AUTHORIZED DOCUMENTATION

Remote Loader Guide

Novell®
Identity Manager

3.6

July 23, 2008

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide contains detailed information about the Remote Loader. It explains how and when you use the Remote Loader as part of your Identity Manager solution. It also contains configuration and management information for the Remote Loader.

Audience

This guide is intended for Identity Manager administrators, partners, and consultants.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Remote Loader Guide*, visit the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36/).

Additional Documentation

For documentation on Identity Manager, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36/index.html).

Documentation Conventions

In Novell® documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Remote Loader Overview

1

Identity Manager has an additional feature that extends Identity Manager functionality across applications. It is called the Remote Loader, and it allows the driver to access the application without having the Identity Vault and the Metadirectory engine installed on the same server as the application. As part of the planning process when installing Identity Manager, you need to decide if you are going to use the Remote Loader or not. This section defines what the Remote Loader is and contains instructions for installing and configuring the Remote Loader.

There are two different ways to configure the installation of the Metadirectory engine. Figure 1-1 illustrates the first way. It shows that the Identity Vault, Metadirectory engine, and the driver shim all are installed and running on the same server. The driver shim is configured to communicate with the application and the Metadirectory engine.

Figure 1-1 *All Components Installed on the Same Server*

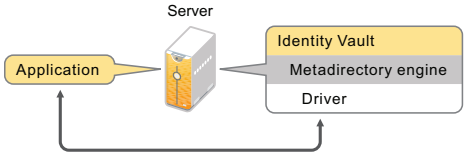
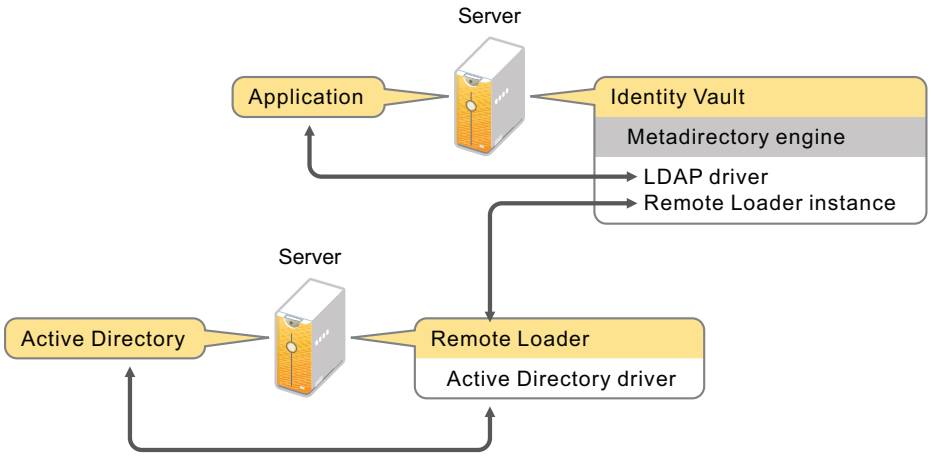


Figure 1-2 illustrates both configurations. The LDAP driver is installed on the same server as the Metadirectory engine and the Identity Vault. The Active Directory* driver is installed on different servers with the Remote Loader. The Remote Loader allows the driver to access the application without having the Identity Vault and Metadirectory engine installed on that same server.

Figure 1-2 *A System Using the Remote Loader*



The Remote Loader enables the Metadirectory engine to exchange data with the Identity Vault as different processes and in different locations, including the following:

- **As a separate process on the server where the Metadirectory engine is running:** The Metadirectory engine runs as part of an eDirectory™ process. The Identity Manager drivers can run on the server where the Metadirectory engine is running. In fact, they can run as part of the same process as the Metadirectory engine.

  However, for strategic reasons and to simplifying troubleshooting, you might want the Identity Manager driver to run as a separate process on the server.

  If the driver is running as a separate process, the Remote Loader provides a communication channel between the Metadirectory engine and the driver.
- **On a server that is not running the Metadirectory engine:** Some of the Identity Manager drivers are unable to run where the Metadirectory engine is running. The Remote Loader enables you to run the Metadirectory engine in one environment while running an Identity Manager driver on a server in a different environment. For example, you cannot run the Active Directory driver on a NetWare® server. The Metadirectory engine can run on the NetWare server while the Remote Loader runs on an Active Directory server.
  - **Scenario: Separate Servers.** The Metadirectory engine is running on a NetWare server. You need to run the Identity Manager Driver for Active Directory. This driver is unable to run on a NetWare server because it must run in an Active Directory environment. You install and run the Remote Loader on a Windows 2003 server. The Remote Loader provides a communication channel between the Active Directory driver and the Metadirectory engine.
  - **Scenario: Non-Host.** The Metadirectory engine is running on Solaris*. You need to communicate with a NIS system where you want to provision user accounts. That system usually doesn't host the Metadirectory engine. You install the Remote Loader and the Identity Manager Driver for NIS on the NIS system. The Remote Loader on the NIS system runs the NIS driver and enables the Metadirectory engine and the NIS driver to exchange data.

Novell® recommends that you use the Remote Loader configuration for use with your drivers where possible. Use the Remote Loader even in cases where the connected system is on the same server as the Metadirectory engine. The following benefits occur by running the driver with the Remote Loader configuration:

- eDirectory is protected from any exceptions encountered by the driver shim.
- It improves the performance of the server running the Metadirectory engine, by offloading driver commands to the remote application or database.
- It allows you to run additional drivers on the server where the Metadirectory engine is not installed.

Installing the Remote Loader

2

The Remote Loader can be installed as a 32-bit application or a 64-bit application. The installation program detects the type of OS that is installed and then installs the corresponding version of the Remote Loader. For the installation instructions, see “Installing the Remote Loader” in the *Identity Manager 3.6 Installation Guide*.

