NetIQ® Enhanced Smart Card Method 3.1.0.0

Installation and Administration Guide

September 2016

Legal Notice

Contents

About this Book and the Library

This guide provides installation and configuration information for the NetIQ Enhanced Smart Card Method.

Intended Audience

This book is intended for network administrators.

Other Information in the Library

The library provides the following information resources:

- For iManager information, refer to the iManager online documentation (https://www.netiq.com/documentation/imanager/).
- For NMAS information, refer to the eDirectory online documentation (https://www.netiq.com/documentation/edir88/) page.
- For Password Management information, refer to the eDirectory online documentation (https://www.netiq.com/documentation/edir88/) page.
- For Certificate Server information, refer to the eDirectory online documentation (https://www.netiq.com/documentation/edir88/) page.
- For NICI information, refer to the NICI online documentation (https://www.netiq.com/documentation/nici27x/).
- For more information about eDirectory, refer to the eDirectory online documentation (https://www.netiq.com/documentation/edir88/).

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Overview

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

The following sections provide an overview to NESCM:

1.1 How NESCM Works

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 the RSA public/private key encryption. On receiving the result, the server decrypts the data by using the public key of the certificate and validates the challenge. If a valid certificate is not found or the challenge is not validated, the login attempt fails. For more information about how the method works, see Appendix C, “How Authentication Works,” on page 47.

1.2 Additional Features

1.2.1 Workstation Only Login

In addition to network authentication, NESCM supports local Windows workstation logins. Workstation Only Login allows the smart card to be used for a local workstation login when eDirectory identity store is not available. This is useful in situations where network connectivity is not always available, such as for laptop users.

For more information about Workstation Only Login, see Section A.4, “Workstation Only Login (Disconnected Support Login),” on page 37.

1.2.2 Card Removal Security

You can also configure NESCM to monitor the smart card reader device. When the smart card is removed, the method can be configured to lock the workstation or to log off. For more information, see Section 3.6, “Card Removal Behavior,” on page 23.

2 Installing NetIQ Enhanced Smart Card Method

This section describes how to install NetIQ Enhanced Smart Card Method (NESCM).

2.1 Software Requirements

NESCM has the following software requirements:

2.1.1 eDirectory Server

eDirectory 8.8 SP7 or later on one of the following platforms:

- Windows Server 2003 SP1 (32-bit) or later
- Windows 2008 (32-bit)
- SUSE Linux Enterprise Server (SLES) 10 (32-bit or 64-bit)
- SUSE Linux Enterprise Server (SLES) 11 (32-bit or 64-bit)
- Red Hat Advanced Server 4.0 Server (32-bit or 64-bit)
- Red Hat Enterprise Linux (RHEL) 5 (32-bit or 64-bit)
- Red Hat Enterprise Linux (RHEL) 6 (32-bit or 64-bit)
- Solaris 10 on Sun SPARC (32-bit)

2.1.2 Client Workstations

Any one of the following workstations is required:

- Novell Client 2 SP4 for Windows 10 (IR4) or later installed on Windows 10 (32-bit or 64-bit)
- Novell Client 2 SP4 for Windows 8.1 (IR4) or later installed on Windows 8.1 (32-bit or 64-bit)
- Novell Client 2 SP3 for Windows 7 (IR4) or later installed on Windows 7 (32-bit or 64-bit)
- Novell Client 2 SP3 for Windows 8 (IR4) or later installed on Windows 8 (32-bit or 64-bit)
- Novell Client 2 SP3 for Windows Server 2008 R2 (IR4) on Windows Server 2008 R2
- Novell Client 2 SP3 for Windows Server 2012 (IR4) on Windows Server 2012
- iManager version 2.7 SP7 with NMAS plug-in version 8.880.20130826

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

- Internet Explorer 8 and 9

  NOTE: Before installing the NESCM card reader plug-in for Internet Explorer, you must install Microsoft Visual C++ 2005 SP1 Redistributable Package (x86), which you can download from the Microsoft Download Site (http://www.microsoft.com/en-in/download/details.aspx?id=5638).

- Mozilla Firefox 23, 22, 21, 8.x.x/7.x.x/6.x.x/5.x.x/4.x.x

  Firefox 4.0 and later accept SSL certificates signed by a Certificate Authority that are natively trusted by Mozilla Firefox for plug-in installation. To install the NESCM plug-in over an SSL connection, set `extensions.install.requireBuiltInCerts` to `false` in the Firefox configuration.

