Novell Modular Authentication Services (NMAS™)

3.2

www.novell.com

ADMINISTRATION GUIDE

October 5, 2007

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 theNovell 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 an overview of the Novell® Modular Authentication Services (NMAS™) technology and software. It includes instructions on how to install, configure, and manage NMAS. It is written primarily for network administrators.

Documentation Updates

For the most recent version of the *NMAS 3.2x Administration Guide*, see the NMAS 3.2x Administration Guide Web site (http://www.novell.com/documentation/lg/nmas32/index.html).

Documentation Conventions

In this 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.

What's New

1

For a complete list of fixed defects and enhancements, see the Security Services 2.0.5 Readme (http://www.novell.com/documentation/nmas32/index.html).

NMAS Overview

2

This section provides an overview of Novell® Modular Authentication Services (NMAS™).

2.1 NMAS Functionality

NMAS is designed to help you protect information on your network. NMAS brings together additional ways of authenticating to Novell eDirectory™ 8.7.3 or later networks to help ensure that the people accessing your network resources are who they say they are.

2.1.1 NMAS Features

NMAS employs three different phases of operation during a user’s session on a workstation with respect to authentication devices. These phases are as follows:

1. User identification (who are you?)
2. Authentication (prove who you say you are)
3. Device removal detection (are you still there?)

All three of these phases of operation are completely independent. Authentication devices can be used in each phase, but the same device need not be used each time.

User Identification Phase

This is the process of gathering the username. Also provided in this phase are the tree name, the user’s context, the server name, and the name of the NMAS sequence to be used during the Authentication phase. This information can be obtained from an authentication device, or it can be entered manually by the user.

Login Phase

This section describes the authentication phase.

Login Factors

NMAS uses three different approaches to logging in to the network called *login factors*. These login factors describe different items or qualities a user can use to authenticate to the network:

- Password authentication (something you know)
- Physical device authentication (something you have)
- Biometric authentication (something you are)

Password Authentication

Passwords (something you know) are important methods for authenticating to networks. NMAS provides several password authentication options:

- **NDS password:** The NDS password is stored in a hash form that is non-reversible and only the NDS system can make use of this password. This option will use the Universal Password if it is enabled and set.
- **Simple password:** The simple password allows administrators to import users and passwords (clear text and hashed) from foreign LDAP directories. This option will use the Universal Password if it is enabled and set.
- **Digest-MD5 SASL:** Digest-MD5 SASL provides the IETF standard DIGEST-MD5 SASL mechanism that validates a password hashed by the MD5 algorithm to be used for a LDAP SASL bind. This option will use the Universal Password if it is enabled and set.
- **Challenge/Response:** Challenge/Response provides a way for a user to prove his or her identity using one or more responses to pre-configured challenge questions.

Physical Device Authentication

Novell developers and third-party authentication developers have written authentication modules for NMAS for several types of physical devices (something you have):

NOTE: NMAS uses the word *token* to refer to all physical device authentication methods (smart cards with certificates, one-time password (OTP) devices, proximity cards, etc.).

- **Smart cards:** A smart card is a plastic card, about the size of a credit card, or a USB device that includes an embedded, programmable microchip that can store data and perform cryptographic functions. With NMAS, a smart card can be used to establish an identity when authenticating to eDirectory.

  Novell provides the the Novell Enhanced Smartcards login method for the use of smart cards. The Novell Enhanced Smartcards login method is provided as part of the Identity Assurance Client.
- **One-Time Password (OTP) device:** An OTP device is a hand-held hardware device that generates a one-time password to authenticate its owner.
- **Proximity cards:** A proximity card is a card worn by a person. This technology locks and unlocks a person's workstation based on the card's proximity to the workstation.

  Novell provides the PC Prox login method, which supports RFID proximity cards. The PC Prox login method is provided as part of the Novell Secure Login product.

Biometric Authentication

Biometrics is the science and technology of measuring and statistically analyzing human body characteristics (something you are). Biometric methods are provided by third-party companies for use with NMAS.

Biometric authentication requires readers or scanning devices, software that converts the scanned information into digital form, and a database or directory that stores the biometric data for comparison with entered biometric data.

In converting the biometric input, the software identifies specific points of data as match points. The match points are processed by using an algorithm to create a value that can be compared with biometric data scanned when a user tries to gain access.

Some examples of biometric authentication include scans of fingerprints, retinas, irises, and facial features. Biometrics can also include recognition of voice, handwriting, typing patterns, etc.

Device Removal Detection Phase

The user's session enters this phase after login is complete. This feature is provided by the Secure Workstation method which is available with Novell Secure Login (NSL). The user's session can be terminated when an authentication device (such as a smart card) is removed. This device need not be used in any of the other phases.

The Novel Enhanced Smarcards login method also provides smart card removal detection without the Secure Workstation method.

2.1.2 Login and Post-Login Methods and Sequences

A *login method* is a specific implementation of a login factor. NMAS provides multiple login methods to choose from based on the three login factors (password, physical device or token, and biometric authentication).

A *post-login method* is a security process that is executed after a user has authenticated to Novell eDirectory™. For example, one post-login method is the Novell Secure Workstation method (available with Novell Secure Login (NSL)), which requires the user to provide credentials in order to access the computer after the workstation is locked.

NMAS software includes support for a number of login and post-login methods from Novell and from third-party authentication developers. Additional hardware might be required, depending on the login method. Refer to the third-party product's documentation for more information.

After you have decided upon and installed a method, you need to assign it to a login sequence in order for it to be used. A *login sequence* is an ordered set of one or more methods. Users log in to the network using these defined login sequences. If the sequence contains more than one method, the methods are presented to the user in the order specified. Login methods are presented first, followed by post-login methods.

Both And and Or login sequences exist with NMAS. An And login sequence requires all of the login methods in the sequence to complete successfully. An Or login sequence requires only one of the login methods in the sequence to complete successfully. An example of an Or login sequence is to allow users to use the same login sequence to login to workstations with different authentication devices.

2.1.3 Graded Authentication

Another feature of NMAS is *graded authentication*. Graded authentication allows you to "grade," or control, users' access to the network based on the login methods used to authenticate to the network.

IMPORTANT: Graded authentication is an additional level of control. It does not take the place of regular eDirectory and file system access rights, which still need to be administered.

Graded authentication is only available on NetWare.

Graded authentication is managed from the Security Policy object in the Security container by using iManager or ConsoleOne®. This object is created when NMAS is installed.

Categories

A category is an element of a set that represents sensitivity and trust. You use categories to define security labels.

NMAS comes with three secrecy categories and three integrity categories (Biometric, Token, Password) defined. You can define additional secrecy and integrity categories to meet your company's needs.

Security Label

Security labels are a set of secrecy and integrity categories. NMAS comes with eight security labels defined. The following table shows the predefined security labels and the set of categories that define the label:

Default Security Labels	Secrecy Categories	Integrity Categories
Biometric & Password & Token	{Biometric, Token, Password}	{0}
Biometric & Password	{Biometric, Password}	{0}
Biometric & Token	{Biometric, Token}	{0}
Password & Token	{Token, Password}	{0}
Biometric	{Biometric}	{0}
Password	{Password}	{0}
Token	{Token}	{0}
Logged In	{0}	{0}

These labels are used to assign access requirements to NetWare volumes and eDirectory attributes. You can define additional security labels to meet your company's needs.

Clearances

Clearances are assigned to users to represent the amount of trust you have in that user. A clearance has a Read label that specifies what a user can read, and a Write label that specifies what information a user can write to. A user can read data that is labeled at the Read label and below. A user can write data that is labeled between the Read label and the Write label.

NMAS defines only one clearance: Multi-level Administrator. Multi-level Administrator has Biometric and Token and Password for the Read label and Logged In for the Write label.

You can define additional clearances to meet your company's needs.

For more information on graded authentication, see Chapter 4, “Using Graded Authentication,” on page 29.

2.2 NMAS Software

NMAS is included as a bundled product with Novell eDirectory and NetWare. NMAS is also available as part of the Security Services bundle, available from the Novell Download Web Site. The software image includes the following:

- NMAS server software
- Login methods software
- Support for multiple login methods per login sequence
- Support for graded authentication
- Universal Password
- iManager plug-ins and ConsoleOne snap-ins

NMAS client software is available with the Novell Client for Windows and with Novell Secure Login.

2.2.1 Server and Client Software Installation

NMAS server-side software must be installed with eDirectory 8.7.3 or later. NMAS client-side software must be installed on each client workstation that will access the network using the NMAS login methods. After installation, NMAS is managed using iManager or ConsoleOne.

The NMAS client software now ships with the Novell Client for Windows 4.9.0 or later.

During the installation, NMAS extends the eDirectory schema and creates new objects in the Security container in the eDirectory tree. These new objects are the Authorized Login Methods container, the Authorized Post-Login Methods container, the Security Policy object, and the Login Policy object. All login methods are stored and managed in the Authorized Login Methods container. All post-login methods are stored and managed in the Authorized Post-Login Methods container.

2.2.2 Login Method Software and Partners

NMAS login methods (server software, plug-ins, and snap-ins) can be installed using

- `nmasinst` (available on all eDirectory platforms) which requires eDirectory to be installed
- iManager plug-in
- ConsoleOne snap-in

Several currently supported login methods are available on the NMAS software image.