Configuring the Remote Loader

3

The Remote Loader uses shims to communicate with the application. A shim is the file or files that contains the code to processes the events that are synchronizing between the Identity Vault and the application.

The Remote Loader can host the Identity Manager application shims contained in `.dll`, `.so`, or `.jar` files. The Java* Remote Loader hosts only Java driver shims. It won't load or host a native (C++) driver shim.

Configuring the Remote Loader is a two-step process; the Remote Loader requires configuration and the Driver object requires configuration. There are different configuration steps depending on if you are using Windows or Linux\UNIX.

3.1 Configuring the Remote Loader on Windows

You can configure the driver on Windows through a graphical utility called the Remote Loader Console utility or from the command line.

The Remote Loader Console utility enables you to manage all Remote Loader instances for Identity Manager drivers running on the Windows server. The utility is installed during the installation of Identity Manager.

If you are upgrading, the Console detects and imports existing instances of the Remote Loader. (To be automatically imported, driver configurations must be stored in the Remote Loader directory, typically `c:\novell\remoteloader`.) You can then use the Console to manage the remote drivers.

1. Double-click the *Remote Loader Console* icon on the desktop to launch the Remote Loader Console.

   The Remote Loader Console allows you to start, stop, add, remove, and edit each instance of a Remote Loader.
2. Click *Add* to add a Remote Loader instance of your driver on this server.
3. Use the information in the following table to configure the Remote Loader instance for your driver.

Headings	Description
Description	Specify a description to identify the Remote Loader instance in the Remote Loader Console utility.

Headings	Description
Driver	Select the Java class name for the driver. If you are using the Active Directory driver, select *ADDriver.dll*. Table A-2 on page 40 contains a list of all of the Java class names for each driver.
Config File	Specify the name of the configuration file. The Remote Loader Console places configuration parameters into this text file and uses those parameters when it runs.
Communications	◆ **IP Address:** Specify the IP address where the Remote Loader listens for connections from the Metadirectory server. ◆ **Connection Port - Metadirectory Server:** Specify the TCP port on which the Remote Loader listens for connections from the Metadirectory server. The default TCP/IP port for this connection is 8090. With each new instance you create, the default port number automatically increases by one. ◆ **Command Port - Local host communication only:** Specify the TCP port number where a Remote Loader listens for commands such as Stop and Change Trace Level. Each instance of the Remote Loader that runs on a particular computer must have a different command port number. The default command port is 8000. With each new instance you create, the default port number automatically increases by one. **NOTE:** By specifying different connection ports and command ports, you can run multiple instances of the Remote Loader on the same server, hosting different driver instances.
Remote Loader Password	Specify the Remote Loader password. This password is used to control access to a Remote Loader instance for a driver. It must be the same case-sensitive password specified in the *Enter the Remote Loader Password* field on the Identity Manager driver configuration page. It is important that this password be difficult to guess and be different from the driver object password.
Driver Object Password	Specify the Driver Object password. The Remote Loader uses this password to authenticate to the Metadirectory server. It must be the same case-sensitive password specified in the *Driver Object Password* field on the Identity Manager driver configuration page. It is important that this password be difficult to guess and be different from the Remote Loader password.
Secure Socket Layer (SSL)	◆ **Use an SSL Connection:** You should always select this option. It is used to encrypt the transfer of data between the Remote Loader and the Metadirectory server. ◆ **Trusted Root File:** This is the exported self-signed certificate from the eDirectory™ tree's Organization Certificate Authority. For more information, see Section 3.4, "Creating a Secure Connection," on page 23.

Headings	Description
Trace File	◆ **Trace Level:** Specify a trace level greater than zero to display a trace window that contains informational messages from both the Remote Loader and the driver. The most common setting is trace level 3. If the trace level is set to 0, the trace window is not displayed. ◆ **Trace File:** Specify a trace filename where trace messages are written. Each Remote Loader instance running on a particular machine must use a different trace file. Trace messages are written to the trace file only if the trace level is greater than zero. ◆ **Maximum Disk Space Allowed for all Trace Logs (Mb):** Specify the approximate maximum size that the trace file for this instance can occupy on disk. **NOTE:** Use the tracing options only for troubleshooting issues. Having the tracing enabled reduces the performance of the Remote Loader. Do not leave the tracing enabled in production.
Establish a Remote Loader service for this driver instance	Select this option if you want the Remote Loader established as a service. When this option is enabled, the operating system automatically starts the Remote Loader when the computer starts.

4 Specify the advanced configuration parameters. To do so:

4a Click Advanced to display the Advanced Configuration dialog box.

4b Modify the following settings as desired.

Parameter	Description
Classpath	Additional paths for the JVM to search for package (.jar) and class (.class) files. Using this parameter is the same as using the java -classpath command. When entering multiple class paths, separate them with a semicolon (;) for a Windows JVM and a colon (:) for a UNIX/Linux JVM.
JVM Options	The options used when starting the JVM instance of the driver.
Heap size	The initial and maximum heap size for the JVM instance.

4c Click *OK*, to save the advanced configuration information.

5 Click *OK* to save the configuration file.

If you need to change any of the parameters:

1 In the Remote Loader Console, select the Remote Loader instance from the *Description* column.

2 Click *Stop*, type the Remote Loader password, then click *OK*.

3 Click *Edit*, then modify the configuration information. See Step 3 on page 13 and Step 4 on page 15 for a description of each parameter.