  - Launch Mozilla Firefox and type `about:config` in the address bar of the browser window.
  - Select **extensions.install.requireBuiltInCerts** in the configuration page that is displayed, right-click, and select **Toggle**. The value is set to false.
  - Install the NESCM card reader plug-in for Firefox.

  If `extensions.install.requireBuiltInCerts` is not already available, create a new one:

  1. Launch Mozilla Firefox and type `about:config` in the address bar of the browser window.
  2. In the configuration page that is displayed, right-click, select **New > Boolean**, then specify the new preference name as `extensions.install.requireBuiltInCerts` in the dialog box, and set this option to `false`.
  3. Install the NESCM card reader plug-in for Mozilla Firefox.

A smart card reader and an appropriate smart card middleware must be installed and configured on the workstation. NESCM works with most Windows compliant PC/SC middleware. It has been tested with the following applications:

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 ◆ GemSAFE libraries 4.2 ◆ Gemalto PKCS11 For .NET V2+ ◆ GemCCID (PC USB PC/SC drivers) ◆ ActivCard* Gold for CAC 3.0.1 ◆ ActivClient* 6.0 PKI Only or later ◆ Cryptovision cv act sc/interface 3.2.1 ◆ eToken* Run Time Environment 3.60 ◆ CIP 4.07 ◆ FNMT Cryptographic Card Interface (Infineon, ST, ST-WG10). RSA keys up to 2048 ◆ eToken PKI Client 5.1 SP1

Device	Tested Applications
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 ◆ ActivCard ActivCard USB Reader V3.0 ◆ C3P0 LTC3X USB Smart Card Reader v1.30
Smart Cards	◆ Axalto Access 64K CAC ◆ Gemplus GemXpresso* CAC ◆ Gemalto .NET V2+ ◆ Oberthur CosmopolIC V4 CAC ◆ Schlumberger Access 32K V2 CAC ◆ Gemplus GemSAFE* SDK GPK16000 ◆ Cryptovision - CardOS M4.01a ◆ Aladdin* - eToken PRO 64K ◆ Aladdin - eToken PRO 72k ◆ Oberthur CosmpolIC 64K V5.2 Fast ATR (PIV) ◆ FNMT-RCM_ST_v2.0 (Ceres Card)

2.2 Installing NESCM

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

- Section 2.2.1, “Installing NESCM on eDirectory Server,” on page 13
- Section 2.2.2, “Installing NESCM on Client Workstation,” on page 14

2.2.1 Installing NESCM on eDirectory Server

1. Log in to NetIQ iManager as an administrator.
2. From the **Roles and Tasks** view, click **NMAS** > **NMAS Login Methods**.
3. Click **New**.

   The method installation wizard opens.
4. Follow the steps in the method installation wizard:

   4a Browse to and double-click the `EnhancedSmartCard_iMan27.zip` file that comes with NESCM. It is located on the client disk under the `NMAS Methods` folder.

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

4b Read and accept the license agreement.

4c Review the method information and modify the values as needed.

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

4d Click **Finish**.

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

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

7 Continue with Chapter 3, “Configuring NESCM on the eDirectory Server,” on page 19 to use the plug-in to configure the NESCM installation on the server.

2.2.2 Installing NESCM on Client Workstation

You must install NESCM on each workstation that you want to use to login to eDirectory by using a smart card. To install NESCM, use the NESCM setup program.

You can also install and configure NESCM silently. For more information about silent installation, see Appendix B, “Silently Installing and Configuring NESCM on Workstations,” on page 41.

1 Log in to a workstation as an administrator.

2 Run the following program from the `...\enhancedsmartcard\client` directory:

On a 32-bit Windows 7/Windows 8 workstation: `Setup.exe`

On a 64-bit Windows 7/Windows 8/Windows Server 2008 R2/Windows Server 2012:

`Setup_64.exe`

This opens the NESCM setup program. Follow the steps in this setup program to install and configure NESCM. For information about specific steps in the setup program for all client platforms, see Table 2-2 on page 14.

For more information about the options, see Appendix A, “Client Configuration Options,” on page 35.

3 Repeat Step 1 and Step 2 for every workstation where you want to install the method.

Table 2-2 *Setup Program Options for all Client Platforms*

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. If the library file is not present in the default system path, you must provide the file path of the library file. For more information about the smart card interface, see Section A.1, “Smart Card Interface,” on page 35.