NMAS software includes support for a number of login methods from third-party authentication developers. Refer to the eDirectory Partners Web site (http://www.novell.com/products/edirectory/) for a list of Novell partners.

Each partner that develops login methods for NMAS addresses network authentication with unique product features and characteristics. Therefore, each login method will vary in its actual security properties.

Novell has not evaluated the security methodologies of these partner products, so although these products might have qualified for the Novell Yes, Tested & Approved or Novell Directory Enabled logos, those logos relate to general product interoperability only.

We encourage you to carefully investigate each partner's product features to determine which product will best meet your security needs. Also note that some login methods require additional hardware and software not included with the NMAS product.

2.2.3 Universal Password

For information on Universal Password, see the Chapter 7, “History of Novell Passwords,” on page 51 and the Novell Password Management Administration Guide (http://www.novell.com/documentation/password_management32/).

2.2.4 iManager and ConsoleOne Management

You can manage NMAS using iManager or ConsoleOne. Novell iManager is a Web-based utility for managing eDirectory. ConsoleOne is the Java* authored, GUI-based utility for managing eDirectory. Specific property pages in each utility let you manage login methods, login sequences, enrollment, and graded authentication.

By default, NMAS installs the standard NDS password login method. Additional login methods can be installed using ConsoleOne and a wizard launched from the Authorized Login Methods container using the Create New Object option. Post-login methods can be installed using a wizard launched from the Authorized Post-Login Methods container using the Create New Object option.

2.3 What's Next

- To set up login methods and sequences, see Chapter 3, “Managing Login and Post-Login Methods and Sequences,” on page 19.
- To set up graded authentication, see Chapter 4, “Using Graded Authentication,” on page 29.
- To log in using NMAS, see Chapter 5, “Logging In to the Network Using NMAS,” on page 45.

Managing Login and Post-Login Methods and Sequences

3

This section describes how to set up and configure login and post-login methods and sequences for NMAS™.

NMAS provides multiple login methods to choose from based on the three login factors (password, physical device or token, and biometric authentication).

NMAS includes support for a number of login and post-login methods from Novell® and from third-party authentication developers. Some methods require additional hardware and software. Make sure that you have all of the necessary hardware and software for the methods you will use.

NMAS includes several login methods in the software build. Other login methods are available from third-party vendors.

See the eDirectory Web site (http://www.novell.com/products/edirectory/) for a list of eDirectory partners. Some partners develop third-party login methods.

3.1 Installing a Login Method

You have three ways of installing a login method for use in Novell eDirectory™:

- nmasinst utility (UNIX)

  The nmasinst utility allows you to install login methods into eDirectory from a UNIX machine.
- Novell iManager (Windows)

  You can use Novell iManager to install login and post-login methods into eDirectory.
- ConsoleOne® (Windows)

  You can use ConsoleOne to install login and post-login methods into eDirectory.

3.1.1 Installing a Login Method Using the nmasinst Utility

IMPORTANT: Before you can install a login method using the nmasinst utility, you must first install and configure NMAS. See the instructions in the installation guide for installing NMAS.

1. From the server console command line, enter:

   `nmasinst -addmethod` *admin.context treename config.txt_ path* [`-h` *hostname*[:*port*]]

   - *admin.context* - The admin name and context.
   - *treename* - The name of the eDirectory tree where you are installing the login method.
   - *config.txt_ path* - The complete or relative path to the config.txt file of the login method. A config.txt file is provided with each login method.
   - [-h *hostname*[:*port*]] - (Optional) The hostname and port of the server. Use this if eDirectory is not running on the default port.
   - [-w password] This option is used to specify the password on the command line.
   - [-checkversion] This option will report an error if the installed method version is the same or newer than the method version being installed.

   If the login method already exists, nmasinst will update it.

3.1.2 Installing a Login or Post-Login Method Using Novell iManager

1. Launch Novell iManager.
2. Authenticate to the eDirectory tree as an administrator or a user with administrative rights.
3. From the Roles and Tasks menu, click NMAS > NMAS Login Methods.
4. Click New.
5. Browse for and select the login method (.zip) file you want to install, then click Next.
6. Follow the installation wizard to completion.

3.1.3 Installing a Login Method Using ConsoleOne

1. In ConsoleOne, select the Security container.
2. Right-click the Authorized Login Methods container.
3. Click New, then click Object.

   The New Object Wizard starts.
4. Select the SAS:NMAS Login Method object class, then click OK.
5. Specify the configuration file, then click Next.

   The configuration file is located in the login method folder and is usually named config.txt.
6. On the license agreement page, click Accept, then click Next.
7. Accept the default method name, then click Next.
8. Review the available modules for this method, then click Next.

9 If you want a login sequence to use only this login method, check the appropriate check box, then click Finish.

10 Review the installation summary, then click OK.

11 If necessary, close and restart ConsoleOne to run the newly installed ConsoleOne snap-ins provided by the login method to configure the login and enroll users to use this login method.

3.1.4 Installing a Post-Login Method Using ConsoleOne

1 In ConsoleOne, select the Security container.

2 Right-click the Authorized Post-Login Methods container.

3 Click New, then click Object.

The New Object Wizard starts.

4 Select the sasPostLoginMethod object class, then click OK.

5 Specify the configuration file, then click Next.

The configuration file is located in the post-login method folder and is usually named config.txt.

6 On the license agreement page, click Accept, then click Next.

7 Accept the default method name, then click Next.

8 Review the available modules for this method, then click Finish.

9 Review the installation summary, then click OK.

10 If necessary, close and restart ConsoleOne to run the newly installed ConsoleOne snap-ins provided by the login method to configure the login and enroll users to use this post-login method.

3.2 Updating Login and Post-Login Methods

When a login method vendor provides an update for a login or post-login method, you can update the method by doing the following:

3.2.1 Updating a Login Method Using the nmasinst Utility

Use the same procedure you used to install a login method using the nmasinst utility (see Section 3.1.1, “Installing a Login Method Using the nmasinst Utility,” on page 20). Include the path to the new config.txt file and the login method will be updated.

3.2.2 Updating a Login Method using Novell iManager

1 Launch Novell iManager.

2 Authenticate to the eDirectory tree as an administrator or a user with administrative rights.

3 From the Roles and Tasks menu, click NMAS > NMAS Login Methods.

4 Click on the login method you want to update.

5 From the login method property page, click Update Method.

6 Follow the update wizard to completion.

3.2.3 Updating a Login Method using ConsoleOne

1. Right-click the login or post-login method to be updated, select Properties, click the General tab, then click Update Method.
2. Specify the configuration file, then click Next.

   The configuration file is located in the post-login method folder and is usually named config.txt.
3. On the license agreement page, click Accept, then click Next.
4. Accept the default method name or rename it, then click Next.
5. Review the available modules for this method, then click Finish.
6. Review the installation summary, then click OK.
7. Close and restart ConsoleOne to use the newly updated method.

The updated method is available to the users the next time they log in.

3.3 Managing Login Sequences

When you install a login or post-login method, you are asked if you want to create a login sequence that uses only the login method you are installing. If you answer yes, a login sequence will be created for you which contains just the one login method.

You can also manually create and manage login sequences. After login and post-login methods are installed, you can view, add, modify, or delete login sequences using iManager or ConsoleOne. Login sequences are not created when methods are modified or updated.

In NMAS, you can set up multiple login and post-login methods per sequence. You must have at least one login method selected to be able to select a post-login method.

When multiple methods are selected for a sequence, they are executed in the order they are listed. Login methods are executed first, then post-login methods.

A login sequence can be an *And* or an *Or* sequence. An *And* sequence is successful if all of the login methods successfully validate the identity of the user. An *Or* sequence only requires that one of the login methods validate the identity of the user for the login to be successful.

The post-login methods are only executed if the login is successful, irregardless of the *And*/*Or* relationship.

After a sequence is created, you can authorize users to use the new sequence to log in to eDirectory.

- “Creating a New Login Sequence (ConsoleOne)” on page 23
- “Creating a New Login Sequence (Novell iManager)” on page 23
- “Modifying a Login Sequence (ConsoleOne)” on page 23
- “Modifying a Login Sequence (Novell iManager)” on page 24
- “Deleting a Login Sequence (ConsoleOne)” on page 24
- “Deleting a Login Sequence (Novell iManager)” on page 25

3.3.1 Creating a New Login Sequence (ConsoleOne)

1. In ConsoleOne, select the Security container.
2. Right-click the Login Policy container, then select Properties.
3. Click New Sequence.
4. Enter a name for the new login sequence, then click OK to continue.

   All available login methods will be listed under Available Login Methods and Available Post-Login Methods.
5. Select the Sequence Type from the drop-down list.

   If you select *And*, a user must log in using every login method that makes up the login sequence. If you select *Or*, the user only needs to log in using one of the login methods that makes up the login sequence.
6. Double-click or use the horizontal arrows to add each method you want to the sequence.

   If you are using multiple methods, use the vertical arrows to change the execution order.

   The Sequence Grade field displays the grade for the login sequence. For *And* sequences, the sequence grade is the union of the grades of the login methods. For *Or* sequences, the sequence grade is the intersection of the method grades.
7. Click OK when you are finished.

3.3.2 Creating a New Login Sequence (Novell iManager)

1. Launch Novell iManager.
2. Authenticate to the eDirectory tree as an administrator or a user with administrative rights.
3. From the Roles and Tasks menu, click NMAS > NMAS Login Sequences.
4. Click New and enter a name for the new login sequence.

