting the Trusted Root Certificates” on page 16.

NOTE: If you do not specify the *-h* option, the name of the local host that *krbldapx_install* is invoked from is used as the default.

If you do not specify the LDAP server port and the trusted root certificate, the default port 389 is used.

If you do not specify the LDAP server port but specify the trusted root certificate, the default port 636 is used.

- 4 Specify the root directory where Novell eDirectory modules are installed.

If you do not specify a directory, `/usr/lib/nds-modules` is used as the default directory.

If the installation is successful, the LDAP server is restarted and a success message is displayed.


INSTALLING THE IMANAGER PLUG-IN FOR NMAS KERBEROS

- 1 Open the browser.
- 2 Enter the following URL in the address field of the browser window:

```
http://hostname/nps/iManager.html
```

where *hostname* is the server name or IP address of the iManager server where you want to install the iManager plug-in for NMAS Kerberos.

NOTE: In case of problems, ensure that the Tomcat and Web server are configured properly. For information, refer to *iManager 2.0 Administration Guide* (<http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/bnpta1r.html>).

- 3 Specify the username and password to log in to eDirectory, then click Login.
- 4 Click Configure  on the iManager toolbar.
- 5 Click Module Configuration > Install Module Package in the left pane.
- 6 Specify the location of the `kerberosPlugin.npm` file or click Browse to select it.

The plug-in package is located at `extracted_folder\NMAK_Kerberos_Method_10\Novell\Kerberos\plugins`, where *extracted_folder* is the directory where you extracted the `NMAK_Kerberos_Method_10.zip` file. If you have moved the `kerberosPlugin.npm` file to a different location, browse to the location and select it.

- 7 Click Install.

This installation will take a few minutes.

NOTE: An "Unexpected end of part" error may be encountered during module package install when running iManager on a Windows IIS Web server with Tomcat. This is due to a known issue with uploading files through the Tomcat redirector for IIS. To successfully run a module package install, connect to iManager directly through Tomcat (for example, through port 8080).


For example, `http://hostname:8080/nps/iManager.html`

For more information, refer to the *iManager Administration Guide* (<http://www.novell.com/documentation/imanager20/index.html>).

- 8 Restart the iManager server after the `Successfully saved module` message appears.

If you are running iManager in an Unrestricted Access mode (no RBS collection in the tree), skip Steps 9-15.

NOTE: For information on restarting the iManager server, refer to the *iManager 2.0 Administration Guide* (<http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/bnpta1r.html>).

- 9 Log in to iManager, then click the Configure .
 - 10 Click RBS Configuration > Configure iManager in the left pane.
 - 11 (Conditional) If you have already created an RBS collection, select Upgrade collections and then click Next > Next.
 - 12 (Conditional) If you do not have an RBS collection, do the following:
 - 12a Select Create a new collection, then click Next.
 - 12b Select the container under which you want to create the Role Based services, then click Next.
 - 13 Select the Novell Kerberos plug-in, assign a scope (tree name or any desired container), then click Start to complete the iManager plug-in for NMAS Kerberos configuration.
- NOTE:** This will assign supervisor rights to the selected scope for the Kerberos Management role.
- 14 Wait for the Completed message, then click Close.
 - 15 Refresh the page.

The Kerberos Management role is displayed on the left pane.

If the Kerberos Management role is not displayed, restart the iManager server as mentioned in [Step 8 on page 8](#).

NOTE: If the iManager server is running on a Windows Web Services (IIS), you must have an RBS collection created before installing the iManager plug-in for NMAS Kerberos.

INSTALLING THE NMAS KERBEROS LCM

Before installing the NMAS Kerberos LCM, you must do the following:

- ♦ Install Novell Client 4.83 or later, if it is not already installed. If you have Novell Client 4.9 Support Pack 1a installed, it automatically installs the NMAS Client 2.3 also. For information on downloading the Novell Client, go to the [Novell Download Web site](http://download.novell.com) (<http://download.novell.com>).

For more information on installing the Novell Client, refer to the [Novell Client online documentation](http://www.novell.com/documentation/lg/noclienu/index.html) (<http://www.novell.com/documentation/lg/noclienu/index.html>).