Window	Options
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 about smart card PIN validation, see Section A.2, "Smart Card PIN Validation," on page 36.
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, such as 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 about the Password Field Descriptor, see Section A.3, "Password Field Descriptor," on page 37.
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 about Workstation Only Login, see Section A.4, "Workstation Only Login (Disconnected Support Login)," on page 37.
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 about User Account Lookup, see Section A.5, "User Account Lookup (Identity Plug-In Functionality)," on page 38.
(Conditional: LDAP Search Options - Page 1) Identity Plugin Configuration	The following options specify how the LDAP search functionality of the Identity plug-in functions: ◆ **LDAP Servers:** In the **Servers** field, specify the server where you want the search to take place. This is the LDAP server IP address or DNS name. ◆ **LDAP Search Base:** In the **Base** field, specify the starting container to use when searching for the user. ◆ **LDAP Search Timeout:** In the **Timeout** field, specify the number of seconds before the search does a timeout.

Window	Options
(Conditional: LDAP Search Options - Page 2) Identity Plugin Configuration	The following options specify how the LDAP search functionality of the Identity Plug-in 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 must match the method's **Match By** configuration setting. ◆ **Search Performance:** Select **Do Complete Search** if you want the search operation to wait 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 must select **Do Complete Search** to ensure that all possible matches are presented to the user.
(Conditional: Progress Message and Login Options) Identity Plugin Configuration	Use the following options to configure progress messages and login options for the Identity Plug-in: ◆ **Status Message:** In the **Message** field, specify the message that you want to display on the Novell Client Login dialog box while the user lookup is in progress. Leave the field blank for no message. The status message is displayed on the Novell Client Login dialog box while the user lookup is in progress. ◆ **Wait Message:** In the **Message** field, specify the message that you want to display in the Novell Client Login dialog box after the user lookup is complete and login has begun. If you do not want to display any message, leave the field blank. The wait message is displayed in the Novell Client Login dialog box after the user lookup is complete and login has begun. ◆ **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 completes. 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 Plug-in, if the login fails. NetIQ recommends that you do not select both **Automatically begin login when user lookup returns** and **Restart user lookup if login fails**. Using these two options simultaneously leads to continuous looping of failed login attempts.

Window	Options
(Conditional: Novell Client Login Dialog Options) Identity Plugin Configuration	Select the following options to hide user interface controls in the Novell Client login dialog box: ◆ **Hide OK Button:** Select this option only if **Automatically begin login when user lookup returns** is selected. See "(Conditional: Progress Message and Login Options) Identity Plugin Configuration" on page 16 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 do not want users to see the additional login dialog box settings. ◆ **Hide Username Field:** Select this option if you are using the user account lookup functionality, because users usually do not interact with the username field. Hiding this field might be considered useful in some circumstances. See "User Account Lookup - Identity Plugin Support" on page 15 for more information. ◆ **Hide Password Field:** Select this option if **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.

2.3 Uninstalling NESCM

To uninstall NESCM, use the **Add or Remove Programs** option in **Control Panel**.

While uninstalling NESCM, a dialog box appears indicating you to close the `ESCPipe` and `ESCSensMonitor` applications. You must select the **Do not close applications** option to continue with the uninstallation.

3 Configuring NESCM on the eDirectory Server

After installing NetIQ Enhanced Smart Card Method (NESCM), you must configure it on the eDirectory server by using the NetIQ iManager Smart Card Login plug-in. If you have not already installed the plug-in, see Section 2.2.1, “Installing NESCM on eDirectory Server,” on page 13. Administrators use this plug-in to configure settings for the whole tree, partitions, containers, or individual users.

The NetIQ iManager Smart Card Login plug-in has the following settings:

- **Global:** The global settings are used to specify policies for the whole tree. Options configured globally apply to all user objects in the tree.
- **Container:** 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:** User settings apply to the individual User object.

Each setting is described in the following sections and identified as a global, container, or user level setting. To display these settings, launch iManager and click **Smart Card Login** in the **Roles and Tasks** view. Many settings can be configured on all levels. Settings configured at lower levels in the directory hierarchy override higher-level configurations.

3.1 Configuring Trusted Root Certificates

Configuration Level: Global

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

The certificate validation process ensures that the login certificate has been issued by a trusted Certificate Authority (CA). This is accomplished by validating that the certificate chain contains only trusted root certificates.

1. In iManager, create a trusted root container:
   - **1a** Click **NetIQ Certificate Server > Create Trusted Root Container**.
   - **1b** Select the object class you want to create and click **OK**.
   - **1c** Specify the container name and location and click **OK**.
2. Import trusted root certificates:
   - **2a** Click **NetIQ Certificate Server > Create Trusted Root**.
   - **2b** Enter the following details:
     - **Name:** Specify a name. 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: Do not include any dot characters in the name. Else, you encounter an NDS-601 error.
     - **Container:** Browse to and select the trusted root container created in Step 1.
     - **Certificate file:** 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.
   - **2c** Click **OK**.
3. Add the trusted root container to the method's global settings:
   - **3a** Click **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**.