   All available login methods are listed under Available Login Methods and Available Post-Login Methods.
5. Select the Sequence Type from the drop-down list.

   If you select *And*, a user must log in using every login method that makes up the login sequence. If you select *Or*, the user only needs to log in using one of the login methods that makes up the login sequence.
6. Use the horizontal arrows to add each method you want to the sequence.

   If you are using multiple methods, use the vertical arrows to change the execution order.

   The Sequence Grade field displays the grade for the login sequence. For *And* sequences, the sequence grade is the union of the grades of the login methods. For *Or* sequences, the sequence grade is the intersection of the method grades.
7. Click Finish to save the login sequence.

3.3.3 Modifying a Login Sequence (ConsoleOne)

1. In ConsoleOne, select the Security container.
2. Right-click the Login Policy container > select Properties.
3. Select a login sequence from the Defined Login Sequences drop-down list.

The Sequence Grade and Login and Post-Login Sequences for the selected method are displayed. All of the available login methods appear in the Available Login and Available Post-Login Methods lists.

4 Select an action:

- To add or remove login or post-login methods from a sequence, use the left- and right-arrows.

  NOTE: You must have at least one login method selected in order to select a post-login method.

- To change the sequence order of the login methods, use the up- and down-arrows.
- To exit without saving changes, click Cancel.

IMPORTANT: Login sequences that don't have a method associated with them will not be saved.

5 Click Apply or OK.

3.3.4 Modifying a Login Sequence (Novell iManager)

1 Launch Novell iManager.

2 Authenticate to the eDirectory tree as an administrator or a user with administrative rights.

3 From the Roles and Tasks menu, click NMAS > NMAS Login Sequences.

4 Click on a login sequence name.

The sequence grade and sequence type are displayed and the Login and Post-Login Methods are listed. All of the available login methods appear in the Available Login and Available Post-Login Methods lists.

5 Select an action:

- To change the sequence type, use the drop-down list next to sequence type.
- To add or remove login or post-login methods from a sequence, use the left-arrow and right-arrow.

  NOTE: You must have at least one login method selected in order to select a post-login method.

- To change the sequence order of the login methods, use the up-arrow and down-arrow.
- To exit without saving changes, click Cancel.

IMPORTANT: Login sequences that don't have a method associated with them will not be saved.

6 Click Apply or OK.

3.3.5 Deleting a Login Sequence (ConsoleOne)

1 In ConsoleOne, select the Security container.

2 Right-click the Login Policy container > select Properties.

3 Select the sequence from the Defined Login Sequences drop-down list (Alt+S).

4 Click Delete Sequence.

5 Click Apply or OK.

3.3.6 Deleting a Login Sequence (Novell iManager)

1 Launch Novell iManager.

2 Authenticate to the eDirectory tree as an administrator or a user with administrative rights.

3 From the Roles and Tasks menu, click NMAS > NMAS Login Sequences.

4 Select the login sequence you want to delete, then click Delete.

5 Click Apply or OK.

3.4 Authorizing Login Sequences for Users (ConsoleOne)

To restrict the login sequences each user can use:

1 In ConsoleOne, right-click a User object, click Properties, click the Security tab, then click Login Sequences.

2 Select either No Restrictions or Restrict the User to the Sequences Authorized Below.

If you select No Restrictions, the user can use any defined login sequence to log in.

If you select Restrict the User to the Sequences Authorized Below, use the arrows to authorize or select the sequences you want this user to use to log in.

3 Click Apply or OK.

See “Assigning Login Sequences” on page 25.

3.5 Authorizing Login Sequences for Users (Novell iManager)

1 Launch Novell iManager.

2 Authenticate to the eDirectory tree as an administrator or a user with administrative rights.

3 From the Roles and Tasks menu, click NMAS > NMAS Users, select the user you want to authorize the login sequences for, then click the NMAS tab.

4 Authorize or de-authorize a login sequence for a user by selecting the login sequence and clicking Authorize or De-authorize.

5 Click Apply or OK.

Assigning Login Sequences

Authorized and default login sequences can be assigned to a user, a container, a partition root, or the login policy object. NMAS will search for the authorized or default login sequences for a user by attempting to read the attributes from first the User object, then the container of the user object, then the partition root of the user object, and finally the login policy object.

The attributes found with the User object supercede any attributes found with container, partition root, or login policy object. So if a login sequence has been assigned to a partition root, that login

sequence will apply to all the users under that partition root only if a login sequence has not already been individually assigned to specific users.

Also, a login sequence assigned to a container will apply only to the users with unassigned sequences in that container, and not to the users in subcontainers of that container.

3.6 Setting Default Login Sequences (ConsoleOne)

To set a default login sequence so that users are not required to specify a login sequence when logging in:

1. In ConsoleOne, right-click a User object, click Properties, click the Security tab, then click Login Sequences.
2. Click the Default Login Sequence drop-down list, then select an authorized login sequence.

   The sequence you select will be the default login sequence. If a user attempts to log in without using a login sequence, this default login sequence is attempted.
3. Click Apply or OK.

NOTE: If a workstation is unable to execute the user's default login sequence, the NDS password login method will be used.

See "Assigning Login Sequences" on page 25.

3.7 Setting Default Login Sequences (Novell iManager)

To set a default login sequence so that users are not required to specify a login sequence when logging in:

1. Launch Novell iManager.
2. Authenticate to the eDirectory tree as an administrator or a user with administrative rights.
3. From the Roles and Tasks menu, click NMAS > NMAS Users, select the user you want to set the default login sequence for, then click the NMAS tab.
4. Select an authorized login sequence, then click Make Default.

   The sequence you select will be the default login sequence. If a user attempts to log in without using a login sequence, this default login sequence will be used.
5. Click Apply or OK.

NOTE: If a workstation is unable to execute the user's default login sequence, the NDS password login method will be used.

See "Assigning Login Sequences" on page 25.

3.8 Deleting a Login Method

The NMAS iManager plug-ins and ConsoleOne snap-ins do not allow you to delete a login method if that method is part of any login sequence. The default installation of a login method creates a login sequence containing only that method. As a result, most methods exist in at least one sequence.

NOTE: nmasinst does not have an option to remove NMAS methods. This must be done using iManager or ConsoleOne.

To delete a login method, you must complete the following two procedures:

- "Remove the Login Method from Any Login Sequence" on page 27
- "Delete the Login Method" on page 27

3.8.1 Remove the Login Method from Any Login Sequence

To remove the login method for any login sequence using ConsoleOne:

1. In ConsoleOne, click the Security container, right-click the Login Policy, then select Properties.
2. Click General.
3. For each sequence in the Defined Login Sequences drop-down list:
   - **3a** Select the sequence.
   - **3b** Verify that the login method you will be deleting is not listed in the Selected Login Methods or Selected Post-Login Methods lists.
   - **3c** If the login method is listed as one of the selected methods, you can move it from the list by selecting it and clicking the left-arrow.

To remove the login method for any login sequence using iManager:

1. In iManager, click NMAS > NMAS Login Sequences.
2. For each sequence in the NMAS Login Sequences list:
   - **2a** Click the sequence name.
   - **2b** Verify that the login method you will be deleting is not listed in the Login Methods or Post-Login Methods lists.
   - **2c** If the login method is listed as one of the selected methods, you can move it from the list by selecting it and clicking the left-arrow.

When the login method has been removed from all login sequences, you can then delete it.

3.8.2 Delete the Login Method

To delete the login method using ConsoleOne:

1. In ConsoleOne, click the Security container and select either the Authorized Login Methods container or the Authorized Post Login Methods container, depending on the type of method you are deleting.
2. Select the login method you want to delete.

3 Press the Delete key, then click Yes.

To delete the login method using iManager:

1 In iManager, click NMAS > NMAS Login Methods.
2 Select the login method or methods you want to delete.
3 Click Delete, then click Yes.

3.9 Deleting a Login Sequence

1 Launch Novell iManager.
2 Authenticate to the eDirectory tree as an administrator or a user with administrative rights.
3 From the Roles and Tasks menu, click NMAS > NMAS Login Sequences.
4 Select the login sequence you want to delete.
5 Click Delete, then click Yes.

3.10 What's Next

- To set up graded authentication, see Chapter 4, “Using Graded Authentication,” on page 29.
- To log in using NMAS, see Chapter 5, “Logging In to the Network Using NMAS,” on page 45.

Using Graded Authentication

4

The graded authentication feature of NMAS™ allows you to control users' access to network resources based on the login methods used to log in to the network. This means that you can set access rights to NetWare® volumes and any attribute in Novell ®eDirectory™ based on how users log in.

NOTE: Graded authentication is only available on NetWare.

Graded authentication is based on the relationship between a user and an object, where an object is a network volume or eDirectory attribute. Graded authentication uses the same NMAS login factors (password, physical device, and biometric authentication) and security grades to establish the user object relationship and to determine the grade or level of authentication.

To set up graded authentication, you need to do the following:

1. Understand the graded authentication rules.
2. Set up and assign security labels to volumes and eDirectory attributes.
3. Assign clearances for each user who will be logging in to the network using NMAS. By default, all users have a clearance.

The following topics provide information on setting up graded authentication:

An example of graded authentication is located at the end of this chapter.

