AUTHORIZED DOCUMENTATION

Installation and Administration Guide

Novell®
Enhanced Smart Card Method

3.0.4

August 29, 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 provides installation and configuration information for the Novell® Enhanced Smart Card Method.

Audience

This guide is written primarily for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment 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 this documentation, see the *Novell Enhanced Smart Card Method Installation Guide* (http://www.novell.com/documentation/ias/index.html?page=/documentation/ias301/nescm_install/data/bookinfo.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.

Overview

1

The Novell® Enhanced Smart Card Method (NESCM) is a Novell Modular Authentication Services (NMAS™) method that provides smart-card-based authentication to eDirectory™. Smart card authentication is a two-factor authentication technique: something you know (smart card PIN) and something you have (smart card).

The login method consists of two components: the server module and the client module. The appropriate modules are loaded during the authentication process by the NMAS server and client components.

During authentication, the client module enumerates the certificates available on the attached smart card and sends them to the server module. The server module chooses a certificate to use for authentication, based on the configuration and validation checks.

After selecting the login certificate, the server module generates a random challenge and sends it to the client module to confirm that the user possesses the private key associated with the certificate. The client module uses the smart card to sign the challenge and encrypt the result by using RSA public/private key encryption. Upon receiving the result, the server decrypts the data by using the certificate's public key and validates the challenge. If a valid certificate is not found or the challenge is not validated, the login attempt fails.

The method supports local Windows* workstation logins. Workstation Only Login allows the smart card to be used for a local workstation login, when the eDirectory identity store isn't available. This is useful in situations where network connectivity isn't always available, such as for laptop users.

The method can also be configured to monitor the smart card reader device. When the smart card is removed, the method can be configured to lock the workstation or log off.

Novell Enhanced Smart Card Method Installation

2

This section describes the installation of the Novell® Enhanced Smart Card Method (NESCM).

2.1 Minimum Requirements

NESCM has the following minimum requirements:

2.1.1 eDirectory Server

eDirectory™ 8.7.3 IR9 or eDirectory 8.8 SP1 on one of the following platforms:

- NetWare® 6.5 SP6 or later
- Windows Server* 2003 SP1 or later
- SUSE® Linux Enterprise Server (SLES) 10 32-bit or 64-bit
- Red Hat* AS 4.0 Server 32-bit or 64-bit

2.1.2 Client Workstations

- Novell Client™ 4.9.1 SP3 or later installed on Windows XP SP2
- iManager version 2.6 SP2 or later with the NMAS™ plug-in version 10.1.20061031 or later.

The NESCM iManager plug-in supports querying certificate information directly from smart cards. This functionality is supported on Windows with the following browsers:

- Firefox* 1.5x or later
- Internet Explorer* 6.0 SP2 or later

A smart card reader and appropriate smart card middleware must be installed and properly configured on the workstation. The method should work with any Windows XP compliant PC/SC middleware. It has been tested with the following:

Table 2-1 Middleware, Smart Card Readers, and Smart Cards

Device	Tested Applications
Middleware	◆ Netsign* CAC version 5.5.71.0 ◆ Gemplus* version 3.2.2 and 4.2 ◆ ActivCard* Gold for CAC 3.01 ◆ ActivClient* 6.0 PKI Only ◆ Cryptovision cv act sc/interface 3.2.1 ◆ eToken* Run Time Environment 3.60 ◆ CIP 4.07
Smart Card Readers	◆ SCM Microsystems* SCR241 PCMCIA ◆ SCM Microsystems SCR 131 Serial (RS232) ◆ Cherry G83-6759LPAUS-2 USB Keyboard ◆ Gemplus GemPC433-SL USB ◆ Schlumberger Reflex 72v2 ◆ Schlumberger Reflex USB ◆ SCM Microsystems SCR531-USB ◆ Precise Biometrics 250 MC ◆ ActivIdentity* USB Reader 2.0 and 3.0
Smart Cards	◆ Axalto Access 64K CAC ◆ Gemplus GemXpresso* CAC ◆ Oberthur CosmopolIC V4 CAC ◆ Schlumberger Access 32K V2 CAC ◆ Gemplus GemSAFE* SDK GPK16000 ◆ Cryptovision - CardOS M4.01a ◆ Aladdin* - eToken PRO 64K ◆ Oberthur CosmpolIC 64K V5.2 Fast ATR (PIV)

2.2 Installing the Method

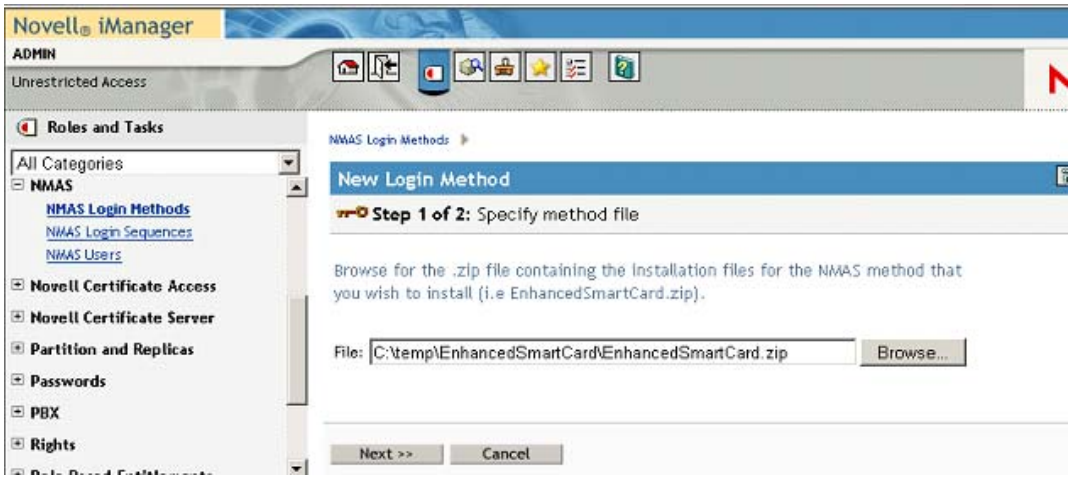
Installation consists of installing the method on the eDirectory server and on the client workstations.

- Section 2.2.1, “eDirectory Server Installation,” on page 12
- Section 2.2.2, “Client Workstation Installation,” on page 15

2.2.1 eDirectory Server Installation

1 Log in to iManager as an Administrator.

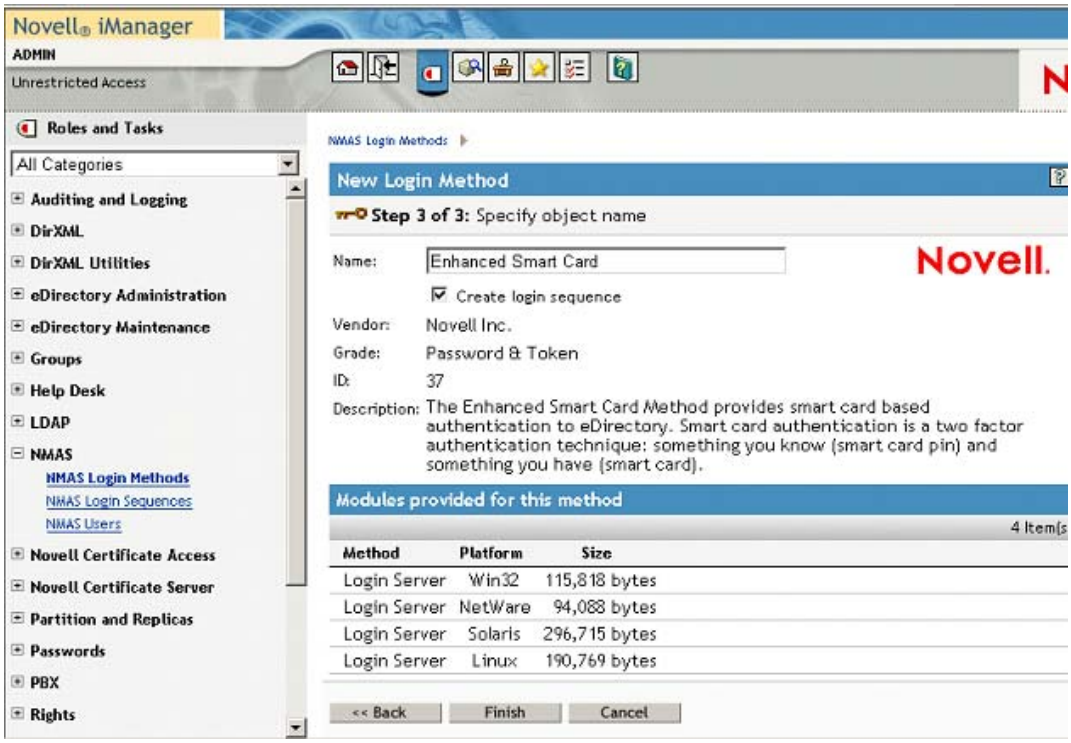
2 From Roles and Tasks, select *NMAS* > *NMAS Login Methods*, then select *New*.



3 Browse to and double-click the `EnhancedSmartCard.zip` file that comes with the method. It is located on the client disk under the `NMAS Methods` folder.

This zip file contains the server components and the iManager components.