3.2 Configuring Certificate Revocation Checking

Configuration Level: Global

Certificate revocation checking is part of the certificate validation process. 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.

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

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 3.2.1, “OCSP Trusted Root Containers,” on page 21
- Section 3.2.2, “CRL Trusted Root Containers,” on page 21

3.2.1 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 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.

3.2.2 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 that are treated as valid, after a CRL has expired. 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 is retrieved from the Distribution Point.

3.3 Configuring Certificate Matching

Configuration Level: Global, Container, User

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

1. Launch iManager, click **Roles and Tasks** view, and select **Smart Card Login > User Settings**.
2. Specify the information according to the type of certificate matching used.

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

- Section 3.3.1, “Subject Name Matching,” on page 21
- Section 3.3.2, “Certificate Matching,” on page 22
- Section 3.3.3, “No Matching,” on page 22
- Section 3.3.4, “Temporary Certificates,” on page 22

3.3.1 Subject Name Matching

You need to configure the subject name from the login certificate for the user object.

1. Click **Add** and then specify 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.
2. If you want to make this a temporary subject, select **Make this a temporary subject** and click **OK**.

   For more information about temporary subjects and certificates, see Section 3.3.4, “Temporary Certificates,” on page 22.

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.

3.3.2 Certificate Matching

Configure the specific login certificate for User object.

1. Click **Add** and then specify 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.

2. If you want to make this a temporary certificate, select **Make this a temporary certificate** and click **OK**.

   For more information about subjects and certificates, see Section 3.3.4, “Temporary Certificates,” on page 22.

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 logging in.

3.3.3 No Matching

No matching means no part of the login certificate must be configured on the target user account. 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.

3.3.4 Temporary Certificates

A temporary classification can be assigned to certificates or subject names. Select the **Make this a temporary subject** check box while adding the certificate information. This is useful in situations where a temporary smart card is assigned to an individual. For example, 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 by using the temporary certificate. If the user attempts a login by using a normal certificate, the login fails. After the temporary certificate expiration date passes, the user can log in again by using the regular certificate. The expired temporary certificate information is automatically deleted from the User object. The regular information still exists for the user, but the temporary configuration overrides it until the expiration date.

3.4 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. For certificate validation to work correctly, the settings for trusted root containers and certificate verification must be properly configured.

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.

3.5 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.

3.6 Card Removal Behavior

Configuration Level: Global, Container, User

A 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. Use this setting with caution because it can result in the user losing work when the forced logout occurs.

3.7 Check for Certificate Policy

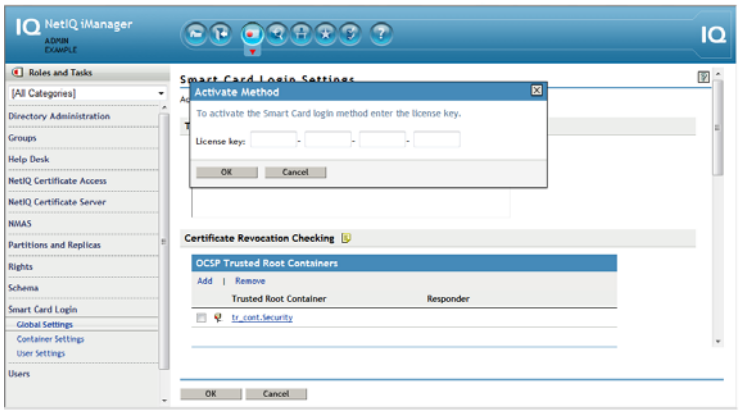
Configuration Level: Global, Container, User

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.

3.8 Activating NESCM

NESCM has a 90-day trial period. After the trial period, a valid license key must be entered to activate the method. You can obtain the license key from the Novell Customer Center (http://www.novell.com/center).