4.1 Graded Authentication Terms

This section describes graded authentication terms.

4.1.1 Security Policy Object

The Security Policy object is the object in Novell eDirectory that you can use to manage the elements of graded authentication. The Security Policy object resides in the Security container.

For more information, see Section 4.3, “Configuring the Security Policy Object,” on page 35.

4.1.2 Category

A category is an element of a set that represents sensitivity and trust. You use categories to define security labels.

There are two types of categories: secrecy and integrity.

- **Secrecy Categories:** Secrecy controls the disclosure of information.

  A user that is assigned a certain secrecy category can't read to an object of a higher level of secrecy, but it can read to an object of the same or lower level of secrecy. The user can't write to an object of a lower level of secrecy, but it can write to an object of the same or higher level.

  Think of it in terms of a government secret agent. The government agency has three levels of secrecy; Unclassified, Secret, and Top Secret. The agent is given a Secret level of secrecy. The agent cannot read information designated as Top Secret, but the agent may read information designated as Unclassified or Secret. The agent cannot write information from his Secret level to the Unclassified level, but the agent can write information to the Secret or Top Secret levels.

- **Integrity Categories:** Integrity controls the validity of information.

  A user that is assigned a certain integrity category can't write to an object of a higher level of integrity, but it can write to an object of the same or lower level. The user can't read to an object of a lower level of integrity, but it can read to an object of the same or higher level.

  Think of this in terms of two newspapers. One newspaper is highly respected for its honesty in reporting the facts. The other newspaper is a supermarket tabloid that manufactures stories. The newspaper with the lower integrity cannot publish stories in the newspaper with higher integrity, but the newspaper with higher integrity could publish a story in the newpaper with less integrity. Likewise, the newspaper with higher integrity would not quote from the stories produced by the newspaper with lower integrity, but the newspaper with lower integrity might quote from the stories produced by the newspaper with higher integrity.

NMAS comes with three secrecy categories (Biometric, Token, Password) and three integrity categories (Biometric, Token, Password) defined. You can define additional integrity categories to meet your company's needs.

For more information, see "Defining User-Defined Categories (Closed User Groups)" on page 36.

4.1.3 Security Label

A security label represents the sensitivity of information. It is a set made up of categories. For example, the Biometric security label contains the Biometric secrecy category. The Biometric and Token and Password security label contains three secrecy categories: Biometric, Token, and Password.

A security label can be assigned to a volume or to any eDirectory attribute. The security label is compared against a user's current clearance to determine what information the user can access.

NMAS comes with eight security labels defined. The following table shows the predefined security labels and single-level clearances:

Default Security Labels	Secrecy Categories	Integrity Categories
Biometric & Password & Token	{Biometric, Token, Password}	{0}

Default Security Labels	Secrecy Categories	Integrity Categories
Biometric & Password	{Biometric, Password}	{0}
Biometric & Token	{Biometric, Token}	{0}
Password & Token	{Token, Password}	{0}
Biometric	{Biometric}	{0}
Password	{Password}	{0}
Token	{Token}	{0}
Logged In	{0}	{0}

Novell only uses secrecy categories to define the default security labels. This meets the needs of most users. However, Novell provides you with the ability to create your own security labels that may be a combination of both secrecy and integrity categories to meet your company's needs. This, however, can become very complex. See Section 4.2.1, "Determining Access with Security Labels Made Up of Both Secrecy and Integrity Categories," on page 33

For information on how to create a security label, see "Defining Security Labels" on page 37.

4.1.4 Clearance

Clearances are assigned to users to represent the amount of trust you have in that user. A clearance has a Read label that specifies what a user can read and a Write label that specifies what information a user can write to. For more information, see "Dominance" on page 32 and Section 4.2, "Graded Authentication Rules," on page 33.

There are two types of clearances: single-level and multi-level.

Single-Level Clearance

A single-level clearance is a clearance in which the Read label and the Write label are the same. For example, the Biometric clearance's Read label and Write label use the same Biometric label. Therefore, a user who is assigned the Biometric clearance can read information labeled with Biometric and below, but can only write to information labeled Biometric. All labels are used as single-level clearances.

Multi-Level Clearance

A multi-level clearance is a clearance in which the Read label and the Write label are different. For example, the Multi-Level Administrator clearance is a multi-level clearance and has Biometric and Token and Password for the Read label and Logged In for the Write label. This clearance will allow the user to read all information and to write to all information that is labeled with the default security labels.

NMAS defines only one multi-level clearance: Multi-Level Administrator.

You can define additional clearances to meet your company's needs.

The following table summarizes the access relationships between the predefined single-level clearances and the predefined security labels. Remember that the Novell predefined security labels use secrecy categories only.

USER AUTHENTICATION LEVEL	NETWORK OBJECT SECURITY LABEL							
	Biometric & Password & Token	Biometric & Password	Biometric & Token	Password & Token	Biometric	Password	Token	Logged In
Biometric & Password & Token	R & W	R	R	R	R	R	R	R
Biometric & Password	NA	R & W	NA	NA	R	R	NA	R
Biometric & Token	NA	NA	R & W	NA	R	NA	R	R
Password & Token	NA	NA	NA	R & W	NA	R	R	R
Biometric	NA	NA	NA	NA	R & W	NA	NA	R
Password	NA	NA	NA	NA	NA	R & W	NA	R
Token	NA	NA	NA	NA	NA	NA	R & W	R
Logged In	NA	NA	NA	NA	NA	NA	NA	R & W
Multi-level Admin	R & W	R & W	R & W	R & W	R & W	R & W	R & W	R & W

NA = No Access R = Read W = Write

For more information, see "Defining Clearances" on page 37.

4.1.5 Dominance

In administering graded authentication, it is vitally important that you understand the concept of dominance.

All access control decisions are based on the relationship between the labels of the information and the session clearance of the user. There are only three such relationships:

- *Dominate Relationship*

  Label A1 is said to dominate Label A2 if:

  A1's secrecy categories include all those of A2

  AND

  A2's integrity categories include all those of A1

- *Equal Relationship*

  Label A1 is equal to Label A2 if:

  A1's secrecy categories are the same as A2's secrecy categories.

  AND

  A1's integrity categories are the same as A2's integrity categories.

  This may also be expressed as:

  A1 dominates A2 and A2 dominates A1.

- *Incomparable Relationship*

  Label A1 is incomparable to Label A2 if none of the previous relationships apply.

For more information, see Section 4.2, “Graded Authentication Rules,” on page 33.

4.2 Graded Authentication Rules

IMPORTANT: Graded authentication is an additional level of control. It does not take the place of regular eDirectory and file system access rights. Regular eDirectory and file system access rights still need to be administered.

The following rules apply to graded authentication in NMAS:

- If the Read label of the clearance dominates or is equal to the assigned security label and the security label dominates or is equal to the Write label of the clearance, then access is Read and Write.
- If the Read label of the clearance dominates or is equal to the assigned security label but the security label does not dominate and is not equal to the write label, then access is Read-only.

  For example, if a user has a clearance with a Read label of Password and Token and a Write label of Password and Token and wants to access a NetWare volume that has a security label of Password and Token, then the user will have Read and Write access to that volume. However, the user will have Read-only access to each NetWare volume assigned a Password security label.

  NOTE: Read-only access prevents passing higher classified data to lower classified areas. Access is always Read-only to security labels that are lower than the clearance's Write label.
- If the Read label of the clearance is dominated by the assigned security label, then no access is allowed.
- Using a login sequence does not grant access rights unless the user is assigned the session clearance.

4.2.1 Determining Access with Security Labels Made Up of Both Secrecy and Integrity Categories

If you were to create a security label with both the Token and Password secrecy categories (Ts and Ps) and the Token and Password integrity categories (Ti and Pi), the possible combinations would look like the following:

{Ts, Ps; 0}

{Ts; 0}

{Ps; 0}

{0; 0}

{Ts, Ps; Ti}

{Ts; Ti}

{Ps; Ti}

{0; Ti}
{Ts, Ps; Pi}
{Ts; Pi}
{Ps; Pi}
{0; Pi}
{Ts, Ps; Ti, Pi}
{Ts; Ti, Pi}
{Ps; Ti, Pi}
{0; Ti, Pi}

Now, using the rules of dominance (see "Dominance" on page 32), you can check these combinations as user clearances against all possible security labels. For the purposes of this example, we will just compare the single-level clearances (Read and Write label are the same) against two randomly selected security labels - {Ts, Ps; Ti} and {Ts; Pi}.