4 Click *OK* to save the changes.

3.2 Configuring the Remote Loader for Linux\UNIX by Creating a Configuration File

For the Remote Loader to run, it requires a configuration file (for example, `LDAPShim.txt`). Windows is the only platform that provides a GUI interface to create this file. You can also create or edit a configuration file by using command line options. The following steps provide information on basic parameters for the configuration file. For information on additional parameters, see Appendix A, "Options for Configuring a Remote Loader," on page 33.

1 To create a configuration file, open a text editor.

2 (Optional) Specify a description by using the `-description` option.

Option	Secondary Name	Parameter	Description

-description	-desc	short description	Specify a short description string (for example, SAP) to be used for the trace window title and for Novell® Audit logging.
			
			Example:
			
			`-description SAP`
			`-desc SAP`
			
			The Remote Loader Console places long forms in the configuration files. You can use either a long form (for example, -description) or a short form (for example, -desc).

3 Specify a TCP/IP port that the Remote Loader instance will use by using the -commandport option.

Option	Secondary Name	Parameter	Description

-commandport	-cp	port number	Specifies the TCP/IP port that the Remote Loader instance uses for control purposes. If the Remote Loader instance is hosting an application shim, the command port is the port on which another Remote Loader instance communicates with the instance that is hosting the shim. If the Remote Loader instance is sending a command to an instance that is hosting an application shim, the command port is the port on which the hosting instance is listening. If a port is not specified, the default command port is 8000. Multiple instances of the Remote Loader can run on the same server, hosting different driver instances by specifying different connection ports and command ports.
			
			Example:
			
			`-commandport 8001`
			`-cp 8001`

4 Specify the parameters for the connection to the Metadirectory server running the Identity Manager remote interface shim by using the -connection option.

Use the format `-connection "`*`parameter`* `[parameter] [parameter]"`.

For example, type one of the following:

```
-connection "port=8091 rootfile=server1.pem"
-conn "port=8091 rootfile=server1.pem"
```

All the parameters must be included within quotation marks. Parameters include the following:

Option	Secondary Name	Parameter	Description

-connection	-conn	connection configuration string	Specifies the connection parameters for the connection to the Metadirectory server running the Identity Manager remote interface shim. The default connection method for the Remote Loader is TCP/IP using SSL. The default TCP/IP port for this connection is 8090. Multiple instances of the Remote Loader can run on the same server. Each instance of the Remote Loader hosts a separate Identity Manager application shim instance. Differentiate multiple instances of the Remote Loader by specifying different connection ports and command ports for each Remote Loader instance.
			
			Example:
			
			`-connection "port=8091 rootfile=server1.pem"`
			`-conn "port=8091 rootfile=server1.pem"`

Option	Secondary Name	Parameter	Description
port		decimal port number	A required parameter. It specifies the TCP/IP port on which the Remote Loader listens for connections from the remote interface shim. Example: `port=8090`

address		IP address	An optional parameter. Specifies that the Remote Loader listens on a particular local IP address. This is useful if the server hosting the Remote Loader has multiple IP addresses and the Remote Loader must listen on only one of the addresses.
			You have three options:
			`address=address number`
			`address='localhost'`
			`Don't use this parameter`
			If you don't use the address, the Remote Loader listens on all local IP addresses.
			Example:
			`address=137.65.134.83`

fromaddress	None	IP address	The Remote Loader only accepts connections from the specified IP address. Any other connections are not allowed.
			Example:
			`--conn "port=8092 fromaddress=10.0.0.2"`
			or
			`-connect "port=8094 fromaddress=metaserver1.company.com "`

handshaketimeout	None	number of milliseconds	Increases the time out period of the handshake between the Remote Loader and the Metadirectory engine. Example: `-connection "port=8091 handshaketimeout=1000"` The value can be some integer greater than or equal to zero. Zero means never time out. The non-zero number is the number of milliseconds for the time out to occur. The default value is 1000 milliseconds.

Option	Secondary Name	Parameter	Description
rootfile			A conditional parameter. If you are running SSL and need the Remote Loader to communicate with a native driver, use `rootfile='trusted certname'`

keystore			Conditional parameter. Used only for the Identity Manager application shims contained in `.jar` files.
			
			Specifies the filename of the Java keystore that contains the trusted root certificate of the issuer of the certificate used by the remote interface shim. This is typically the Certificate Authority of the eDirectory tree that is hosting the remote interface shim.
			
			If you are running SSL and need the Remote Loader to communicate with a Java driver, use a key-value pair:
			
			`keystore='keystorename'`
			`storepass='password'`

storepass		storepass	Used only for the Identity Manager application shims contained in `.jar` files. Specifies the password for the Java keystore specified by the keystore parameter. Example: `storepass=mypassword` This option applies only to the Java Remote Loader.

5 (Optional) Specify a trace parameter by using the -trace option.

Option	Secondary Name	Parameter	Description

-trace	-t	integer	Specifies the trace level. This is only used when hosting an application shim. Trace levels correspond to those used on the Metadirectory server.
			
			Example:
			
			`-trace 3`
			`-t 3`

6 (Optional) Specify a trace file by using the -tracefile option.

Option	Secondary Name	Parameter	Description

-tracefile	-tf	filename	Specify a file to write trace messages to. Trace messages are written to the file if the trace level is greater than zero. Trace messages are written to the file even if the trace window is not open.
			
			Example:
			
			`-tracefile c:\temp\trace.txt`
			`-tf c:\temp\trace.txt`

7 (Optional) Limit the size of the trace file by using the -tracefilemax option.

Option	Secondary Name	Parameter	Description

-tracefilemax	-tfm	size	Specifies the approximate maximum size that trace file data can occupy on disk. If you specify this option, there will be a trace file with the name specified using the tracefile option and up to 9 additional “roll-over” files. The roll-over files are named using the base of the main trace filename plus *_n*, where n is 1 through 9.
			