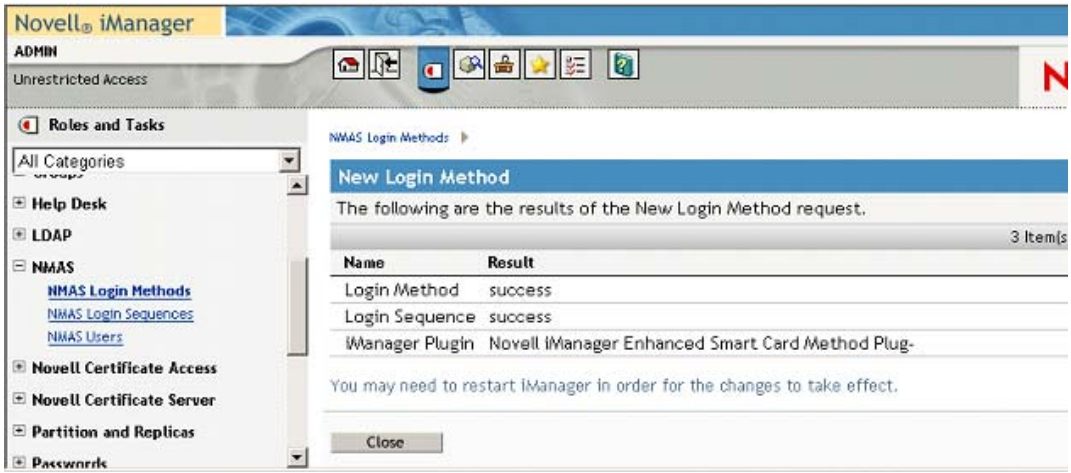
4 Read and accept the license agreement.



5 Review the method information and modify the values as needed.

If you don't change the name, the default name (Enhanced Smart Card) is used for the method and login sequence name.

6 Click *Finish*.



7 Review the installation summary page, then click *Close*.

8 Restart iManager to ensure that the plug-in is enabled.

2.2.2 Client Workstation Installation

The method must be installed on each workstation. To install the method, use the NESCM setup program.

The method can also be installed and configured silently. For more information on silent installation, see Appendix A, "Silently Installing and Configuring the Method on Workstations," on page 49.

1. Log in to a workstation as an Administrator.
2. Run `Setup.exe`.

   This installation program is located in the `...\enhancedsmartcard\client` directory.

   This launches the NESCM setup program. Follow the steps in this setup program to install NESCM. For information concerning specific steps in the setup program, see Table 2-2 on page 15. For extended information on the options, see Chapter 3, "Client Configuration Options," on page 21.
3. Repeat Step 1 and Step 2 for every workstation where you want to install the method.

Table 2-2 explains the configuration options that are available when you use the setup program to install the method on a workstation.

Table 2-2 *Setup Program Options*

Window	Options
Smart Card Interface	The method can communicate with the smart card by using a Windows Cryptographic Service Provider (CSP) or PKCS#11 library. The recommended communication method is CSP with PC/SC Interfaces. Use PKCS#11 interfaces only if you know your smart card vendor does not provide a CSP. ◆ ***CSP with PC/SC Interfaces*****:** Select this option to use MS Crypto APIs and the vendor's CSP. ◆ ***PKCS#11 Library*****:** Select this and specify a PKCS#11 library to use PKCS#11 interfaces. For more information on the smart card interface, see Section 3.1, "Smart Card Interface," on page 21.
Smart Card PIN	The smart card PIN is always validated during login unless this option is turned off (not selected). If this option is off, the PIN is not validated during login. It might be desirable to turn off PIN validation if another application has established a smart card session and previously validated the PIN. This prevents users from having to re-enter the PIN. ◆ ***Require Smart Card PIN Validation*****:** Select this option to validate the PIN during login. For more information on smart card PIN validation, see Section 3.2, "Smart Card PIN Validation," on page 22.

Window	Options
Password Field Descriptor	The Novell Client login dialog box labels the *Password* field with the word “Password.” When using NESCM, enter the smart card PIN in the *Password* field. This option allows you to change the label to a more intuitive description, like “PIN.” ◆ ***Use Custom Descriptor*:** Select this option and enter a new label to change the descriptor. This option is only available if the Novell Client is installed. For more information on the Password Field Descriptor, see Section 3.3, “Password Field Descriptor,” on page 22.
Workstation Only Login	Normally, workstation only logins are password-based. The following options allow the smart card to be used during a workstation only login: ◆ **Use Smart Card for Workstation Only Login:** Select this option to use the smart card for workstation only logins. ◆ ***Require Smart Card for Workstation Only Login*:** Select this option to disable password-based workstation only logins. This option is only available if the Novell Client is installed. For more information on Workstation Only Login, see Section 3.4, “Workstation Only Login (Disconnected Support Login),” on page 23.
User Account Lookup - Identity Plugin Support	The method can use eDirectory to look up the username that is associated with the smart card. The method uses the certificate information on the smart card and performs an LDAP search to locate the user account. ◆ ***Automatically Look Up User Account:*** Select this option if you want the method to automatically look up the user account. This option is only available if the Novell Client is installed. For more information on User Account Lookup, see Section 3.5, “User Account Lookup (Identity Plug-In Functionality),” on page 24.

Window	Options
(Conditional: LDAP Search Options - Page 1) Identity Plugin Configuration	The following options specify how the LDAP search functionality of the Identity Plugin functions: ◆ ***LDAP Servers*:** Specify the server where you want the search to take place. This is the LDAP server IP address or DNS name. ◆ ***LDAP Search Base*:** Specify the starting container to use when searching for the user. ◆ ***LDAP Search Timeout*:** Specify the number of seconds to wait before the search aborts.
(Conditional: LDAP Search Options - Page 2) Identity Plugin Configuration	The following options specify how the LDAP search functionality of the Identity Plugin functions: ◆ ***Search By*:** Select how the search matches user accounts. If you select *Certificate Subject Name*, it searches by the certificate's subject name. If you select *Certificate*, it searches using the complete certificate. This setting should match the method's *Match By* configuration setting. ◆ ***Search Performance*:** Select *Do Complete Search* if you want the search operation to complete the search before returning. Select *Use First Account Returned* if you want the search to quit after receiving the first result. For large directories where searches can take a significant amount of time, selecting *Use First Account Returned* can increase performance. However, if in your environment one certificate is associated with multiple accounts, you should select *Do Complete Search* to ensure that all possible matches are presented to the user.

Window	Options
(Conditional: Progress Message and Login Options) Identity Plugin Configuration	The following options allow you to configure progress messages and login options for the Identity Plugin: ◆ ***Status Message*:** Specify the message that you want to be displayed on the Novell Client Login dialog box while the user lookup is in progress. Leave the field blank for no message. ◆ ***Wait Message*:** Specify the message that you want to be displayed in the Novell Client Login dialog box after user lookup is complete and login has begun. Leave the field blank for no message. ◆ ***Login Options:*** The following login options are available: ◆ **Automatically begin login when user lookup returns:** Select this option to automatically start the login process after the account lookup finishes. If you select this option, the user does not need to click the *OK* button to begin the login process. ◆ **Restart user lookup if login fails:** Select this option to automatically restart the Identity Plugin if the login fails. Selecting both *Automatically begin login when user lookup returns* and *Restart user lookup if login fails* is not recommended. Using these two options simultaneously can lead to failed login attempts that continuously loop.

Window	Options
(Conditional: Novell Client Login Dialog Options) Identity Plugin Configuration	Selecting the following options allows you to hide user interface controls in the Novell Client login dialog: ◆ ***Hide OK Button:*** Select this option only when *Automatically begin login when user lookup returns* is selected. See "(Conditional: Progress Message and Login Options) Identity Plugin Configuration" on page 18 for more information. ◆ ***Hide Cancel Button:*** Select this option if you don't want users to see the *Cancel* button. ◆ ***Hide Advanced Button:*** Select this option if you don't want users to see the additional login dialog box settings. ◆ ***Hide Username Field:*** You might want to select this option when using the user account lookup functionality, because users usually do not interact with the username field. Hiding this field might be considered useful in these circumstances. See "User Account Lookup - Identity Plugin Support" on page 16 for more information. ◆ ***Hide Password Field:*** You might want to select this option when *Automatically begin login when user lookup returns* is selected. After the lookup returns, the login begins and the method prompts the user for a PIN unless PIN validation is turned off. See "Smart Card PIN" on page 15 for more information.

Client Configuration Options

3

When you install the method, you select configuration options for each workstation. This section provides additional information about the workstation configuration options.

For information on how to set these configuration options using the NESCM setup program, see Section 2.2.2, “Client Workstation Installation,” on page 15. Or, if you are installing the method silently, see Appendix A, “Silently Installing and Configuring the Method on Workstations,” on page 49.

3.1 Smart Card Interface

3.1.1 CSP with PC/SC Interfaces

The recommended way for NESCM to communicate with the smart card is by using PC Smart Card interfaces (PC/SC). When using PC/SC interfaces, the smart card middleware vendor provides a Windows Cryptographic Service Provider (CSP). The method automatically detects and uses the proper CSP.

CSP with PC/SC interfaces works with most smart card middleware on Windows.