User Clearances (A1)	Security Label (A2)	Security Label (A2)
Read = R . . . Write = W	{Ts, Ps; Ti}	{Ts; Pi}
R {Ts, Ps; 0} W {Ts, Ps; 0}	Dominate	Dominate
R {Ts; 0} W {Ts; 0}	Incomparable	Incomparable
R {Ps; 0} W {Ps; 0}	Incomparable	Incomparable
R {0; 0} W {0; 0}	Incomparable	Incomparable
R {Ts, Ps; Ti} W {Ts, Ps; Ti}	Equal	Incomparable
R {Ts; Ti} W {Ts; Ti}	Incomparable	Incomparable
R {Ps; Ti} W {Ps; Ti}	Incomparable	Incomparable
R {0; Ti} W {0; Ti}	Incomparable	Incomparable
R {Ts, Ps; Pi} W {Ts, Ps; Pi}	Incomparable	Incomparable
R {Ts; Pi} W {Ts; Pi}	Incomparable	Equal
R {Ps; Pi} W {Ps; Pi}	Incomparable	Incomparable
R {0; Pi} W {0; Pi}	Incomparable	Incomparable
R{Ts, Ps; Ti, Pi} W {Ts, Ps; Ti, Pi}	Incomparable	Incomparable
R {Ts; Ti, Pi} W {Ts; Ti, Pi}	Incomparable	Incomparable
R {Ps; Ti, Pi} W {Ps; Ti, Pi}	Incomparable	Incomparable
R {0; Ti, Pi} W {0; Ti, Pi}	Incomparable	Incomparable

Once you have determined the dominance for each combination, you can refer to the graded authentication rules (see Section 4.2, "Graded Authentication Rules," on page 33) to determine the access the user will have, as follows:

User Clearances (A1)	Security Label (A2)	Security Label (A2)
R = Read . . . W=Write	{Ts, Ps; Ti}	{Ts; Pi}
R {Ts, Ps; 0} W {Ts, Ps; 0}	Read	Read
R {Ts; 0} W {Ts; 0}	NA	NA
R {Ps; 0} W {Ps; 0}	NA	NA
R {0; 0} W {0; 0}	NA	NA
R {Ts, Ps; Ti} W {Ts, Ps; Ti}	Read/Write	NA
R {Ts; Ti} W {Ts; Ti}	NA	NA
R {Ps; Ti} W {Ps; Ti}	NA	NA
R {0; Ti} W {0; Ti}	NA	NA
R {Ts, Ps; Pi} W {Ts, Ps; Pi}	NA	NA
R {Ts; Pi} W {Ts; Pi}	NA	Read/Write
R {Ps; Pi} W {Ps; Pi}	NA	NA
R {0; Pi} W {0; Pi}	NA	NA
R{Ts, Ps; Ti, Pi} W {Ts, Ps; Ti, Pi}	NA	NA
R {Ts; Ti, Pi} W {Ts; Ti, Pi}	NA	NA
R {Ps; Ti, Pi} W {Ps; Ti, Pi}	NA	NA
R {0; Ti, Pi} W {0; Ti, Pi}	NA	NA

The above example is provided to help you understand the details of how security access is determined. NMAS provides a tool calculates this access information for you. See “Viewing Security Clearance Access” on page 39.

For another example of how Graded Authentication works, see Section 4.6, “Graded Authentication Example,” on page 41.

4.3 Configuring the Security Policy Object

When you install and configure NMAS, a Security container is created and a Security Policy object is created in the Security container. The Security Policy object allows you to create, view, and rename names for clearances, security labels and categories for your NMAS implementation. You can then use these names to assign the security labels to any eDirectory attribute or NetWare volumes. You can also assign clearances to User objects in your eDirectory tree from the user's property page.

Authorized and default clearances can be assigned to a user, a container, a partition root, or the login policy object. NMAS will search for the authorized or default authorized and default clearances for a user by attempting to read the attributes from first the User object, then the container of the user object, then the partition root of the user object, and finally the login policy object.

The clearances assigned to the User object supercede any clearances assigned to the container, partition root, or login policy object. So if a clearance has been assigned to a partition root, that

clearance will apply to all the users under that partition root only if a clearance has not already been individually assigned to specific users.

Also, a clearance assigned to a container will apply only to the users with unassigned clearances in that container, and not to the users in subcontainers of that container.

4.3.1 Defining User-Defined Categories (Closed User Groups)

You can define secrecy and integrity categories that can be used to create security labels in addition to the three integrity and three secrecy categories (Biometric, Token, Password) that are predefined. For example, Biometric integrity and secrecy categories represent that access to an object is restricted to users logging in with a biometric method.

After you have created a category, you cannot delete it. You can view or rename it.

Creating a New Category Using ConsoleOne

1. In ConsoleOne, double-click the Security Container > click Security Policy.
2. Click the Define Categories tab, then select either Secrecy Categories or Integrity Categories.
3. Click Add, then specify a name for the category.
4. Click OK.

The new category will now be available for use in defining a security label.

Creating a New Category Using iManager

1. In iManager, click eDirectory Administration > Modify Object.
2. Browse for and select the Security Container > Security Policy, then click OK.
3. Click the Define Categories tab, then select either Secrecy Categories or Integrity Categories.
4. Click Add, specify a name for the category, then click OK.
5. Click OK or Apply.

Renaming a Category Using ConsoleOne

1. In ConsoleOne, double-click the Security Container > click Security Policy.
2. Click the Define Categories tab, then select either Secrecy Categories or Integrity Categories.
3. Select the category you want to rename, then click Rename Category.
4. Specify the new name, click OK, then click OK or Apply.

Renaming a Category Using iManager

1. In iManager, click eDirectory Administration > Modify Object.
2. Browse for and select the Security Container > Security Policy, then click OK.
3. Click the Define Categories tab, then select either Secrecy Categories or Integrity Categories.
4. Select the category you want to rename, then click Rename.
5. Specify the new name, click OK, then click OK or Apply.

4.3.2 Defining Security Labels

NMAS provides eight security labels by default. Security labels are also used as single-level security clearances.

After you have created a security label, you cannot modify it or delete it. You can view its properties and rename it.

Creating a New Security Label Using ConsoleOne

1. In ConsoleOne, double-click the Security Container > click Security Policy.
2. Click Define Labels.
3. Click New Label, then specify a name for the label.
4. Assign integrity and secrecy categories to the new label using the horizontal arrows.
5. Click OK.

Creating a New Security Label Using iManager

1. In iManager, click eDirectory Administration > Modify Object.
2. Browse for and select the Security Container > Security Policy, then click OK.
3. Click Define Labels.
4. Click New, specify a name for the label, then click OK.
5. Assign integrity and secrecy categories to the new label using the horizontal arrows.
6. Click OK or Apply.

Renaming a Security Label Using ConsoleOne

1. Select a label from the Defined Security Labels drop-down list.
2. Click Rename Label.
3. Specify a new name for the label.
4. Click OK.

Renaming a Security Label Using iManager

1. Select a label from the Defined Security Labels drop-down list.
2. Click Rename.
3. Specify a new name for the label, then click OK.
4. Click OK or Apply.

4.3.3 Defining Clearances

When you create a clearance, you will select two labels, a Read label and a Write label. The Read label must dominate or be equal to the Write label. In fact, when creating a security clearance, you won't have the option to select a Write label that dominates the Read label.

For example, the Password & Token security label has dominance over the Password security label, so you could select the Password & Token label as your Read label and the Password label for your Write label.

You can also define your own security clearances to meet your company's authentication needs.

After you have created a clearance, you cannot modify it or delete it. You can view its properties and rename it.

Creating a New Clearance Using ConsoleOne

1. In ConsoleOne, double-click the Security Container > Security Policy.
2. Click the Clearances tab > Definition.
3. Click New Clearance, then specify a name for the clearance.
4. Select a security label from the Read label drop-down list.

   This label is the Read label for this clearance. You must select a Read label before you can select a Write label.
5. Select a security label from the Write label drop-down list.

   This label is the Write label for this clearance. You can't select a Write label that has greater dominance than the Read label.
6. Click OK or Apply.

Creating a New Clearance Using iManager

1. In iManager, click eDirectory Administration > Modify Object.
2. Browse for and select the Security Container > Security Policy, then click OK.
3. Click the Clearances tab.
4. Click New, specify a name for the clearance, then click OK.
5. Select a security label from the Read label drop-down list.

   This label is the Read label for this clearance. You must select a Read label before you can select a Write label.
6. Select a security label from the Write label drop-down list.

   This label is the Write label for this clearance. You can't select a Write label that has greater dominance than the Read label.
7. Click OK or Apply.

Viewing the Properties of a Clearance in ConsoleOne

1. Select a clearance from the Clearance drop-down list.
2. You can see the Read and Write labels that are used to define the clearance.

Viewing the Properties of a Clearance in iManager

1. Select a clearance from the Default Clearance drop-down list.
2. The Read and Write labels that are used to define the clearance are displayed.

Renaming a Clearance in ConsoleOne

1. Select a clearance from the Default Clearance drop-down list.
2. Click Rename Clearance.
3. Specify the new name for the clearance.
4. Click OK.

Renaming a Clearance in iManager

1. Select a clearance from the Default Clearance drop-down list.
2. Click Rename.
3. Specify the new name for the clearance, then click OK.
4. Click OK or Apply.

4.3.4 Viewing Security Clearance Access

A quick way to determine the access rights a clearance will allow to objects assigned to a particular label is to view the Access page. Click Clearance > Access. This page tells you the clearance that a user will need to have Read and Write access, Read-only access, and No access to information and resources with a specific label.

To view the access rights for a clearance using ConsoleOne:

1. In ConsoleOne, double-click the Security Container > Security Policy.
2. Click the Clearances tab > Access.
3. Select a clearance from the Clearance drop-down box.

   Each defined label is grouped by the access the clearance has to the labeled object.

To view the access rights for a clearance using iManager.

1. In iManager, click eDirectory Administration > Modify Object.
2. Browse for and select the Security Container > Security Policy. Then click OK.
3. Click the Clearances tab > Access.
4. Select a clearance from the Clearance drop-down box.

   Each defined label is grouped by the access the clearance has to the labeled object.