- ♦ Install NMAAS Client 2.1 or later, if it is not already installed. For more information on installing the NMAAS Client, refer to the [NMAAS online documentation \(http://www.novell.com/documentation/lg/nmas23/index.html\)](http://www.novell.com/documentation/lg/nmas23/index.html).

To install and set up the NMAAS Kerberos LCM:

- 1 Double-click clientsetup.exe from *extracted_folder\NMAAS_Kerberos_Method_10\Novell\Kerberos\client*, where *extracted_folder* is the directory where you extracted the NMAAS_Kerberos_Method_10.zip file.
- 2 Read the Welcome screen, then click Next.
- 3 Accept the License Agreement.
- 4 Select the Installation folder where the client method is to be installed, then click Next.
Browse to select the installation folder or create a new folder.
- 5 Select the check box if you want to retain the Novell Credential Cache.

IMPORTANT:

- ♦ The advantage of retaining the Novell credential cache is that the Kerberos tickets acquired during eDirectory login can be populated to other clients' cache.
 - ♦ The Novell credential cache is a file cache and retaining this cache poses a security risk.
- 6 Click Next.
 - 7 Click Finish to complete the installation.

For more information on various features supported by this method, refer to the **"Supported Features"** section on page 10 of the *Kerberos Login Method for NMAAS Administration Guide*.

CREATING A SERVICE PRINCIPAL FOR eDIRECTORY

You must create a service principal for eDirectory in the same Kerberos realm as the users that use the Kerberos Login Method for NMAAS in order to log in to both eDirectory and KDC (to access the eDirectory services and the Kerberized services). This can be done with the help of your Kerberos administrator.

Use the Kerberos Administration tool that is available with your KDC to create the eDirectory Service principal with the encryption type and salt type as DES-CBC-CRC and Normal respectively.

The name of the principal must be novledir/*TREENAME@REALMNAME*.

NOTE: The *TREENAME* in novledir/*TREENAME@REALMNAME* must be in uppercase.

For example, if you are using MIT KDC, execute the following command:

```
kadmin:addprinc -e des-cbc-crc:normal novledir/MYTREE@MYREALM
```

For example, if you are using Heimdal KDC, execute the following command:

```
kadmin -l  
kadmin> add --random-key novledir/MYTREE@MYREALM
```

To delete the unsupported encryption types for the service principal, execute the following command:

```
kadmin> del_etype novledir/MYTREE@MYREALM des-cbc-md4  
kadmin> del_etype novledir/MYTREE@MYREALM des-cbc-md5  
kadmin> del_etype novledir/MYTREE@MYREALM des3-cbc-sha1
```

where *MYTREE* is the treename and *MYREALM* is the Kerberos realm.

EXTRACTING THE KEY OF THE SERVICE PRINCIPAL FOR EDIRECTORY

Use the Kerberos Administration tool that is available with your KDC to extract the key of the eDirectory service principal created in the ["Creating a Service Principal for eDirectory"](#) on [page 10](#) and store it in the local file system. This can be done with the help of your Kerberos administrator.

For example, if you are using an MIT KDC, execute the following command:

```
kadmin: ktadd -k /directory_path/keytabfilename -e des-cbc-crc:normal  
novledir/MYTREE@MYREALM
```

For example, if you are using Microsoft KDC, create a user novledirMYTREE in Active Directory and then execute the following command:

```
ktpass -princ novledir/MYTREE@MYREALM -mapuser novledirMYTREE -pass  
mypassword -out MYTREE.keytab
```

This command maps the principal (novledir/*MYTREE@MYREALM*) to the user account (novledirMYTREE), sets the host principal password to mypassword, and extracts the key into the *MYTREE.keytab* file.

For example, if you are using Heimdal KDC, execute the following command:

```
kadmin> ext_keytab -k /directory_path/keytabfilename novledir/  
MYTREE@MYREALM
```

where *keytabfilename* is the name of the file that contains the extracted key, *MYTREE* is the treename, and *MYREALM* is the Kerberos realm.

CONFIGURING THE KERBEROS LOGIN METHOD FOR NMAS

After you install the Kerberos Login Method for NMAS, you must use iManager to configure it. The iManager server must have the plug-in for NMAS Kerberos installed, and the LDAP server that is used to administer must have the Kerberos LDAP Extensions installed.