3.1.2 PKCS#11 Library

If CSP with PC/SC interfaces communication is failing or you know that your smart card vendor doesn’t provide a CSP, you might want to try a PKCS#11 library. When you use a PKCS#11 library, you must specify the correct library (DLL) name. PKCS#11 libraries are vendor-specific, so you need to check with your vendor for the name of the library. Table 3-1 lists common PKCS#11 libraries:

Table 3-1 *Common Vendors and PKCS#11 Libraries*

Vendor	PKCS#11 Library Name
ActivCard	`acpkcs211.dll`
Netsign	`core32.dll`

Vendor	PKCS#11 Library Name
GemPlus	`gclib.dll`
eToken	`eTpkcs11.dll`
Cryptovision	`cvP11.dll`
Rainbow iKey*	`ckdk201.dll` (Only the PKCS#11 mode is functional for iKey devices)

For information on choosing the smart card interface, see “Smart Card Interface” on page 15.

3.2 Smart Card PIN Validation

During the login process, the smart card method needs access to the keys on the smart card. Access is obtained by opening a session with the card and specifying the correct PIN. The card validates the PIN and grants appropriate access.

3.2.1 Turning Off PIN Validation

The default procedure it to always validate the PIN, but this functionality can be turned off. Turning off PIN validation might be desirable if another application has established a public session and has previously validated the PIN.

If PIN validation is turned off, a session with the smart card is established, but the PIN is not presented to the smart card for validation. This prevents the user from needing to enter the PIN a second time.

When smart card PIN validation is off, however, the method still needs access to the keys on the smart card in order to successfully log in. If access is not granted by the smart card, login fails. Therefore, it is recommended that you turn off PIN validation only if you know another application has already validated the PIN for the card. For information on how to turn off PIN validation, see “Smart Card PIN” on page 15.

3.2.2 Hiding the Password Field When PIN Validation is Off

If you are using the Novell Client™ and are turning off PIN validation, you might also want to set the Novell Client properties to hide the login dialog box *password* field. This is because the smart card PIN is not used during the login, so there is no need to show the field. For information on how to hide the login dialog box *password* field, see “(Conditional: Novell Client Login Dialog Options) Identity Plugin Configuration” on page 19.

3.3 Password Field Descriptor

The Novell Client login dialog box uses the string “Password” as the label for the password entry field. When using a smart card for login, the user enters the smart card PIN to log in. To help eliminate confusion, a custom string can be specified that is used instead of the “Password” string.

For example, `&PIN:` could be specified. The ampersand (&) in the string is used to enable the Windows Alt+letter focus functionality. The setup program uses a default descriptor string of "&PIN:".

For information on changing the password field descriptor, see "Password Field Descriptor" on page 16.

NOTE: This option is only available if NESCM is installed with the Novell Client.

3.4 Workstation Only Login (Disconnected Support Login)

Windows workstation login is usually password-based; however, the method supports using the smart card for Windows workstation logins. Workstation smart card login is designed to provide the basic smart card login experience for users when they are not able to connect to the network. An example of this is laptop users who switch between connected and disconnected states.

3.4.1 Certificate Validation

Because Workstation Only Login is designed to work in limited connectivity conditions, only limited certificate validation is performed. Therefore, a successful eDirectory™ smart card authentication must occur before workstation smart card authentication is available. This ensures that the certificate used for login is valid. During a Workstation Only Login, the method verifies that the certificate has not expired and that it was used previously in a successful eDirectory authentication.

3.4.2 Local Account Information

When smart card workstation login is enabled, the method integrates with the Novell Client and stores information on the local machine. This information identifies the Windows account and the certificate used for authentication. The account password is also stored encrypted with a 128-bit AES key.

The 128-bit AES key is generated by using random seed data and the certificate's private key. This links the AES key to the certificate's private key and ensures that each account password is encrypted with a unique encryption key. The random seed data used in the key generation process is stored locally, along with the account information. However, the private key itself is never stored.

During a workstation only login, the encryption key is regenerated and the stored password is decrypted. To successfully generate the encryption key and decrypt the password, the smart card must be present and the user must know the PIN. The account name and decrypted password are then passed to Windows to complete the workstation login.

3.4.3 Fall-Back Procedure

If the workstation only login attempt fails with the smart card, for any reason, the process automatically falls back and attempts a password-based local login. This allows users who know their local account information to log in locally without using a smart card. If *Require Smart Card for Workstation Only Login* is turned on, the method does not fall back and attempt a password-based login, and users are required to use a smart card for a local login. Enabling *Require Smart Card for Workstation Only Login* forces all local logins to use a smart card; no password-based logins are allowed. This means that successful eDirectory smart card logins must occur before any workstation only logins can occur.

Workstation Only Login works best when the local account and eDirectory account names are synchronized. This is because when the account names are synchronized, the user does not need to remember different names for connected (eDirectory) and disconnected (local workstation) logins.

For information on how to implement Workstation Only Login, see "Workstation Only Login" on page 16.

NOTE: Smart card workstation login is only available if NESCM is installed with the Novell Client.

3.5 User Account Lookup (Identity Plug-In Functionality)

NESCM can look up the user account in eDirectory that is associated with the smart card. This eliminates the requirement for users to enter their account names.

3.5.1 LDAP Search

NESCM looks up the user account in eDirectory that is associated with the smart card by running the account lookup functionality before the login. It performs an LDAP search by using the certificate information and an anonymous clear-text connection.

In order to successfully perform the LDAP search, the User Account Lookup settings must be properly configured. See "(Conditional: LDAP Search Options - Page 1) Identity Plugin Configuration" on page 17 for a list of settings and how to configure them.

3.5.2 Optimizing Search Results

Searching large directories spread across numerous servers can take a long time. To optimize search results, create servers that host read-only replicas of all partitions in a sub-tree. You can also configure groups of clients to use these lookup servers.

You should create indexes to optimize search performance. When you search by *Certificate Subject Name*, the sasAllowableSubjectNames attribute should be indexed. When you search by *Certificate*, the userCertificate attribute should be indexed. See "(Conditional: LDAP Search Options - Page 2) Identity Plugin Configuration" on page 17 for information on how to choose search performance options.

3.5.3 User Account Lookup Functionality in Workstation Only Login

The account lookup functionality also is used during smart card workstation only login. (See Section 3.4, "Workstation Only Login (Disconnected Support Login)," on page 23.) During a workstation only login, the lookup functionality searches the locally cached account information.

NOTE: User Account Lookup is only available if NESCM is installed with the Novell Client.

3.6 Novell Client Options

3.6.1 Single Sign-On

When using the smart card method, users enter the card's PIN for eDirectory login and are then prompted to enter a password for the workstation login. The Novell Client Single Sign-On feature can be used to automatically log in to the workstation after the eDirectory login. This is accomplished by securely storing the workstation credentials in eDirectory and using them for future logins.

During Single Sign-On, the Novell Client prompts for the workstation password the first time and stores it in eDirectory. On subsequent logins, the user is not prompted for the workstation password. This improves the user's login experience and is recommended for all advanced eDirectory authentication methods.

3.6.2 Passive Mode Login

Passive Mode Login is functionality added to the Novell Client 4.91 SP3. In passive mode, the Novell Client defers to the default MS GINA for the initial Windows login. After authentication to the workstation, the Novell Client attempts to authenticate to the Novell environment. The functionality was added to the Novell Client to allow environments that use Windows Active Directory* smart card authentication to function correctly. It allows the smart card to be used to authenticate to Active Directory and eDirectory.

In passive mode, the Windows username used for workstation authentication is also used for eDirectory authentication. In order to successfully authenticate, the username must exist in eDirectory, and the client's default location profile must be properly configured with the tree and context information.

To enable passive mode login, the following registry keys must be set:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NWGINA]
```

```
"PassiveMode"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login]
"PassiveModeNDSLogin"=dword:00000001
"PassiveModeNDSLoginSilent"=dword:00000000 or 00000001
"PassiveModeNDSLoginRequired"=dword:00000000 or 00000001
```

Registry setting descriptions:

```
PassiveMode: (0/1) default is 0
0 = normal mode
1 = passive mode

PassiveModeNDSLogin: (0/1) default is 0
0 = don't do Novell login
1 = do Novell login

PassiveModeNDSLoginSilent: (0/1) default is 0
0 = report Novell login errors
1 = don't report Novell login errors

PassiveModeNDSLoginRequired: (0/1) default is 0
0 = don't require Novell login
1 = require Novell login
```

- If PassiveModeNDSLoginRequired is set to True (1), the login experience requires a successful Novell authentication in order to succeed.

  Login scripts are not processed by NWGINA in passive mode. The workaround is to run them after the GINA login. You can do this by placing a run entry in the registry, or you can create an entry in the startup file for Novell login:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\R
    un]
  "nwscript=reg_expand_sz:loginw32.exe %username% /NA /CONT
  ```

- In passive mode, the method's card monitoring functionality does not work when the card removal behavior is set to *Lock Workstation*. This is because MSGINA (not NWGINA) is used for the workstation Lock/Unlock functionality.

Configuring the Server

4

The Novell® Enhanced Smart Card Method is configured by using the Novell iManager Smart Card Login plug-in. For plug-in installation instructions, see Section 2.2.1, “eDirectory Server Installation,” on page 12. Administrators use the plug-in to configure settings for the whole tree, partitions, containers, or individual users.

