Novell
Enhanced Smart Card Method

3.0.3

www.novell.com

INSTALLATION GUIDE

March 21, 2008

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.

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 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).

Additional Documentation

To view other related Identity Assurance Solution (IAS) documentation, see the *Novell Identity Assurance Solution 3.0.2 documentation website* (http://www.novell.com/documentation/ias302/index.html).

Documentation Conventions

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

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

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

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 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 disconnected or local Windows* workstation logins. Disconnected support 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. Upon smart card removal, the method can be configured to lock the workstation, log off the workstation, or take no action.

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 2003 Server 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

Web-Based Administration Using iManager

- 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 ◆ Crypto Vision 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 ◆ Crypto Vision - 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.

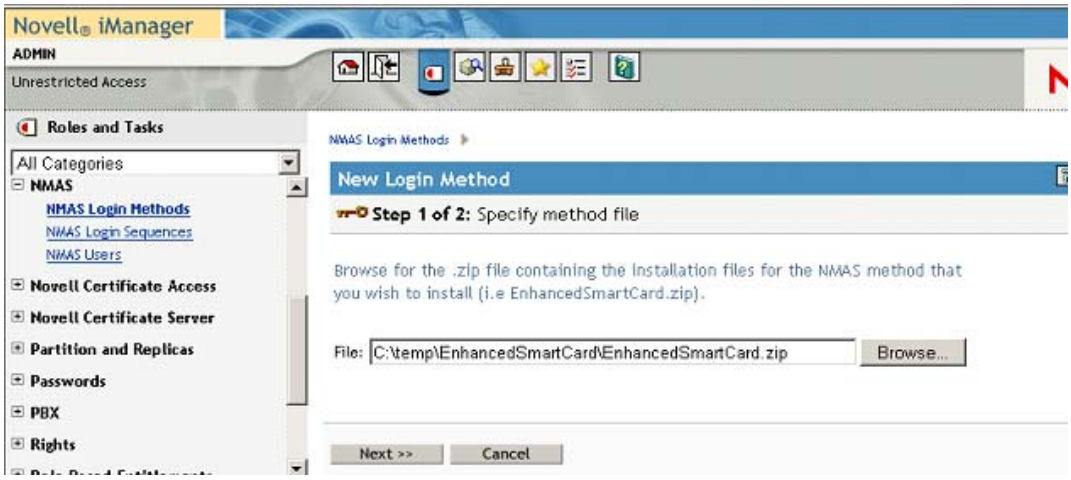
- Section 2.2.1, “eDirectory Server Installation,” on page 12
- Section 2.2.2, “Client Workstation Installation,” on page 15

2.2.1 eDirectory Server Installation

The method is installed by using iManager.

1 Log in to iManager as an Administrator.

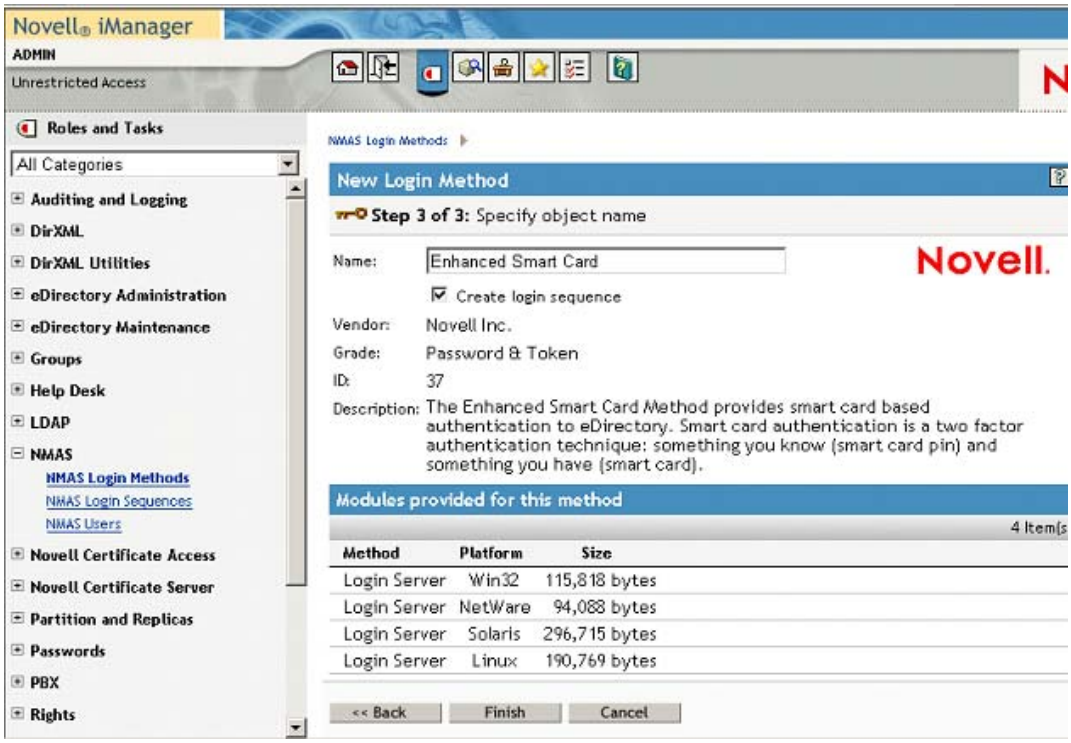
2 From Roles and Tasks, select *NMAS* > *NMAS Login Methods*, then select *New*.



