

Novell Certificate Login

2.0

June 24, 2005

INSTALLATION GUIDE

www.novell.com



Novell®

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.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2005 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, 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 at <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

Novell Certificate Login Installation Guide

June 24, 2005

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Client32 is a trademark of Novell, Inc. in the United States and other countries.

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.

DirXML is a registered trademark of Novell, Inc. in the United States and other countries.

eDirectory is a trademark of Novell, Inc. in the United States and other countries.

NMAS is a trademark of Novell, Inc. in the United States and other countries.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Certificate Server is a trademark of Novell, Inc. in the United States and other countries.

Novell Client is a trademark of Novell, Inc. in the United States and other countries.

Novell Directory Services and NDS are a registered trademarks of Novell, Inc. in the United States and other countries.

Novell SecretStore is a registered trademark of Novell, Inc. in the United States and other countries.

Nsure is a registered trademark of Novell, Inc. in the United States and other countries.

SUSE is a registered trademark of SUSE LINUX AG, a Novell business.

Third-Party Materials

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

1 Overview

This section provides an overview of Novell® Certificate Login (NCL).

Features

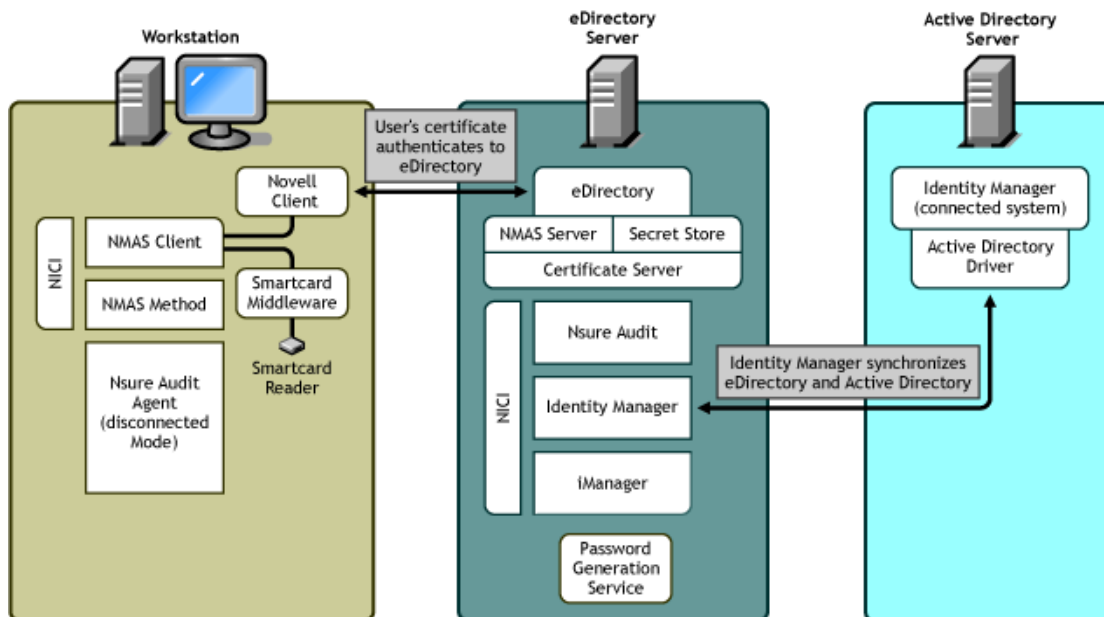
NCL allows users to authenticate to an Active Directory domain using a PKI certificate stored on a smart card. NCL features the Novell Enhanced Smart Card Method (NЕСSM). NCL also includes the Password Generation Service which allows the Active Directory passwords to be changed at regular intervals to a random value, supporting a strong password policy.

The NCL Architecture

The basic solution is made up of three systems:

- ♦ eDirectory™ Server
- ♦ Active Directory Server
- ♦ Workstation

The following graphic details the products and the relationship between the systems.



A workstation, equipped with a smart card reader and middleware, allows a user to authenticate to the eDirectory server using the NMAS™ client and the Novell Enhanced Smart Card Method

(NЕСM). The NЕСM authenticates using a certificate stored on the user’s smart card. Certificate login events are also securely logged for auditing and administrative purposes.

What’s Next

Review [Chapter 2, “Preparing to Install,”](#) on page 7.

2

Preparing to Install

This section describes the minimum requirements that must be met for each machine before starting the installation. It also describes the contents of each CD distributed with this solution.

Minimum Requirements

eDirectory Server

The eDirectory™ server must be running Windows* 2000 Server SP4 or later, or Windows 2003 Server SP1 or later (English versions only).

Active Directory Server

The Active Directory server must be running Windows* 2000 Server SP4 or later, or Windows 2003 Server SP1 or later (English versions only) and must be a domain controller.

Workstations

Each workstation must meet the following minimum requirements:

- ♦ Windows* 2000 Server SP4 or later, Windows 2003 Server SP1 or later, or Windows XP SP2 or later (English versions only) installed.
- ♦ Is a member of the Active Directory server's domain (configured domain user).
- ♦ Smart Card reader is connected and Smart Card middleware is installed.
- ♦ Use supported Smart Cards—NCL supports cards that use PKCS#11 certificates. This release of NCL has been tested with the following cards:
 - ♦ Axalto Access 64K
 - ♦ GemPlus GemXpresso
 - ♦ Oberthur CosmopolIC V4
 - ♦ Schlumberger Access 32K V2

Web Browser

For this release, NCL supports Internet Explorer only.

Contents of Each CD

The NCL software is contained on four CDs. The following table can serve as a reference as you go through the installation of each component.

CD Name	CD Contents
CD 1—NCL Server Components CD	<ul style="list-style-type: none">♦ NCL documentation (NCL Installation Guide, the Readme file, and all product documentation)♦ iManager 2.5 (standard iManager structure, plug-ins, custom utilities, and Web applications)♦ Nsure Audit 1.0.3♦ eDirectory patch IR6 and Security Update (Novell® Modular Authentication Services (NMASTM) 2.3.8 Server and Novell Certificate ServerTM 2.7.7)♦ NCI 2.6.7♦ Novell ClientTM 4.9.1♦ Novell Enhanced Smart Card Method (NЕСM)♦ Novell SecretStore® 3.3.4 - server♦ Password Generation Service♦ Licenses (eDirectory license file, NCI .nfk file, and IDM credential)
CD 2—NCL Client Components CD	<ul style="list-style-type: none">♦ NCL documentation (NCL Installation Guide, the Readme file, and all product documentation)♦ Client Umbrella Install♦ Novell Client 4.9.1♦ Novell Enhanced Smart Card Method (NЕСM)♦ Nsure Audit/Platform Agent 1.0.3
CD 3—eDirectory 8.7.3	The software to install eDirectory 8.7.3
CD 4—Novell Nsure Identity Manager Pro 2.0.1	<ul style="list-style-type: none">♦ AD drivers♦ Standard activation step via the Web

What's Next

Install the eDirectory server by following the instructions in [Chapter 3, “Installing and Configuring the eDirectory Server,”](#) on page 9.

3

Installing and Configuring the eDirectory Server

This section describes how to install and configure the following products needed on the eDirectory Server:

1. [NICI \(page 9\)](#)
2. [Novell Client 4.9.1 \(page 10\)](#)
3. [eDirectory 8.7.3 \(page 10\)](#)
4. [iManager 2.5 \(page 11\)](#)
5. [Identity Manager 2.0 Server \(page 12\)](#)
6. [SecretStore 3.3.4 \(page 15\)](#)
7. [eDirectory IR6 Patch \(page 15\)](#)
8. [Novell Enhanced Smart Card Method \(NЕСM\) - Server Component \(page 15\)](#)
9. [Nsure Audit \(page 16\)](#)
10. [Password Generation Service \(page 17\)](#)

IMPORTANT: These products must be installed in the order specified.

This section also describes the following post-install tasks:

- ♦ [Enable New iManager Plug-ins \(page 19\)](#)
- ♦ [Configure Auditing for the Novell Enhanced Smart Card Method \(NЕСM\) \(page 20\)](#)

Minimum Requirements

- ☐ The eDirectory™ server must be running Windows* 2000 Server SP4 or later, or Windows 2003 Server SP1 or later (English versions only).
- ☐ You must be authenticated as Administrator or a user with equivalent rights on the Windows server.

Installation Procedure

Install the eDirectory™ server components *in the order they are presented in this section*. Each section lists the product to install and which CD the product is on.

NICI

CD: NCL Server Components - CD 1

Location: \nici

- 1 Run wcniciu0.exe.

- 2 Follow the installation wizard to completion.

Novell Client 4.9.1

CD: NCL Server Components - CD 1

Location: \novellclient\winnt\i386

- 1 Run setupnw.exe.
- 2 Select Typical Installation.
- 3 Follow the installation wizard to completion.
- 4 Reboot the computer when prompted.
- 5 At the Novell® Client™ login screen, select Workstation Only and log in as the local Administrator.

NOTE: On a Windows 2003 server, after you install the Novell Client, the network load balancing service will report a failure on startup. This is not a problem. See [TID 10086698](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086698.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086698.htm>) and [MSKB 833375](http://support.microsoft.com/default.aspx?scid=kb;en-us;833375) (<http://support.microsoft.com/default.aspx?scid=kb;en-us;833375>) for information about turning this service startup failure message off.

eDirectory 8.7.3

CD: eDirectory 8.7.3 - CD 3

Location: \nt

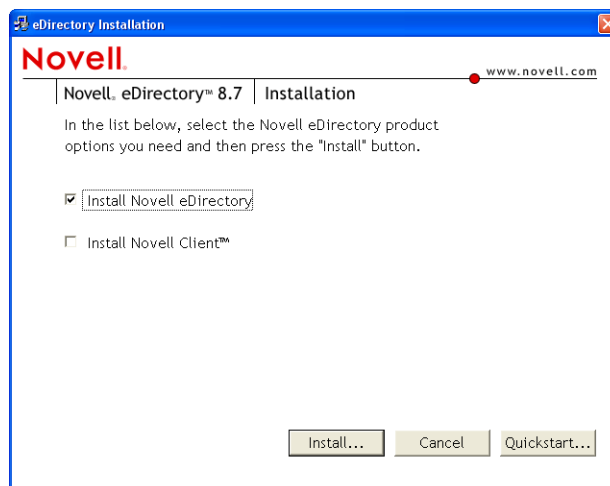
eDirectory License Installation

- 1 Copy the \license directory on CD 1 to a local drive.

You will point to this \license directory later in the eDirectory installation.

- 2 Insert the eDirectory 8.7.3 CD (CD 3) into the CD-ROM drive.

The eDirectory installation should auto-launch. If it does not, run setup.exe in the \nt directory. The following screen should appear:



- 3 Select Install eDirectory, then click Install.
Do not install Novell Client.