The plug-in has the following options:

- **Global Settings:** The global settings are used to specify policies for the whole tree. Options configured globally apply to all user objects in the tree.
- **Container Settings:** If the container object is a partition root, the settings are effective for all user objects in the partition. If the container is not a partition root, the settings are effective only for objects in the immediate container. The settings do not affect users in subcontainers below the container.
- **User Settings:** User settings apply to the individual User object.

Each setting is described below and identified as a global, container, or user level setting. Many settings can be configured on all levels. Settings configured at lower levels in the directory hierarchy override higher-level configurations.

4.1 Trusted Root Certificate Containers

Configuration Level: Global

The list of trusted root containers is used for certificate validation. During certificate validation, the method builds the certificate chain. In order to be valid, the certificate chain must end with a trusted root certificate. Trusted root certificates are stored in trusted root containers.

4.2 Certificate Revocation Checking

Configuration Level: Global

Certificate revocation checking is part of the certificate validation process. In order to be considered valid, a certificate must not be revoked. The method supports On-Line Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) checking. The type of revocation checking performed is configured on a per trusted root container basis.

If a trusted root container is not listed in the OCSP or CRL list, revocation checking is not performed for certificates that chain to the trusted root container. If a trusted root container is listed in both the OCSP and the CRL list, both types of revocation checks are performed.

- Section 4.2.1, "OCSP Trusted Root Containers," on page 28
- Section 4.2.2, "CRL Trusted Root Containers," on page 28

4.2.1 OCSP Trusted Root Containers

Certificates that chain to trusted root certificates in containers in this list use OCSP checking. An OCSP responder URL can be specified for each container in the list. If specified, the responder URL overrides OCSP information in a user's certificate.

An OCSP response is signed by using the responder's certificate, and the responder's certificate must be trusted in order for the response to be considered valid. Place the OCSP responder's certificate in the trusted root container to ensure that the certificate is trusted.

4.2.2 CRL Trusted Root Containers

Certificates that chain to trusted root certificates in containers in this list use CRL checking. The CRL distribution point information in the user certificate is used to retrieve the CRL. CRLs are cached in memory on the server after retrieval. This improves the performance of future logins.

The *Grace Period* setting specifies the number of days after a CRL has expired that it is treated as valid. This allows revocation checking to continue, if a new CRL cannot be retrieved from the CRL Distribution Point. If a grace period is not specified and the CRL expiration date has passed, all certificates are considered invalid until a new CRL can be retrieved from the distribution point.

4.3 Certificate Validation

Configuration Level: Global, Container, User

Certificate validation ensures that the user certificate used for login was issued by a trusted Certificate Authority and has not been revoked. In order for certificate validation to work correctly, the settings for trusted root containers and certificate verification must be properly configured.

The certificate chain validation and revocation checking can be enabled or disabled. However, under normal operations there should be no reason to change the default settings.

4.4 Certificate Matching

Configuration Level: Global, Container, User

Certificate matching specifies what part of the certificate presented during login is matched to the target user account. There are three options:

- **Subject Name:** Subject name matching checks the subject name of the login certificate against the subject names configured for the user object. Matching by a certificate subject name is less restrictive than matching by a specific certificate.

- **Certificate:** Certificate matching checks the login certificate against the list of certificates configured for the user object. Certificate-based matching is more restrictive than subject name matching because only a configured certificate can be used for login.
- **No Matching:** No matching means no part of the login certificate must be configured on the target user account. Typically, this option is not used for regular user accounts. A potential use would be for guest accounts. A guest account could be configured as no matching, and then anyone with a valid certificate could log in to the account.

4.5 Certificate Expiration Warning

Configuration Level: Global, Container, User

During login, a user can be notified of an impending certificate expiration. This setting defines the number of days in advance to notify the user of the upcoming certificate expiration. A value of zero means no certificate expiration warnings are given.

4.6 Card Removal Behavior

Configuration Level: Global, Container, User

Card removal behavior defines the action taken when a user removes the smart card from the card reader. There are three options:

- **No Action:** Nothing happens when the smart card is removed from the card reader.
- **Lock Workstation:** The workstation is locked when the smart card is removed from the card reader.
- **Forced Log Off:** The user is logged out of the workstation when the smart card is removed from the card reader. This setting should be used with caution because it can result in the user losing work when the forced logout occurs.

4.7 Check for Certificate Policy

Configuration Level: Global, Container, User

A certificate policy is used to define a specific policy OID that must exist in a login certificate. If this setting is enabled, login certificates must contain the specified policy OID to be considered valid. The policy name and OID information are defined once globally. The check for certificate policy setting can be enabled or disabled throughout the directory hierarchy.

Post-Installation Configuration

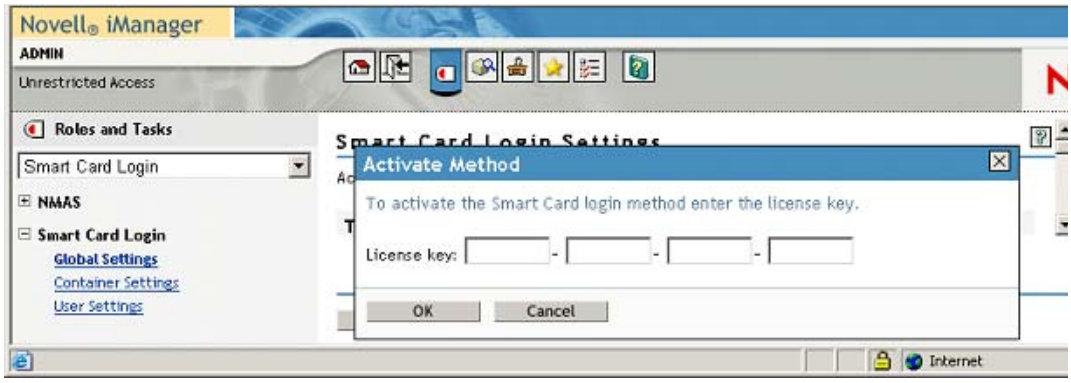
5

After installing the Novell® Enhanced Smart Card Method (NESCM), it is important to use Novell® iManager to complete the configuration steps outlined below.

5.1 Activating the Method

The method has a 90-day trial period. After the trial period, a valid license key must be entered to activate the method. A license key can be obtained from your Novell sales representative.

1 To enter a license key in iManager, click *Smart Card Login* > *Global Setting*. Click *Activate Method* and specify a valid license key.



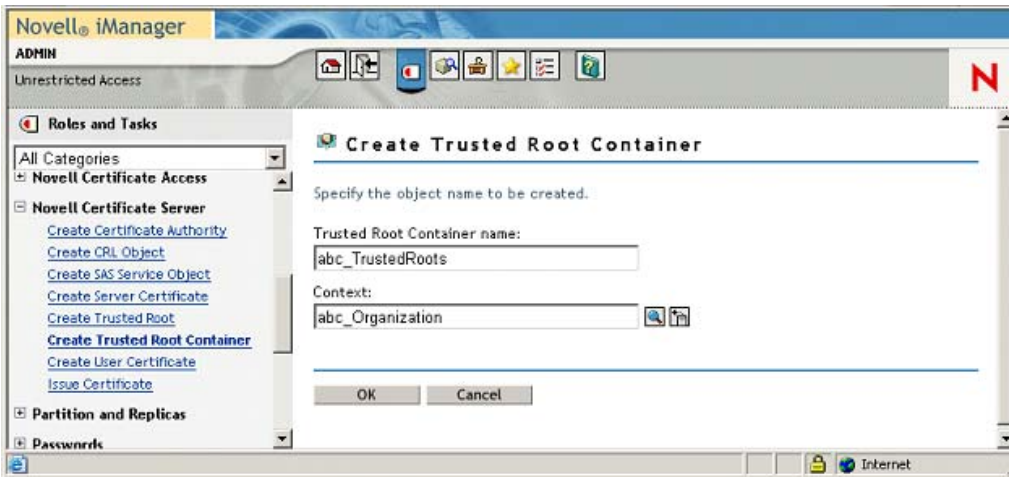
2 Click *OK*.

5.2 Configuring Trusted Root Certificates

The certificate validation process ensures that the login certificate has been issued by a trusted Certificate Authority. This is accomplished by validating that the certificate chain contains only trusted root certificates. Trusted root certificates are stored in trusted root containers in eDirectory™.

1 In iManager, create a trusted root container:

1a Select *Novell Certificate Server* > *Create Trusted Root Container*.