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


NetIQ iManager
ADMIN
EXAMPLE
Roles and Tasks
[All Categories]
Directory Administration
Groups
Help Desk
NetIQ Certificate Access
NetIQ Certificate Server
NMAS
Partitions and Replicas
Rights
Schema
Smart Card Login
Global Settings
Container Settings
User Settings
Users
Activate Method
To activate the Smart Card login method enter the license key.
License key:
OK
Cancel
Certificate Revocation Checking
OCSP Trusted Root Containers
Add | Remove
Trusted Root Container
Responder
tr_cont.Security
OK
Cancel

2 Click **OK**.

4 Troubleshooting

For a user to successfully log in, the NetIQ Enhanced Smart Card Method (NESCM) and the smart card must be properly configured. This section describes common issues and techniques to help diagnose problems.

4.1 Method Tracing

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

4.1.1 Enabling Server Tracing

On the server, NESCM reports information to the NMAS trace functionality, which is integrated with eDirectory tracing. To turn on tracing, use the NetIQ eDirectory iMonitor tool and select the **NMAS** option in the trace configuration settings. For more information about iMonitor, see “Using NetIQ iMonitor”, in the *NetIQ eDirectory 8.8 SP8 Administration Guide* (http://www.netiq.com/documentation/edir88/edir88/data/agwkqvb.html).

4.1.2 Enabling Client Tracing

On the client, NESCM 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.

4.2 Workstation Issues

The following issues apply to workstations:

4.2.1 Smart Card Issues

If the login fails with an error message of No Certificates Found, NESCM 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 are locked 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 that it can be loaded by the method. If it is not in the system path, you must specify the absolute path of the library. Contact the middleware vendor for the specific PKCS#11 library name. For a list of common vendors and PKCS#11 libraries, see Table A-1 on page 36.

4.2.2 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.
- If the ID plug-in does not find a user account in the first server, it does not search for the user account in other servers that are specified in the Identity plug-in configuration and displays an error.
- Sometimes Identity plug-in might not return users associated with the smart card when the system is restarted. To work around this issue,
  1. Manually enter the user name

     or

     Wait for sometime, then click the **Workstation only Logon** option.
  2. Click the **NetIQ Logon** option.

     The Identity plug-in displays the correct user names.

4.3 Method Configuration Issues

The following issues apply to method configuration:

- Section 4.3.1, “Method Activation,” on page 26
- Section 4.3.2, “Certificate Validation,” on page 27

4.3.1 Method Activation

If a valid license key is not entered by using iManager, NESCM stops functioning after the 90-day trial period has expired. Enter a valid license key to enable the method. For information about how to enable NESCM, see Section 3.8, “Activating NESCM,” on page 23.

4.3.2 Certificate Validation

If NESCM 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.
- NESCM is properly configured with a trusted root container that contains a valid trusted root certificate. For information about configuring the trusted root container, see Section 3.1, “Configuring Trusted Root Certificates,” on page 19.
- Certificate revocation checking is properly configured. For more information, see Section 3.2, “Configuring Certificate Revocation Checking,” on page 20.
- Certificate Revocation List (CRL) and On-Line Certificate Status Protocol (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. 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.

5 Security Guidelines

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

5.1 Trusted Root Containers

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

5.2 Certificate Validation/Revocation Checking

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

5.3 Smart Card Enrollment eDirectory Attributes

Restrict the administration of the user attributes used for smart card authentication 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`

5.4 Certificate Matching

Set the certificate matching settings 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 must be used only in specific guest account scenarios, as described in Section 3.3.3, “No Matching,” on page 22. For information about how to configure certificate matching options by using iManager, see Section 3.3, “Configuring Certificate Matching,” on page 21.

5.5 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. For more information, see “Managing Login Sequences” in the NetIQ Modular Authentication Services Administration Guide (https://www.netiq.com/documentation/edir88/nmas88/data/bookinfo.html).

5.6 User Account Lookup (Identity Plug-In)

User Account Lookup searches the directory by using an anonymous LDAP clear text connection. You must consider this when choosing to use the User Account Lookup functionality.

5.7 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. You must consider this when choosing to use the Workstation Only Login functionality.

6 Using NESCM for Access Manager Authentication

NetIQ 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 NetIQ Enhanced Smart Card Method (NESCM) to authenticate to Access Manager.

The following prerequisites apply:

- Be able to authenticate to eDirectory.
- Install NetIQ Enhanced Smart Card Method. For information about how to install NESCM, see Section 2.2, “Installing NESCM,” on page 13. 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 3, “Configuring NESCM on the eDirectory Server,” on page 19.
- Provision your smart card according to your company policy.
- Ensure that 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 *NetIQ Access Manager Installation Guide* (https://www.netiq.com/documentation/netiqaccessmanager32/installation/data/bookinfo.html) and the *NetIQ Access Manager Setup Guide* (https://www.netiq.com/documentation/novellaccessmanager31/basicconfig/data/bookinfo.html).