- 4** Accept the license agreement.
- 5** Install the licenses from a file.
 - 5a** Browse to the local copy of the \license directory that you created in **Step 2**.
 - 5b** Select the license file (.nfk file).

After the licenses are installed, the eDirectory installation continues.

eDirectory Installation

- 1** Accept the license agreement.
- 2** Accept the default installation path (c:\novell\nds).
- 3** Create a new eDirectory Tree.
- 4** Fill in values for Tree name, Server object context, Admin name, Admin context, and password.

Example values:

Tree Name:	NCL-TREE
Server Object Context:	NCL-eDir.ncl
Admin Name:	Admin
Admin Context:	ncl
Password:	ncl-test

NOTE: The server object context and the admin context should normally be the same. The above example uses ncl.

You should write down these values so you can reference them later.

- 5** Accept the defaults for the HTTP stack ports.
- 6** Accept the defaults for the LDAP ports.

If the eDirectory server is being installed on a Windows 2000 AD Domain Controller, you must change the ports to avoid a conflict with the AD LDAP server. We recommend changing the ports to 390 for clear text and 637 for SSL/TLS.

- 7** Clear all the NMAST[™] methods.

The Novell Enhanced Smart Card Method (NЕСM) will be installed in a separate step.

- 8** Click Finish to complete the installation.

iManager 2.5

CD: NCL Server Components - CD 1

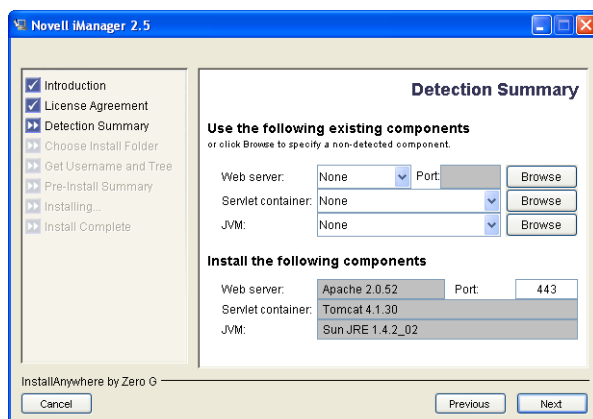
Location: \imanager\installs\win

IMPORTANT: If you are running IIS on your server, you must remove it before running the iManager installation. Also, iManager is a Java-based utility. You may need to decrease your Internet Explorer security settings to use it.

- 1** Run imanagerinstall.exe.

- 2 Accept the license agreement.
- 3 Configure iManager to use the following:

Web Server:	Apache
Servlet Container:	Tomcat
JVM:	Sun* JRE



- 4 Accept the default installation folder.
- 5 Enter the Tree name and Admin username.

Previous example values:

Tree Name:	NCL-TREE
Admin Name:	admin.ncl

- 6 Complete the installation.

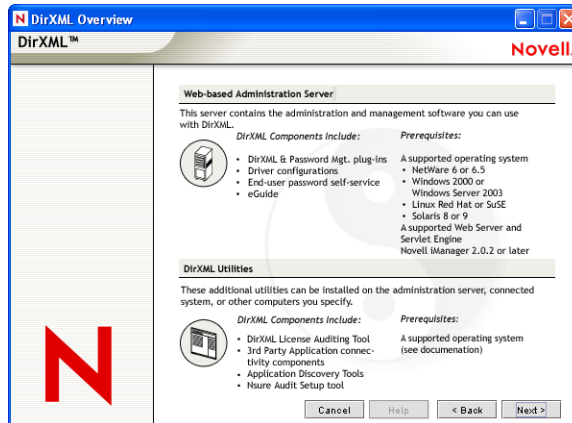
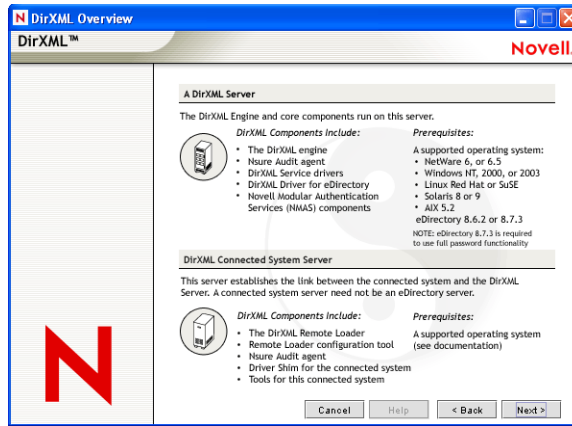
NOTE: When logging in to iManager, use the fully distinguished Admin user DN (for example, admin.ncl). If the tree can't be located, use the IP address or DNS name of the eDirectory server.

Identity Manager 2.0 Server

CD: Novell Nsure Identity Manager Pro 2.0.1 - CD 4

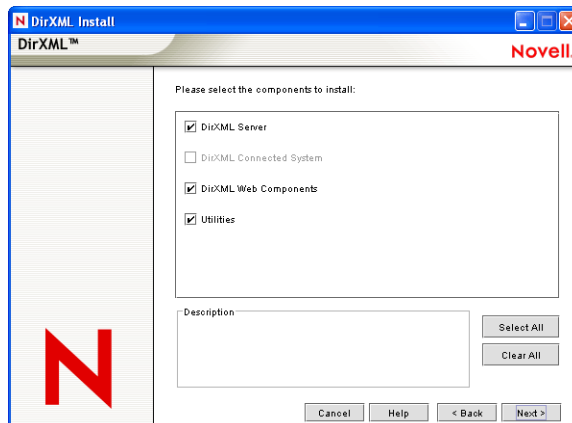
Location: \nt

- 1 (Conditional) If the installation does not auto-launch, run install.exe located in the \nt directory on CD 4.
- 2 Accept the license agreement.
- 3 Review the Overview pages about the various systems and components.



4 Click Next to begin the installation.

5 Select the following three DirXML components, then click Next:



- ♦ **DirXML Server:** Installs the DirXML[®] engine and service drivers, DirXML drivers, NMAS components, and Nsure Audit agent, and also extends the eDirectory schema.

Select the DirXML engine and the Active Directory driver.

- ♦ **DirXML Web Components:** Installs the DirXML plug-ins, DirXML driver configurations, and Novell eGuide.

- ♦ **Utilities:** Installs the application utilities you select.
- 6** Select the following drivers for the engine installation, deselect all other drivers, then click Next:
 - ♦ DirXML engine
 - ♦ Active Directory driver
 - 7** Click OK on any informational messages.
 - 8** In the Schema Extension page, specify the following:

- ♦ **User Name:** Username (in LDAP format) of a user who has rights to extend the schema
- ♦ **User Password:** The user's password

Previous example values:

Tree Name:	NCL-TREE
User Name:	cn=admin,o=ncl
Password:	ncl-test

- 9** Accept the default Web components:
 - ♦ iManager plug-ins
 - ♦ Driver configurations
- 10** Accept the default utilities:
 - ♦ Application Components
- 11** Accept the default installation location for the utilities.
- 12** Select Active Directory Discovery Tool and deselect all other utilities.
- 13** Click Finish to complete the installation program.

NOTE: You need to activate Identity Manager within 90 days of purchase. For instructions on how to activate Identity Manager, see [“Activating Identity Manager” on page 29](#).

SecretStore 3.3.4

CD: NCL Server Components - CD 1

Location: \secretstore\server\windows

- 1 Run secretstoreserverinstall.exe.
- 2 Install Novell SecretStore® in the same location as eDirectory.
The default location is c:\novell\sss\server.
- 3 Accept the license agreement.
- 4 Accept the default destination folder (c:\novell\nds).
- 5 Enter the eDirectory Admin username and password.

Previous example values:

User DN:	admin.ncl
Password:	ncl-test

eDirectory IR6 Patch

General eDirectory Patch

CD: NCL Server Components - CD 1

Location: \edirectory\interimreleases

- 1 Run edir8736_win32.exe.
- 2 Accept the default installation path (c:\novell\nds)

Security Updates

CD: NCL Server Components - CD 1

Location: \edirectory\securityupdate

- 1 Copy the entire \securityupdate folder to a local drive.
- 2 From the local \securityupdate folder, run .\secupd\nt\install.bat.
Ignore messages about ConsoleOne® not being detected.
- 3 From the local \securityupdate folder, run .\nmsrv238\mmaswin\install.bat.

NOTE: The local copy of the \securityupdate folder is not needed after installation.

Novell Enhanced Smart Card Method (NЕСM) - Server Component

CD: NCL Server Components - CD 1

Location: \nmasmethods

- 1 Run methodinstaller.exe.
- 2 Select the Novell Enhanced Smart Card method.
- 3 Enter the eDirectory login information.

Previous example values:

User Name:	Admin
Password:	ncl-test
Context:	ncl
Server:	127.0.0.1 Port 636

- 4** Accept the SSL certificate information.
- 5** Accept the license agreement.
- 6** Accept the NESCM details.
- 7** Accept the default NMAS sequence name.
- 8** Accept the default iManager plug-in location.

Nsure Audit

CD: NCL Server Components - CD 1

Location: \nsureaudit\windows

- 1** Run naudit_win32.exe.
- 2** Accept the license agreement.
- 3** Accept the defaults for the username and company information.
- 4** Accept the default destination folder.
- 5** Select the full installation.
- 6** Accept the default loop back address for the logging server.
- 7** Enter the eDirectory Admin information when prompted.

Previous example values:

User Name:	admin.ncl
Password:	ncl-test

- 8** Accept the default log server name.
- 9** Reboot the computer when prompted.
- 10** After installing Nsure Audit, import the schemata if you want to use the advanced query and reporting options.

You'll get an error if you try to access the advanced options before importing the schemata.

- 10a** Click Start > Programs > Nsure Audit > Reporting Application.
- 10b** From the main menu, select File > Import > Application Schemata.
- 10c** Specify the server name and IP address of the eDirectory server, then click OK.

The license takes effect the next time the application is started.

Password Generation Service

CD: NCL Server Components - CD 1

Location: \passwordgenerationservice

Prerequisite Procedure

Before installing the Password Generation Service, you must first extend the eDirectory schema by doing the following:

1 Copy the passwordgenerationservice.sch file located on CD 1 in the \passwordgenerationservice\schema directory to a location on your hard drive.

2 Click Start > Settings > Control Panel.

3 Double-click Novell eDirectory Services.

4 Verify that you are on the Services page.

This is the default tab.

5 Select Install.dlm.

6 Click Start.

TIP: The Novell eDirectory Install utility will come up behind the Novell eDirectory Services window.

7 Under the DS Install and Uninstall section, select Install Additional Schema Files (selected by default) and then click Next.