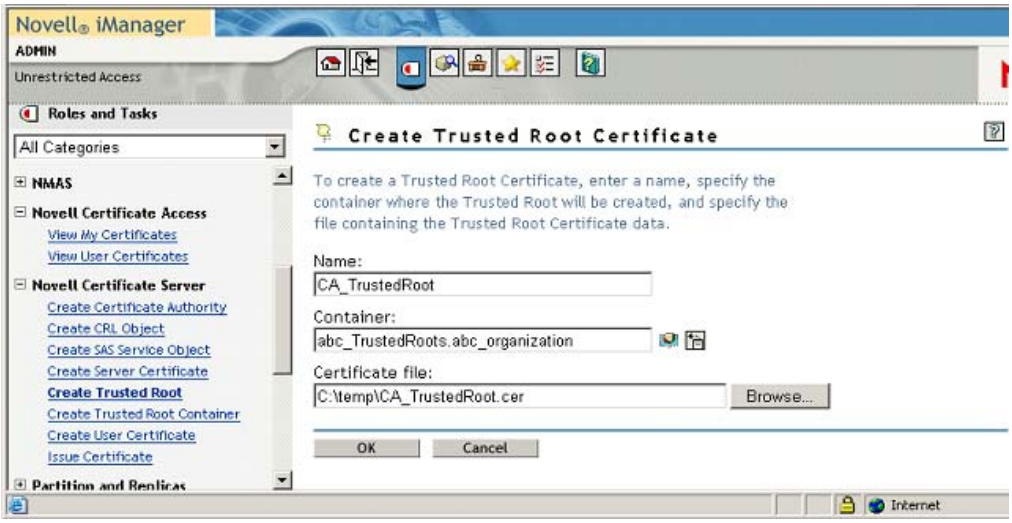


1b Specify the container name and location.

1c Click *OK*.

2 Import trusted root certificates:

2a Select *Novell Certificate Server* > *Create Trusted Root*.



2b Provide a name in the *Name* field. This name is the Trusted Root object that is created in the directory to hold the certificate material. Choose a name that allows you to recognize which CA this issuing certificate came from.

IMPORTANT: This name cannot contain any dot characters. If it does, you encounter an NDS-601 error.

2c For the *Container* field, browse to and select the trusted root container created in Step 1.

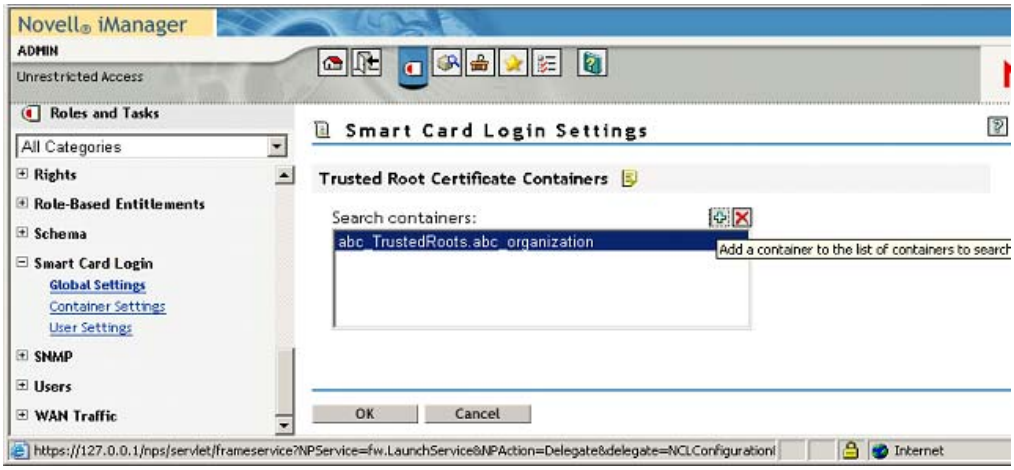
2d For the *Certificate file* field, browse to and select a standard DER file (`*.der` or `*.cer`) or Base 64 encoded DER file (`*.b64`, `*.pem`, or `*.cer`). This file contains the material for the issuing certificate.

If you do not already have this file, consult your CA for information and instructions on how to obtain it.

2e Click *OK*.

3 Add the trusted root container to the method's global settings:

3a Select *Smart Card Login* > *Global Settings*.



3b Click the plus sign to add the trusted root container to the *Trusted Root Certificate Containers* list.

3c Click *OK*.

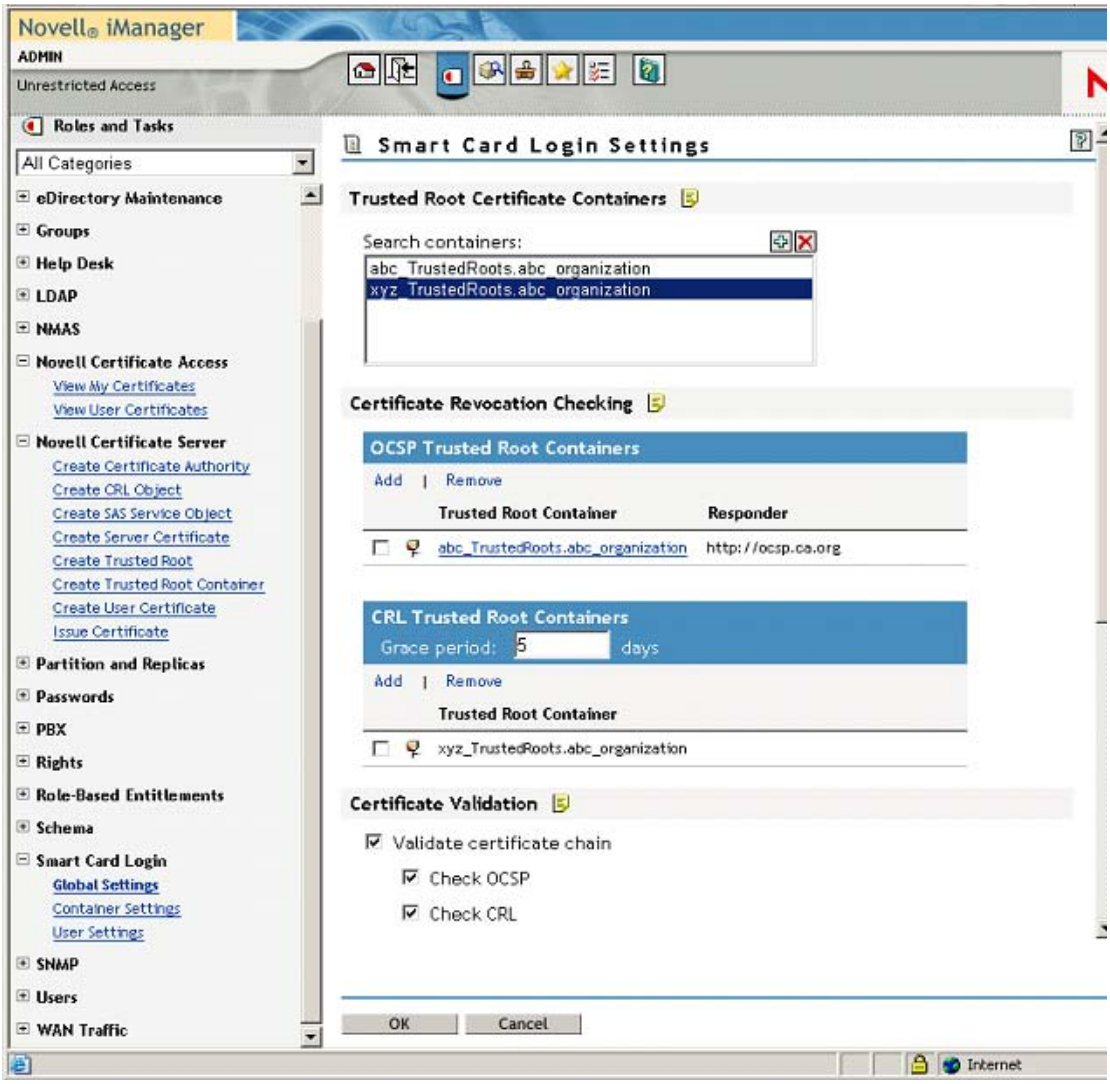
5.3 Configuring Certificate Revocation Checking

Trusted root containers are automatically added to the OCSP and CRL certificate revocation checking lists. Modify the lists as necessary and enable the proper revocation checking option.

In Figure 5-1 on page 34, both OCSP and CRL revocation checking are enabled. OCSP revocation checking is performed for certificates chaining to the abc_TrustedRoots container. CRL checking is performed for certificates chaining to the xyz_TrustedRoots container.

When using OCSP validation, the OCSP response is signed by the responder's certificate. In order for the response to be considered valid, the responder's certificate must be trusted. Place the OCSP responder's trusted root certificate in the trusted root container to identify it as trusted.

Figure 5-1 *Certificate Validation and Search Containers*



5.4 Configuring Users

User objects must be configured with the proper certificate information for login.

1. Using iManager, select *Smart Card Login* > *User Settings*.
2. Fill in the information, depending on the type of certificate matching used:

- Section 5.4.1, “Subject Name Matching,” on page 35
- Section 5.4.2, “Certificate Matching,” on page 36
- Section 5.4.3, “Temporary Certificates,” on page 37

5.4.1 Subject Name Matching

You need to configure the subject name from the login certificate for the user object. You do this by selecting *Add* and specifying the subject name. The subject name can be entered directly, read from a smart card in an attached card reader, or read from a certificate file. DER and PEM certificate files are supported.