4.4 Assigning Security Labels to Network Resources

With NMAS, you can assign NetWare volumes and any eDirectory attribute a security label. Users who log in to the network can access only those areas based upon their clearance and the resource's label.

For example, if you label a volume as Biometric & Token, an NMAS user must be assigned the Biometric and Token clearance and authenticate to the network using a Biometric and Token clearance in order to access the volume.

Authorized and default clearances can be assigned to a user, a container, a partition root, or the login policy object. NMAS will search for the authorized or default authorized and default clearances for a user by attempting to read the attributes from first the User object, then the container of the user object, then the partition root of the user object, and finally the login policy object.

The clearances assigned to the User object supercede any clearances assigned to the container, partition root, or login policy object. So if a clearance has been assigned to a partition root, that clearance will apply to all the users under that partition root only if a clearance has not already been individually assigned to specific users.

Also, a clearance assigned to a container will apply only to the users with unassigned clearances in that container, and not to the users in subcontainers of that container.

IMPORTANT: Labels assigned to traditional NetWare volumes (non-NSS volumes) are not effective until the volume is dismounted and mounted again.

To assign a security clearance to a volume using ConsoleOne:

1. In ConsoleOne, right-click a volume.
2. Click Properties > click the Security tab.
3. Select a security label from the Security Label drop-down list.
4. Click OK to finish.
5. (Conditional) If you are using traditional NetWare volumes (non-NSS volumes), you must dismount and mount the volume again for the labels to take effect.

To assign a security clearance to a volume using iManager:

1. In iManager, click eDirectory Administration > Modify Object.
2. Browse for and select a volume, then click OK.
3. Click the Security tab.
4. Select a security label from the Security Label drop-down list.
5. Click OK or Apply.
6. (Conditional) If you are using traditional NetWare volumes (non-NSS volumes), you must dismount and mount the volume again for the labels to take effect.

To assign a security clearance to eDirectory attributes using ConsoleOne:

1. In ConsoleOne, click the Security Container > double-click the Security Policy object > click Directory Attribute Labels.
2. Click the label next to the directory attribute.
3. Click the down-arrow, then select a new label from the drop-down list.
4. After making all necessary changes, click Apply or OK to save the changes.

To assign a security clearance to eDirectory attributes using iManager:

1. In iManager, click eDirectory Administration > Modify Object.
2. Browse for and select the Security Container > Security Policy, then click OK.
3. Click the Directory Attribute Labels tab.
4. Click the label next to the directory attribute.

5 Click the Down-arrow, then select a new label from the drop-down list.

6 After making all necessary changes, click OK or Apply to save the changes.

4.5 Assigning User Clearances

To assign user clearances using ConsoleOne:

1 In ConsoleOne, right-click the desired User object > click Properties > Security > Clearances.

2 On the Security Clearance page, select the user clearances.

3 Select the desired Default Login Clearance.

4 Click OK.

To assign user clearances using iManager:

1 In iManager, click eDirectory Administration > Modify Object.

2 Browse for and select a User object, then click OK.

3 Click the Security tab > Clearances.

4 Select the desired Default Clearance.

5 Use the horizontal arrows to assign authorized clearances for this user.

6 Click OK or Apply.

4.6 Graded Authentication Example

Departments within a company are often assigned security classifications that are based on the department's function and the kind of information that it handles. For example:

- Human Resources handles sensitive information such as personnel files.
- Engineering handles restricted or confidential information such as product specifications and schematics.
- Sales handles public information that is freely accessible.
- Finance handles sensitive information critical to the operation and survival of the company.

Depending upon the sensitivity of the information, it might be secured in locked filing cabinets that serve as access control mechanisms. Access control to this information is with a separate key for each filing cabinet issued to a person authorized to access the information.

Graded authentication replaces the physical key given to users with a clearance. Also, NMAS replaces the filing cabinet with NetWare file system volumes that are also assigned security labels. These security labels replace the filing cabinet lock type.

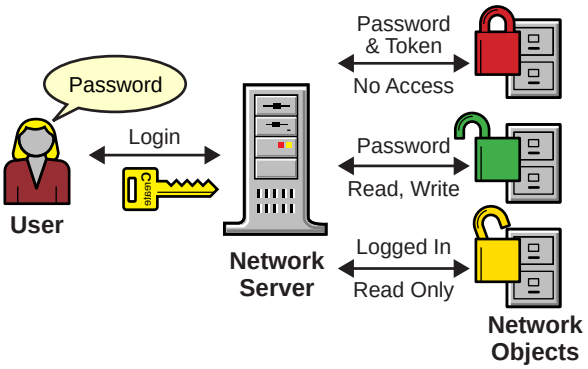
As the network administrator, you assign users authorization levels for login. When a user logs in, the user is assigned a clearance for that login session. The clearance becomes the key that is necessary for access. Access is granted to the user based on the clearance (key) that the user is authorized to hold and the security label (lock) that is being accessed.

Although a user can be authorized to have more than one clearance, only one clearance is assigned at login, and it is this clearance that determines what information can be unlocked. For example, the

following would apply (as illustrated in Figure 4-1 on page 42) to a user logging in with an authentication grade of Password:

- Read/Write access to network resources labeled Password.
- No access to resources labeled Password and Token, because this label is higher than the Password clearance.
- Read-only access to any information labeled with a lower label than Password (for example, Logged In).

Figure 4-1 *Single-Factor Authentication*

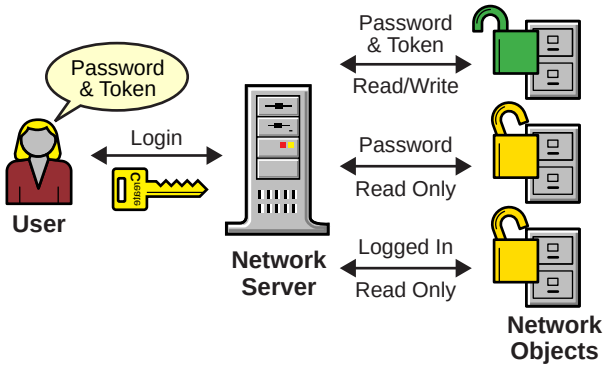


Single Factor Authentication

The following would apply (as illustrated in Figure 4-2 on page 42) to a user logging in with a password and token:

- Read/write access to network resources labeled Password and Token.
- Read-only access to any information labeled with a lower label than Password and Token, including Password and Logged In.

Figure 4-2 *Multiple-Factor Authentication*



Multiple Factor Authentication

A user working in Human Resources with information classified as sensitive logs in with a password and token clearance. The information that the user needs is on a network volume that is also labeled Password and Token. Because the user's clearance and the volume security label match (the Read

label dominates the volume label and the volume label dominates the Write label), the user is able to read from and write to the NetWare volume.

However, suppose the same user attempts to copy the sensitive information to a network area that requires only a password for access. Graded authentication prevents this action because copying or moving information from a higher label to a lower label is not allowed. This prevents the user from compromising the sensitive information.

The following table shows how several departments within a company might classify their information. Security labels and clearances are assigned based on the information classification and not on a user.

Department	Information Classification	Assigned Security Label (Lock)	Assigned Clearance (Key)
Human Resources	Sensitive	Password & Token	Password & Token
Engineering	Confidential	Password	Password
Sales	Public	Logged In	Logged In
Finance	Sensitive	Biometric & Token	Biometric & Token

In this example, because Sales has been assigned a Public clearance and Sales information is freely accessible, a user only needs to be logged in to access Sales information.

However, users who work in Engineering must use a password to access the confidential information needed for their job function. Engineering's data volumes would also be labeled Password for read/write access.

Human Resources often deals with sensitive information related to personnel records. A password and token are required to access this information.

Finance also has sensitive classified information and considers financial information critical to the company's operation and survival. A biometric and token are required to access this information.

4.7 What's Next

- To set up login methods and sequences, see Chapter 3, “Managing Login and Post-Login Methods and Sequences,” on page 19.
- To log in using NMAS, see Chapter 5, “Logging In to the Network Using NMAS,” on page 45.

Logging In to the Network Using NMAS

5

After NMAS™ is installed , you are ready for users to log in to the network. This section describes some of the additional features of the login experience that you should communicate to your network users.

5.1 Password Field

Depending upon how the NMAS client software was installed, there might or might not be a password field on the Novell® Client™ login dialog box. If users are using a biometric or physical device (token) login factor, they might not need a password to log in to the network.

See the Novell Client For Windows (http://www.novell.com/documentation/noclienu/index.html) documentation for more information on hiding the password field.

5.2 Advanced Login

Those using NMAS login methods to log in to the network can customize the login by selecting a desired clearance and login sequence. Otherwise, the last login sequence and clearance (if any) are used. If no clearance or login sequence has been previously specified, the user defaults are used.

1. When the Novell Client dialog box appears, click Advanced.
2. Click the NMAS tab.
3. Select the desired login sequence from the Login drop-down list or browse the Novell® eDirectory™ tree for a complete and current list.

   NOTE: You can browse only if an eDirectory tree has been specified on the eDirectory tab.

4. Specify the desired user session clearance or browse the eDirectory tree for a complete and current list.

   NOTE: By default, the clearance field is disabled. To enable the clearance field:

   4a Right-click the red N in the taskbar.

   4b Click Novell Client Properties > Location Profiles.

   4c Select the desired profile, click Properties, then click Properties.