8 When the Authentication window comes up, type your eDirectory Admin name, context and password. Then click OK.

Previous example values:

User Name:	Admin
Context:	ncl
Password:	ncl-test

9 Browse for and select the passwordgenerationservice.sch file that you copied to your local drive.

If the Finish button is not active, copy the passwordgenerationservice.sch file to a different directory and repeat this step.

10 Click Finish.

The schema is now extended.

Installation Procedure

To install the Password Generation Service:

CD: NCL Server Components - CD 1

Location: \passwordgenerationservice

1 Run setup.exe.

2 On the Welcome screen, click Next.

- 3 When you receive a reminder message about manually extending the eDirectory schema. Click OK to close the message.

You already extended the schema in the previous section.

- 4 Specify the Password Generation Policy values.

Password Generation Policy

NCL Password Change

The Password Change service automatically changes user's passwords in the specified Active Directory domain and eDirectory tree, at the specified time, ensuring users can only login using the Novell Certificate Login method.

Directory Information

AD Domain:

eDirectory tree:

eDirectory admin:

Admin password:

Password Change

Change password every: days

Change password at: (ex. 02:00, 23:00)

Password Specifications

Password length: min. max.

Character case:

Repeated characters: max.

Password Special Characters

☐ Allow special characters

min. max.

☐ Password may begin with special characters

☐ Password may end with special characters

☐ Allow Numbers

min. max.

☐ Password may begin with numbers

☐ Password may end with numbers

Disallowed characters:

☐ ! ☐ *

☐ \$ ☐ ?

☐ % ☐ #

☐ > ☐ ^

☐ @ ☐ <

☐ %

OK Cancel

Make sure the policy does not contain conflicting rules.

A conflicting policy would be as follows:

Min Password Length = 10

Max Password Length = 20

Minimum Numeric Characters = 25

- 5 Click OK > Finish.

Post-Install Procedure

After you have the Password Generation Service installed and running, you need to give the service rights to log on to the Active Directory Domain.

- 1 Click Start > Settings > Control Panel > Administrative Tools > Services.
- 2 Right-click PasswordGenerationService, then click Properties.
- 3 Click the LogOn tab.

- 4** Select This Account.
- 5** Click the browse button and select your Active Directory Domain/Administrator user.
- 6** Type the password, then retype the password where instructed to do so.
- 7** Click Apply, then click OK.
- 8** Restart the PasswordGenerationService.
You have to restart the service before changes take effect.
- 9** (Optional) Check the passwordgen.log file in the \system32 directory to make sure the service was started correctly.

For information on using the Password Generation Service plug-in and command line utilities, see [“Using the Password Generation Service” on page 50](#).

Post-install Tasks

Complete the following post-installation tasks:

Enable New iManager Plug-ins

- 1** Launch iManager.
- 2** Click the Configure icon.
- 3** Add the password generation service plug-in to the Available plug-in list.
 - 3a** Click New.
 - 3b** Browse for and select the pcs.npm file located on CD 1 in the \passwordgenerationservice\plugin directory.
 - 3c** Click OK.
- 4** Install the NCL plug-ins
 - 4a** Click Module to select all available modules or select just the NCL modules listed below:
 - ♦ ncl.npm
 - ♦ sharedcontentv1.npm
 - ♦ naudit.npm
 - ♦ pcs.npm
 - 4b** Click Install.
- 5** Close iManager.
- 6** Restart Tomcat by either rebooting the server or doing the following:
 - 6a** Click Start > Settings > Control Panel.
 - 6b** Double-click Administrative tool > Services.
 - 6c** Right-click Tomcat, then click Restart.

Configure Auditing for the Novell Enhanced Smart Card Method (NЕСM)

- 1** Launch iManager.

- 2** Under Roles and Tasks, click Auditing and Logging > Logging Server Options.
- 3** Specify the Logging Server object name, then click OK.
You created this object during the Nsure Audit install.
- 4** Click the Log Applications tab.
- 5** Check the Applications check box > New Log Application.
- 6** Type a name for the log application name (for example: ncl).
- 7** Import the nsureaudit.lsc file located on CD 1 into the \nmasmethods\novell\nclsmartcard directory.

Optional Configuration

Client Configuration

Hide the Last Known User

You can edit the registry and change a setting so that Windows does not display the last user who authenticated. Change the following setting to the value indicated:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\
system
```