NOTE: All Kerberos information collected from your Kerberos administrator is case-sensitive and must be specified exactly in the same case.

To configure the Kerberos Login Method for NMAS, do the following:

- 1 The iManager plug-in for NMAS Kerberos will not work if iManager is not configured to use SSL/TLS connection to eDirectory. A secure connection is mandated to protect the realm's master key and principal keys.

By default, iManager is usually configured for SSL/TLS connection to eDirectory. If you want to configure the Kerberos Login Method for NMAS on a tree other than the one that hosts the iManager configuration, you need to configure iManager for SSL/TLS connection to eDirectory.

For information on configuring iManager with SSL/TLS connection to eDirectory, refer to the *iManager 2.0 Administration Guide* (<http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html#bow4dv4>).

- 2 Complete the following procedures:
 - ♦ "Extending the Kerberos Schema" on page 12
 - ♦ "Creating a New Realm Object" on page 13
 - ♦ "Creating a New KDC Service Object" on page 13
 - ♦ "Creating a Service Principal Object in eDirectory" on page 14

Extending the Kerberos Schema

- 1 In iManager, click Kerberos Management > Extend Schema to open the Extend Schema page.
- 2 If the schema has not already been extended, click OK to extend the schema.

If the schema has been extended, a message is displayed with the status. Click Close.

NOTE: This will automatically update your eDirectory schema with the Kerberos object classes and attributes as defined in the *kereberos.ldif* file located at the *extracted_folder\NMA_S_Kerberos_Method_10\Novell\Kerberos*, where *extracted_folder* is the directory where you extracted the *NMA_S_Kerberos_Method_10.zip* file.

Creating a New Realm Object

1 In iManager, click Kerberos Management > New Realm to open the New Realm page.

2 Specify a name for the Kerberos realm that is to be created.

The realm name must be the same as the one with which you want to configure this Login Method and must conform to the RFC 1510 conventions.

3 Specify a master password for the realm and confirm the password.

4 Select the key type that is to be used for generating the master key for this realm.

The available key types are DES-CBC-CRC, DES-CBC-MD5, and DES3-CBC-MD5.

The default is DES3-CBC-MD5.

5 Specify the encryption types for this realm.

5a Select the supported encryption types.

5b Select the default encryption type.

The available encryption types are DES-CBC-CRC, DES-CBC-MD5, and DES3-CBC-MD5.

The default value is DES-CBC-CRC.

NOTE: The selected default encryption type must be present in the Supported Encryption type list.

6 Specify the subtree you want the Kerberos realm to be configured with or use the Object Selector icon to select it.

This is the FDN of the subtree or the container that contains the eDirectory service principals of this realm. This subtree is not applicable to user principals (**Foreign Principal names**).

If you do not select a subtree or a container, the root of the tree is used as the default.

7 Specify the scope of the subtree search.

- ♦ One-level: Searches the immediate subordinates of the realm subtree.
- ♦ Subtree: Searches the entire subtree starting with, and including the realm subtree.


8 Specify the KDC service that serves this realm or use the Object Selector icon to select it.

NOTE: If you have not created any KDC Service Object, leave this field blank. You can create one using **"Creating a New KDC Service Object" on page 13** and associate it with this realm. This will automatically update the KDC service entry for this realm.

9 Click OK.

Creating a New KDC Service Object

1 In iManager, click Kerberos Management > New KDC Service to open the New KDC Service page.

- 2 Specify a name for the KDC service that is to be created.
This will represent the KDC service in eDirectory.
- 3 Specify the name of the container where the KDC service is to be created or use the Object Selector icon to select it.
- 4 Specify the host servers.
 - 4a Click Add  to open the Host server entry pop-up window.
 - 4b Specify the DNS name or IP address of the server that hosts the KDC service.
 - 4c Specify the port number of the server.
If it is not specified, the default port 88 is used.
 - 4d Select the protocol for the host server.
The default is UDP.
 - 4e Click OK to add the host server entry.
- 5 Specify the FDN of the Kerberos realm object or use the Object Selector icon to select it.
- 6 Click OK.