			The size parameter is the number of bytes. Specify the size by using the suffixes K, M, or G for kilobytes, megabytes, or gigabytes.
			
			If the trace file data is larger than the specified maximum when the Remote Loader is started, the trace file data remains larger than the specified maximum until roll-over is completed through all 10 files
			
			Example:
			
			`-tracefilemax 1000M`
			`-tfm 1000M`
			
			In this example, the trace file can be only 1 GB.

8 Specify the class by using the -class option, or specify the module by using the -module option.

Option	Secondary Name	Parameter	Description

-class	-cl	Java class name	Specifies the Java class name of the Identity Manager application shim that is to be hosted.
			
			For example, for a Java driver, use one of the following:
			
			`-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
			`-cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
			
			Java uses a keystore to read certificates. The -class option and the -module option are mutually exclusive.
			
			To see a list of the Java class names see Table A-2 on page 40.

-module	-m	modulename	Specifies the module containing the Identity Manager application shim that is to be hosted.
			
			For example, for a native driver, type one of the following:
			
			`-module "c:\Novell\RemoteLoader\ADDriver.dll"`
			`-m "c:\Novell\RemoteLoader\ADDriver.dll"`
			
			or
			
			`-module "usr/lib/dirxml/NISDriverShim.so"`
			`-m "usr/lib/dirxml/NISDriverShim.so"`
			
			The `-module` option uses a rootfile certificate. The `-module` option and the `-class` option are mutually exclusive.

9 Name and save the file.

You can change some settings while the Remote Loader is running. See Table 3-1 for a list of some of these settings. For a complete list of these settings, see Appendix A, “Options for Configuring a Remote Loader,” on page 33.

Table 3-1 *Selected Remote Loader Parameters*

Parameter	Description
-commandport	Specifies an instance of the Remote Loader.
-config	Specifies a configuration file.

Parameter	Description
-javadebugport	Specifies that the Remote Loader instance is to enable Java debugging on the specified port.
-password	Specifies the password for authentication.
-service	Installs an instance as a service. Windows only.
-tracechange	Changes the trace level.
-tracefilechange	Changes the name of the trace file being written to.
-unload	Unloads the Remote Loader instance.
-window	Turns the trace window on or off in a Remote Loader instance. Windows only.

3.2.1 Setting Environment Variables on Solaris, Linux, or AIX

After installing the Remote Loader, you can set the environment variable `RDXML_PATH`, which changes the current directory for rdxml. This directory is then taken as the base path for files that are subsequently created. To set the value of the `RDXML_PATH` variable, specify the following commands:

- `set RDXML_PATH=path`
- `export RDXML_PATH`

3.3 Configuring the Identity Manager Drivers for Use with the Remote Loader

You can configure a new driver or enable an existing driver to communicate with the Remote Loader. This section provides general information on configuring drivers so that they communicate with the Remote Loader. For driver-specific information, refer to the relevant driver implementation guide at the Identity Manager Driver Documentation Web page (http://www.novell.com/documentation/idm36drivers/index.html).

When you create a new Driver object in either Designer or iManager, there are additional fields to populate to enable the Remote Loader. You add information to these same fields if you modify an existing driver.

To configure the driver:

1. In the properties of the Driver object, fill in the following fields:

   Driver Module: Select *Connect to Remote Loader*.

   Driver Object Password: The driver object password is used by the Remote Loader to authenticate itself to the Metadirectory server. This password must match the password for the driver object defined on the Remote Loader.

   Remote Loader Connection Parameters: Specify the information required to connect to the Remote Loader. The parameter format is `hostname=`*`xxx.xxx.xxx.xxx`* `port=`*`xxxx`* `kmo=`*`certificatename`*, where `hostname` is the IP address of the Remote Loader server and `port` is the port the Remote Loader is listening on (the default is 8090). The `kmo`

parameter is used only when an SSL connection exists between the Remote Loader and the Metadirectory engine; tt defines the Key Name of the Key Material Object containing the keys and certificate used for SSL.

Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`

Remote Loader Password: Specify the password required for the Metadirectory engine (or Remote Loader shim) to authenticate to the Remote Loader.

2 Define a security-equivalent user, click *Next*, then click *Finish*.

3.4 Creating a Secure Connection

If you plan to use the Remote Loader, the first step is to provide secure data transfer between the Remote Loader and the Metadirectory engine. This requires you to use the Secure Socket Layer (SSL) to setup a connection between the Remote Loader and the Metadirectory engine.

To accomplish this, complete the following tasks:

- Section 3.4.1, "Creating a Server Certificate," on page 23
- Section 3.4.2, "Exporting a Self-Signed Certificate," on page 24
- Section 3.4.3, "Creating a Keystore," on page 25

3.4.1 Creating a Server Certificate

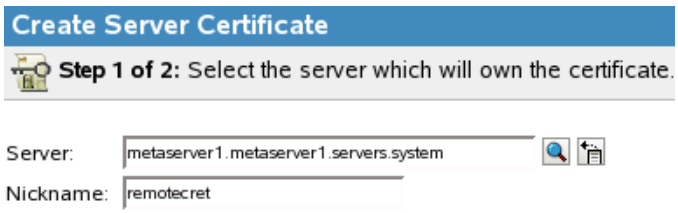
If you are unfamiliar with certificates, it is easy to create a new one.

1 In Novell iManager, click *Novell Certificate Server* > *Create Server Certificate*.

2 Select the server to own the certificate, and give the certificate a nickname (for example, remotecert).

IMPORTANT: We recommend that you don't use spaces in the certificate nickname. For example, use remotecert instead of remote cert.

Also, make a note of the certificate nickname. This nickname is used for the KMO name in the driver's remote connection parameters.