To integrate NESCM as an authentication agent to NetIQ Access Manager, complete the tasks described in the *NetIQ Access Manager Administration Console Guide* (https://www.netiq.com/documentation/novellaccessmanager31/adminconsolehelp/data/bookinfo.html).

7 Reporting Login Events

NetIQ Enhanced Smart Card Method (NESCM) reports Workstation Only login events to the Windows Event system, where the event source is Nescm Audit. The smart card login events include specific information about the certificate used for login such as Serial Number, Subject Name, Issuer, and Expiration Date.

A Client Configuration Options

When you install NESCM, you select configuration options for each workstation. The following sections provide additional information about the workstation configuration options:

For information about how to set these configuration options using the NESCM setup program, see Section 2.2.2, “Installing NESCM on Client Workstation,” on page 14. Or, if you are installing the method silently, see Appendix B, “Silently Installing and Configuring NESCM on Workstations,” on page 41.

A.1 Smart Card Interface

A.1.1 CSP with PC/SC Interfaces

We recommend that you allow NESCM to communicate with the smart card 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). NESCM automatically detects the uses of the CSP.

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

A.1.2 PKCS#11 Library

If CSP with PC/SC interfaces communication fails or if you are aware that your smart card vendor does not provide a CSP, try a PKCS#11 library. When using 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.

If the library file is not present in the default system path, you must provide the file path of the library file.

Table A-1 lists common PKCS#11 libraries:

Table A-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)

For information about choosing the smart card interface, see “Smart Card Interface” on page 14.

A.2 Smart Card PIN Validation

During the login process, NESCM needs access to the keys on the smart card. It obtains access by opening a session with the card and specifying the PIN. The card validates the PIN and then grants appropriate access.

A.2.1 Turning Off PIN Validation

The default procedure is 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 having to enter the PIN a second time.

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

A.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 about how to hide the login dialog box **password** field, see “(Conditional: Novell Client Login Dialog Options) Identity Plugin Configuration” on page 17.

A.3 Password Field Descriptor

The password field descriptor is only available if NESCM is installed with the Novell Client.

The Novell Client login dialog box uses the **Password** string 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 and used instead of the “Password” string.

For example, `PIN:` could be specified. The setup program uses a default descriptor string of *&PIN:*.

For information about changing the password field descriptor, see “Password Field Descriptor” on page 15.

A.4 Workstation Only Login (Disconnected Support Login)

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

Windows workstation login is usually password-based; however, NESCM supports using 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.

A.4.1 Certificate Validation

Because Workstation Only Login is designed to work in conditions where connectivity is limited, only a 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.

A.4.2 Local Account Information

When smart card workstation login is enabled, NESCM 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.

A.4.3 Workstation Only Login Exception

During Workstation Only Login, the **Disconnected_Required** registry key determines whether to enforce smart card login for all users on that workstation. If **Disconnected_Required** is set to 1, all the users must use smart card during workstation login.

However, there may be certain local users, who may not use smart card during login and there must be an exception on these users to not enforce smart card login.

To configure workstation only login exception list, see Creating an Exception List (http://www.novell.com/documentation/windows_client/windows_client_admin/data/bzgxlql.html) in the Novell Client 2 SP3 for Windows Administration Guide (http://www.novell.com/documentation/windows_client/windows_client_admin/data/h4rudg93.html).

A.5 User Account Lookup (Identity Plug-In Functionality)

User Account Lookup is available if NESCM is installed with Novell Client.

Users are typically required to enter their username and password to authenticate. NESCM provides the functionality to look up the user account in eDirectory that is associated with the smart card, eliminating the requirement for users to enter their login names.

A.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 login. It performs an LDAP search by using the certificate information and an anonymous clear-text connection.

To successfully perform the LDAP search, the User Account Lookup settings must be properly configured. For a list of settings and how to configure them, see “(Conditional: LDAP Search Options - Page 1) Identity Plugin Configuration” on page 15.

A.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.

Create indexes to optimize search performance. When you search by **Certificate Subject Name**, the `sasAllowableSubjectNames` attribute must be indexed. When you search by **Certificate**, the `userCertificate` attribute must be indexed. For information about how to choose search performance options, See “(Conditional: LDAP Search Options - Page 2) Identity Plugin Configuration” on page 16.

A.6 Novell Client Options

A.6.1 Single Sign-On

When using NESCM, users enter the card's PIN for eDirectory login and are then prompted to enter a password for 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.