3 Click *Browse* and select 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.

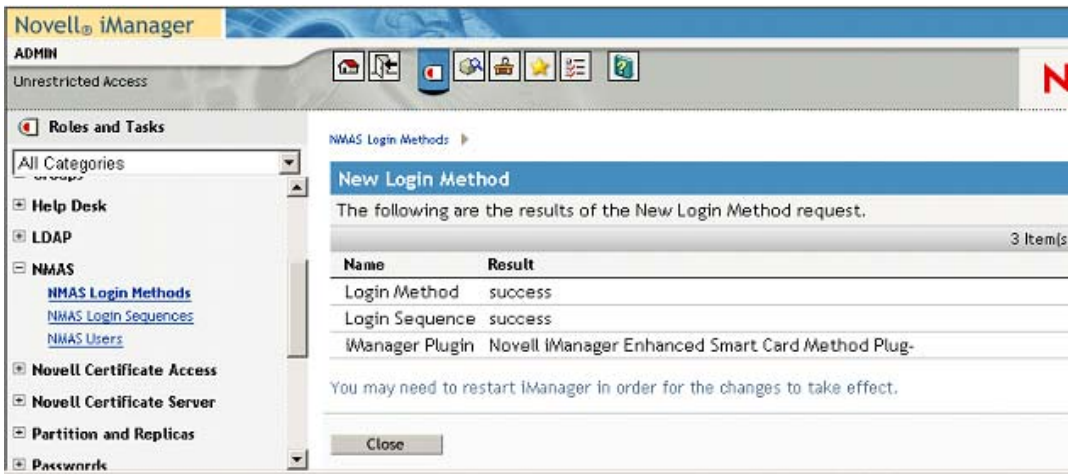
4 Read and accept the license agreement.



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. This can also be done with a silent install. For more information on silent method installation, see Appendix A, “Silent Method Installation on Workstations,” on page 47.

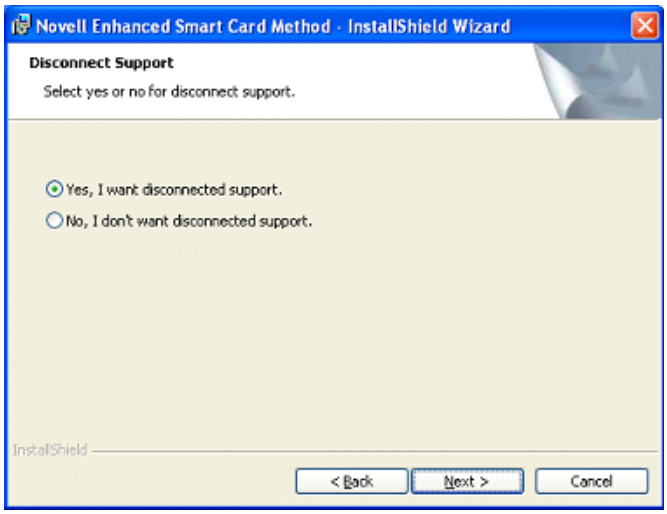
1 Log in to each workstation as an Administrator.

2 Run `Setup.exe`.

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

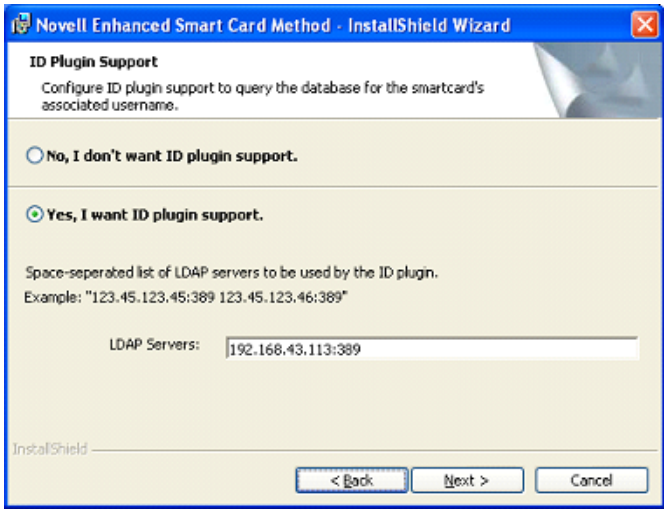
3 Review the Welcome Screen, then click *Next*.

4 Accept the License Agreement, then click *Next*.



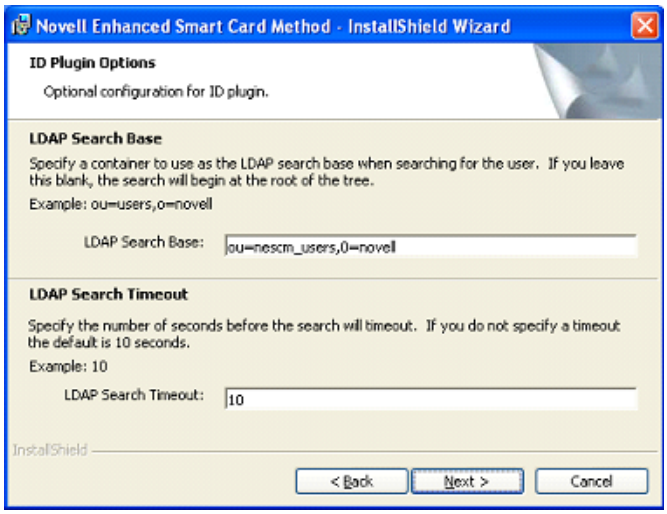
5 Choose whether you need disconnected support, then click *Next*.

Disconnected support allows you to log in to the workstation locally by using the smart card. For more information on disconnected support, see Section 3.1, “Disconnected Support,” on page 19.



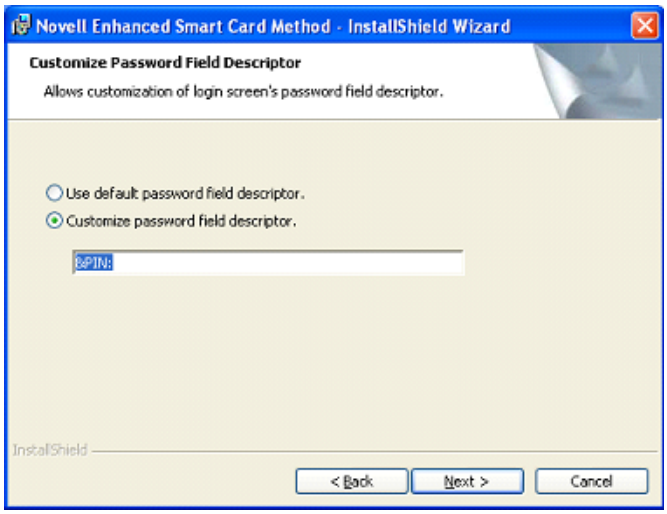
6 If you want ID Plugin support, select *Yes* and specify the LDAP server’s DNS name or IP address, then click *Next*.