   4d On the NMAS tab, check Display Clearance Field.

4e Click OK three times.

IMPORTANT: Users might have multiple session clearances for each login sequence. Make sure that the Clearance field is filled in with the desired user session clearance.

5 Click OK.

5.3 Unlocking the Workstation

With the addition of NMAS to a user's workstation, the process to unlock Windows workstations changes. Normally, users can enable password protection for their workstations by using a screen saver configured from the Windows Display control panel. With NMAS, users must instead go through the same authentication process used to originally log in to unlock a workstation.

For example, if you used NMAS to authenticate to the network and you used a biometric login method, you must use the same biometric login method again to unlock and use the workstation.

If you are using a Windows workstation, you must unlock the workstation using the login method that was used to log into the tree. If you have connections to multiple eDirectory trees, the login sequence for any eDirectory tree may be used. The default is the first eDirectory tree.

5.4 Capturing an NMAS Client Trace

Capturing an NMAS client trace can help in troubleshooting NMAS authentication problems. For more information, see TID # 3331372 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3331372&sliceId=SAL_Public&dialogID=2494055&stateId=1%200%202492379).

5.5 Viewing NMAS Clearance Status

To view your NMAS clearance status, do the following:

1 Right-click the red N in the taskbar.

2 Click NetWare Connections.

3 Scroll over to view the NMAS Clearance associated with each connection.

5.6 Single Sign-on Tab

In the properties of the Novell Client for Windows, a Single Sign-on tab is available for the convenience of users authenticating via an NMAS login method.

When you use SecretStore, you eliminate the need to remember or synchronize all the multiple passwords required for accessing password-protected applications, Web sites, and mainframes.

To configure the Single Sign-on tab:

1 Open the Novell Client Windows property page.

2 Click the Single Sign-on tab.

3 Check the Enable Single Sign On check box to enable this feature.

4 Click OK.

Other Administrative Tasks

6

This section describes other administrative tasks for NMAS™.

6.1 Using the Policy Refresh Rate Command

With NMAS 3.1 or later, you can configure NMAS, on a per-server basis, to refresh the cached NMAS login policy from the NMAS login policy stored in the Security container at scheduled intervals instead of upon every login attempt. This configuration is set using the NMAS policy refresh rate command.

NOTE: The server accesses the Security container once during startup to cache the policy. Then, based on the configured intervals, the server attempts to access the Security container to refresh the policy.

The policy refresh rate command has the following syntax:

```
nmas RefreshRate minutes
```

where minutes is the number of minutes between each attempt to check if the cached NMAS login policy needs to be updated from the NMAS login policy stored in the Security container.

The following describes how the policy refresh rate command can be invoked for each NMAS Server platform:

6.1.1 NetWare

The autoexec.ncf file can contain the policy refresh rate command as described above. Because this command can only be executed after nmas.nlm is loaded, the command should be place near the end of the autoexec.ncf file.

The policy refresh rate command can also be entered at the NetWare® console, but the setting will be lost if it isn’t included in the autoexec.ncf file.

6.1.2 Windows

When NMAS is started, it processes the nmas.cfg configuration file located in the same directory as the DIB files (typically c:\novell\nds\dibfiles\). The configuration file can contain the policy refresh rate command as described above.

The policy refresh rate command can also be invoked after NMAS has been started. This is done from the Novell® eDirectory™ Services console by selecting nmas.dlm, typing the policy refresh command in the Startup Parameters field, then clicking Configure.

6.1.3 UNIX

When NMAS is started, it processes the nmas.config configuration file located in the same directory as the DIB files (typically `/var/nds` or `/var/opt/novell/eDirectory/data`). The configuration file can contain the policy refresh rate command as described above.

6.2 Setting Delay Time for Failed Login Attempts

You can adjust the amount of time between failed login attempts by doing the following:

1. Install the NMAS 3.1.3 plug-in into iManager.

   The NMAS 3.1.3 plug-in can be downloaded from the Novell Download site (http://download.novell.com/index.jsp)
2. From the Roles and Tasks menu, click *Directory Administration* > *Modify Object*.
3. Browse for and select the Login Policy object, then click *OK*.
4. Click the NMAS tab, then click Settings.
5. Type the number of seconds you want the login screen to be delayed between failed login attempts, then click *OK*.

6.3 Using DSTRACE

You can use the DSTRACE utility to get trace information from NMAS.

For information on how to capture a NMAS client trace, see TID # 3331372 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3331372&sliceId=SAL_Public&dialogID=2494055&stateId=1%200%202492379).

For information on how to capture an NMAS server trace, see TID # 3815371 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3815371&sliceId=SAL_Public&dialogID=2494055&stateId=1%200%202492379).

6.4 Disabling and Uninstalling the NMAS Client

To disable the NMAS Client:

1. On the workstation, right-click the Red N.
2. Click Novell Client Properties.
3. Click the Advanced Login tab.
4. From the Parameter Groups list, select NMAS Authentication.
5. Under Setting, select Off.
6. Click OK.

You can uninstall the NMAS Client using the Add/Remove Programs option of Control Panel.

NOTE: Disabling or removing NMAS does not remove support for changing the Universal Password from the Novell Client for Windows.

6.5 Disabling NMAS on the Server

NMAS is defined as a core service after it is installed because other services (such as eDirectory) might auto-integrate to use NMAS features. Because of these dependencies, it is not possible to fully uninstall this release of NMAS. However, you can disable NMAS on a server-by-server basis by performing the following steps:

On NetWare

1. Rename the `nmas.nlm` file from sys:\system.
2. Restart the server.

On Windows with Novell eDirectory

1. Stop the eDirectory service.
2. Rename the `nmas.dlm` file.
3. Restart the eDirectory service.

On Linux, Solaris, and AIX

1. Stop the eDirectory service.
2. Rename the `libnmas.so` file.
3. Restart the eDirectory service.

On HP-UX

1. Stop the eDirectory service.
2. Rename the `libnmas.sl` file.
3. Restart the eDirectory service.

6.6 Auditing NMAS Events

There are two products you can use to audit NMAS events:

- Novell Audit Secure Logging Server

  You can use the Novell Audit Secure Logging Server to install the `nmas_en.lsc` file. This file is located in the following directories:

  NetWare: `sys:\system\schema`

  Windows: `novell\nds`

  Linux, Solaris, AIX and HP-UX: `/opt/novell/eDirectory/lib/nds-schema` (relative to where eDirectory is installed)

For information on installing and managing Novell Audit, see the Novell Audit online documentation (http://www.novell.com/documentation/novellaudit20/index.html).

- Novell Sentinel

  For information on installing and managing Novell Sentinel, see the Novell Sentinel online documentation (http://www.novell.com/documentation/sentinel5/index.html).

With either product, you also need to enable NMAS Audit by using the NMAS 3.1.3 or later plug-in for iManager.

1. Install the NMAS 3.1.3 or later plug-in into iManager.

   You can download the NMAS 3.1.3 or later plug-in from the Novell Download site (http://download.novell.com/index.jsp)
2. From the *Roles and Tasks* menu, click *Directory Administration* > *Modify Object*.
3. Browse for and select the Login Policy object, then click *OK*.
4. Click the *NMAS* tab, then click *Settings*.
5. Click the box next to *Enable auditing*, then click *OK*.

6.6.1 Using External Certificates with Novell Audit

To use an external certificate with NMAS and Novell Audit, you must first convert the certificate into two `.pem` files with the following names:

- `nmascert.pem`: This is the file containing the certificate.
- `nmaskey.pem`: This is the file containing the private key.

These files need to be copied to the following directories on each platform for each NMAS server in the system:

- NetWare: `sys:system directory`
- Linux/Unix: `/etc`
- Windows: the return from GetWindowsDirectory (typically `c:\windows`)

NMAS provides the `nmascert.pem` and the `nmaskey.pem` files to the Novell Audit platform agent when the log is open, if they exist. If the files don't exist, NMAS provides the internal certificate and key to the Novell Audit platform agent.

History of Novell Passwords

7

In the past, administrators have had to manage multiple passwords (simple password, NDS® password, enhanced password) because of password limitations. Administrators have also had to deal with keeping the passwords synchronized.

- NDS Password: The older NDS password is stored in a hash form that is non-reversible. Only the NDS system can make use of this password, and it cannot be converted into any other form for use by any other system.
- Simple Password: The simple password was originally implemented to allow administrators to import users and passwords (clear text and hashed) from foreign LDAP directories such as Active Directory* and iPlanet*.

  The limitations of the simple password are that no password policy (minimum length, expiration, etc.) is enforced.
- Enhanced Password: The enhanced password (no longer supported), the forerunner of Universal Password, offers some password policies, but its design is not consistent with other passwords. It provides a one-way synchronization and it replaces the simple or NDS password.

Universal Password was created to address these password problems. It provides:

- One password for all access to eDirectory.
- Enables the use of extended characters in password.
- Enables advanced password policy enforcement.
- Allows synchronization of passwords from eDirectory to other systems.

Universal Password is managed by the Secure Password Manager (SPM), a component of the NMAS module (nmas.nlm on NetWare). SPM simplifies the management of password-based authentication schemes across a wide variety of Novell products as well as Novell partner products. The managment tools only expose one password and do not expose all of the behind-the-scenes processing for backwards compatibility.