```
REG_DWORD
```

```
dontdisplaylastusername=1
```

What's Next

Install the Active Directory Server by following the instructions in [Chapter 4, “Installing and Configuring the Active Directory Server,”](#) on page 21.

4

Installing and Configuring the Active Directory Server

This section describes how to install and configure all components needed on the Active Directory (AD) server.

1. [Installing Identity Manager 2 As a Connected System \(page 21\)](#)
2. [Providing for Secure Data Transfers \(page 22\)](#)
3. [Setting Up Remote Loaders \(page 24\)](#)
4. [Post-Install Tasks \(page 30\)](#)
5. [Optional Configuration \(page 32\)](#)

For more information, see the *Novell Nsure Identity Manager 2.0.1 Administration Guide* located on CD 1 or 2 in the \documentation\idm directory.

Overview

This server will have only Identity Manager 2 (formerly DirXML[®]) installed as a connected system. The DirXML engine runs on a server as part of eDirectory[™]. A DirXML driver shim and its configured driver communicate with an application and with the DirXML engine. A connected system extends DirXML functionality across platforms and requires a Remote Loader. This service enables the DirXML engine to exchange data with DirXML drivers running as different processes and in different locations.

Make a note of the AD server's DNS address. You need this later to add to the workstation's server list. Also, you need to have users added to the domain.

Minimum Requirements

- ❑ The Active Directory server must be running Windows* 2000 Server SP4 or later, or Windows 2003 Server SP1 or later (English versions only), and it must be a domain controller.

Installation Procedure

Installing Identity Manager 2 As a Connected System

Using the Remote Loader involves the following tasks:

1. If you plan to use the Secure Socket Layer (SSL), provide certificates (.b64 format) for secure data transfers.
2. Install, configure, and run the Remote Loader.

3. Import, configure, and start the DirXML driver.

Providing for Secure Data Transfers

If you plan to use the Secure Socket Layer (SSL) so that you can provide secure data transfers, complete the following tasks:

- 1.

Create a server certificate.

If you are unfamiliar with certificates, create a new one.

However, 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.

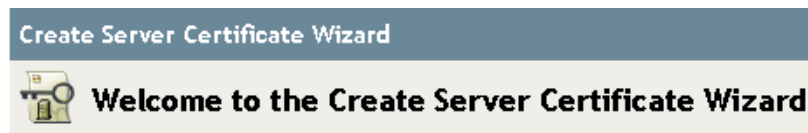
When a server joins a tree, eDirectory creates the following default certificates:

- ♦ SSL CertificateIP
- ♦ SSL CertificateDNS

2. Export a self-signed certificate.

Creating a Server Certificate

- 1 In Novell® iManager, click Novell Certificate Server > Create Server Certificate.



Select the server which will own the certificate.

Server:

RDev31 

Certificate nickname:

remotecert

Creation method

- ☒ Standard
(Default parameters)
- ☐ Custom
(User specifies parameters)
- ☐ Import
(Allows a PKCS12 file to provide the keys and certificates)

- 2 Select the server that is to own the certificate, and then 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. You will use this nickname for the KMO name in the driver's remote connection parameters.

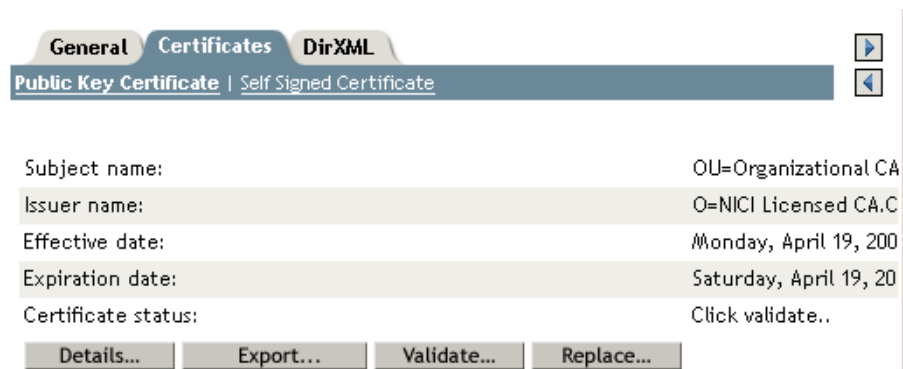
- 3 Leave the Creation method set to Standard, then click Next.
- 4 Review the Summary, then click Finish > Close.
Continue with “Exporting a Self-Signed Certificate” on page 23.

Exporting a Self-Signed Certificate

- 1 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). For example:



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



- 4 In the Export Certificate Wizard, select No and then click Next.
You don't want to export the private key with the certificate.
- 5 Select to export the file in Base64 format (for example, akranes-tree CA.b64), then click Next.



Select an output format.

- ☐ File in binary DER format
☒ File in Base64 format

- 6 Click the link to Save the Exported Certificate to a File and then specify a filename, specify a location, then click Save.
Rootfile names require .pem as an extension.
- 7 In the Save As dialog box, copy this file to a local directory.

- 8 Click Close.

Setting Up Remote Loaders

This section provides information on the following:

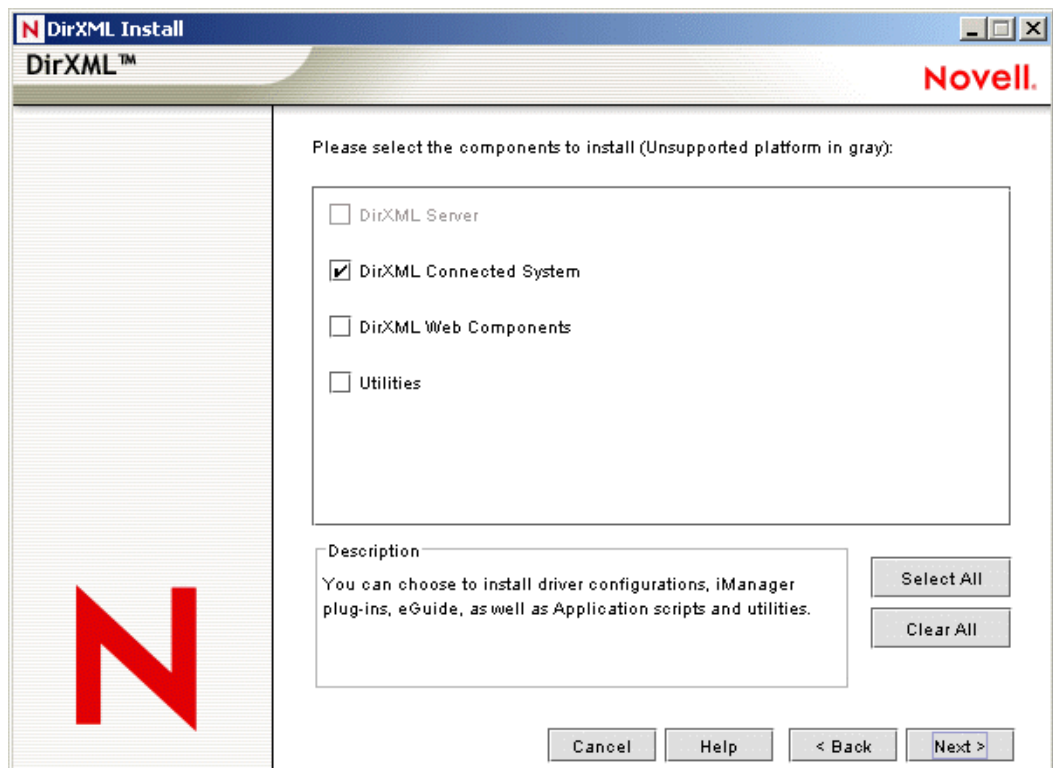
- ♦ [Installing a Remote Loader on a Windows Server \(page 24\)](#)
- ♦ [Configuring the Remote Loader on Windows \(page 26\)](#)
- ♦ [Running the Remote Loader \(page 30\)](#)
- ♦ [Stopping Remote Loaders \(page 30\)](#)

Installing a Remote Loader on a Windows Server

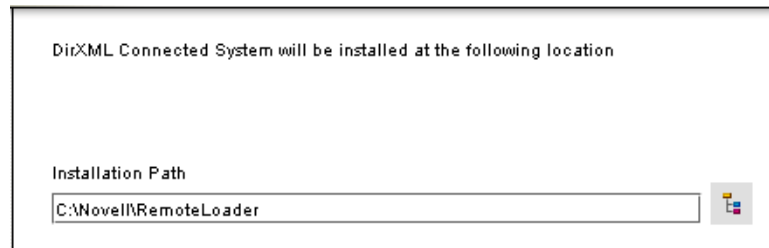
- 1 Insert the Identity Manager 2 CD 2 into the CD-ROM drive.

The installation program should auto-launch. If not, you can run install.exe from the \nt directory.

- 2 View the Welcome page, accept the license agreement, then view the two Overview pages.
- 3 In the DirXML Install dialog box, deselect all components except DirXML Connected System and then click Next.

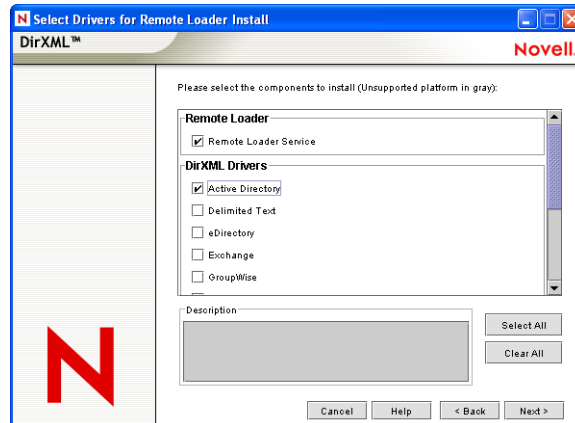


- 4 Select a location for the connected system (the Remote Loader and remote driver shims), then click Next.



- 5 Select the DirXML Remote Loader Service and remote driver shims (drivers), then click Next.

For this implementation, select the Active Directory shim only.



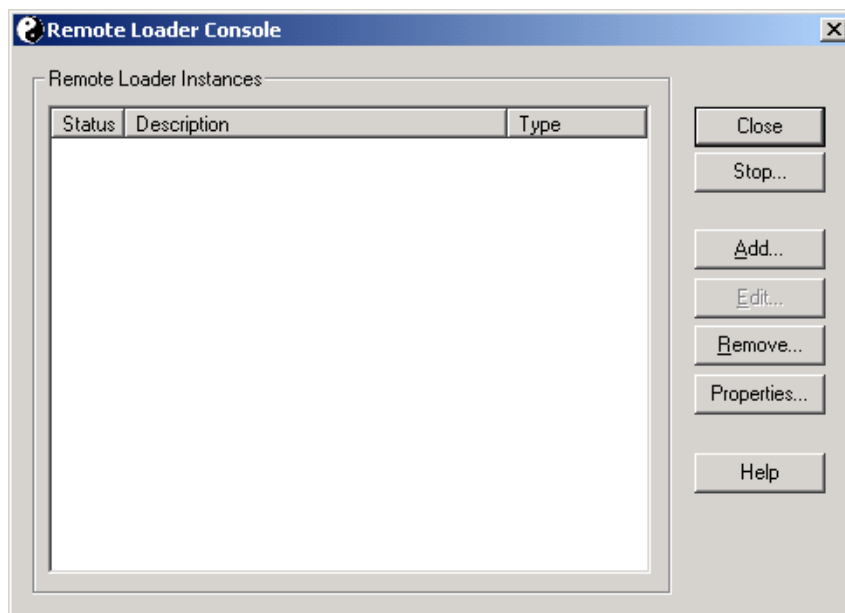
- 6 Acknowledge the activation requirement, view products to be installed, then click Finish.
- 7 Select whether to place the Remote Loader Console icon on your desktop.

Configuring the Remote Loader on Windows

The Remote Loader Console is a new feature in Identity Manager 2. It runs only on Windows. The Console enables you to manage all DirXML drivers running under the Remote Loader on that computer:

- ♦ Add and configure new Remote Loader instances on the local computer
- ♦ Edit configuration settings
- ♦ Start and stop Remote Loader instances
- ♦ Start and stop the trace for each driver instance

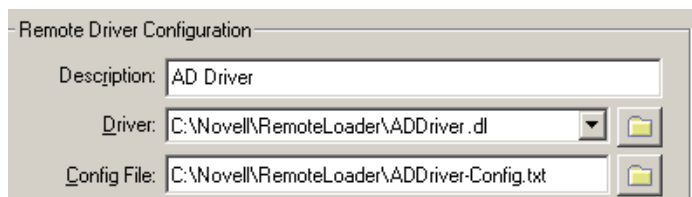
To launch the Remote Loader Console, click the Remote Loader Console icon on your desktop. If you did not choose to place the Remote Loader Console icon on your desktop during installation, you can launch the Remote Loader Console from `c:\remoteloader\rlconsole.exe`. The following figure illustrates the Console.



If you type `dirxml_remote` at the command line, without any parameters, the Remote Loader Application Wizard is launched. To launch the wizard manually, double-click `dirxml_remote.exe` located in the `c:\novell\remoteloader` directory.

To configure a new Remote Loader instance, click **Add**, then provide the information outlined in the following sections.

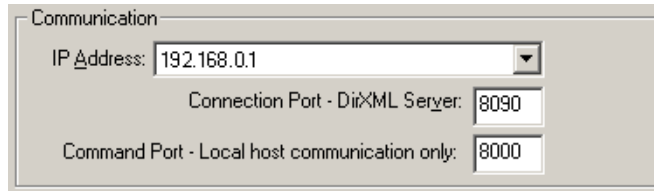
Remote Driver Configuration



- ◆ **Description:** Specify a description to identify the Remote Loader instance. For example, AD Driver.
- ◆ **Driver:** Browse to and select the AD Driver shim.
By default, this shim (`addriver.dll`) is located in the `c:\novell\remoteloader` directory.
- ◆ **Config File:** Specify a name and location for the configuration file. For example, `c:\novell\remoteloader\addriver-config.txt`.

The Remote Loader Console places configuration parameters into this text file and uses these parameters when it runs.

Communication

A dialog box titled "Communication" with three input fields. The first field is "IP Address:" with a dropdown menu showing "192.168.0.1". The second field is "Connection Port - DirXML Server:" with a text box containing "8090". The third field is "Command Port - Local host communication only:" with a text box containing "8000".

- ♦ IP Address: Specify the IP address where the Remote Loader listens for connections from the DirXML server.
- ♦ Connection Port - DirXML Server: Specify the TCP port where the Remote Loader listens for connections from the DirXML 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 where the 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

A dialog box titled "Remote Loader Password" with two input fields. The first field is "Password:" with a text box containing "XXXXXXXXXX". The second field is "Confirm:" with a text box containing "XXXXXXXXXX".

- ♦ Password: This password is used to control access to a Remote Loader instance for a driver.
The password must be the same case-sensitive password that you typed in the Enter the Remote Loader Password edit box in the Authentication section on the DirXML Configuration page, when you configured the driver.
- ♦ Confirm: Re-enter the password.

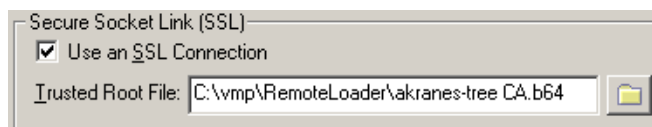
Driver Object Password

A dialog box titled "Driver Object Password" with two input fields. The first field is "Password:" with a text box containing "XXXXXXXXXX". The second field is "Confirm:" with a text box containing "XXXXXXXXXX".

- ♦ Password: The Remote Loader uses this password to authenticate itself to the DirXML server.
This password must be the same password you typed in the Driver Object Password edit box on the Driver Configuration page when you configured the driver.

- ◆ Confirm: Retype the password.

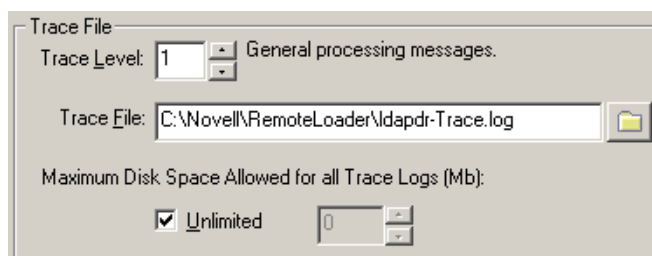
Secure Socket Link (Secure Socket Layer)



- ◆ Use an SSL Connection: To specify an SSL connection, select this option.
- ◆ Trusted Root File: Browse to and select the certificate file that contains the appropriate trusted root certificate (in b64 format).

This is the exported self-signed certificate from the eDirectory tree's Organization Certificate Authority. See [“Exporting a Self-Signed Certificate” on page 23](#).

Trace File



- ◆ Trace Level: For the Remote Loader instance to display a trace window that contains informational messages from both the Remote Loader and the driver, set a trace level greater than zero (0).

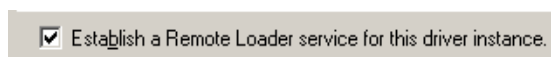
IMPORTANT: If the trace level is set to 0, the trace window won't appear or display messages.

- ◆ 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 (0).

- ◆ Maximum Disk Space Allowed for All Trace Logs (MB): Specify the approximate maximum size that trace file data for this instance can occupy on disk.

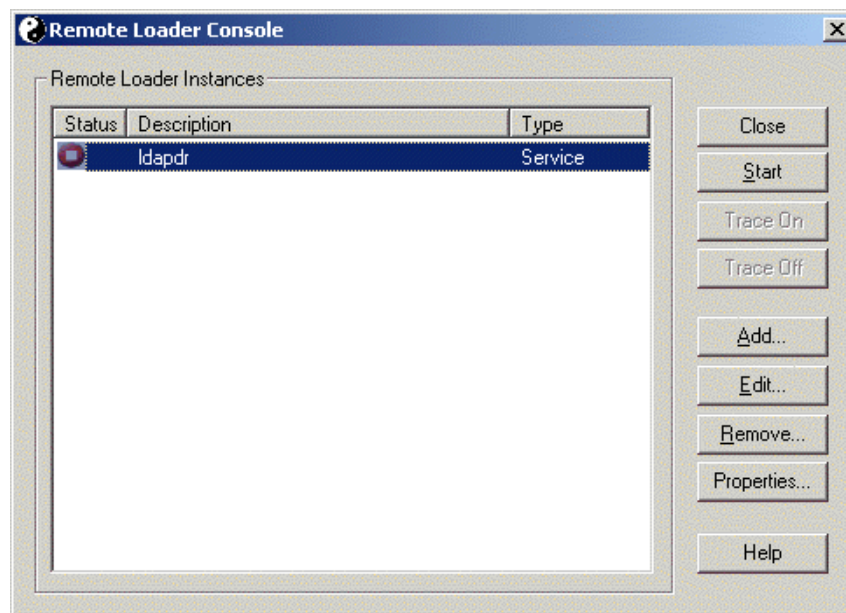
Establish a Remote Loader Service



- ◆ To configure the Remote Loader instance as a service, select this option. When the option is enabled, the operating system automatically starts the Remote Loader when the computer starts.

Running the Remote Loader

- 1 Click the Remote Loader Console icon on the Windows desktop.



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

Stopping Remote Loaders

In Windows, use the Remote Loader Console to stop a remote loader.

Post-Install Tasks

Activating Identity Manager

After you purchase NCL, Novell Product Delivery sends you an e-mail that contains a URL to the Novell Electronic Product Delivery site where you can obtain a generic credential. If you do not receive your email, call the Novell Activation Center at 1-800-418-8373 in the U.S. In all other locations, call 1-801-861-8373. (You will be charged for calls made using the 801 area code.)

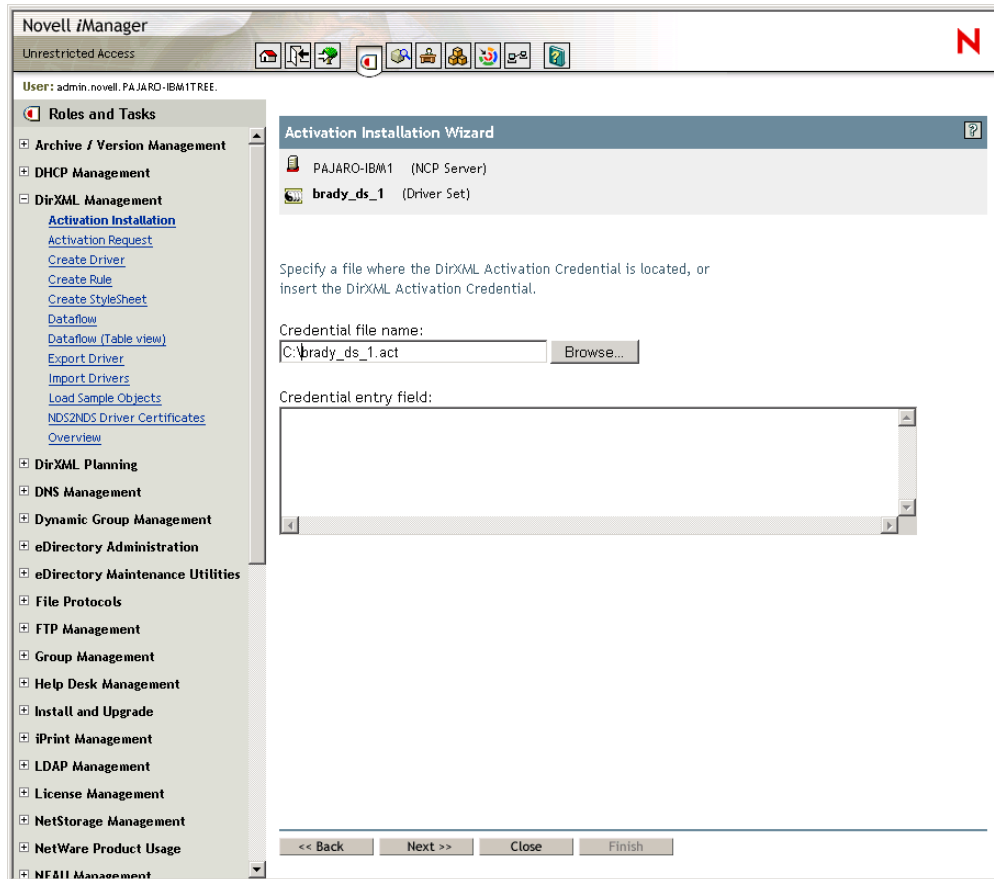
Activating Identity Manager Using a Generic Credential

- 1** In the after-purchase email, click the product link (Identity Manager for NCL) under the Products Ordered section.

This link takes you to the Electronic Product Delivery site where you can obtain your generic credential.

- 2** Click the Download link next to your product's (Identity Manager for NCL) license type, then click Open.

After the file is opened, its content should be similar to the content shown in the following illustration:



4e Paste the contents of the DirXML Activation Credential into the text area, then click Next.

4f Click Finish.

NOTE: You need to activate each driver set that has a driver. You can use the same Product Activation Credential to activate other driver sets as long as the driver sets are in the same tree.

Optional Configuration

Setting Up Identity Manager 2 to Bilaterally Synchronize eDirectory and Active Directory

For information on doing bilateral synchronization between eDirectory and Active Directory, see the *Identity Manager 2 Administration Guide* located on CD 2 - NCL Client Components in the \idm directory.

What's Next