For more information on ID Plugin functionality, see Section 3.2, “Identity Plug-In (ID-Plugin) Functionality,” on page 19.



7 (Conditional) If you selected ID Plugin support, you must also specify the container to search and the search timeout period, then click *Next*.

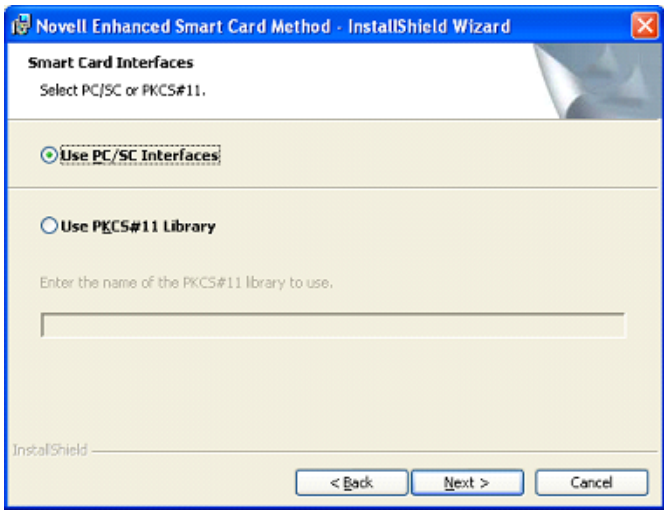
The ID Plugin does a sub-tree search starting at the specified base.



8 To use a custom password field description, select *Customize password field description* and type the custom description, then click *Next*.

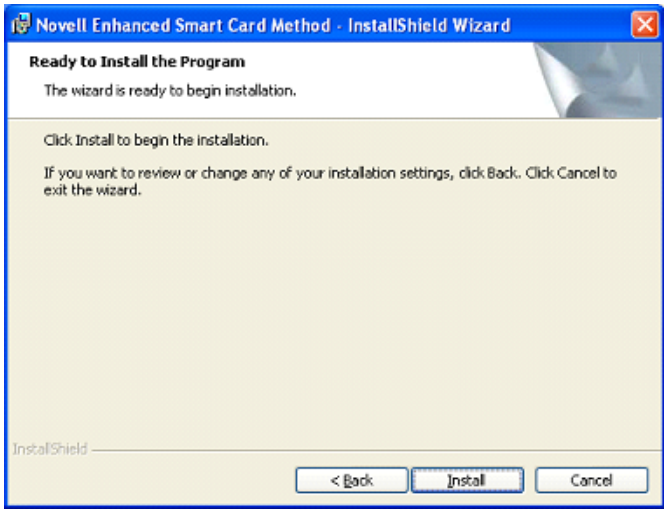
Use an ampersand (&) in the description to enable Windows Alt+letter functionality. In the example above, Alt+P would place focus on the field labeled with the “PIN:” description.

For more information on the custom password field description, see Section 3.3, “Custom Password Field Descriptor,” on page 20.



9 Select the communication interface the method will use to connect to the smart card, then click *Next*.

PC/SC functionality is the preferred interface. Select PKCS#11 if you know the smart card middleware does not integrate with the Windows PC/SC functionality. If you select PKCS#11, you must also specify a name of the module that is to be used. For more information on the smart card interface, see Section 3.4, “Smart Card Interface,” on page 20.



10 Click *Install*.

You can automatically distribute the method to each workstation by using tools such as ZENworks®. See Appendix A, “Silent Method Installation on Workstations,” on page 47 for detailed information about scripting the method install.

Configuring the Client

3

The section provides information about the client configuration options that are selected during the install. If you need to change the configuration after an install, remove and reinstall the method.

3.1 Disconnected Support

Disconnected support allows the smart card to be used for a local workstation login when eDirectory™ isn't available. This is useful in situations where network connectivity isn't always available, such as for laptop users. After a connected eDirectory login, the disconnected functionality stores the local username and password on the local machine for future disconnected logins. The local account password is encrypted with a 128-bit AES key generated from the smart card private key. This means that a successful connected login must occur before disconnected functionality is available.

To perform a disconnected login, select the Novell® Client™ *Workstation only* check box when you first log in, then enter the local account name and smart card PIN. The previously stored local account information is decrypted by the smart card and passed on to Windows for the workstation login.

Disconnected support works best in situations where the local account and eDirectory account names are synchronized. When the account names are synchronized, the user does not need to remember different names for connected (eDirectory) and disconnected (local workstation) logins.

If the disconnected login fails, the default process is to attempt a normal username/password local login. This allows users who know local account information to log in without using the smart card. If this is not desirable, the process is changed by using the disconnected_required configuration setting.

3.2 Identity Plug-In (ID-Plugin) Functionality

The ID-Plugin functionality automatically looks up the user account based on the smart card's certificate. In order to do this, the Identity plug-in runs before the login and performs an LDAP directory search for a user account match. When installing, you must specify the LDAP server and LDAP search base. The ID-Plugin does an LDAP subtree search starting at the specified search base.

3.3 Custom Password Field Descriptor

The Novell Client uses a default password string to label the password entry field. When using a smart card for login, users enter the card's PIN, not a password, for login. To help eliminate confusion, a custom string can be specified that is used instead of the default password string. For example, `&PIN:` could be specified. The ampersand (&) in the description is used to enable the Windows Alt+letter focus functionality.

3.4 Smart Card Interface

The method can communicate with the smart card by using PC/SC interfaces or PKCS#11 interfaces. When using PC/SC interfaces, the smart card middleware vendor provides an MS CAPI provider. The method can automatically detect and use the proper MS CAPI provider. PC/SC mode is the recommended setting and should work with most smart card middleware on Windows.