Figure 5-2 *Add Subject Name Page*

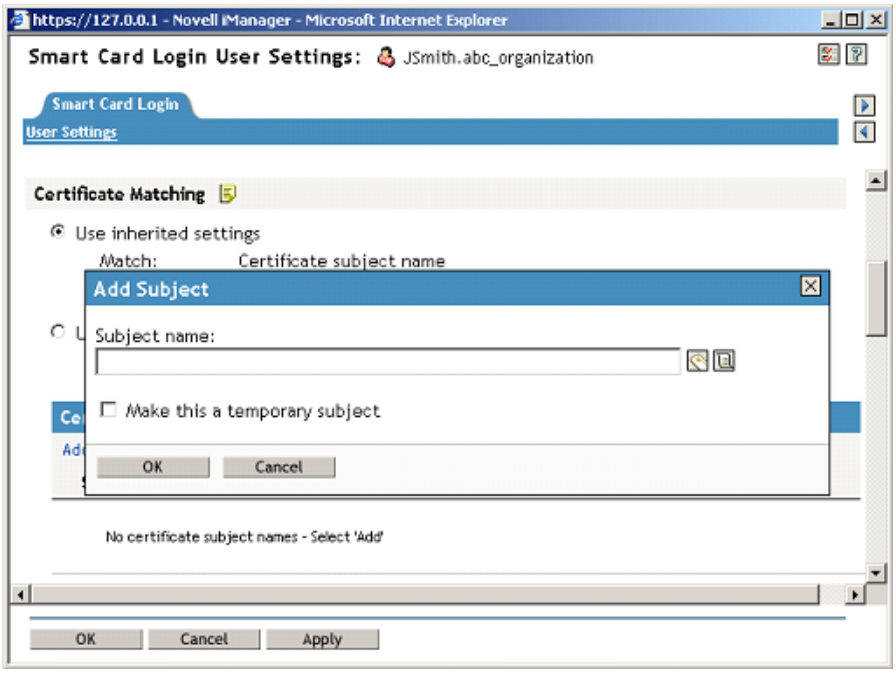
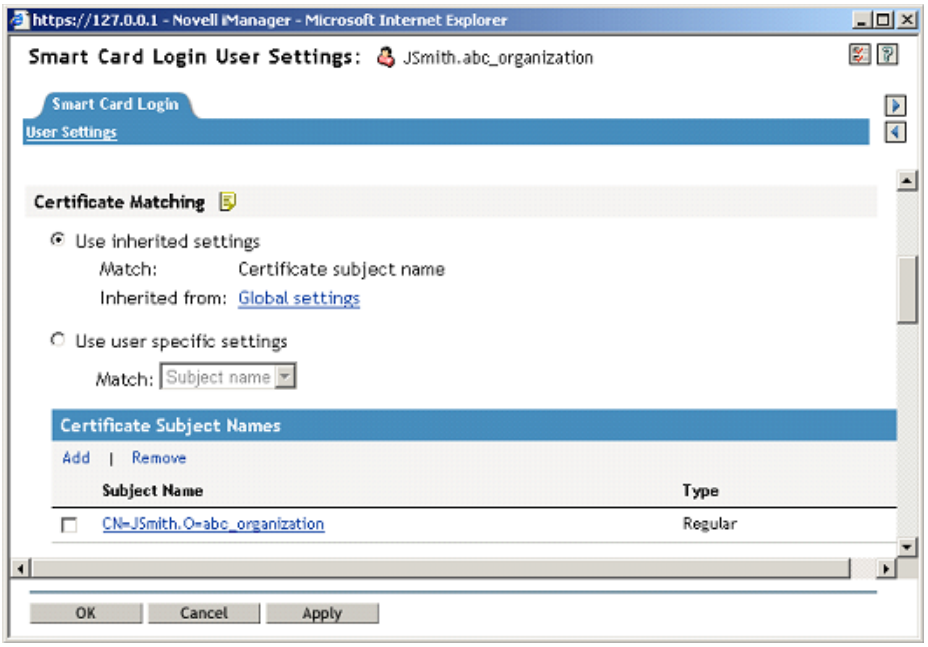


Figure 5-3 is an example of a User object properly configured for subject name matching:

Figure 5-3 *Subject Name Matching Page*



5.4.2 Certificate Matching

You need to configure the specific login certificate for the User object. You do this by selecting *Add* and specifying the certificate. The certificate can be read from a smart card in an attached card reader, or read from a certificate file. DER and PEM certificate files are supported.

Figure 5-4 *Add a Certificate Page*

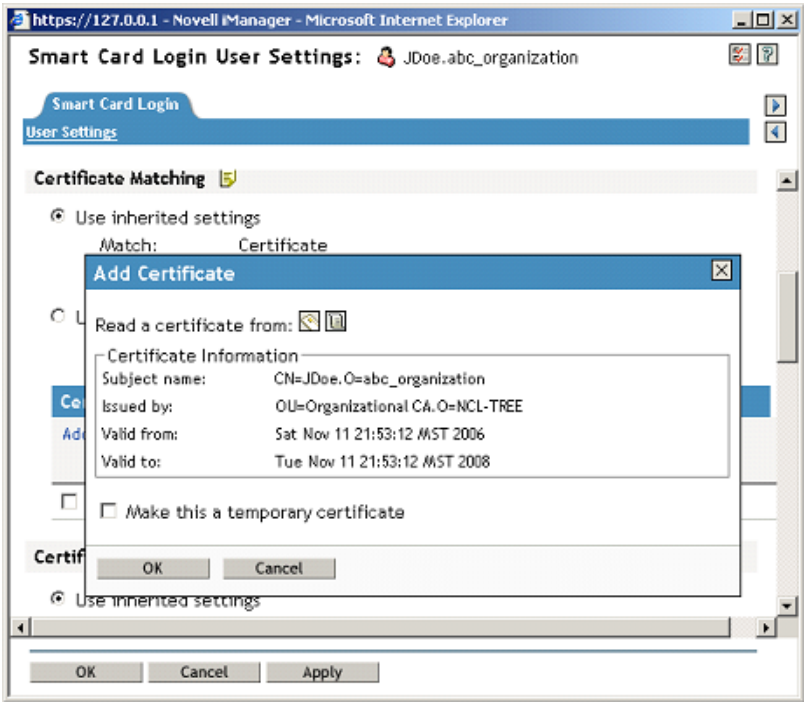
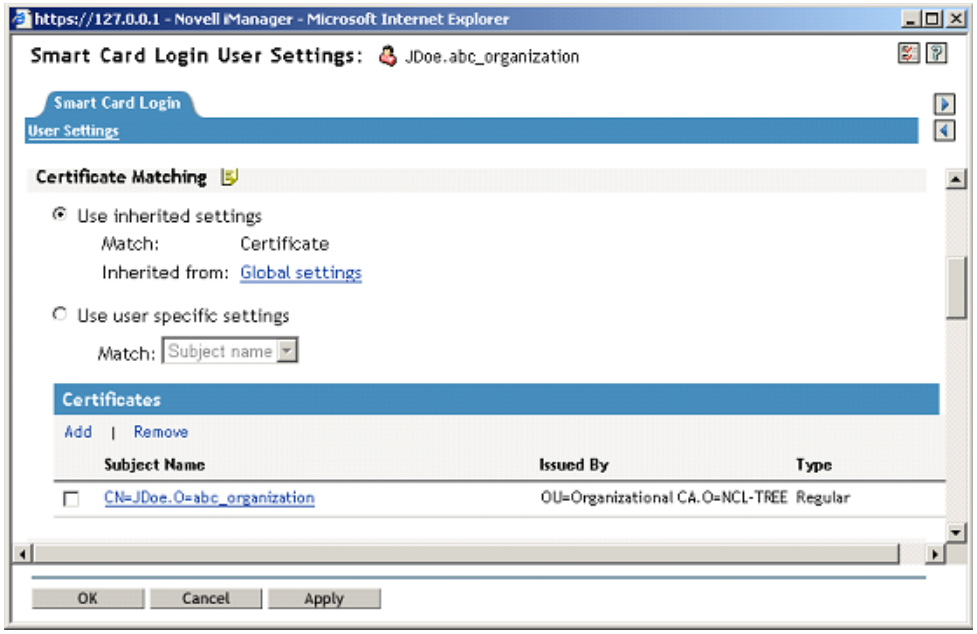


Figure 5-5 is an example of a User object properly configured for certificate matching:

Figure 5-5 *Certificate Matching Page*



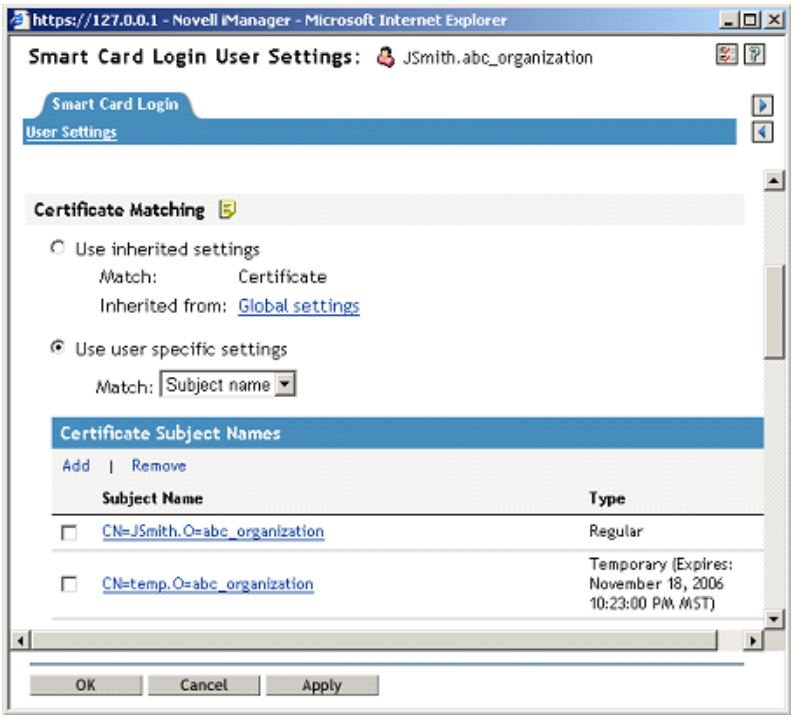
5.4.3 Temporary Certificates

A temporary classification can be assigned to certificates or subject names. You do this by selecting the *Temporary* check box when adding the certificate information. This can be useful in situations where a temporary smart card is assigned to an individual. A typical case might be when an individual misplaces or forgets his or her regular smart card. In this situation, a temporary smart card can be issued to the individual and configured for a short period of time.