Install a workstation by following the instructions in [Chapter 5, “Installing and Configuring a Workstation,”](#) on page 33.

5

Installing and Configuring a Workstation

This section describes how to install and configure the necessary components needed for a workstation by explaining the following:

- ♦ “Installation Procedure” on page 33
- ♦ “Workstation Configuration” on page 34
- ♦ “Optional Configuration” on page 40

Minimum Requirements

The workstation must meet the following minimum requirements before you install the software:

- ☐ Windows* 2000 Server SP4 or later, Windows 2003 Server SP1 or later, or Windows XP SP2 or later (English versions only) installed.
- ☐ Is a member of the Active Directory server’s domain (configured domain user)
- ☐ The workstation’s DNS contains the AD server IP address.
- ☐ The Smart Card reader is connected and the Smart Card middleware is installed.
- ☐ Use supported Smart Cards—NCL supports cards that use PKCS#11 certificates. This release of NCL has been tested with the following cards:
 - ♦ Axalto Access 64K
 - ♦ GemPlus GemXpresso
 - ♦ Oberthur CosmopolIC V4
 - ♦ Schlumberger Access 32K V2

Installation Procedure

CD: NCL Client Components - CD 2

Location: Root of the CD

You can install all components for the workstation by running the umbrella install provided on CD 2.

- 1** Run setup.exe.
- 2** At the Welcome screen, click Next.
- 3** Accept the License Agreement, then click Next.
- 4** Select Novell® Client™ and, optionally, Nsure® Audit Platform Agent, then click Next.

During a disconnected login, the NCL client records a login audit event. If NSure Audit Server connectivity isn't available, the audit agent on the client machine can take up to 25 seconds to

cache the audit record. This significantly increases workstation login and unlock times. The default client install will not install the audit agent, which means disconnected login events will not be audited. Install the NSure Audit Platform Agent only if disconnected login events are desired and the 25 second delay is acceptable. This issue will be fixed in NSure Audit in a future release.

5 Click Install.

6 On the Novell Client Installation screen, accept the license agreement by clicking Yes.

7 Click Yes to install the Enhanced Smart Card Method, then follow the installation wizard to completion.

8 On the Disconnected Support page, select Yes, I Want Disconnected Support, and then click Next.

This feature allows you to authenticate to the Workstation Only using the Smart Card login method.

9 Choose whether or not to customize the password field description on the login screen, then click Next.

If you choose to customize the login screen's password field, you must type in the new text for the field.

10 Select either PC/SC or PKCS#11, then click Next.

PC/SC and PKCS#11 are technical standards used to communicate between a server and PKI-enabled applications. PC/SC is a standard used for integrating smart cards and smart card readers. PKCS#11 is a standard for public key message exchanges.

Select the standard that best supports your hardware. For more information, see the manufacturer's specifications.

If you select PKCS#11, you must also select a provider that best suits your needs.

11 (Conditional) If you decided to install the Nsure Audit Platform Agent in [Step 4](#), click Next on the Nsure Audit Platform Agent page. If not, skip to [Step 17](#).

12 Accept the License Agreement, then click Next.

13 Fill in the customer information, then click Next.

14 Type the IP address or DNS name of the Secure Logging Server, then click Next.

This is the IP address or DNS name of the Nsure Audit server (the eDirectory™ server set up previously).

15 Select Complete, then click Next > Install.

16 Click Finish > Finish.

17 Reboot the workstation.

Workstation Configuration

Synchronizing the eDirectory Username and the Active Directory Username

When Client32™ has been installed and you restart the workstation, you can synchronize the Active Directory username with the eDirectory username you use to log in to eDirectory. This keeps you from having to log in twice, once to eDirectory and once to the Windows workstation.

- 1** Log in using your eDirectory name and password.
- 2** Right-click the red N on the tool bar, then click Novell Client Properties.
- 3** Click the Advanced Login tab.
- 4** Select Copy NetWare Username to Windows and change the Settings to On.
- 5** Click OK.

Setting Up LDAP Contextless Login

LDAP Contextless Login makes it easier for users to work in the new global tree because it makes it unnecessary for the users to manage or know about changes to their organization's name or its placement in the hierarchy. Because users no longer need to specify their context to authenticate, the context can be changed on the back end as many times as necessary without the users having to know and without the costs associated with managing and supporting these changes.

If your network has LDAP Services for Novell eDirectory set up on your eDirectory tree and you are running Novell eDirectory 8.5 or later, users who are logging in to the network from Windows 2000/XP can log in to the network without having to type their context in the Novell Login screen. To log in, users need to know only their username, password, and the name of the tree that is running LDAP Services. Optionally, you can also have users log in to the network without having to specify the eDirectory tree name.

User objects can be located in the tree by username or e-mail address. You can also enable wildcard searches. If wildcard searches bring up multiple usernames, the user is prompted to select his username.

Generally, when a user connects to the network using LDAP, the connection is made through an LDAP client. Now, the Novell Client Login acts as an LDAP client and connects to the network. All LDAP clients bind (connect) to Novell eDirectory as one of the following types of users:

- ◆ [Public] User (Anonymous Bind)
- ◆ Proxy User (Proxy User Anonymous Bind)
- ◆ NDS[®] or eDirectory User (NDS User Bind)

NOTE: The NDS User Bind is not used by LDAP Contextless Login.

The type of bind and the rights assigned to the corresponding User object determine the content that the LDAP client can access. LDAP clients access a directory by building a request and sending it to the directory. When an LDAP client sends a request through LDAP Services for eDirectory, eDirectory completes the request for only those attributes that the LDAP client has the appropriate access rights to. There are additional restrictions that can be set to further secure connections.

This documentation assumes that you are familiar with LDAP. It contains links to information about LDAP and eDirectory; it is not meant to replace or supersede the documentation about LDAP running on eDirectory. If you are unfamiliar with LDAP, you should familiarize yourself with LDAP and how it operates in your network.

For more information on LDAP for Novell eDirectory, see “Understanding How LDAP Works with eDirectory” in the *Novell eDirectory 8.7 Administration Guide*.

Before users can log in to the network without their context or tree information, you must complete the following steps:

- 1** Set up Novell LDAP Services for eDirectory.

See [“Setting Up Novell LDAP Services for eDirectory” on page 36](#).

2 Do one of the following:

- ♦ If you are installing Novell Client software on a few workstations, install the software and then configure the Novell Client property pages so that the LDAP port number and SSL settings in the client properties match the settings on your LDAP server. See [“Setting Up LDAP Contextless Login on One Workstation” on page 38](#).
- ♦ If you are installing Novell Client software on multiple workstations, preconfigure the LDAP contextless login property pages prior to installing the client software so that the LDAP port number and SSL settings in the client properties match the settings on your LDAP server (see [“Setting Up LDAP Contextless Login on Multiple Workstations” on page 40](#)). Then install the Client software.

3 Inform users about contextless login.

See [“Logging In Using LDAP Contextless Login” on page 40](#).

If you experience problems with LDAP Contextless Login, check the Server and Group object configurations. Most problems occur in the access rights given to the Proxy User. You can use any LDAP browser available from the Internet to check the access rights. Browse to the user and verify that you can read the inetOrgPerson property and other properties you are searching for, such as CN and MAIL. If these cannot be seen through the LDAP browser by logging in anonymously, contextless login cannot perform the proper searches to resolve the User object’s context in the tree.

Setting Up Novell LDAP Services for eDirectory

Before users can take advantage of LDAP Contextless Login, the network must be running Novell LDAP Services for eDirectory 8.5 or later and you must have completed the following steps:

1 Install and configure the LDAP Services for eDirectory on the LDAP server.

See Understanding LDAP Services for Novell eDirectory and Configuring LDAP Services for Novell eDirectory in the *Novell eDirectory 8.7 Administration Guide*.

2 Do one of the following:

- ♦ Grant the Read right to the Public Object.
See [“Connecting As a \[Public\] User” on page 36](#).
- ♦ Create a Proxy User object that has the correct rights.
See [“Connecting As a Proxy User” on page 37](#).

Connecting As a [Public] User

An anonymous bind is a connection that does not contain a username or password. If an LDAP client without a name and password binds to LDAP Services for eDirectory and the service is not configured to use a Proxy User, the user is authenticated to eDirectory as user [Public].

User [Public] is a nonauthenticated eDirectory user. By default, user [Public] is assigned the Browse right to the objects in the eDirectory tree. The default Browse right for user [Public] allows users to browse eDirectory objects but blocks user access to the majority of object attributes.

The default [Public] rights are typically too limited for most LDAP clients. Although you can change the [Public] rights, doing so gives these rights to all users. Because of this, we recommend that you use the Proxy User Anonymous Bind. For more information, see [“Connecting As a Proxy User” on page 37](#).

To give user [Public] access to object attributes, you must do the following in iManager or ConsoleOne®:

- 1 Make user [Public] a trustee of the appropriate containers.
- 2 Grant the Read right to user [Public].

Without the Read right, user [Public] cannot search containers for the User object information.

You can grant the Read right to the specific attributes that LDAP Contextless Login searches for User objects or you can grant rights to all attributes. For example, you can grant rights only to the e-mail address or telephone number; when LDAP Contextless Login searches the tree as user [Public], it searches only these attributes.

Connecting As a Proxy User

A proxy user anonymous bind is an anonymous connection linked to an eDirectory username. If an LDAP client binds to LDAP for eDirectory anonymously, and the protocol is configured to use a Proxy User, the user is authenticated to eDirectory as the Proxy User. The name is then configured in both LDAP Services for eDirectory and in eDirectory.

The key concepts of proxy user anonymous binds are as follows:

- ♦ All LDAP client access through anonymous binds is assigned through the Proxy User object.
- ♦ The Proxy User must have a null password and must not have any password restrictions (such as password change intervals). Do not force the password to expire or allow the Proxy User to change passwords.
- ♦ You can limit the locations that the Proxy User can log in from by setting address restrictions for the Proxy User object.
- ♦ The Proxy User object must be created in eDirectory and assigned rights to the eDirectory objects you want to publish. The default user rights provide Read access to a limited set of objects and attributes. Assign the Proxy User Read and Search rights to all objects and attributes in each subtree where access is needed.