For information about setting up Single Sign-On, refer to Setting Up Single Sign-On (SSO) (http://www.novell.com/documentation/windows_client/windows_client_admin/data/bxii3sl.html) in the Novell Client 2 SP3 for Windows Administration Guide (http://www.novell.com/documentation/windows_client/windows_client_admin/data/h4rudg93.html).

B Silently Installing and Configuring NESCM on Workstations

In NetIQ Enhanced Smart Card Method (NESCM) versions prior to 3.0.4, you must enter options on a command line to silently install the method. However, because NESCM 3.0.4 has so many options that are configured during an interactive install, we recommended you to silently install the method with the default options, and then change the configuration settings as needed, after you have installed NESCM.

Before silently installing NESCM from a command line, you must become familiar with the graphical installation and its options. For more information about the graphical installation, see Section 2.2.2, “Installing NESCM on Client Workstation,” on page 14.

B.1 Installing NESCM

B.1.1 Installing NESCM on a Computer without the Novell Client

If you are installing NESCM on a computer without the Novell Client, use the following command to install it silently with the default options.

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

To see what the default installation options are, see Section B.1.3, “Default Installation Options,” on page 42.

B.1.2 Installing NESCM on a Computer with the Novell Client

If you are installing on a computer 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"
```

B.1.3 Default Installation Options

Table B-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 Plug-in Support	Automatically look up the user account = FALSE

B.2 Configuring NESCM

There are two ways to configure NESCM when installing silently:

- Section B.2.1, “Using the Registry to Configure NESCM After Installation (Recommended),” on page 42
- Section B.2.2, “Using the Command Line to Configure NESCM During Installation,” on page 42

B.2.1 Using the Registry to Configure NESCM After Installation (Recommended)

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.

B.2.2 Using the Command Line to Configure NESCM During Installation

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 B-2 for details.) However, if you need to specify numerous options, you might find it easier to install with the default settings, and then modify the `nescm.reg` file, as described in Section B.2.1, “Using the Registry to Configure NESCM After Installation (Recommended),” on page 42.

For additional information about installation options for all client platforms (Windows 7 and 8), see Table 2-2, “Setup Program Options for all Client Platforms,” on page 14.

Table B-2 *Installation Command Line Options for all Client Platforms*

Functionality	Options
Smart Card Interface	◆ **NESCM_SCINTERFACE:** The possible values are: ◆ PCSC (Default) ◆ PKCS11 ◆ **NESCM_PKCS11LIBRARY:** The value of the PKCS#11 library is: ◆ PKCS#11 library name The following example changes the interface mode to PKCS#11 on the command line: **Windows 7 (32-Bit):** `setup.exe/S/v"/qn NESCM_SCINTERFACE=PKCS11 NESCM_PKCS11LIBRARY=abc.dll"`
Smart Card PIN Validation	◆ **NESCM_CARD_LOGIN:** The possible values are: ◆ 1 = True, validate smart card PIN (Default) ◆ 0 = False The following example turns off smart card PIN validation: **Windows 7 (32-Bit):** `setup.exe/S/v"/qn NESCM_CARD_LOGIN=0"`
Workstation Only Login - Disconnected Login	◆ **NESCM_DISCONNECTED_SUPPORT:** The possible values are: ◆ 1 = True, enable disconnected support ◆ 0 = False (Default) ◆ **NESCM_DISCONNECTED_REQUIRED:** The possible values are: ◆ 1 = True, require disconnected support ◆ 0 = False (Default) The following example turns on disconnected support and makes it required: **Windows 7 (32-Bit):** `setup.exe/S/v"/qn NESCM_DISCONNECTED_SUPPORT=1 NESCM_DISCONNECTED_REQUIRED=1"`

Functionality	Options