If PC/SC communication is failing, you might want to try PKCS#11. When using PKCS#11, you must specify the correct vendor PKCS#11 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. Below is a table of common PKCS#11 libraries.

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

Vendor	PKCS#11 Library Name
ActivCard	`acpkcs211.dll`
Netsign	`core32.dll`
GemPlus	`gclib.dll`
eToken	`eTpkcs11.dll`
CryptoVision	`cvP11.dll`
Rainbow iKey	`ckdk201.dll` (Only the PKCS#11 mode is functional for iKey devices)

3.5 Novell Client 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 into the workstation after the eDirectory login. This is accomplished by securely storing the workstation credentials in eDirectory and using them for future logins.

When using 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 Novell Client Passive Mode Login

Passive Mode Login is new 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
```

The following is additional information regarding the Novell Client passive mode and the method:

- 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
```

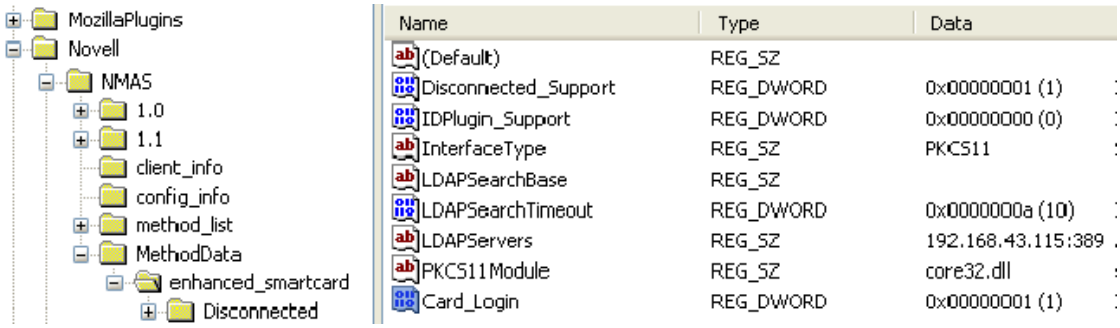
- In passive mode, the method's card monitoring functionality does not work when set to *Lock Workstation* on card removal. This is because MSGINA (not NWGINA) is used for the workstation Lock/Unlock functionality.

3.7 NESCM Client Configuration Options

The Novell Enhanced Smart Card Method (NESCM) registry values are located in the following key:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NMAS\MethodData\enhanced_smartcard`

Figure 3-1 *NESCM Registry Directory*



3.7.1 NESCM Registry Values

The basic descriptions for the NESCM registry values are listed in the following table:

Table 3-2 *NESCM Registry Values*

Registry Value	Description
`InterfaceType`	Defines the type of interface used to communicate with the smart card: • **PCSC:** The method uses Windows PC/SC functionality in conjunction with a MS CAPI provider. The method automatically detects the proper MS CAPI provider to use. PC/SC mode is the recommended operating mode. • **PKCS11:** The method uses PKCS#11 interfaces. If this mode is specified, the PKCS11Module setting must also be specified.
`PKCS11Module`	Specifies the name of the PKCS#11 library (DLL) to use.

Registry Value	Description
Card_Login	Directs the Client-side login client method (LCM) to skip the smart card login step. ◆ 1=TRUE (default): The method uses the PIN to log in to the smart card. ◆ 2=FALSE: The method does not use the PIN to log in to the smart card. If another process has already used the pin to log in to the smart card and you do not want to require another smart card login, skipping the smart card login step might be desirable. **NOTE:** A valid smart card login must occur in order for the method to succeed. Only set the setting to FALSE (Card_Login = 0) if another process is performing the smart card login.
Disconnected_Support	Specifies to use the smart card login during a workstation-only login: ◆ 1=TRUE ◆ 2=FALSE (default)
Disconnected_Required	Directs the Disconnected_Support setting to specify how disconnected support works. ◆ 1=TRUE: The smart card must be used for a successful workstation-only login. ◆ 2=FALSE (default): The smart card login is not required for workstation-only login and a standard username/password login is performed if the smart card login fails.
IDPlugin_Support	Specifies to use the ID-Plugin to find the username associated with the smart card: ◆ 1=TRUE ◆ 2=FALSE
LDAPServers	Lists the LDAP servers to be used by the ID-Plugin; for example, 123.45.123.45:389.
LDAPSearchBase	Specifies the LDAP search base used by the ID-Plugin. Leave this setting blank to search from the root of the directory; for example, ou=users,o=novell.
LDAPSearchTimeout	Specifies the LDAP search timeout (in seconds) for the ID-Plugin. The default timeout is 10 seconds

Configuring the Server

4

The Novell® Enhanced Smart Card Method is configured by using the Novell iManager Smart Card Login plug-in. The method allows administrators 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 26
- Section 4.2.2, “CRL Trusted Root Containers,” on page 26

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 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.

Basic Configuration Requirements

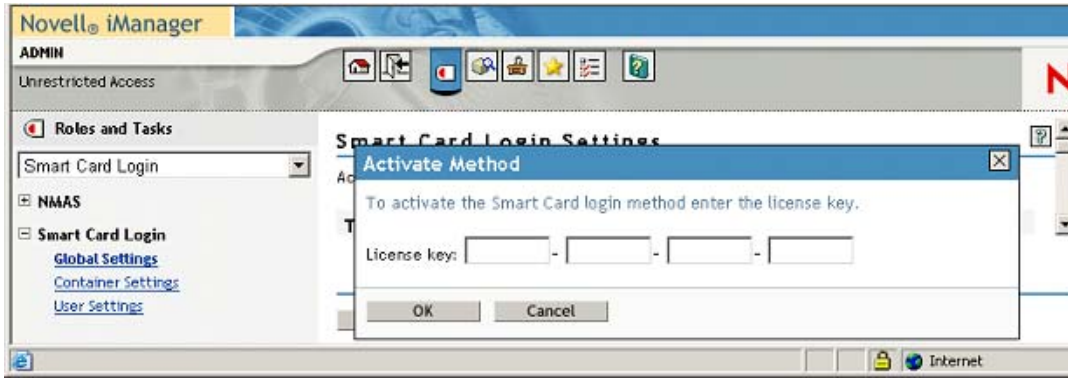
5

After installing the Novell® Enhanced Smart Card Method, it is important to use Novell iManager to complete the configuration steps outlined below. Completing these steps ensures that the method is properly configured.