3 Leave the Creation method set to *Standard*, then click *Next*.

4 Review the Summary, click *Finish*, then click *Close*.

You have created a server certificate. Continue with Section 3.4.2, "Exporting a Self-Signed Certificate," on page 24.

3.4.2 Exporting a Self-Signed Certificate

You can export a newly created certificate. Or, if an SSL server certificate already exists and you have experience with SSL certificates, you can use the existing certificate instead of creating and using a new one.

When a server joins a tree, eDirectory creates the following default certificates:

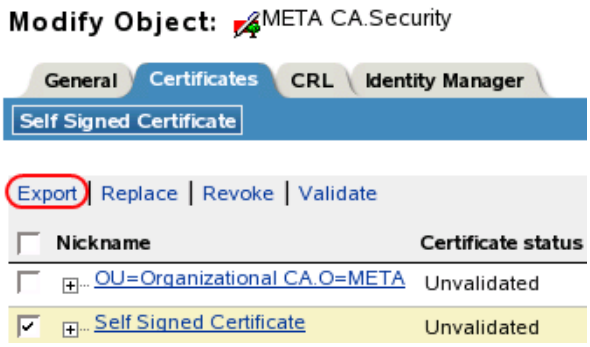
- SSL CertificateIP
- SSL CertificateDNS

1 In iManager, click *eDirectory Administration* > *Modify Object*.

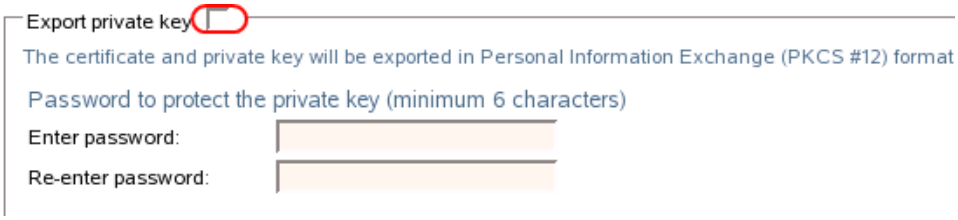
2 Browse to and select the Certificate Authority in the Security container, then click *OK*.

The Certificate Authority (CA) is named after the tree name (Treename-CA.Security).

3 Click the *Certificates* tab, select the *Self-Signed Certificate*, then click *Export*.

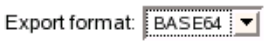


4 In the Export Certificate Wizard, deselect *Export private key*.



You don't want to export the private key with the certificate.

5 Set the export format to *BASE64*, then click *Next*.



IMPORTANT: When the Remote Loader is running on a Windows 2003 R2 SP1 32-bit server, the certificate must be in Base64 format. If you use the DER format, the Remote Loader fails to connect to the Identity Manager engine.

6 Click the link to *Save the exported certificate*, specify a location, then click *Save*.

7 Click *Close*.

3.4.3 Creating a Keystore

A keystore is a Java file that contains encryption keys and, optionally, certificates. If you want to use SSL between the Remote Loader and the Metadirectory engine, and you are using a Java shim, you need to create a keystore file.

- "Keystore on Windows" on page 25
- "Keystore on Solaris, Linux, or AIX" on page 25
- "Keystore on All Platforms" on page 25

Keystore on Windows

On Windows, run the Keytool utility, typically found in the `c:\novell\remoteloader\jre\bin` directory.

Keystore on Solaris, Linux, or AIX

On Solaris, Linux, or AIX environments, use the `create_keystore` file. `Create_keystore` is installed with rdxml. It is located in the *`install_directory`*`/dirxml/bin` directory. The create_keystore file is also included in the `dirxml_jremote.tar.gz` file, found in the `\dirxml\java_remoteloader` directory. The `create_keystore` file is a shell script that calls the Keytool utility.

On UNIX, when the self-signed certificate is used to create the keystore, the certificate can be exported in Base64 or binary DER format.

Enter the following at the command line:

```
create_keystore self-signed_certificate_name keystorename
```

For example, type one of the following

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

The `create_keystore` script specifies a hard-coded password of "dirxml" for the keystore password. This is not a security risk because only a public certificate and public key are stored in the keystore.

Keystore on All Platforms

To create a keystore on any platform, you can enter the following at the command line:

```
keytool -import -alias trustedroot -file self-
signed_certificate_name -keystore filename -storepass
```

The filename can be any name (for example, `rdev_keystore`).

Managing the Remote Loader

4

The Remote Loader is either a service or a daemon. At times the server or daemon must be restarted. The following procedures explain how to start and stop the Remote Loader.

4.1 Starting the Remote Loader

Each platform has a different way to start the Remote Loader.

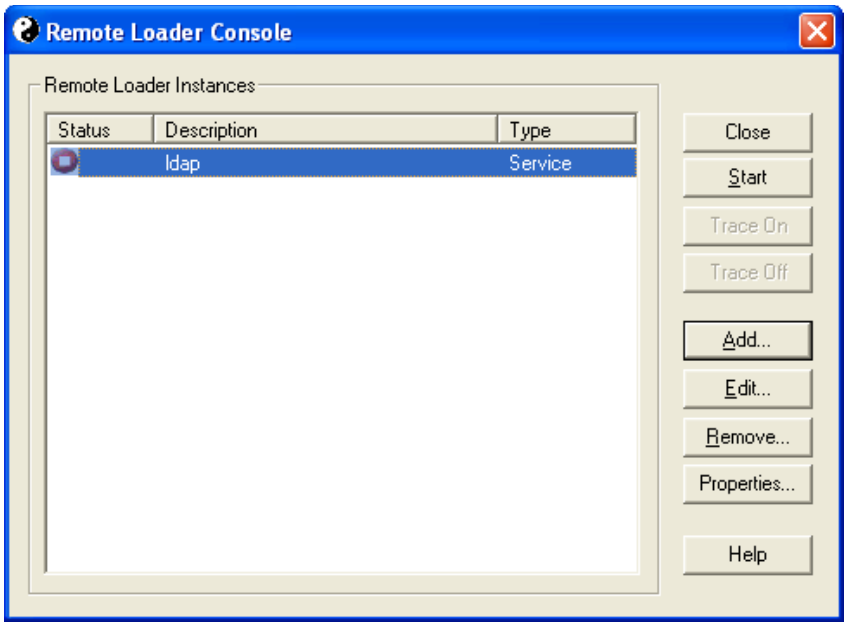
4.1.1 Starting the Remote Loader on Windows