- ♦ The Proxy User object must be enabled on the General page of the LDAP Group object that configures LDAP Services for eDirectory. Because of this, there is only one Proxy User object for all servers in an LDAP group.
- ♦ You can grant a Proxy User object rights to All Properties (default) or Selected Properties. In order for contextless login or treeless login to work, the Read right must be granted so that LDAP can search the container or tree for the User object. Typically, you assign the Proxy user rights to the Root of the tree so that LDAP can view the attributes of the User objects throughout the tree. However, you might want to restrict access by assigning the Read right only to individual Organizational Units that you want LDAP to search.

For more information, see “Configuring LDAP Objects” in the *Novell eDirectory 8.7 Administration Guide*.

NOTE: LDAP Contextless Login requires clear text passwords to be enabled for LDAP. This does not affect the eDirectory password required during login. They remain encrypted.

To give the Proxy User rights to only selected properties on eDirectory 8.7 or later, complete the following steps.

NOTE: LDAP Contextless Login works with eDirectory 8.5 or later. However, these steps apply specifically to eDirectory 8.7. If you are using a compatible version other than eDirectory 8.7, check the documentation that corresponds to your version for the appropriate steps.

- 1 In iManager, click the Roles and Tasks button.

- 2** Click Rights Management > Modify Trustees.
- 3** Specify or browse to the top container the Proxy User is to have rights to, then click OK.
- 4** On the Modify Trustees screen, click Add Trustee.
- 5** On the Contents screen, browse to and click the Proxy User's object.
On the same screen, notice that the Proxy User's object appears in the Selected Objects area near the bottom.
- 6** Click OK.
- 7** On the Modify Trustees screen, click Assigned Rights for the Proxy User.
- 8** Select the All Attributes Rights and Entry Rights options, then click Delete Property.
- 9** Click Add Property, then select the Show All Properties in Schema options.
- 10** Select an inheritable right for the Proxy User, such as mailstop (in the lowercase section of the list) or Title, then click OK.
To add additional inheritable rights, repeat **Step 9** and **Step 10**.
- 11** Click Done.

To implement proxy user anonymous binds on eDirectory 8.7 or later, you must create the Proxy User object in eDirectory and assign the appropriate rights to that user. Assign the Proxy User the Read and Browse rights to all objects and attributes in each subtree where access is needed. You also need to enable the Proxy User in LDAP Services for eDirectory by specifying the same proxy username.

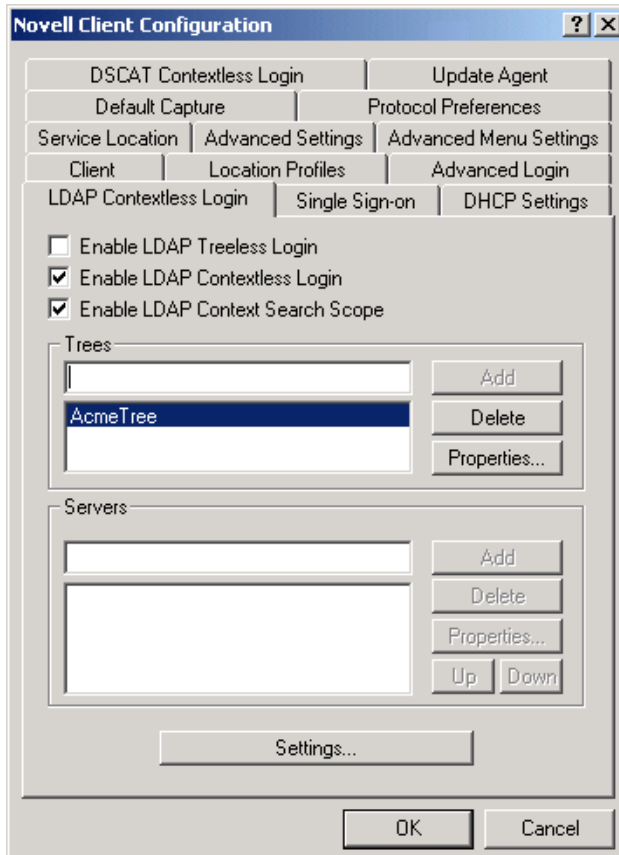
- 1** In iManager, click the Roles and Tasks button.
- 2** Click LDAP Management > LDAP Overview.
- 3** On the LDAP Overview screen, click the name of an LDAP Group object to configure.
- 4** In the Authentication Options area, type the name and context of an eDirectory User object in the Proxy User field.
- 5** Click Apply > OK.

Setting Up LDAP Contextless Login on One Workstation

After you have set up the LDAP Group object and assigned the correct rights to the User object that is associated with the proxy username, you need to set up LDAP Contextless Login on the workstations.

If you want to install on a few workstations, complete these steps. If you want to install on many workstations, see [“Setting Up LDAP Contextless Login on Multiple Workstations” on page 40](#).

- 1** At the user's workstation, right-click the N icon on the tool bar and then click Novell Client Properties.
- 2** Click the LDAP Contextless Login tab.



3 Do one of the following:

- ♦ To enable treeless login, select Enable Treeless Login. This is automatically selected for you because you must set up contextless login to enable treeless login.
- ♦ To enable only LDAP contextless login, select Enable LDAP Contextless Login.

4 In the Trees field, specify the name of an eDirectory tree running LDAP services and then click Add.

5 In the Servers field, specify the IP address or DNS names of the server running LDAP services and then click Add.

Order is important for speed and efficiency because servers are queried for their tree until one is found that matches the tree specified by the user.

6 (Conditional) If this is the first time this server has been added to the list, check the server properties on the LDAP Server Properties page that appears to make sure that the timeout settings and data encryption settings are correct.

If you are using Secure Socket Layer (SSL) to establish a secure connection, you must specify the path and name of the certificate on the workstation. You should also check to make sure that the correct port number is specified.

7 (Conditional) If there are additional servers running LDAP, repeat **Step 5** and **Step 6** for each server.

8 (Optional) Start searching for users in a certain context.

8a Select Enable Context Search Scope.

8b Select the tree, then click Properties.

8c Do one of the following:

- ♦ To enable a search in the specified context and any containers in that context, select Search Context and Subtree.
- ♦ To enable a search in the specified context only, select Search Context Only.

8d Type the distinguished context delimited by commas (standard LDAP format), then click Add.

For example: OU=TOKYO,O=DIGITALAIRLINE

TIP: The LDAP property page does not ensure that this context is correct. If users have problems logging in, check that you typed this information correctly.

8e (Optional) Add multiple contexts to be searched by repeating **Step 8d** for each context.

The servers and contexts are searched in order. You can set the order they are searched by selecting a server or context and then clicking Up or Down to move its position in the search list.

9 Click OK.

10 (Optional) Specify additional eDirectory trees to use by repeating **Step 4** through **Step 9** for each tree.

11 (Optional) Set the optional search and display parameters that LDAP Contextless login uses to search the eDirectory tree for users by clicking Settings.

For example, because users do not need to specify their context, you might want to disable the Display Context parameter so that the context is not displayed during login.

12 Click OK to effect the changes and close the property page.

Setting Up LDAP Contextless Login on Multiple Workstations

As with all property page settings, you can set these properties for multiple workstations both before and after installation. For more information, see the *Novell Client for Windows Installation and Administration Guide*.

Logging In Using LDAP Contextless Login

When users log in to the network using LDAP Contextless Login, they must specify the necessary information based on the options you specified in the LDAP Contextless Login Settings Protocol page, the password, and the name of the tree running LDAP Services for eDirectory. The context information is added automatically to the Novell Login window when the username is found.

If you choose to allow wildcard searches, users can perform a wildcard search and the LDAP database lists all possible users that meet the search criteria.

Optional Configuration

Customizing the Novell Login Dialog Box

For information on customizing the Novell Login dialog box, see Managing Login in the *Novell Client for Windows Installation and Administration Guide* located on CD 2 - NCL Client Components in the \client directory.

What's Next

Finish configuring NCL by following the instructions in [Chapter 6, “Configuring the Solution,”](#) on page 43.

6

Configuring the Solution

This section explains the following configuration processes:

1. [Identity Manager Configuration - Active Directory Server \(page 43\)](#)
2. [Identity Manager Configuration - eDirectory Server \(page 43\)](#)
3. [Identity Manager: Importing Active Directory Users to the eDirectory Server \(page 46\)](#)
4. [Configuring the Novell Enhanced Smart Card Method \(NЕСM\) \(page 47\)](#)
5. [Using the Password Generation Service \(page 50\)](#)

Identity Manager Configuration - Active Directory Server

See [Chapter 4, “Installing and Configuring the Active Directory Server,” on page 21](#) for detailed information on configuring the remote loader and driver.

- 1 Run the remote loader configuration tool.
- 2 Accept the defaults for port, etc.
- 3 Enter passwords.

Identity Manager Configuration - eDirectory Server

The suggested configuration for NCL is presented here. For more information on custom configuration, see the *Identity Manager 2 Administration Guide* located on CD 2 - NCL Client Components in the \documentation directory.

Creating a Container on eDirectory for the Active Directory User Objects

You need to create a container on the eDirectory™ server to house the Active Directory User objects. You will point to this container when you migrate the Active Directory User objects into eDirectory.

- 1 Launch iManager.
- 2 Click eDirectory Administration > Create Object.
- 3 Select Organization, then click OK.
- 4 Specify a name for the container (for example, ADUsers).
- 5 Browse for and select a context for the container, then click OK.

Configuring Identity Manager on the eDirectory Server

- 1 Launch iManager.

- 2** Click DirXML Management > Overview.
- 3** Create a new driver in the new driver set.
- 4** Type the driver name, context, and the DNS name of the eDirectory server.
- 5** Deselect Create New Partition.
- 6** Import a driver configuration by selecting ActiveDirectory.XML.
- 7** Specify the following driver configuration information:

Driver Configuration Parameter	Value
Driver name	Active Directory
Authentication Method	Negotiate
Authentication ID	<i>Active Directory Administrator ID</i>
Authentication Password	<i>Active Directory Administrator Password</i>
Authentication Server	<i>DNS of AD server</i> Example: computer_name.domain.com
Domain Name	<i>LDAP Distinguished name of AD server domain</i>
Domain DNS Name	<i>Domain name of AD server domain</i>
Driver Polling Interval	1
Password Synch Timeout	5
Base Container in eDirectory	<i>NCP Name of Container in eDirectory</i> This is the container you created in “Creating a Container on eDirectory for the Active Directory User Objects” on page 43.
Base Container in Active Directory	<i>LDAP Distinguished Name of Container in Active Directory</i> There is the base container where you want the user migration to start from.
Data Flow	AD to eDirectory
Publisher Placement	Mirrored
Subscriber Placement	Mirrored
Password Failure Notification	[Leave blank]
Support Exchange	No
Enable Entitlements	No

Configuring DirXML Drivers for Use with Remote Loaders

You can configure a new driver or enable an existing driver to communicate with the Remote Loader. This section provides general information on configuring new or existing drivers so that

they communicate with the Remote Loader. For additional and driver-specific information, refer to the the relevant driver implementation guide.

Importing and Configuring a New Driver

- 1 In Novell® iManager, import or create and then configure a new driver.
- 2 Scroll to the bottom of the configuration options, select Remote from the drop-down list, then click Next.

Do you want this driver to run locally, or remotely with the Remote Loader service?

Driver is Local/Remote:

Local

Local

Remote

<< Back Next >> Cancel Finish

- 3 Type a remote hostname and port.

 **SAP-HR** (1 of 1)

The driver writer requested that the following information be supplied in order to import this driver configuration file. An * indicates required information.

Enter the Host Name or IP Address and Port Number where the Remote Loader Service has been installed and is running for this driver. The Default Port is 8090.

[Host Name or IP Address and Port;

###.###.###.###:####]

Remote Host Name and Port:

hostname : 8090

- 4 Type and retype a password for the Driver object.