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, click *Smart Card Login* > *Global Setting*. Click *Activate Method* and specify a valid license key.



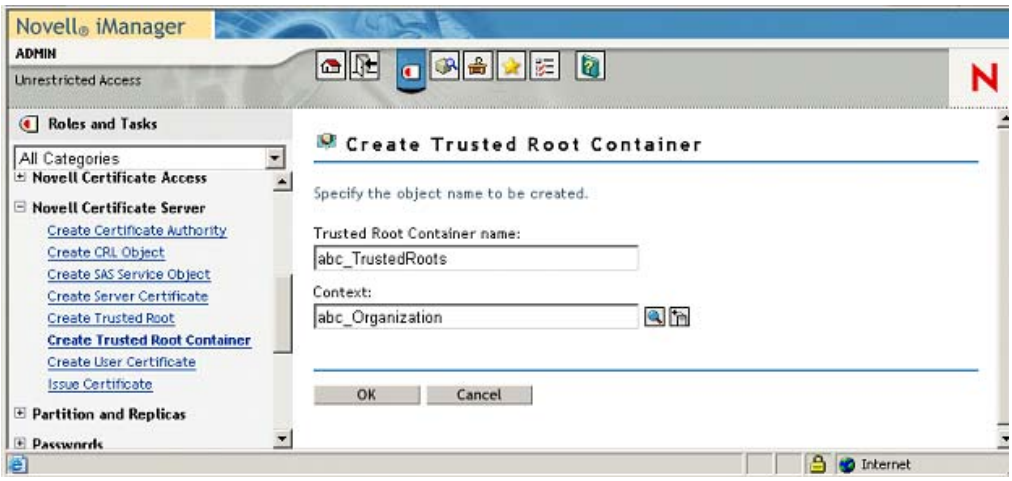
2 Click *OK*.

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 Create a trusted root container:

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

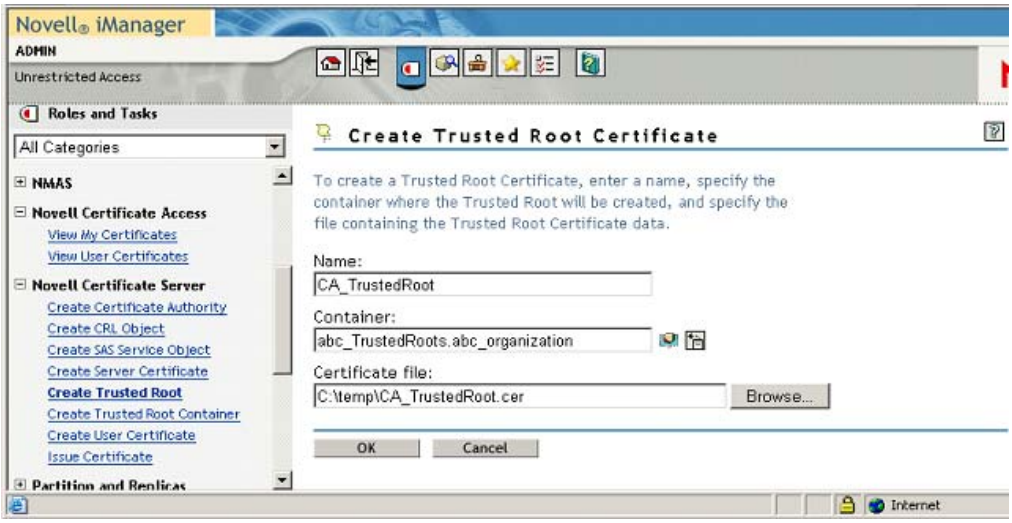


1b Specify the container name and location.

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 a cryptic NDS-601 error.

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

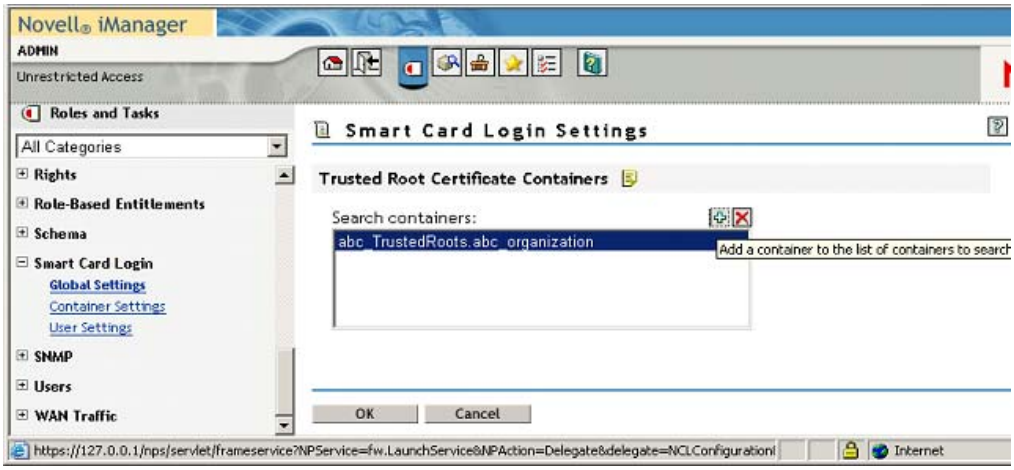
2d For the *Certificate file* field, browse to and select a standard DER file (`*.der` or `*.cer`) or Base 64 encoded DER file (`*.b64`, `*.pem`, or `*.cer`). This file contains the material for the issuing certificate.

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 button to add the trusted root container to the *Trusted Root Certificate Containers* list.

3c Click *OK*.