Secure Password Manager and the other components that manage or make use of Universal Password are installed as part of the NetWare 6.5 or later and eDirectory 8.7.3 install; however, Universal Password is not enabled by default. Because all APIs for authentication and setting passwords are moving to support Universal Password, all the existing management tools, when run on clients with these new libraries, automatically work with the Universal Password.

NOTE: The Password Management plug-in is available for download at the Novell Free Download Site (http://download.novell.com).

The Novell Client supports the Universal Password. It will also continue to support the NDS password for older systems in the network. The Novell Client has the capability of automatically migrating the NDS password to the Universal Password at the time of the first log in.

NOTE: When the NDS password is migrated to the Universal password, the password expiration time is recalculated from the current time plus the password expiration interval.

For more information about deploying and managing Universal Password, see the *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html).

Troubleshooting

8

The information in this section is provided to help you troubleshoot problems with NMAS™.

8.1 NMAS Error Codes

A complete list of NMAS error codes can be found in the *NMAS NDK* (http://developer.novell.com/documentation/nmas/index.html?page=/ndk/doc/nmas/nmas_enu/data/bqx8m3i.html).

8.2 Installation Issues

1. When upgrading NMAS on a Unix platform, it is possible that you will be prompted to replace libspmdclnt.so. If this happens, answer yes.
2. If you uninstall the Novell Client, you must uninstall and reinstall the NMAS Client if it is used by another application.
3. We strongly recommended that you upgrade NMAS to the latest version on all servers.
4. You must have NMAS installed on a server that holds a writeable replica of the user's object in order for the user to use NMAS.
5. You must have the NICI Client installed on each client workstation that will run ConsoleOne and NMAS software.
6. If you do not restart the server after installing NMAS and you try to reset passwords, you will receive an error message.

8.3 Login Method and Sequence Issues

1. For products to use NMAS login methods properly, at least one NMAS 2.3 or later server in the eDirectory partition needs to hold a R/W replica of the User objects that will be using NMAS.
2. Not all login or post-login methods use the initial password field when they are activated. If you are prompted to enter a password, you can ignore the password field and close it.
3. If a login method's ConsoleOne snap-ins are already present and you try to install the same login method again, you will receive a failed status displayed in the login methods installation summary dialog box. This occurs only when running ConsoleOne from the server.
4. Two password methods, such as Simple and NDS, cannot be used in an AND sequence if the Novell Client™ is set to display the password field, which it is by default.
5. If you use a login sequence that has a non-password method (for example, the X.509 method) followed by a password method (for example, the NDS password method), the user must type the credential for the password method in the initial Novell Client Login Dialog Password field before providing the non-password credential. After typing the credential for the password method, the user is then be prompted to type the password to unwrap the certificate, thus providing the credential for the non-password method.

8.4 Administration Issues

1. You must give explicit rights to users with graded authentication. Inherited rights do not work. For example, an administrator's Supervisor right is defined at the [Root] container. Rights for the administrator are not defined in the Volume object. If the administrator changes the volume's security label from Logged In to any other security label, the administrator cannot get the appropriate rights. The administrator must assign explicit rights to the volume, directories, or files in the volume.
2. If the Universal Password is not enabled, the simple password is used for various authentication services in NetWare 6.5 SP1. This includes the authentication support for CIFS and AFP.

   A problem might arise if you set or change a user's simple password from the ConsoleOne administrative snap-ins using Force Password Change. If you experience problems setting an initial password, you might need to check the Force Password Change check box. If the user already has a password set, Force Password Change might not work unless you remove the current password and specify a new one.
3. If Universal Password is enabled and you attempt to set the simple password, an -1697 error message will be returned.
4. eDirectory 8.7.3 utilities like ndsbackup, ndsrepair, and ndsmerge work with NDS passwords alone but will not work with NMAS Simple password. eDirectory 8.8 uses Universal Password.

   See
5. Pressing OK or switching between tabs when creating or renaming a label will always create or rename the label even if you respond No to the Save Changes made for Labels? prompt. You must press the Cancel button to cancel any changes. After a label is created, it cannot be deleted; however, you can rename it to an unused name, such as Unused_x.

Security Considerations

A

This section contains specific information related to security with Novell® Modular Authentication Services. It contains the following subsections:

A.1 Partner Login Methods

Novell has not evaluated the security methodologies of partner login methods. Although the partner products might have qualified for the Novell Yes, Tested & Approved or Novell Directory Enabled logos, those logos relate to general product interoperability only.

A.2 Login Policies

- If authorized login sequences, default login sequences, authorized clearances, or default clearances are assigned to a container that is not a partition root, the policy is only effective for user objects in the container, and not for user objects in subcontainers.
- If authorized login sequences, default login sequences, authorized clearances, or default clearances are assigned to a container that is a partition root, the policy is effective for all users in the partition that do not have these values assigned to the user object or to the object's parent container.
- If authorized login sequences, default login sequences, authorized clearances, or default clearances are assigned to a Login policy, that policy is effective for all users in the tree that do not have these values assigned to the user object, to the object's parent container, or to the object's partition root.
- When users are assigned passwords or other guessable login secrets such as challenge question responses, you should enable intruder detection to slow down or prevent intruders from guessing the login secrets.
- By default, failed login attempts are delayed by three seconds. This delay is intended to slow down the attempts of intruders to guess passwords. The length of the failed login delay is configurable. You should use the default of three seconds.
- Login policies such as intruder detection, network address restrictions, and time of day restrictions are enforced for all login sequences. For example, the forgotten password self-service feature of several Novell products makes the login policy enforce the challenge/response method.
- You should enable NMAS™ Auditing so that you can track login attempts and changes in configuration.

- Using the policy refresh rate command to check if the cached password policy needs to be refreshed on defined intervals instead of during each login causes a delay in the application of login policy changes.
- The `LoginInfo` command can be used to disable updating login-related attributes during login. These attributes include the intruder detection attributes. Disabling the update of these login-related attributes improves login performance. However, disabling the update of these attributes might lessen the security of the system.

A.3 Graded Authentication

Graded authentication for file system and eDirectory™ attributes is only enforced on NetWare®.

Carefully plan and test the use of Graded Authentication. Misuse of graded authentication might lock out users from NetWare volumes or eDirectory attributes.

A.4 NMASInst

When you are upgrading a login method, `nmasinst` replaces a newer version with the older version unless the `-checkversion` option is used.

Although `nmasinst` provides an option to specify the password on the command line, it is not recommended because the password could be compromised.

A.5 Universal Password

- Because the Security container contains global policies, you should be careful where you place writable replicas. Some servers can modify the overall security policies specified in the eDirectory tree. In order for users to log in with NMAS, replicas of the User objects and security container must be on the NMAS server.
- If a Password policy is assigned to a container that is not a partition root, that policy is only effective for the user objects in the container, and not for user objects in subcontainers.
- If a Password policy is assigned to a container that is a partition root, that policy is effective for all users in the partition that do not have these values assigned to the user object or to the object's parent container.
- If a Password policy is assigned to a Login policy, that policy is effective for all users in the tree that do not have these values assigned to the user object, to the object's parent container, or to the object's partition root.
- When the NDS® Password is migrated to the Universal Password during a user login, the password expiration time might be changed in the following circumstances:
  - If the password expiration time (calculated by adding the time that the NDS Password was set with the Password policy password expiration interval) is sooner than the user's current password expiration, the password expiration time is set to the calculated value.
  - If the password policy does not have a password expiration interval, the user's password expiration time attribute is removed.
- Password policies can be configured to allow the user or a password administrator to read the Universal Password by using documented NMAS LDAP extensions. These options should not be enabled unless required for your specific installation. If you require user passwords to be

readable, you should configure the Password policy to only allow selected users to read the passwords.

- You should configure a password policy to synchronize to the Distribution Password only if IDM Password Synchronization is being used to synchronize passwords between connected systems.
- You should only configure a password policy to synchronize to the Simple Password only if
  - You have servers that hold a writable replica of user objects
  - Those servers are running NetWare 6.0 or earlier
  - Users access those servers using Native File Access Protocols such as CIFS and AFP.
- When advanced password rules are enabled for a password policy, the legacy password rules on the User object are ignored, and are updated to match the password policy rules when users change their passwords or log in.
- The password exclusion rules (password history, excluded passwords, and disallowed attribute vales) are not enforced when NMAS is used to generate random passwords.
- When selecting password rules, you should balance the requirements for hard-to-guess passwords with hard-to-remember passwords.
- When an administrator specifies that the NDS Password is to be removed, the result is that the NDS Password Hash is set to a random value that is unknown to anyone but eDirectory. There may or may not be a password value that could be hashed to that random value.
- XML Password Complexity
  - If there are duplicate rule tags, the most restrictive rule is used (others are ignored) for checking passwords against the policy and for random password generation.
  - The *ViolationsAllowed* and *NumberOfCharactersToEvaluate* rule set attributes are ignored for random password generation.
  - Only the first policy in an XML policy is used for random password generation.

For additional information on Universal Password security, see "*How Secure Is Universal Password?*" in the *Novell Password Management Administration Guide*.

A.6 SDI Key

You should make the Security Domain Infrastructure (SDI) key, also known as the tree key, a Triple DES key (3DES). The SDI key can be checked and upgraded by using the SDIDiag utility. See "Step 4: Verify That Your SDI Domain Key Servers Are Ready for Universal Password" in the *Password Management Administration Guide*.