User Account Lookup - Identity Plugin Support	◆ **NESCM_IDPLUGIN_SUPPORT:** The possible values are: ◆ 1 = True, enable Identity Plug-in support ◆ 0 = False (Default) ◆ **NESCM_IDPLUGIN_SERVERS:** The value is: ◆ LDAP server address or DNS name ◆ **NESCM_IDPLUGIN_SEARCHBASE:** The value is: ◆ Search container ◆ **NESCM_IDPLUGIN_SEARCHTIMEOUT:** ◆ **NESCM_IDPLUGIN_SEARCHBY:** The possible values are: ◆ 1 = Search by certificate subject name (Default) ◆ 2 = Search by certificate ◆ **NESCM_IDPLUGIN_USEFIRSTMATCH:** The possible values are: ◆ 1 = True, use first account returned ◆ 0 = False, do a complete search (Default) ◆ **NESCM_IDPLUGIN_PROMPTMSG:** The value is: ◆ Status message string ◆ **NESCM_IDPLUGIN_WAITMSG:** The value is: ◆ Wait message string ◆ **NESCM_IDPLUGIN_AUTOLOGIN:** The possible values are: ◆ 1 = True, begin login when plug-in returns ◆ 0 = False (Default) ◆ **NESCM_IDPLUGIN_AUTORESTART:** The possible values are: ◆ 1 = True, restart plug-in if login fails ◆ 0 = False (Default) ◆ **NESCM_IDPLUGIN_HIDEOK:** The possible values are: ◆ 1 = True, hide **OK** button ◆ 0 = False - (Default) ◆ **NESCM_IDPLUGIN_HIDECANCEL:** The possible values are: ◆ 1 = True, hide **Cancel** button ◆ 0 = False (Default) ◆ **NESCM_IDPLUGIN_HIDEADVANCED:** The possible values are: ◆ 1 = True, hide **Advanced** button ◆ 0 = False (Default)

Functionality	Options

(Continued) User Account Lookup - Identity Plugin Support	◆ **NESCM_IDPLUGIN_HIDEUSERNAME:** The possible values are:
	◆ 1 (Hide **Username** field)
	◆ 0 (Default)
	◆ **NESCM_IDPLUGIN_HIDEPASSWORD:**
	◆ 1 (Hide **Password** field)
	◆ 0 (Default)
	NOTE: String values are enclosed in double quotes and the quotes are escaped with a backslash.
	The following example enables Identity Plug-in support and sets parameters, while having unspecified parameters use the default values:
	`setup.exe/S/v"/qn NESCM_IDPLUGIN_SUPPORT=1`
	`NESCM_DISCONNECTED_REQUIRED=1 "`
	`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_AUTOSTART=0 "`

Password Field Descriptor	◆ **NESCM_PWDFIELD_DESC:** The value is: ◆ Description string 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: **Windows 7 (32-Bit):** `setup.exe/S/v"/qn NESCM_PWDFIELD_DESC=\"Card PIN\" "`

C How Authentication Works

To successfully log in, NESCM 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. 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 to use and challenge. 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.

D Registry Configuration Settings

NetIQ Enhanced Smart Card Method (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 B.2.1, “Using the Registry to Configure NESCM After Installation (Recommended),” on page 42

E Documentation Updates

This document was updated on the following dates:

E.1 November 6, 2013

- Removed all graphics
- Updated the graphic for activating the method.
- Updated Section 2.1, “Software Requirements,” on page 11
- Updated Section 3.3, “Configuring Certificate Matching,” on page 21

E.2 March 30, 2012

- Updated Table 2-2 on page 14.
- Updated iManager screenshots in Chapter 3, “Configuring NESCM on the eDirectory Server,” on page 19.
- Added more issues in Chapter 4, “Troubleshooting,” on page 25.
- Replaced the earlier audit chapter with new Chapter 7, “Reporting Login Events,” on page 33.
- Updated Section A.5, “User Account Lookup (Identity Plug-In Functionality),” on page 38 to include support only for Windows XP.

E.3 March 18, 2010

- Updated Section 1.2.1, “Workstation Only Login,” on page 9.
- Updated Section 2.1, “Software Requirements,” on page 11
- Updated Section 2.2.2, “Installing NESCM on Client Workstation,” on page 14.
- Updated Section 2.2.2, “Installing NESCM on Client Workstation,” on page 14 to update the commands. Also divided Table 2-2 on page 14 into two tables.
- Updated Table 2-1 on page 12 to include the newly supported Middleware, Smart Card Readers, and Smart Cards.
- Divided Table B-2 on page 43 into two tables.

E.4 December 09, 2009

Added the following two sub-sections to the section Section A.4, “Workstation Only Login (Disconnected Support Login),” on page 37:

- Section A.4.3, “Workstation Only Login Exception,” on page 38

E.5 January 20, 2009

Changes have been made to the following sections. The changes are explained below.

Table E-1 *Document Changes*

Location	Change
Chapter 1, “Overview,” on page 9	Divided this chapter into sections.
Section 2.2.1, “Installing NESCM on eDirectory Server,” on page 13	Removed screenshots in procedure.
Chapter 3, “Configuring NESCM on the eDirectory Server,” on page 19	Combined information from two chapters to create this chapter.
Appendix A, “Client Configuration Options,” on page 35	Moved this information from a chapter to an Appendix.