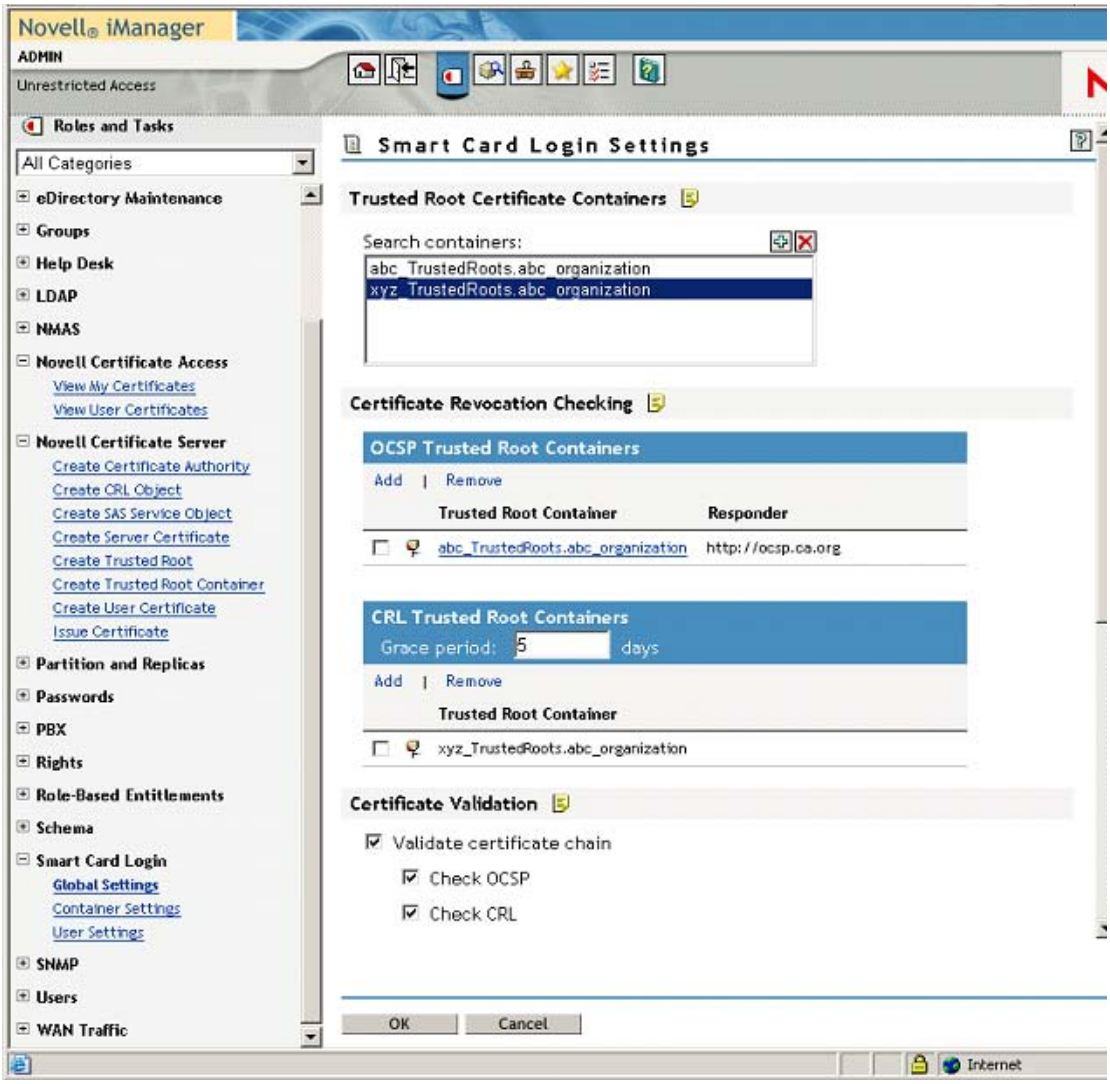
5.3 Configuring Certificate Revocation Checking

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 32, 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. Using iManager, select *Smart Card Login > User Settings*.

The information required depends on the type of certificate matching used.

- Section 5.4.1, “Subject Name Matching,” on page 32
- Section 5.4.2, “Certificate Matching,” on page 34
- Section 5.4.3, “Temporary Certificates,” on page 35

5.4.1 Subject Name Matching

The subject name from the login certificate is configured for the user object. This is done by selecting *Add* and entering 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*