A temporary certificate is valid until the specified expiration date. The user is only able to log in using the temporary certificate. If the user attempts a login by using his or her normal certificate, the login fails. After the temporary certificate expiration date passes, the user can log in again by using the regular certificate. Expired temporary certificate information is automatically deleted from the User object.

Figure 5-6 shows a User object configured with a temporary certificate subject name. The regular information still exists for the user, but the temporary configuration overrides it until the expiration date.

Figure 5-6 *Temporary Certificate Subject Name Page*



Troubleshooting

6

In order for a user to successfully log in, the Novell® Enhanced Smart Card Method and the smart card must be properly configured. This section describes common issues and techniques to help diagnose problems.

6.1 Method Tracing

When diagnosing problems, it is often helpful to enable the method's trace functionality. The method reports many problems and failures in the trace logs.

6.1.1 Enabling Server Tracing

On the server, the method reports information to the NMAS™ trace functionality, which is integrated with eDirectory™ tracing. To turn on tracing, use the Novell eDirectory iMonitor tool and select the NMAS option in the trace configuration settings. For more information about iMonitor, see “Using Novell iMonitor”, in the *Novell eDirectory 8.8.3 Administration Guide* (http://www.novell.com/documentation/edir88/edir88/data/agwkqvb.html).

6.1.2 Enabling Client Tracing

On the client, the method reports information to the NMAS Client trace functionality. To turn on tracing, use the NMAS Client Configuration tool (`ncc.exe`).

The following example enables tracing:

```
ncc.exe -ta file=trace_file status=on mode=append
```

After turning tracing on, reboot the workstation to ensure that all processes use the new settings. The trace messages are written to the specified file.

6.2 Workstation Issues

The following issues apply to workstations:

6.2.1 Smart Card Issues

If the login fails with an error message of No Certificates Found, the method failed to read the smart card's certificates. Check the following items:

- The smart card reader is installed and functional.
- The smart card is configured with a valid certificate and associated private key.
- Ensure that the smart card is not locked. Smart cards require a valid PIN to access them. Most smart cards lock after three invalid PIN attempts.
- The proper smart card middleware is installed and operational. Most middleware includes tools for viewing the information on the smart card.
- The method is properly configured to communicate with the middleware. During installation, a smart card communication interface is selected. The recommended setting is PC/SC. If PC/SC communication is failing, you might want to try PKCS#11. When using PKCS#11, you must also specify the correct vendor library (DLL). The library must be in the system path so it can be loaded by the method. You might need to contact the middleware vendor for the specific PKCS#11 library name. For a list of common vendors and PKCS#11 libraries, see Table 3-1 on page 21.

6.2.2 User Account Lookup (Identity Plug-In) Issues

Because the User Account Lookup searches the directory before the actual login, it requires anonymous browse rights to be enabled in eDirectory. If the directory restricts anonymous browse, User Account Lookup does not work.

6.2.3 Novell Client Single Sign-On Issues

The single sign-on functionality in Novell Client™ 4.91 SP3 does not work correctly. The problem has been identified and the Novell Client team has released a fix. Download and install the fix from the Novell Support Web site (http://www.novell.com/support/supportcentral/supportcentral.do?id=m1).

6.3 Method Configuration Issues

The following issues apply to method configuration:

- Section 6.3.1, “Method Activation,” on page 40
- Section 6.3.2, “Certificate Validation,” on page 41

6.3.1 Method Activation

If a valid license key is not entered by using iManager, the method stops functioning after the 90-day trial period has expired. Enter a valid license key to enable the method. For information on how to enable the method, see Section 5.1, “Activating the Method,” on page 31.

6.3.2 Certificate Validation

If the method fails with an Invalid Certificate or Certificate Validation Failed message, the method was unable to validate the certificate sent by the workstation. Check the following items:

- The certificate on the smart card is not expired or has not been revoked by the issuing Certificate Authority.
- The method is properly configured with a trusted root container that contains a valid trusted root certificate. See Section 5.2, “Configuring Trusted Root Certificates,” on page 31 for information about configuring the trusted root container.
- Certificate revocation checking is properly configured. See Section 5.3, “Configuring Certificate Revocation Checking,” on page 33 for more information.
- CRL and OCSP revocation checking requires connectivity to the CRL Distribution Point or OCSP Responder. If the information is unavailable, the validation process fails.

  When using OCSP validation, the OCSP response is signed by the responder's certificate. In order for the response to be considered valid, the responder's certificate must be trusted. Place the OCSP responder's trusted root certificate in the trusted root container to identify it as trusted.

Security Guidelines

7

As with any system, good security requires proper configuration. This section lists recommendations to ensure that the Novell® Enhanced Smart Card Method functions securely.

7.1 Trusted Root Containers

These containers must include only certificates from trusted Certificate Authorities. Administration of the certificates in these containers should be restricted.

7.2 Certificate Validation/Revocation Checking

Certificate validation should be enabled and revocation checking properly configured. If a CRL Grace Period is used, the grace period should be limited to a few days. Do not use the CRL Grace Period as a mechanism to work around a dysfunctional CRL infrastructure.

7.3 Smart Card Enrollment eDirectory Attributes

Administration of the user attributes used for smart card authentication should be restricted to administrators who are enrolling smart cards for users.

When matching by subject names, the attributes are:

- sasAllowableSubjectNames
- nclTmpCertSubject
- nclTmpCertExpiration

When matching by certificates, the attributes are:

- userCertificate
- nclTmpCert
- nclTmpCertExpTime

7.4 Certificate Matching

The certificate matching settings should be set to *Subject name* matching or *Certificate* matching. Certificate matching is more restrictive because it checks the login certificate against the list of certificates configured for the user. The *No matching* option should be used only in specific guest

account scenarios as described in Section 4.4, “Certificate Matching,” on page 28. For information on how to configure certificate matching options by using iManager, see Section 5.4, “Configuring Users,” on page 34.

7.5 Restricting Authentication Methods

Users can be restricted to using the smart card authentication method only. This is accomplished by restricting the user to a specified NMAS™ authentication sequence. “Managing Login Sequences” in the *NMAS Administration Guide* (http://www.novell.com/documentation/nmas311/pdfdoc/admin/admin.pdf) describes how to do this.

7.6 User Account Lookup (Identity Plug-In)

User Account Lookup searches the directory by using an anonymous LDAP clear text connection. This should be a consideration when choosing whether to use the User Account Lookup functionality.

7.7 Workstation Only Login (Disconnected Login)

The Workstation Only Login functionality encrypts the password used to log in to the Windows local account and stores it in the registry. The password is encrypted by using a 128-bit AES key generated by using the private key on the smart card. This should be a consideration when choosing whether to use the Workstation Only Login functionality.

Using NESCM for Access Manager Authentication

8

Novell® Access Manager is a comprehensive access management solution that provides secure access to Web and enterprise applications. Access Manager also provides single sign-on across technical and organizational boundaries, and uses Secure Assertions Markup Language (SAML) and Liberty Alliance protocols.

You can use the Novell® Enhanced Smart Card Method (NESCM) to authenticate to Access Manager.

The following prerequisites apply:

- Be able to authenticate to eDirectory™.
- Install the Novell Enhanced Smart Card Method. For information on how to install NESCM, see Section 2.2, "Installing the Method," on page 12. These instructions require you to install the method on the eDirectory server and on the client workstation, and assume that a functioning smart card reader is already installed. Follow instructions from your manufacturer and verify the workstation's ability to read data from your card.
- Configure the NESCM server by following the guidelines presented in Chapter 4, "Configuring the Server," on page 27.
- Properly provision your smart card according to your company policy.
- Make sure you have a basic Access Gateway configuration with a protected resource that you want to protect with a smart card. For more information, see the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager/installation/data/bookinfo.html) and the *Novell Access Manager Setup Guide* (http://www.novell.com/documentation/novellaccessmanager/basicconfig/data/bookinfo.html).

To integrate NESCM as an authentication agent to Novell Access Manager, complete the tasks described in the *Novell Access Manager Administration Guide* (http://www.novell.com/documentation/novellaccessmanager/adminguide/data/bdptdqh.html).

Novell Audit Integration

9

The Novell® Enhanced Smart Card Method can report login events to the Novell Audit system. The smart card login events include specific information about the certificate used for login (Serial Number, Subject Name, Issuer, Expiration Date).

In order to report audit events, the audit system must be installed and properly configured for eDirectory™. The method includes an audit configuration file (`esc_en.lsc`), which is used to create a audit log application.

See the Novell Audit Documentation Web site (http://www.novell.com/documentation/novellaudit20/index.html) for specifics on configuring audits and creating log applications.

Silently Installing and Configuring the Method on Workstations

A

The Novell® Enhanced Smart Card Method (NESCM) has many options that are configured during an interactive install. The recommended procedure for silently installing the method is to install the method using the default options, and then change the configuration settings as needed, after the method is installed.

- Section A.1, "Using the Default Options to Silently Install and Configure the Method," on page 49
- Section A.2, "Specifying Options on the Command Line to Silently Install and Configure the Method," on page 50

Before silently installing NESCM from a command line, you should become familiar with the graphical install and its options. For more information on the graphical install, see Section 2.2.2, "Client Workstation Installation," on page 15.

A.1 Using the Default Options to Silently Install and Configure the Method

- Section A.1.1, "Installing the Method With the Default Options," on page 49
- Section A.1.2, "Using the Registry File to Configure NESCM After Installation (Recommended)," on page 50
- Section A.1.3, "Default Installation Options," on page 50

A.1.1 Installing the Method With the Default Options

Use the following command to install the method silently with the default options:

```
setup.exe /s /v"/qn".
```

NOTE: If you are installing on a machine with the Novell Client™, the install sets the Windows Installer REBOOT flag to trigger a reboot at the end of the install. You can suppress the reboot by specifying a reboot option on the command line. The following example demonstrates installing silently and setting the REBOOT option:

```
setup.exe /s /v"/qn REBOOT=reallysuppress"
```

To see what the default installation options are, see Table A-1, "Default Installation Options," on page 50.

A.1.2 Using the Registry File to Configure NESCM After Installation (Recommended)

In order to facilitate modifying the configuration after an install, the `nescm.reg` registry file is included with the install. This file documents the method's options. All registry settings in the file are initially commented out. To configure NESCM, uncomment and modify the desired settings, then apply the settings to the registry.

A.1.3 Default Installation Options

Table A-1 *Default Installation Options*

Functionality	Option
Smart Card Interface	CSP with PC/SC Interfaces
Smart Card PIN	Require Smart Card PIN Validation = TRUE
Password Field Descriptor	Use Custom Descriptor = TRUE
	Custom Descriptor: &PIN:
Workstation Only Login - Disconnected Login	Use Smart Card for Workstation Only Login = FALSE
User Account Lookup - Identity Plugin Support	Automatically look up the user account = FALSE

A.2 Specifying Options on the Command Line to Silently Install and Configure the Method

The setup program allows options to be specified on the command line. If you need to change only a few of the default options during an install, you can specify them on the command line. (See Table A-2 through Table A-6 for details.) However, if you need to specify numerous options, you might find it easier to install the method with the default settings, and then modify the `nescm.reg` file, as described in Section A.1.2, "Using the Registry File to Configure NESCM After Installation (Recommended)," on page 50.

The following tables are functionalities that can be configured on the command line:

- Table A-2, "Smart Card Interface," on page 51
- Table A-3, "Smart Card PIN Validation," on page 51
- Table A-4, "Password Field Descriptor," on page 51
- Table A-5, "Workstation Only Login - Disconnected Login," on page 51
- Table A-6, "User Account Lookup - Identity Plugin Support," on page 52

For additional information about installation options, see Table 2-2, "Setup Program Options," on page 15.

Table A-2 *Smart Card Interface*

Options	Values
NESCM_SCINTERFACE	◆ PCSC (Default) ◆ PKCS11
NESCM_PKCS11LIBRARY	◆ PKCS#11 library name

The following example changes the interface mode to PKCS#11 on the command line:

```
setup.exe /s /v"/ qn NESCM_SCINTERFACE=PKCS11 NESCM_PKCS11LIBRARY=abc.dll"
```

Table A-3 *Smart Card PIN Validation*

Option	Values
NESCM_CARD_LOGIN	◆ 1 = True, validate smart card PIN (Default) ◆ 0 = False

The following example turns off smart card PIN validation:

```
setup.exe /s /v"/qn NESCM_CARD_LOGIN=0"
```

Table A-4 *Password Field Descriptor*

Option	Values
NESCM_PWDFIELD_DESC	◆ 1 = True, validate smart card PIN (Default) ◆ 0 = False The default value is “&PIN:”. To remove the default, specify an empty string. If nothing is specified, the Novell Client uses the string “Password:”. If the new string contains spaces, the string must be enclosed in double quotes, and the quotes must be escaped with a backslash.

The following example specifies a new value that contains spaces:

```
setup.exe /s /v"/qn NESCM_PWDFIELD_DESSC=\"Card PIN\" "
```

The following example specifies nothing, and therefore results in a default value of “Password.”:

```
setup.exe /s /v"/qn NESCM_PWDFIELD_DESC=\"\" "
```

Table A-5 *Workstation Only Login - Disconnected Login*

Options	Values
NESCM_DISCONNECTED_SUPPORT	◆ 1 = True, enable disconnected support ◆ 0 = False (Default)

Options	Values
NESCM_DISCONNECTED_REQUIRED	◆ 1 = True, require disconnected support ◆ 0 = False (Default)

The following example turns on disconnected support and makes it required:

```
setup.exe /s /v"/qn NESCM_DISCONNECTED_SUPPORT=1
NESCM_DISCONNECTED_REQUIRED=1 "
```

Table A-6 *User Account Lookup - Identity Plugin Support*

Options	Values
NESCM_IDPLUGIN_SUPPORT	◆ 1 = True, enable Identity Plugin Support ◆ 0 = False (Default)
NESCM_IDPLUGIN_SERVERS	◆ LDAP server address or DNS name
NESCM_IDPLUGIN_SEARCHBASE	◆ Directory container name
NESCM_IDPLUGIN_SEARCHTIMEOUT	◆ Timeout value
NESCM_IDPLUGIN_SEARCHBY	◆ 1 = Search by certificate subject name (Default) ◆ 2 = Search by certificate
NESCM_IDPLUGIN_USEFIRSTMATCH	◆ 1 = True, use first account returned ◆ 0 = False, do a complete search (Default)
NESCM_IDPLUGIN_PROMPTMSG	◆ Status message string
NESCM_IDPLUGIN_WAITMSG	◆ Wait message string
NESCM_IDPLUGIN_AUTOLOGIN	◆ 1 = True, begin login when plug-in returns ◆ 0 = False (Default)
NESCM_IDPLUGIN_AUTORESTART	◆ 1 = True, restart plug-in if login fails ◆ 0 = False (Default)
NESCM_IDPLUGIN_HIDEOK	◆ 1 = True, hide *OK* button ◆ 0 = False (Default)
NESCM_IDPLUGIN_HIDECANCEL	◆ 1 = True, hide *Cancel* button ◆ 0 = False (Default)
NESCM_IDPLUGIN_HIDEADVANCED	◆ 1 = True, hide *Advanced* button ◆ 0 = False (Default)
NESCM_IDPLUGIN_HIDEUSERNAME	◆ 1 = True, hide *Username* field ◆ 0 = False (Default)
NESCM_IDPLUGIN_HIDEPASSWORD	◆ 1 = True, hide *Password* field ◆ 0 = False (Default)

Options	Values

The following example enables Identity Plugin support and sets basic parameters. Unspecified parameters use the default values.

NOTE: String values are enclosed with double quotes, and quotes are escaped with a backslash.

```
setup.exe /s /v"/qn NESCM_IDPLUGIN_SUPPORT=1
NESCM_IDPLUGIN_SERVERS=\"192.168.43.113:389\"
NESCM_IDPLUGIN_SEARCHBASE=\"ou=searchbase\" NESCM_IDPLUGIN_SEARCHTIMEOUT=20
NESCM_IDPLUGIN_AUTOLOGIN=0 NESCM_IDPLUGIN_AUTORESTART=0 "
```

How the Authentication Works

B

In order to successfully log in, the smart card must contain an X.509 certificate and the certificate's private key. The following information details the process used by the method during the login:

1. The Login Client Module (LCM) enumerates the certificates on the smart card and sends them to the Login Server Module (LSM).
2. The LSM selects the certificate to use for login. In order to be selected, a certificate must be valid and must be associated with the user account. The validation process uses the PKI functionality in eDirectory™ to verify that the certificate meets the following requirements:
   - It has been issued by a trusted authority
   - It has not been revoked
   - It has not expired

   CRL and OCSP revocation checking are supported.
3. The LSM sends a message to the LCM telling it which certificate and challenge to use. The challenge is random data, and is used in step 5.
4. The LCM presents the PIN to the smart card for validation.
5. The LCM requests for the smart card to sign the challenge (received in Step 3), using the certificate's private key. The signature is SHA1 with RSA encryption or MD5 with RSA encryption.

   The LCM proves it has access to the certificate's private key by being able to successfully sign the LSM challenge.
6. The LCM sends the signed challenge to the LSM for verification. The LSM can verify the signature because it has the X.509 certificate from Step 1, which contains the certificate's public key. If the challenge is verified, the LSM reports login success to the NMAS™ service.

Registry Configuration Settings

C

NESCM configuration settings are stored in the Windows registry. The `nescm.reg` file, which is included with the client setup program, documents the registry settings. For more information, see Section A.1.2, “Using the Registry File to Configure NESCM After Installation (Recommended),” on page 50