You can start the Remote Loader from the Remote Loader Console icon or from the command line.

Starting from the Remote Loader Console

1 Click the *Remote Loader Console* icon on the desktop.

2 Select a driver instance, then click *Start*.



Starting from the Command Line in Windows

The command line functionality is provided by `dirxml_remote.exe`. By default, it is located in `c:\novell\RemoteLoader\dirxml_remote.exe`.

1. At a command prompt, set the password for the Remote Loader. For password command options, see Table 4-1 on page 29.

   ```
   dirxml_remote -config path_to_config_file -sp password password
   ```

2. Start the Remote Loader.

   ```
   dirxml_remote -config path_to_config_file
   ```

3. Use iManager to start the driver.

4. Confirm that the Remote Loader is working properly.

   The Remote Loader loads the Identity Manager application shim only when the Remote Loader is in communication with the remote interface shim on the Metadirectory server. This means, for example, that the application shim shuts down if the Remote Loader loses communication with the Metadirectory server.

Table 4-1 *Password Command Line Options*

Option	Secondary Name	Parameter	Description

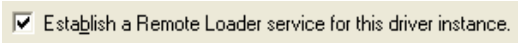
-password	-p	password	Specifies the password for command authentication. This password must be the same as the first password specified with setpasswords for the loader instance being commanded. If a command option (for example, unload or tracechange) is specified and the `password` option isn't specified, the user is prompted to enter the password for the loader that is the target of the command.
			
			Example:
			
			`-password novell4`
			`-p novell4`

-setpasswords	-sp	password password	Specifies the password for the Remote Loader instance and the password of the Identity Manager Driver object of the remote interface shim that the Remote Loader communicates with. The first password in the argument is the password for the Remote Loader. The second password in the optional arguments is the password for the Identity Manager Driver object associated with the remote interface shim on the Metadirectory server. Either no password or both passwords must be specified. If no password is specified, the Remote Loader prompts for the passwords. This is a configuration option. Using this option configures the Remote Loader instance with the passwords specified but doesn't load an Identity Manager application shim or communicate with another loader instance.
			
			Example:
			
			`-setpasswords novell4 staccato3`
			`-sp novell4 staccato3`

4.1.2 Auto-Starting the Remote Loader

To auto-start the Remote Loader on a Windows platform, see Step 9 in Section 3.1, "Configuring the Remote Loader on Windows," on page 13.

Select *Establish a Remote Loader service for this driver instance* if you want the Remote Loader as a service.



When this option is enabled, the operating system automatically starts the Remote Loader when the computer starts.

To auto-start the Remote Loader on a Linux platform, place your configuration file in `/etc/opt/novell/dirxml/rdxml`. Your Remote Loader instance starts automatically when the computer starts

4.1.3 Starting the Remote Loader on Solaris, Linux, or AIX

On Solaris, Linux, or AIX, the binary component rdxml provides the Remote Loader functionality. The default location of this component is in the `/usr/bin/` directory.

1 Set the password for the Remote Loader. For command password options, see Table 4-1 on page 29.

Platform	Command
Solaris LInux AIX	`rdxml` -config *path_to_config_file* -sp *password password*
HP-UX* AS/400* OS/390* z/OS	`dirxml_jremote` -config *path_to_config_file* -sp *password password*

2 Start the Remote Loader.

Platform	Command
Solaris LInux AIX	`rdxml` -config *path_to_config_file*
HP-UX AS/400 OS/390 z/OS	`dirxml_jremote` -config *path_to_config_file*

3 Use iManager to start the driver.

4 Confirm that the Remote Loader is operating properly.

The Remote Loader loads the Identity Manager application shim only when the Remote Loader is in communication with the remote interface shim on the Metadirectory server. This means, for example, that the application shim shuts down if the Remote Loader loses communication with the Metadirectory server.

For Linux, Solaris, or AIX, use the `ps` command or a trace file to find out whether the command and connection ports are listening.

For HP-UX and similar platforms, monitor the Java Remote Loader by using the `tail` command on the tracefile:

```
tail -f trace filename
```

If the last line of the log shows the following, the loader is successfully running and awaiting connection from the Identity Manager remote interface shim:

```
TRACE: Remote Loader: Entering listener accept()
```

To configure the Remote Loader (rdxml) to start automatically on UNIX, see TID 10097249 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097249.htm).

4.2 Stopping the Remote Loader

Each platform has a different way to stop the Remote Loader. Table 4-2 contains the instructions for each platform.

Table 4-2 *How to Stop the Remote Loader*

Platform	Command
Windows	Use the Remote Loader Console to stop a driver instance.
Solaris LInux AIX	`rdxml -config path_to_config_file -u`
HP-UX AS/400 OS/390 z/OS	`dirxml_jremote -config path_to_config_file -u`

If multiple instances of the Remote Loader are running on the computer, pass the `-cp` *command port* option so that the Remote Loader can stop the appropriate instance.