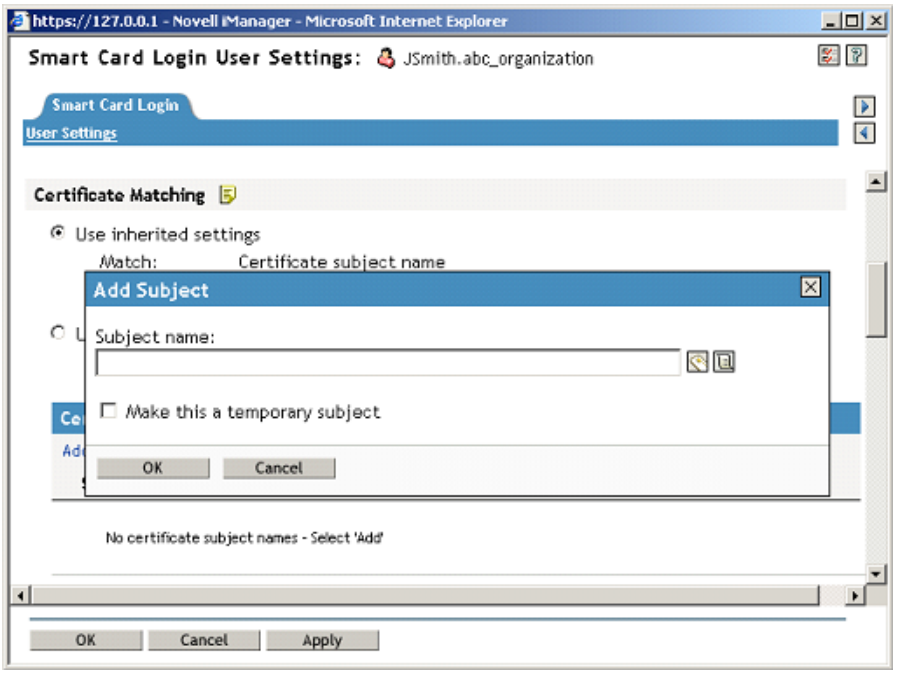
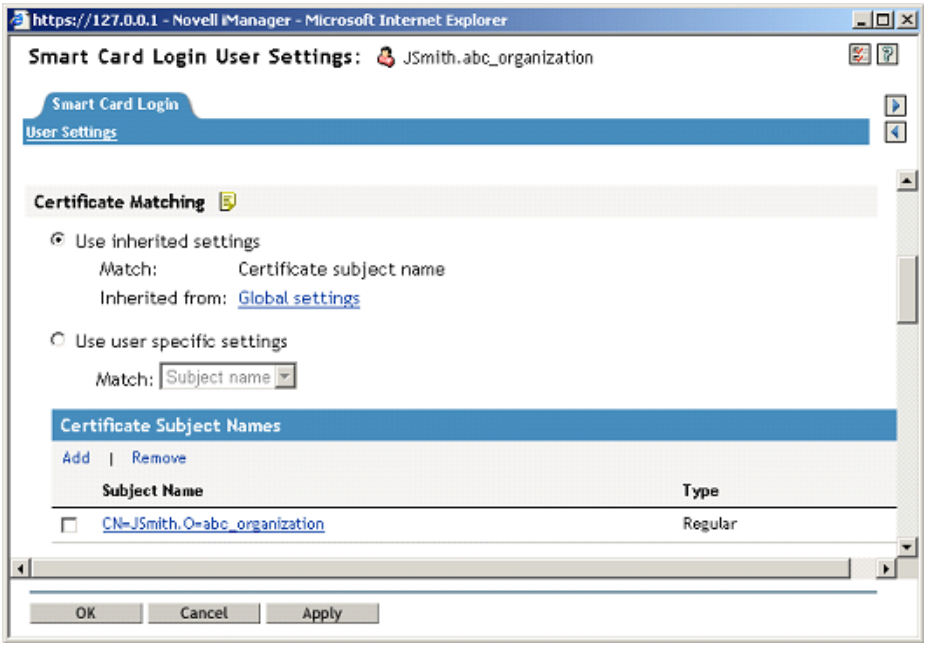


Figure 5-3 is an example of a User object properly configured for subject name matching:

Figure 5-3 *Subject Name Matching Page*



5.4.2 Certificate Matching

The specific login certificate is configured for the User object. This is done by selecting *Add* and entering 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*

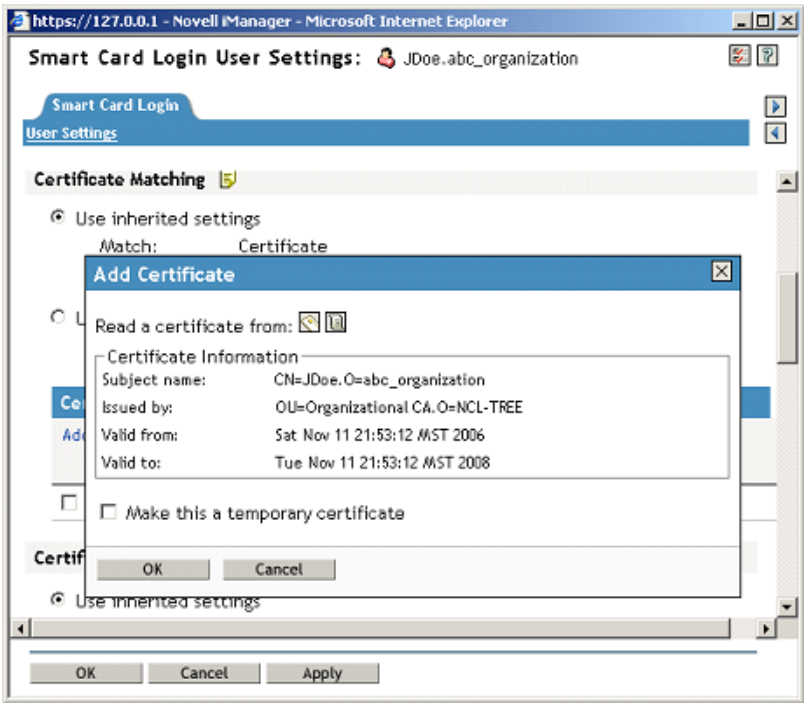
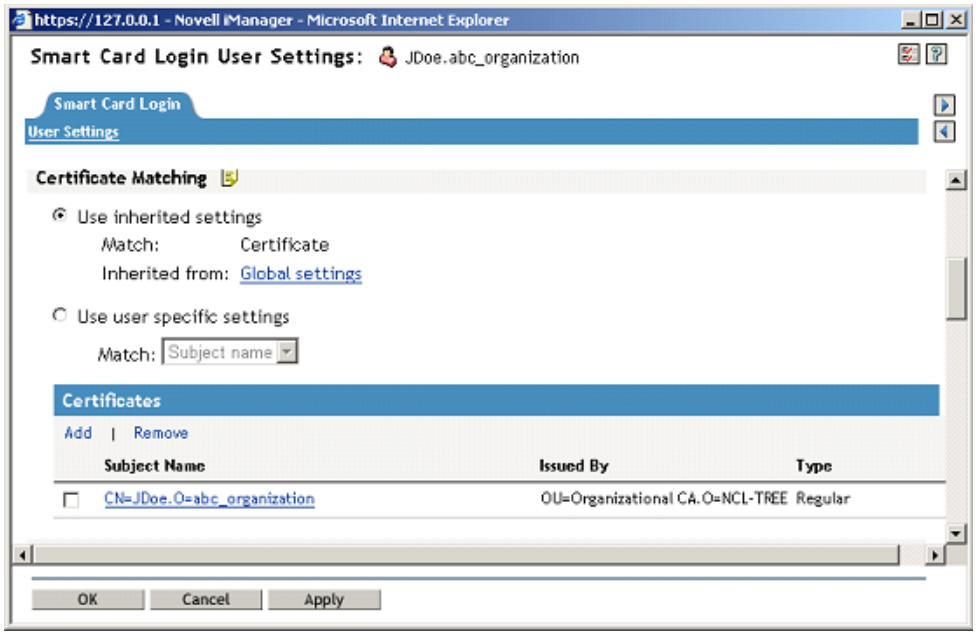


Figure 5-5 is an example of a User object properly configured for certificate matching:

Figure 5-5 *Certificate Matching Page*



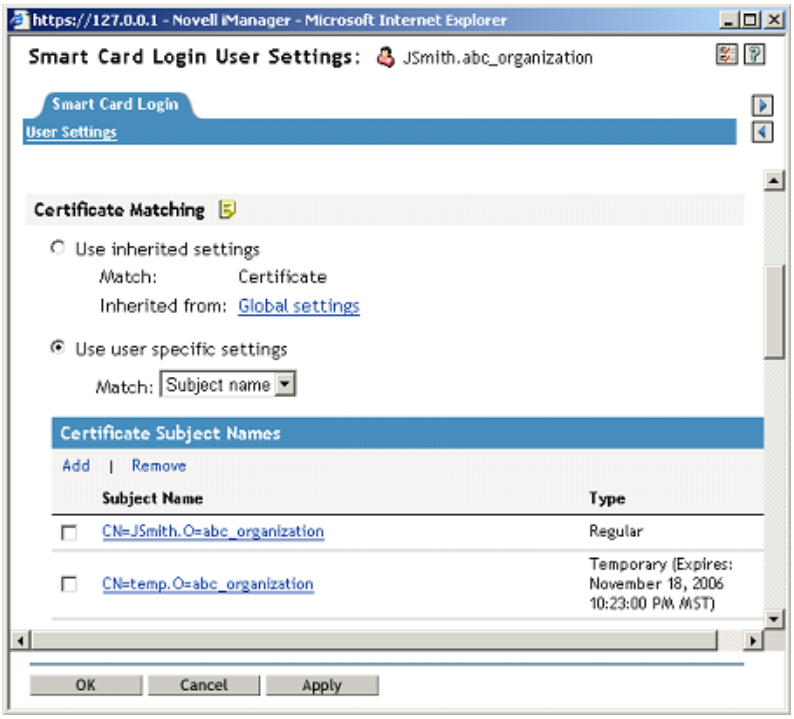
5.4.3 Temporary Certificates

A temporary classification can be assigned to certificates or subject names. This is done 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 could be issued to the individual and configured for a short period of time.

A temporary certificate is valid until the specified expiration date. When configured, the user is only able to log in using the temporary certificate. If the user attempts a login using his normal certificate, the login fails. After the temporary certificate expiration date passes, the user can log in again using his 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 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.

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 may 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. To see common vendors and PKCS#11 libraries, see Table 3-1 on page 20.

6.2.2 Identity Plug-In Issues

Because the ID Plugin searches the directory before the actual login, it requires anonymous browse rights enabled in eDirectory. If the directory restricts anonymous browse, the Identity plug-in 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 is releasing 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 38
- Section 6.3.2, “Certificate Validation Issues,” on page 39

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 29.

6.3.2 Certificate Validation Issues

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 29 for information about configuring the trusted root container.
- Certificate revocation checking is properly configured. See Section 5.3, “Configuring Certificate Revocation Checking,” on page 31 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 properly.

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 5.4.2, “Certificate Matching,” 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 Identity Plug-In

The Identity plug-in searches the directory by using an anonymous LDAP clear text connection. This should be a consideration when choosing whether to use the Identity plug-in functionality.

7.7 Disconnected Login

The disconnected 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 disconnected login functionality.

Using NESCM for Access Manager Authentication

8

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.

This section explains how the Novell® Enhanced Smart Card Method (NESCM) can be used to authenticate to Novell Access Manager.

The following prerequisites apply when using NESCM for Access Manager authentication:

- 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 25.
- 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.

Silent Method Installation on Workstations

A

You can silently run the Novell® Enhanced Smart Card Method (NESCM) install by passing in parameters from the command line.

Before silently installing the 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, "Installing the Method," on page 12.

Table A-1 lists the parameters that can be passed to the method install (`setup.exe`). The method install is 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 A-1 *Parameters for the Novell Enhanced Smart Card Method Installer*

Parameter	Required	Description	Value
ALLUSERS	Yes	Determines who can install and uninstall this program.	NULL for current user only. 1 for Administrators. 2 for Administrators if rights exist; otherwise, for the current user.
BOOL_PASSWORD_FIELD_DESC	Yes	Set to 1 for a custom password field descriptor. If it is 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

Parameter	Required	Description	Value
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 should be less than 15 characters.	String
PKCS11LIBRARY	No	If SMARTCARD_INTERFACE is set to 2, this value must be specified.	PKCS#11 DLL name
REBOOT	Yes	Set to 1 for reboot or 0 to suppress reboot.	1 or 0
SMARTCARD_INTERFACE	Yes	For PC/SC support, set it to 1. For PKCS#11 support, set it to 2.	1 or 2
ID_PLUGIN_SUPPORT	Yes	Set it to 1 for no support or set it to 2 for support.	1 or 2
ID_PLUGIN_LDAP_SEARCH_BASE	No	LDAP search base DN, specified if ID_PLUGIN_SUPPORT=2.	Example: ou=users,o=novell
ID_PLUGIN_LDAP_SEARCH_TIMEOUT	No	LDAP search timeout integer, specified if ID_PLUGIN_SUPPORT=2.	Example: 10
ID_PLUGIN_LDAP_SERVERS	No	Space-separated list of LDAP servers, specified if ID_PLUGIN_SUPPORT=2.	Example: “123.45.123.45:389 123.45.123.46:389”