The Driver Object Password is used by the Remote Loader to authenticate itself to the DirXML server. It must be the same password that is specified as the Driver Object Password on the DirXML Remote Loader.

Driver Password:

●●●●●●

Reenter the password:

●●●●●●

- 5 Type and retype the Remote Loader password, then click Next.

The Remote Loader password is used to control access to the Remote Loader instance. It must be the same password that is specified as the Remote Loader password on the DirXML Remote Loader.

Remote Password:

••••••

Reenter the password:

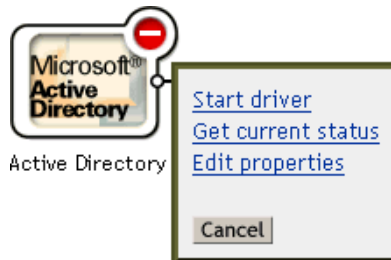
••••••

- 6 Define a security-equivalent user, then click Next > Finish.

Identity Manager: Importing Active Directory Users to the eDirectory Server

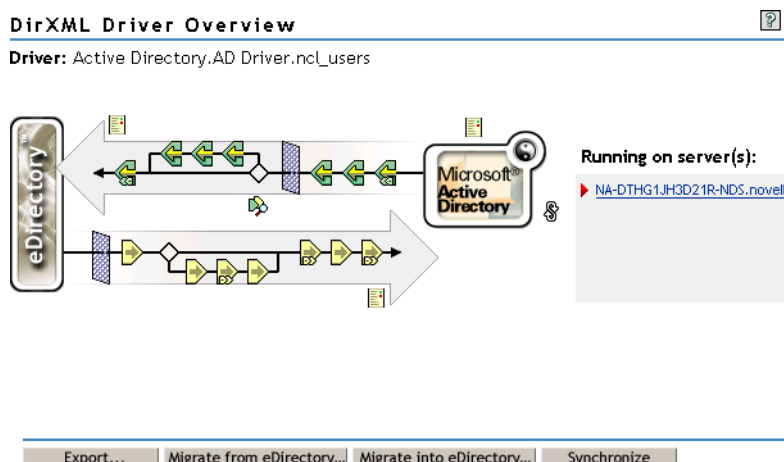
- 1 Launch iManager.
- 2 Click DirXML Management > Overview.
- 3 Browse to and select the driver that you want to modify.

In this case, select AD driver.



- 4 Click the Active Directory graphic.

The following screen appears:



- 5** Click the Active Directory on this screen to start the driver.

The icon in the upper right-hand corner will change, showing that the driver is running.

- 6** Migrate the containers into eDirectory.

You must migrate the containers first, then migrate the users.

- 6a** Click Migrate into eDirectory.

- 6b** Click Edit List, select Organizational Unit, then click OK.

- 6c** Click Edit Class, modify the following values, then click OK.

- ♦ Enter the path where you want the migration to start.

This is the base container in Active Directory (in LDAP format) that was entered previously.

- ♦ Select All descendants.

- 7** Migrate the users into eDirectory.

- 7a** Click Edit List, select User, then click OK.

- 7b** Click Edit Class, modify the following values, then click OK.

- ♦ Enter the path where you want the migration to start.

This is the base container in Active Directory (in LDAP format) that was entered previously.

- ♦ Select All descendants.

Configuring the Novell Enhanced Smart Card Method (NЕСSM)

After the NESCM server and client components have been installed, there are three more procedures you need to complete before the login method is ready for use:

- ♦ [“Configuring a Trusted Root Container” on page 48](#)
- ♦ [“Enrolling a Smart Card for a User” on page 48](#)
- ♦ [“Restricting Users to the Novell Enhanced Smart Card Method” on page 49](#)

There are also other settings you can configure for use with NESCM. See [“Other Settings” on page 48](#).

Configuring a Trusted Root Container

- 1** Create a trusted root container in eDirectory.

- 1a** In iManager, click the Novell Certificate Server task.

- 1b** Click Create Trusted Root Container.

- 1c** Follow the wizard to completion.

- 2** Import the trusted root certificate of your Certificate Authority (CA) into the trusted root container.

- 2a** In iManager, click the Novell Certificate Server task and then click Create Trusted Root.

- 2b** Type the name, select the trusted root container you created in [Step 1](#), then select the certificate you want to import into the Trusted Root object.

This should be the trusted root certificate of the Certificate Authority (CA) you are using for the certificates on your smart cards.

3 Configure the NESCM method to use the trusted root container.

3a In iManager, click Smart Card Login > Global Settings.

3b Under Certificate Search Containers, add the trusted root container.

3c Click OK.

Enrolling a Smart Card for a User

1 In iManager, click Smart Card Login > User Settings.

2 Select a user, then click OK.

3 Under Certificate Settings, specify an allowable Subject name for this user.

You have several ways of doing this:

- ♦ Read the subject from the card in the card reader.

NOTE: If you are using an unsupported card, you might not be able to read the subject name from the card for this release. Use one of the other methods to specify an allowable subject name.

- ♦ Read the subject from a file.
- ♦ Enter a subject by hand.

You can also edit and delete the subject.

4 Click OK or Apply.

Other Settings

The NESCM allows you to configure global, container, or user settings. Global settings apply to the entire tree. The container and user settings give you the option to use inherited settings from the global settings or you can set container-specific or user-specific settings.

Container settings can be configured for a specific container and apply to all objects in that container. Container-specific settings override global settings.

User settings can be configured for a specific user. User-specific settings override global and container settings.

You can configure the following global, container, and user settings.

Global Settings

- ♦ Trusted Root Certificate Containers: Specifies the trusted root containers the method uses for certificate validation.
- ♦ Certificate Revocation Checking: Defines how certificate revocation is performed. OCSP or CRL revocation checking can be configured for each trusted root container.
- ♦ Certificate Expiration Warning: Defines the number of days in advance that a user is given a warning message before his certificate expires.
- ♦ Card Removal Behavior: Defines the action taken when the user removes his card from the card reader.

- ♦ Check for Certificate Policy: Specifies a certificate policy. If this setting is enabled, user certificates must contain this policy to be valid.

Container Settings

Select a container and then configure the following settings:

- ♦ Certificate Expiration Warning: Specifies the number of days in advance that a user is given a warning message before his certificate expires.
- ♦ Card Removal Behavior: Defines the action taken when the user removes his card from the card reader.
- ♦ Check for Certificate Policy: Specifies a certificate policy. If this setting is enabled, user certificates must contain this policy to be valid.

User Settings

Select a user and then configure the following settings:

- ♦ Certificate Subject Names: Specifies the certificate subject names that can be used for login.
- ♦ Temporary Certificate Subject Names: Specifies a temporary certificate subject name that is used for login. A temporary certificate subject name is valid until the expiration date and overrides the certificate subject names.
- ♦ Certificate Expiration Warning: Specifies the number of days in advance that a user is given a warning message before his certificate expires.
- ♦ Card Removal Behavior: Defines the action taken when the user removes his card from the card reader.
- ♦ Check for Certificate Policy: Specifies a certificate policy. If this setting is enabled, user certificates must contain this policy to be valid.

Restricting Users to the Novell Enhanced Smart Card Method

You can restrict users so they can use only the NESCM method.

- 1** Launch iManager.
- 2** Authenticate to the eDirectory tree as administrator or a user with administrative rights.
- 3** From the Roles and Tasks menu, select NMAS > NMAS Users, select the user you want to authorize the login sequences for, and then click the NMAS Login Sequences tab.
- 4** Select the Restrict the User to the Authorized Login Sequences Below option.
If you deselect the option, the user can use any defined login sequence to log in.
If you select the option, use the arrows to authorize or select the sequences you want this user to use to log in. In this case, move all other login methods to the Available Methods list and leave only the NESCM method in list.
- 5** Click Apply or OK.

Using the Password Generation Service

Using the Password Generation Service Plug-in

The Password Generation Service plug-in allows you to turn on or off the Password Generation Service for an individual user.

- 1** In iManager, click eDirectory Administration > Modify Object.
- 2** Select a User object, then click OK.
- 3** Click the Password Generation Service tab.
- 4** From the Manage Windows Password drop-down menu, select True if you want the Password Generation Service to automatically generate a new random password for this user or False if you do not.
- 5** Click OK or Apply.

Using the Password Generation Service Command Line Utilities

The Password Generation Service installation lays down the following items in the \system32 directory:

- ♦ passwordgenerationservice.exe

Use to uninstall and install the Password Generation Service at the command line. It has the following command line options:

-i	install service
-u	uninstall service
-r	run service
-s	stop service
-p	pause service
-c	resume service
status	current status of the service
help	returns the help syntax

NOTE: If you uninstall using the -u option, the service is uninstalled but it does not remove registry entries.

- ♦ passwordgenerationpolicy.exe

Use to view or modify the password generation policy. This program displays the password generation policy page.

- ♦ passwordgenerationutility.exe

Use to force a password change outside the normally scheduled password change defined in the policy. The password change utility changes the Active Directory password. At the same time it stores that password as a secret in the SecretStore of a user in eDirectory.

The Password Generation Utility has only one command line option:

passwordgenerationutility nds username

For example, passwordgenerationutility *user.context*

When the Password Generation Utility is run, it logs an event in the passwordgen.log file. The entry indicates if the event failed.

- ♦ passwordgen.log

The log file.

A

Manually Installing the Novell Certificate Login (NCL) Workstation Products

The Novell Certificate Login (NCL) workstation install is composed of three separate product installs:

- ♦ Novell Client
- ♦ Novell Enhanced Smart Card Method
- ♦ Nsure Audit Platform Agent

You can install all three products silently while suppressing reboots. For the NCL workstation to function, the machine being installed to must be rebooted after all three products have been installed.

The following are instructions for installing the three products silently:

Novell Client

You can run the Novell Client installer (setupnw.exe) silently from the command line using a `/U` flag. The setupnw.exe file is on the CD2 - NCL 2.0 Client CD under the \novellclient\winnt\i386\ directory. For a complete list of parameters to setupnw.exe run it with the `/?` flag.

The `/U` flag tells the client to use the default unattend.txt. The `/U:<unattend.txt>` flag and parameter let you specify a path to an unattend.txt file. For example, the NCL Workstation umbrella install calls `setupnw.exe /U:\install\unattend.txt`. The Novell Client's install options can all be specified in the unattend.txt file, including silence.

To create an unattend.txt file, use nciman.exe. The nciman.exe file is located under the \novellclient\winnt\i386\admin directory of the CD2 - NCL 2.0 Client CD.

NOTE: Nciman.exe must be run on a machine that already has the Novell Client installed.

The unattend.txt file used in the NCL workstation umbrella install is on the CD2 - NCL 2.0 Client CD under the \install directory. The NCL workstation umbrella install's unattend.txt file only suppresses the reboot dialog at the end of a typical Novell Client install.

For more information see the [Novell Client for NT documentation \(http://www.novell.com/documentation/client/index.html?page=/documentation/client/clintenu/data/hw27o7aw.html\)](http://www.novell.com/documentation/client/index.html?page=/documentation/client/clintenu/data/hw27o7aw.html).

Novell Enhanced Smart Card Method (NЕСSM)

You can run the Novell Enhanced Smart Card Method (NЕСSM) install silently by passing in parameters from the command line. Unlike the Novell Client, there is no parameter file to pass in like unattend.txt.

Before installing the NESCM silently from a command-line, you should become familiar with the graphical install and its options. **Table 1** lists the parameters that can be passed to the method install (setup.exe). The method install is on the CD2 - NCL 2.0 Client CD in the \nmasmethods\novell\enhancedsmartcard\client directory. Parameters passed to setup.exe after the /s /v flags are wrapped in quotes with the /qn flag first. For example:

```
setup.exe /s /v"/qn BOOL_PASSWORD_FIELD_DESC=0 DISCONNECT=1
REBOOT=0 SMARTCARD_INTERFACE=1"
```

This example uses the standard password field descriptor, turns disconnected support on, suppresses the reboot, and specifies PC/SC as the smart card interface.

NOTE: You cannot use spaces in the *PASSWORD_FIELD_DESC* parameter on the command line. If spaces are required in the password field descriptor, you need to set the following registry setting manually:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\Tab
Settings\Credentials\PasswordFieldDescription
```

Table 1 Parameters for Novell Enhanced Smart Card Method Installer

Parameter	Required	Description	Value
BOOL_PASSWORD_FIELD_DESC	Yes	Set to 1 for a custom password field descriptor. If set to true then PASSWORD_FIELD_DESC must be set to a string.	1 or 0
DISCONNECT	Yes	Set to 1 for disconnected support otherwise set to 0.	1 or 0
PASSWORD_FIELD_DESC	No	Set to a string for a custom password field descriptor. BOOL_PASSWORD_FIELD_DESC must be set to 1 for the custom string to take effect. The password field descriptor's maximum length is approximately 10 characters. There cannot be spaces in the password field descriptor passed in through the command line. If you require spaces in your password field descriptor, then you will have to set a registry key.	String
PKCS11LIBRARY	No	Set to an integer 1 through 7 depending on which PKCS#11 library is desired (see Table 2). Must be set if SMARTCARD_INTERFACE is set to 2. Also USERSPECPATH must be set if PKCS11LIBRARY is set to 7.	1 through 7
REBOOT	Yes	Set to 1 for reboot or 0 to suppress reboot.	1 or 0
SMARTCARD_INTERFACE	Yes	For PC/SC support set to 1 and for PKCS#11 support set to 2	1 or 2
USERSPECPATH	No	Set to the PKCS#11 library name. SMARTCARD_INTERFACE must be set to 2 and PKCS11LIBRARY must be set to 7 for the USERSPECPATH to register a user-specified PKCS#11 library.	String

Table 2 PKCS#11 Library Integer Reference

Library	Integer
ActivCard	1
NetSign	2
SmartTrust	3
iD2 Technologies	4
Gemplus (GEMSAFE)	5
Rainbow iKey USB	6
User Specified Library	7

Nsure Audit Platform Agent

You can run the Nsure Audit Platform Agent in silent mode in much the same way as the Novell Enhanced Smart Card Method. The Platform Agent has only one command line parameter to set; *LOGHOSTADDR*. *LOGHOSTADDR* is a string that must either be the IP address or DNS name of the Secure Log Server. For log server failover, you can also have multiple comma-delimited addresses with no spaces between the entries. For example:

```
pa_win32.exe /s /v"/qn
LOGHOSTADDR=XXX.XXX.XXX.XXX,YYY.YYY.YYY.YYY,ZZZ.ZZZ.ZZZ.ZZZ"
```