When you stop the Remote Loader, you must have sufficient rights or specify the Remote Loader password. For example, the Remote Loader is running as a Windows service. You have sufficient rights to stop it. You enter a password, but realize that it is incorrect. The Remote Loader stops anyway, because the Remote Loader isn't "accepting" the password. Instead, it is ignoring the password because the password is redundant in this case. If you run the Remote Loader as an application rather than as a service, the password is used.

Options for Configuring a Remote Loader

A

The options in the following table enable you to configure a Remote Loader.

Table A-1 *Remote Loader Options*

Option	Secondary Name	Parameter	Description
address		IP address	An optional parameter. Specifies that the Remote Loader listens on a particular local IP address. This is useful if the server hosting the Remote Loader has multiple IP addresses and the Remote Loader must listen on only one of the addresses. You have three options: address=*address number* address='localhost' Don't use this parameter. If you don't use the address, the Remote Loader listens on all local IP addresses. Example: `address=137.65.134.83`

-class	-cl	Java class name	Specifies the Java class name of the Identity Manager application shim that is to be hosted.
			
			For example, for a Java driver, use one of the following:
			
			`-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
			
			`-cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
			
			Java uses a keystore to read certificates. The -class option and the -module option are mutually exclusive.
			
			To see a list of the Java class names see Table A-2 on page 40.

Option	Secondary Name	Parameter	Description

-commandport	-cp	port number	Specifies the TCP/IP port that the Remote Loader instance uses for control purposes. If the Remote Loader instance is hosting an application shim, the command port is the port on which another Remote Loader instance communicates with the instance that is hosting the shim. If the Remote Loader instance is sending a command to an instance that is hosting an application shim, the command port is the port on which the hosting instance is listening. If it is not specified, the default command port is 8000. Multiple instances of the Remote Loader can run on the same server hosting different driver instances by specifying different connection ports and command ports.
			
			Example:
			
			`-commandport 8001`
			
			`-cp 8001`

-config	None	filename	Specifies a configuration file. The configuration file can contain any command line options except the config option. Options specified on the command line override options specified in the configuration file. Example: `-config config.txt`

-connection	-conn	connection configuration string	Specifies the connection parameters for the connection to the Metadirectory server running the Identity Manager remote interface shim. The default connection method for the Remote Loader is TCP/IP using SSL. The default TCP/IP port for this connection is 8090. Multiple instances of the Remote Loader can run on the same server. Each instance of the Remote Loader hosts a separate Identity Manager application shim instance. Differentiate multiple instances of the Remote Loader by specifying different connection ports and command ports for each Remote Loader instance.
			
			Example:
			
			`-connection "port=8091 rootfile=server1.pem"`
			
			`-conn "port=8091 rootfile=server1.pem"`

Option	Secondary Name	Parameter	Description

-description	-desc	short description	Specify a short description string (for example, SAP) to be used for the trace window title and for Novell® Audit logging.
			
			Example:
			
			`-description SAP`
			
			`-desc SAP`
			
			The Remote Loader Console places long forms in the configuration files. You can use either a long form (for example, -description) or a short form (for example, -desc).

fromaddress	None	IP address	The Remote Loader only accepts connections from the specified IP address. Any other connections are not allowed.
			
			Example:
			
			`--conn "port=8092 fromaddress=10.0.0.2"`
			
			or
			
			`-connection "port=8094 fromaddress=metaserver1.company.com"`

handshaketimeout	None	number of milliseconds	Increases the time out period of the handshake between the Remote Loader and the Metadirectory engine. Example: `-connection "port= 8093 handshaketimeout=1000"` The value can be some integer greater than or equal to zero. Zero means never time out. The non-zero number is the number of milliseconds for the time out to occur. The default value is 1000 milliseconds.

-help	-?	None	Displays help.
			
			Example:
			
			`-help`
			
			`-?`

-java	-j	None	Specifies that the passwords are to be set for a Java shim instance. This option is only useful in conjunction with the setpasswords option. If -class is specified with -setpasswords, this option isn't necessary.

Option	Secondary Name	Parameter	Description

-javadebugport	-jdp	Port number	Specifies that the Remote Loader instance is to enable Java debugging on the specified port. This is useful for developers of the Identity Manager application shims.
			
			Example:
			
			`-javadebugport 8080`
			
			`-jdp 8080`

keystore			Conditional parameters. Used only for Identity Manager application shims contained in `.jar` files.
			
			Specifies the filename of the Java keystore that contains the trusted root certificate of the issuer of the certificate used by the remote interface shim. This is typically the Certificate Authority of the eDirectory™ tree that is hosting the remote interface shim.
			
			If you are running SSL and need the Remote Loader to communicate with a Java driver, use a key-value pair:
			
			`keystore='keystorename'`
			
			`storepass='password'`

-module	-m	modulename	Specifies the module containing the Identity Manager application shim that is to be hosted.
			
			For example, for a native driver, use one of the following:
			
			`-module "c:\Novell\RemoteLoader\Exchange5Shim.dll"`
			
			`-m "c:\Novell\RemoteLoader\Exchange5Shim.dll"`
			
			or
			
			`-module "usr/lib/dirxml/NISDriverShim.so"`
			
			`-m "usr/lib/dirxml/NISDriverShim.so"`
			
			The -module option uses a rootfile certificate. The -module option and the -class option are mutually exclusive.

Option	Secondary Name	Parameter	Description

-password	-p	password	Specifies the password for command authentication. This password must be the same as the first password specified with the setpasswords option for the Remote Loader instance being commanded. If a command option (for example, unload or tracechange) is specified and the password option isn't specified, the user is prompted to enter the password for the loader that is the target of the command.
			
			Example:
			
			`-password novell4`
			
			`-p novell4`

port		decimal port number	A required parameter. It specifies the TCP/IP port on which the Remote Loader listens for connections from the remote interface shim. Example: `port=8090`
rootfile			A conditional parameter. If you are running SSL and need the Remote Loader to communicate with a native driver, use `rootfile='trusted certname'`

-service	-serv	None, or install/ uninstall	To install an instance as a service, use the install argument together with any other arguments necessary to host an application shim. For example, the arguments used must include -module, but any argument can include -connection, -commandport, and so forth.
			
			This option installs the Win32 service but doesn't start the service.
			
			To uninstall an instance running as a service, use the uninstall argument together with any other arguments necessary to host the application shim.
			
			The no-argument version of this option is only used on the command line to an instance being run as a Win32* service. This is automatically set up when installing an instance as a service.
			
			Example:
			
			`-service install`
			
			`-serv uninstall`
			
			This option isn't available on rdxml or the Java Remote Loader.

Option	Secondary Name	Parameter	Description

-setpasswords	-sp	password password	Specifies the password for the Remote Loader instance and the password of the Identity Manager Driver object of the remote interface shim that the Remote Loader communicates with. The first password in the argument is the password for the Remote Loader. The second password in the optional arguments is the password for the Identity Manager Driver object associated with the remote interface shim on the Metadirectory server. Either no password or both passwords must be specified. If no password is specified, the Remote Loader prompts for the passwords. This is a configuration option. Using this option configures the Remote Loader instance with the passwords specified but doesn't load a Identity Manager application shim or communicate with another loader instance.
			
			Example:
			
			`-setpasswords novell4 staccato3`
			
			`-sp novell4 staccato3`

storepass		storepass	Used only for Identity Manager application shims contained in .jar files. Specifies the password for the Java keystore specified by the keystore parameter. Example: `storepass=mypassword` This option applies only to the Java Remote Loader.

-trace	-t	integer	Specifies the trace level. This is only used when hosting an application shim. Trace levels correspond to those used on the metadirectory server.
			
			Example:
			
			`-trace 3`
			`-t 3`

-tracechange	-tc	integer	Commands a Remote Loader instance that is hosting an application shim to change its trace level. Trace levels correspond to those used on the metadirectory server.
			
			Example:
			
			`-tracechange 1`
			
			`-tc 1`

Option	Secondary Name	Parameter	Description

-tracefile	-tf	filename	Specify a file to write trace messages to. Trace messages are written to the file if the trace level is greater than zero. Trace messages are written to the file even if the trace window is not open.
			
			Example:
			
			`-tracefile c:\temp\trace.txt`
			
			`-tf c:\temp\trace.txt`

-tracefilechange	-tfc	None, or filename	Commands a Remote Loader instance that is hosting an application shim to start using a trace file, or to close one already in use and use a new one. Using the no-argument version of this option causes the hosting instance to close any trace file being used.
			
			Example:
			
			`-tracefilechange c:\temp\newtrace.txt`
			
			`tfc c:\temp\newtrace.txt`

-tracefilemax	-tfm	size	Specifies the approximate maximum size that trace file data can occupy on disk. If you specify this option, there is a trace file with the name specified using the tracefile option and up to 9 additional “roll-over” files. The roll-over files are named using the base of the main trace filename plus *_n*, where n is 1 through 9.
			
			The size parameter is the number of bytes. Specify the size by using the suffixes K, M, or G for kilobytes, megabytes, or gigabytes.
			
			If the trace file data is larger than the specified maximum when the Remote Loader is started, the trace file data remains larger than the specified maximum until roll-over is completed through all 10 files
			
			Example:
			
			`-tracefilemax 1000M`
			
			`-tfm 1000M`
			
			In this example, the trace file can be only 1 GB.

-unload	-u	None	Unloads the Remote Loader instance. If the Remote Loader is running as a Win32 Service, this command stops the service.
			
			Example:
			
			`-unload`
			
			`-u`

Option	Secondary Name	Parameter	Description

-window	-w	On/Off	Turns the trace window on or off in a Remote Loader instance.
			
			Example:
			
			`-window on`
			
			`-w off`
			
			This option is available only on Windows platforms. It isn't available on the Java Remote Loader.

-wizard	-wiz	None	Launches the Configuration Wizard. Running `dirxml_remote.exe` with no command line parameters also launches the wizard. This option is useful if a configuration file is also specified. In this case, the wizard starts with values from the configuration file and the wizard can be used to change the configuration without editing the configuration file directly.
			
			Example:
			
			`-wizard`
			
			`-wiz`
			
			This option is available only on Windows platforms. It isn't available on the Java Remote Loader.

Table A-2 *Java Class Names*

Java Class Name	Driver
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Avaya* PBX Driver
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Delimited Text Driver
com.novell.nds.dirxml.driver.nds.DriverShimImpl	eDirectory Driver
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Entitlements Service Driver
com.novell.gw.dirxml.driver.gw.GWdriverShim	GroupWise® Driver
com.novell.nds.dirxml.driver.jdbc.JDBCDriverShim	JDBC* Driver
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP Driver
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Loopback Driver
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Manual Task Driver
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS Driver
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes Driver
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft* Driver

Java Class Name	Driver
com.novell.nds.dirxml.driver.SAPShim.SAPDriverShim	SAP HR Driver
com.novell.nds.dirxml.driver.sapusershim.SAPDriverShim	SAP User Management Driver
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP Driver
com.novell.idm.driver.ComposerDriverShim	User Application
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Driver for Remedy* ARS
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	WorkOrder Driver
com.novell.idm.drivers.idprovider.IDProviderShim	ID Provider Driver