Creating a Service Principal Object in eDirectory

You must create a Kerberos service principal with the same name (novledir/
TREENAME@REALMNAME) as specified in ["Creating a Service Principal for eDirectory" on page 10](#).

BEST PRACTICE

Service principals for eDirectory must be readily accessible to all servers enabled for Kerberos Login Method for NMAS. If these eDirectory service principals are not created under the Kerberos Realm container inside the Security container, we strongly recommend that you create the container that contains these eDirectory service principals as a separate partition, and that the container be widely replicated.

- 1 In iManager, click Kerberos Management > New Principal to open the New Principal page.
- 2 Specify the name of the principal that is to be created.
The principal name must be in the format novledir/*TREENAME@REALMNAME*.
- 3 Specify the name of the container where the Principal object is to be created or use the Object Selector icon to select it.
- 4 Specify the name of the realm.
If you have already specified the realm name in Step 2, leave this field blank.

5 Do either of the following:

- ◆ Specify the keytab filename or click Browse to select the location where the keytab file is stored.

This is the file that contains the key extracted in “Extracting the Key of the Service Principal for eDirectory” on page 11.


- ◆ Specify the password and confirm the password and then select the encryption type and salt type combination.

The password and encryption type/salt type combination must be the same as those specified while creating the service principal in the KDC database.


6 Click OK.

MANAGING THE NMAS KERBEROS USERS

Using iManager, you can add Kerberos principal names to the eDirectory users.

- 1 Click Kerberos Management > Edit Foreign Principals to open the Edit Foreign Principals page.
- 2 Specify the FDN of a valid User object or use the Object Selector icon to select the User object reference.
- 3 Click OK.
- 4 Specify the foreign principal names and click Add .

A principal name must be in the format *principalname@REALMNAME*.

To delete a foreign principal name, select the name and click Delete .

5 Click OK.

CREATING A LOGIN SEQUENCE

See the *NMAS 2.3 Administration Guide* (<http://www.novell.com/documentation/lg/nmas23/index.html>) for information on creating a login sequence.

AUTHORIZING LOGIN SEQUENCES FOR USERS

See the *NMAS Administration Guide* (<http://www.novell.com/documentation/lg/nmas23/index.html>) for information on authorizing a login sequence for users.

ADDITIONAL INFORMATION

Setting a Password for the Kerberos Service Principal

If the eDirectory service principal key has been reset in your KDC, you must update the key for

this principal in eDirectory also.

For information on extracting the key, refer to [“Extracting the Key of the Service Principal for eDirectory” on page 11.](#)

For information on updating the key for this principal, refer to [“Setting a Password for the Kerberos Service Principal” on page 22 of the *Kerberos Login Method for NMAS Administration Guide.*](#)

Error Messages

The Kerberos LSM error messages are displayed in the Directory Services Trace (DSTrace) or NMASTMon (on NetWare only). The error messages are prefixed with NMASKRB.

For example,

NMAS: 0: NMASKRB: Unable to accept the context from the *eDirectory user FDN.*

To capture an NMAS trace using iMonitor, DSTTRACE.NLM and NMASTMON.NLM, refer to *How to capture an NMAS Server trace* (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10092261.htm>).

Exporting the Trusted Root Certificates

- 1 In iManager, click eDirectory Administration > Modify Object to open the Modify Object page.
- 2 Select Single Object, then specify the name of the server certificate object.
- 3 Click OK.
- 4 Click the Certificates tab, then select Trusted Root Certificate and view the details of the certificate.
- 5 Click Export to launch the Certificate Export Wizard.
- 6 Select the option button, depending on whether you want to export the private key or not, then click Next.
- 7 Select the File in binary DER format, then click Next.
- 8 Click Save the exported certificate to a file to save the certificate.
- 9 After you save the certificate to a file, click Close.

Copyright© 2004 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher. Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. eDirectory, NetWare Loadable Module and NLM, NMAS, and Novell Client are trademarks of Novell, Inc. SUSE is a registered trademark of SUSE LINUX AG, a Novell company.

All third-party trademarks are the property of their respective owners. A trademark symbol (®, TM, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark.