Novell Modular Authentication Services (NMAS™)

2.4.0

www.novell.com

ADMINISTRATION GUIDE

December 22, 2005

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.

Novell Modular Authentication Services (NMAS)TM software includes support for a number of login methods from third-party authentication developers. Refer to the NMAS Partners Web site (http://www.novell.com/products/nmas/partners/) for a list of authorized NMAS partners and a description of their login methods.

Each NMAS partner 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, and while these products may have qualified for the Novell Yes, Tested and Approved or Novell Directory Enabled logos, those logos only relate to general product interoperability. Novell encourages you to carefully investigate each NMAS partner's product features to determine which product will best meet your security needs. Also, some login methods require addtional hardware and software not included with the NMAS product.

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

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Novell Modular Authentication Services (NMAS) 2.4 Administration Guide
December 22, 2005

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

Novell Trademarks

Third-Party Materials

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 2.3 Administration Guide*, see the NMAS 2.3 Administration Guide Web site (http://www.novell.com/documentation/lg/nmas23/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.

1 NMAS Overview

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

NMAS Functionality

NMAS is designed to help you protect information on your network. NMAS brings together additional ways of authenticating to Novell eDirectory™ on NetWare® 5.1 or later, Windows* NT*\2000 and UNIX* networks to help ensure that the people accessing your network resources are who they say they are.

NMAS Features

With previous releases of NMAS, authentication devices, such as smart cards, tokens, etc., could be used only for authentication. Now, 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.

See "User Identification Plug-Ins" on page 25 for more information on user identification.

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 the standard NDS password login method, as well as login methods common with LDAP, Internet browsers, and other directories.

- **Standard NDS password authentication:** The standard NDS® password method uses a secure password challenge-response authentication. Because of the increased security it offers, the standard NDS password authentication is somewhat slower than other password methods.
- **Clear text:** Clear text (or plain text) authentication sends the password over the wire in an unencrypted form. Aside from no authentication at all, this is the least effective form of user authentication from a security standpoint. Because there is no encryption process, plain text authentication is normally quite fast.

  This authentication method is included in NMAS to provide faster authentication in networks requiring less security, as well as to provide interoperability with systems that use cleartext authentication (for example, FTP/Telnet and POP3 e-mail).
- **SHA-1:** The secure hash algorithm (SHA-1) is a popular method of network authentication. A *hash* (or message digest) is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.

  In terms of security, SHA-1/MD5 authentication is more secure than clear text because the password is altered when it travels across the network. Authentication is relatively fast because it is easy to compute a shorter hashed value.
- **MD-5:** This message-digest algorithm takes a message of arbitrary length and produces a 128-bit message digest (hash) output. MD-5 was, at one time, the most widely used secure hash algorithm.
- **Enhanced Password**

Physical Device Authentication

Third-party authentication developers have written authentication modules for NMAS for two types of physical devices (something you have): smart cards and tokens.

NOTE: NMAS uses the word *token* to refer to all physical device authentication methods (smart cards, tokens, etc.).

- **Smart cards:** A smart card is a plastic card, about the size of a credit card, 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.
- **Tokens:** A token is a hand-held hardware device that generates a one-time password to authenticate its owner. Token authentication systems are based on one of two schemes: challenge-response and time-synchronous authentication.
    - **Challenge-response authentication:** With this approach, the user logs in to an authentication server, which then issues a prompt for a personal identification number (PIN) or a user ID. The user provides the PIN or ID to the server, which then issues a *challenge*—a random number that appears on the user's workstation. The user enters that challenge number into the token, which then encrypts the challenge with the user's encryption key and displays a response. The user types in this response and sends it to the authentication server.

      While the user is obtaining a response from the token, the authentication server calculates what the appropriate response should be based on its database of user keys. When the server receives the user's response, it compares that response with the one it has calculated. If the two responses match, the user is authenticated to the network.
    - **Time-synchronous authentication:** With this method, an algorithm that executes both in the token and on the server generates identical numbers that change over time. The user logs in to the authentication server, which issues a prompt for an access code. The user then enters a PIN followed by the digits displayed at that moment on the token. The authentication server compares this entry with the sequence it generated; if they match, the server grants the user access to the network.
    - **X.509 Certificates**
    - **Entrust and Advanced X509 Certificates**

Biometric Authentication

Biometrics is the science and technology of measuring and statistically analyzing human body characteristics (something you are).

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.

Biometric authentication can be classified into two groups:

- **Static biometric authentication:** This captures and verifies physiological characteristics linked to the individual. Common static biometric characteristics include fingerprints, eye retinas and irises, and facial features.
- **Dynamic biometric authentication:** This captures and verifies behavioral characteristics of an individual. Common dynamic biometric characteristics include voice or handwriting.

Device Removal Detection Phase

The user's session enters this phase after login is complete. This feature is provided by the Secure Workstation method. 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.

Example

You could use a pcProx* device for identification, the NDS password for authentication, and the Universal SmartCard plug-in during the device removal detection phase. In this example, the Secure Workstation method starts the device removal plug-in for the Universal SmartCard plug-in when the shell starts. Then, the Universal SmartCard plug-in monitors the card in the reader when the shell starts, and triggers a device removal event when that card is removed.

You do not need to execute an NMAS login sequence that contained the Universal SmartCard method in the above example. However, most administrators would want the user to log in with the smart card if they are concerned about detecting its removal. The above functionality is probably most useful in scenarios where, for example, an Entrust* certificate is read from the smart card, and the Entrust method is used for authentication. The Universal SmartCard device removal plug-in could be used in this scenario even though the Universal SmartCard method was not used during the authentication process.

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 Secure Workstation method, 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 NMAS Partners Web site (http://www.novell.com/products/nmas/partners) for a list of authorized NMAS partners and a description of their methods.

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.

Graded Authentication

An important 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 managed from the Security Policy object in the Security container by using 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 3, "Using Graded Authentication," on page 27.

NMAS Software

The NMAS software image is available for download as a standalone product or it can also be bundled with other products, such as Novell eDirectory or NetWare. The software image includes the following:

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

Server and Client Software Installation

NMAS server-side software must be installed on a NetWare 5.1 or later server, Windows NT/2000, or a UNIX server with eDirectory. NMAS client-side software must be installed on each Windows client workstation that will access the network using the NMAS login methods. After installation, NMAS is managed using the ConsoleOne or Novell iManager utility.

The NMAS server software is installed from a Windows client workstation. You must have Admin rights to the eDirectory Tree object and be connected to the NetWare server to install the NMAS server product.

The NMAS client software must be installed on each client workstation you want to use the NMAS login methods. The latest Novell Client™ software must be installed on the client workstation before you install the NMAS client software.

Login Method Software and NMAS Partners

All NMAS login methods (server software and snap-ins) are installed using the Login Method installation utility. The client software is installed using a Windows installation program. 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 NMAS Partners Web site (http://www.novell.com/products/nmas/partners) for a list of authorized NMAS partners and a description of their login methods.

Each NMAS partner 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 NMAS 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.

Universal Password

Universal Password enforces password policy uniformly across multiple authentication systems (such as Native File Access). Universal password also manages multiple types of password authentication methods from disparate systems. This is done by creating a common password that can be used by all protocols to authenticate users.

For information on deploying Universal Password, see the Chapter 6, "Deploying Universal Password," on page 43.

ConsoleOne and Novell iManager Management

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

During the installation of these modules, 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.

By default, NMAS installs the standard NDS password login method. Additional login methods can be installed using 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.

IMPORTANT: Run ConsoleOne from a Windows client workstation by using the ConsoleOne executable located on the server at *server_name*: sys\public\mgmt\consoleone\1.2\bin\consoleone.exe.

What's Next

- To install NMAS as a standalone product, see the nmas_install.pdf file included with this software image. To install NMAS as part of another product's installation process, see that product's installation guide.
- To set up login methods and sequences, see Chapter 2, "Managing Login and Post-Login Methods and Sequences," on page 17.
- To set up graded authentication, see Chapter 3, "Using Graded Authentication," on page 27.
- To log in using NMAS, see Chapter 4, "Logging In to the Network Using NMAS," on page 37.

2 Managing Login and Post-Login Methods and Sequences

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 software 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 not included with the NMAS product. 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 in the nmasmethods folder. Other third-party methods are available for download.

See the NMAS Partners Web site (http://www.novell.com/products/nmas/partners) for a description of the third-party login methods. Each method will have a readme.txt file or a readme.pdf file that will include specific installation and configuration instructions.

- "Installing a Login Method" on page 17
- "Updating Login and Post-Login Methods" on page 20
- "Managing Login Sequences" on page 20
- "Authorizing Login Sequences for Users (ConsoleOne)" on page 23
- "Authorizing Login Sequences for Users (Novell iManager)" on page 23
- "Setting Default Login Sequences (ConsoleOne)" on page 23
- "Setting Default Login Sequences (Novell iManager)" on page 24
- "Deleting a Login Method" on page 24
- "User Identification Plug-Ins" on page 25
- "What's Next" on page 25

Installing a Login Method

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

- The Login Method Installer (Windows)

  The login method installer (methodinstaller.exe) is a standalone utility that installs login methods into eDirectory.

- nmasinst utility (UNIX)

The nmasinst utility allows you to install login methods into eDirectory from a UNIX machine. The nmasinst utility is located in the \usr\bin\nmasinst directory.

- ConsoleOne® (Windows)

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

Installing a Login Method Using the Method Installer

1. Double-click the login method installer executable (methodinstaller.exe).
2. Read the Welcome screen, then click Next.
3. Click the boxes next to the methods you want to install.

   If you want to install a login method that does not appear on the list, click Change Directory and locate the nmasmethod directory that contains the login method you want to install, then click Next.
4. Log in to the eDirectory tree as an administrator or a user with administrative rights. Provide the required authentication information, then click Next.
5. (Conditional) If your LDAP server requires encrypted passwords, you will be prompted to accept the server's certificate for establishing a secure SSL connection or provide a certificate of your own. Accept or provide the certificate, then click Next.
6. Read the license agreement, click Accept, then click Next.

   Review the login method information. You can change the name of the login method. The method name is used as the object name in eDirectory.
7. Click Next.
8. Review the Module list, then click Next.
9. If you want to create a login sequence that will use this login method, check the box next to Create Login Sequence and accept the default name, or provide a different name for the login sequence. If you don't want to create a login sequence, uncheck the box next to Create Login Sequence.
10. Click Next.
11. If the login method you are installing has ConsoleOne snap-ins that need to be installed, use the Browse button to provide a path to the directory where consoleone.exe resides on your server. Double-click the consoleone.exe file, then click Next.
12. Review the list of methods that have been successfully installed, then click Finish.

Installing a Login Method Using the nmasinst Utility (UNIX)

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

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 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 DHost is not running on the default port.

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

Installing a Login Method Using ConsoleOne

IMPORTANT: Run ConsoleOne from a Windows client workstation by using the ConsoleOne executable located on the server at: *server*:sys\public\mgmt\consoleone\1.2\bin\consoleone.exe.

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 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 or rename it, 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.

Installing a Post-Login Method Using ConsoleOne

IMPORTANT: Run ConsoleOne from a Windows client workstation by using the ConsoleOne executable located on the server at *server*:sys\public\mgmt\consoleone\1.2\bin\consoleone.exe.

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 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 or rename it, 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.

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:

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.

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 ConsoleOne or Novell iManager.

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 21
- "Creating a New Login Sequence (Novell iManager)" on page 21
- "Modifying a Login Sequence (ConsoleOne)" on page 22

- “Modifying a Login Sequence (Novell iManager)” on page 22
- “Deleting a Login Sequence (ConsoleOne)” on page 22
- “Deleting a Login Sequence (Novell iManager)” on page 23

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.

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 the Add (+) button and enter a name for the new login sequence, then click OK to continue.

   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 OK when you are finished.

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.

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. Select a login sequence from the 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.
5. Select an action:
   - 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.

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.

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 from the Login Sequences drop-down list, then click the Delete (-) button.
5. Click OK, then Apply or OK.

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.

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 Login Sequences tab.
4. Check or uncheck the Restrict the User to the Sequences Authorized Below check box.

   If you uncheck the check box, the user can use any defined login sequence to log in.

   If you check 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.
5. Click Apply or OK.

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.

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 Login Sequences tab.
4. In the Default Login Sequence drop-down list, 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 will be used.
5. Click Apply or OK.

Deleting a Login Method

The NMAS 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 ConsoleOne.

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

- "Remove the Login Method from Any Login Sequence" on page 24
- "Delete the Login Method" on page 24

Remove the Login Method from Any Login Sequence

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.

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

Delete the Login Method

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.

User Identification Plug-Ins

The pcProx method and Universal SmartCard method both provide user identification plug-ins. The user identification plug-in is a DLL that is loaded by the NMAS client login dialog box. It can obtain the user's name, context, tree name, server name, and NMAS sequence from an authentication device.

The Universal SmartCard identification plug-in gets the user name from the subject name in the certificate stored on the smart card. If a smart card is inserted while the login dialog box is displayed, the ID plug-in will do an LDAP search for a user with an "allowable subject name" that matches the name on the certificate. If a user is found, his username and context are automatically entered in the login dialog box.

The pcProx identification plug-in reads a 32-bit number from the pcProx card. It then does an LDAP search for a user who has that number assigned as his or her pcProx login ID. This is set from the Login IDs > pcProx tab in ConsoleOne.

After a user ID has been obtained from the ID plug-in, the username and context fields are populated with the user's DN. The tree, server, and sequence fields are updated with information provided by the administrator when he or she installed the client module (LCM) for the method that is registered as the ID plug-in. The client then automatically clicks the OK button to start the authentication phase.

To configure either the pcProx or Universal SmartCard method as the ID plug-in, you must click the Use Device to Obtain Username for Login check box during the LCM install for the method. When you click this check box, you are presented with two additional dialog boxes.

The first dialog box asks you to supply a tree name, server name, and NMAS login sequence that are used when a user name is obtained from the device. These fields are optional. If they are not provided, then the ID plug-in does not update the corresponding fields in the login dialog box.

The second dialog box asks you for a list of up to three LDAP servers. These are the servers that are used when the ID plug-in does its LDAP search for the user. Because the LDAP protocol is being used, you must enter either an IP address or DNS name for the server.

What's Next

- To set up graded authentication, see Chapter 3, "Using Graded Authentication," on page 27.
- To log in using NMAS, see Chapter 4, "Logging In to the Network Using NMAS," on page 37.

3 Using Graded Authentication

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.

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:

- "Graded Authentication Terms" on page 27
- "Graded Authentication Rules" on page 31
- "Configuring the Security Policy Object" on page 31
- "Assigning Security Labels to Network Resources" on page 33
- "Assigning User Clearances" on page 34
- "Graded Authentication Example" on page 34
- "What's Next" on page 36

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

Graded Authentication Terms

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 "Configuring the Security Policy Object" on page 31.

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 or reading of information. You can define additional secrecy categories to meet your company's needs.
- **Integrity Categories:** Integrity controls the modification or writing of information.

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 31.

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}
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}

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

For more information, see "Defining Security Labels" on page 32.

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 30 and "Graded Authentication Rules" on page 31.

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.

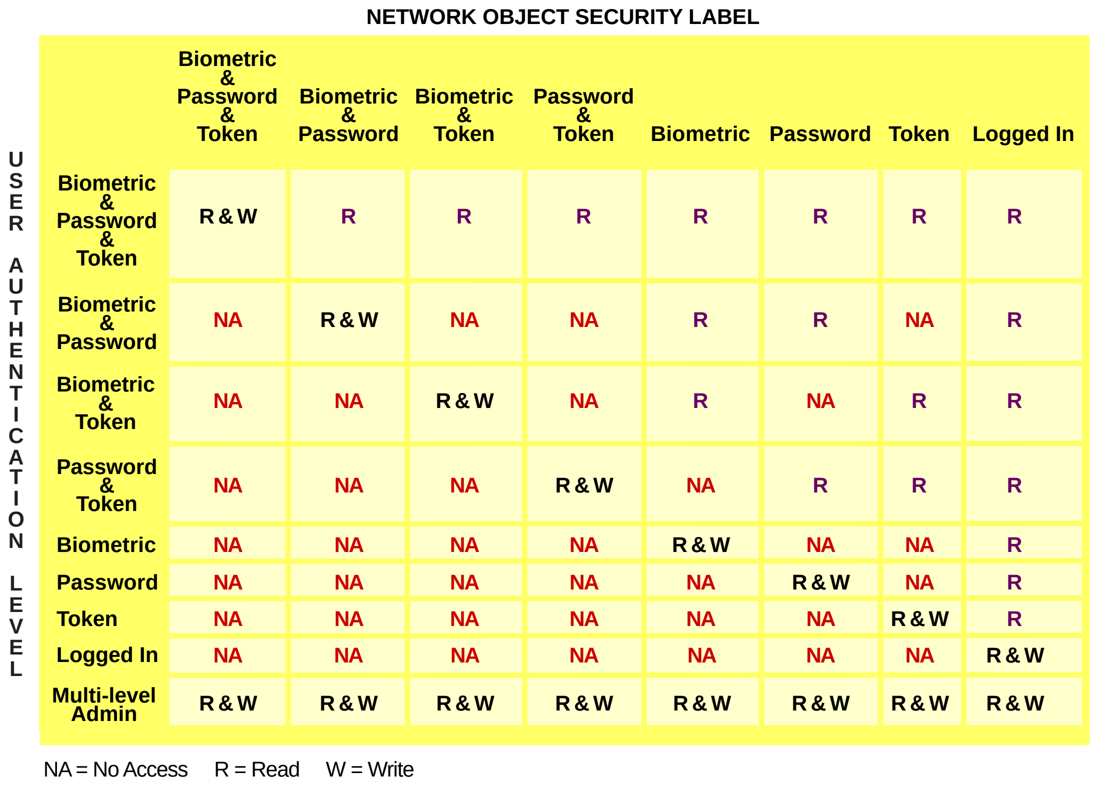
Multi-Level Clearance

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 figure summarizes the access relationships between the predefined clearances and the security labels. For more information, see "Defining Clearances" on page 32.



NETWORK OBJECT SECURITY LABEL

USER AUTHENTICATION LEVEL	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

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 "Graded Authentication Rules" on page 31.

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.

Configuring the Security Policy Object

A Security Policy object is created in the Security container when you install NMAS. 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.

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

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.

Renaming a Category

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 the category you want to rename, then click Rename Category.
4. Specify the new name, click OK, then click OK or Apply.

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

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.

Renaming a Security Label

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.

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

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.

Viewing the Properties of a Clearance

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.

Renaming a Clearance

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.

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:

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.

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.

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:

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. 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:

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.

Assigning User Clearances

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.

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.

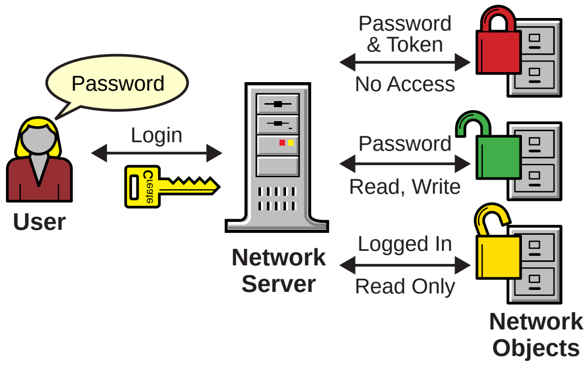
Graded authentication replaces the physical key given to users with a clearance. Also, NMAS replaces the filing cabinet with NetWare file system volumes that are also assigned security labels. These security labels replace the filing cabinet lock type.

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 1, "Single-Factor Authentication," on page 35) 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 1 Single-Factor Authentication

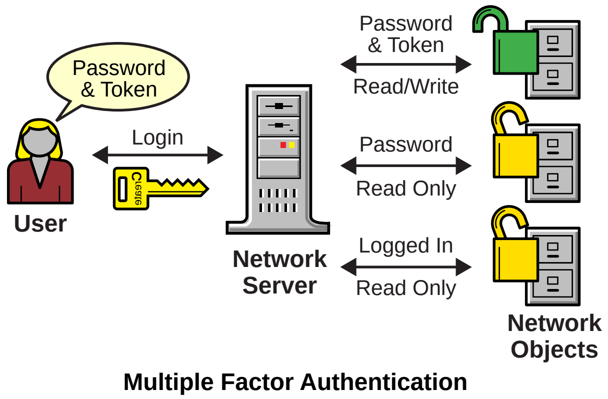


Single Factor Authentication

The following would apply (as illustrated in Figure 2, “Multiple-Factor Authentication,” on page 35) 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 2 **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.

What's Next

- To set up login methods and sequences, see Chapter 2, "Managing Login and Post-Login Methods and Sequences," on page 17.
- To log in using NMAS, see Chapter 4, "Logging In to the Network Using NMAS," on page 37.

4 Logging In to the Network Using NMAS

After NMAS™ is installed and graded authentication is configured, 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.

- "Password Field" on page 37
- "Advanced Login" on page 37
- "Unlocking the Workstation" on page 38
- "Client Log File" on page 38
- "Tray Icon" on page 38
- "Single Sign On Tab" on page 38

Additional information is available to help your network users understand the NMAS login process. You can print the nmas_user.pdf file in the NMAS software build and distribute it to your network users.

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.

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.

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 NT 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.

Client Log File

You can create a client log file that can help in troubleshooting NMAS authentication problems. The NMAS client log file is re-created every time you log in.

1 Open the Novell Client Windows property page.

2 Click the Location Profiles tab.

3 Select the desired location profile from the Location Profiles window, then click Properties.

4 In Service and Service Instance, click Properties.

5 From the NMAS tab, click Log NMAS Client Activity, then click the Log File button to set the location of the log file.

The default location for the log file is at the root of your primary hard disk (C:\).

Tray Icon

When you log in using NMAS, a lock/document icon displays in your Windows 95/98/Me/NT/2000 tray. Double-click the icon to see your graded authentication status.

Single Sign On Tab

For Windows NT, 2000, or XP, a Single Sign On tab is available in properties of the Novell Client for the convenience of users authenticating via an NMAS login method.

NOTE: The Single Sign On tab does not take the place of the Novell Single Sign-on product. This is an added feature for Windows NT users logging in with NMAS software.

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.

5 Other Administrative Tasks

This section describes other administrative tasks for NMAS™.

- "Using the Policy Refresh Rate Command" on page 41
- "Using DSTRACE" on page 42
- "Disabling and Uninstalling the NMAS Client" on page 42
- "Disabling NMAS on the Server" on page 42

Using the Policy Refresh Rate Command

With NMAS 2.3 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:

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.

The policy refresh rate command can also be entered at the NetWare® console.

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.

UNIX

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

Using DSTRACE

You can use the DSTRACE utility to get trace information from NMAS. See the DSTRACE section (http://www.novell.com/documentation/lg/edir873/edir873/data/a5zemw0.html) of the eDirectory documentation for more information.

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. Uncheck NMAS Authentication.
5. Click OK.

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

Disabling NMAS on the Server

NMAS is defined as a core service after it is installed because other services (such as eDirectoryeDirectory) 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:

NetWare:

1. Remove the nmas.nlm file in sys:\system.
2. Restart the server.

Windows NT/2000 with Novell eDirectory:

1. Stop the eDirectoryeDirectory Service.
2. Remove the nmas.dlm file.
3. Restart the service.

6 Deploying Universal Password

As Novell® executed on its One Net vision of integrating heterogeneous systems and allowing for native systems to interoperate, the traditional Novell password has proven troublesome for integration with these heterogeneous systems. Novell introduces Universal Password, a way to simplify the integration and management of different password and authentication systems into a coherent network.

Password History

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 in eDirectory. 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. Also, by default, users do not have rights to change their own simple passwords.
- Enhanced Password: The enhanced password offers some password policy, but its design is not consistent with other passwords. It provides a one-way synchronization and it replaces the simple or NDS password.

  To ensure that the password is secure, NMAS uses either a DES key or a triple DES (key depending upon the strength of the Secure Domain Key) to encrypt the data in the NMAS Secret and Configuration Store.

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 our partner's 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 8.7.1 install; however, Universal Password is disabled 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). Select Nsure Identity Manager as the product and click Submit Search. The Password Management plug-in is listed on this page. It requires eDirectory 8.7.3 and iManager 2.02.

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 upgrading to the new Password from the NDS password.

How Secure is Universal Password?

Reversible encryption of Universal Password is required for convenient interoperation with other password systems. So administrators have to evaluate the costs and benefits of the system. Using a single copy of the Univeral Password stored in eDirectory may be more secure and/or convenient than attempting to manage several different passwords. Novell provides several levels of security to make sure Universal Password is protected while stored in eDirectory.

A Universal Password is protected by three levels of security; tripleDES encryption of the password itself, eDirectory rights and file system rights.

The Universal Password is encrypted by a triple DES, user-specific key. Both the Universal Password and the user key are flagged with a hidden attribute that only eDirectory can read. The user key (3DES) is stored encrypted with the tree key and the tree key is protected by a unique NICI key on each machine. (Note that neither the tree key nor the NICI key is stored within eDirectory. They are not stored with the data they protect.) The tree key is present on each machine within a tree, but each tree has a different tree key. So, data encrypted with the tree key can only be recovered on a machine within the same tree. Thus, while stored, the Universal Password is protected by three layers of encryption.

Each key is also secured via eDirectory rights. Only the administrators with supervisor rights or the user themselves have the rights to change Universal Passwords.

File system rights ensure that only a user with the proper rights can access these files.

If Universal Password is deployed in an environment requiring high security, you can take the following precautions:

1. Make sure that the following directories and files are secure:

NetWare	%system32%\novell\nici
Windows	%system32%\novell\nici %system32% where the NICI DLL is installed

Linux/Unix	/var/novell/nici etc/nici.cfg /usr/locall/lib/libccs2.so and the NICI shared libraries in the same directory On LSB-compliant systems: The above mentioned directories and files as well as /var/opt/novell/nici etc/opt/novell /opt/novell/lib

Consult the documentation for your system for specific details of the location of NICI and eDirectory files.

2. As with any security system, restricting physical access to the server where the keys reside is very important.

Deployment Steps

Step 1 - Review the Services You Currently Use and Understand their Current Password Limitations

The following table outlines some Novell services and the password limitations they have. These limitations are addressed by Universal Password:

Service	Description	Limitations
Novell Client^{TM} for Windows* NT*/ 2000/XP versions prior to 4.9 and Novell Client for Windows 95/98 versions prior to 3.4.	The Novell Client software for file and print services. Uses the NDS® password, which is based on the RSA public/private key system.	◆ Limited support for passwords with extended characters ◆ Passwords inaccessible from non-Novell systems ◆ Password is stored in such a way as to prevent extraction, thus disallowing interoperability with simple password
Windows Native Networking (CIFS) in NetWare 6 and NetWare 5.1 (NFAP add-on pack for NetWare 5.1)	Novell's CIFS server as part of the Native File Access Protocols. It allows Windows* clients to access Novell services using the built-in Windows Client Networking Services.	◆ Uses a separately administered password called the simple password ◆ Has no expiration or restriction capabilities for the simple password ◆ Attempts to synchronize with NDS password, but can get out of sync
Macintosh* Native Networking (AFP) in NetWare 6 and NetWare 5.1 (NFAP add-on pack for NetWare 5.1)	Novell's AFP server as part of the Native File Access Protocols. It allows Macintosh clients to access Novell services using the built-in Macintosh Client Networking Services.	◆ Uses a separately administered password called the simple password ◆ Has no expiration or restriction capabilities for the simple password ◆ Attempts to synchronize with the NDS password, but can get out of sync

Service	Description	Limitations
LDAP	Novell's LDAP services allow a user to bind using username and password across a Secure Sockets Layer (SSL) connection.	- Limited interoperability with the Novell Client Services (NDS password) for extended character or international versions - Attempts to utilize the simple password if bind is not a simple bind (that is, the bind is using an encrypted password).
LDAP User Import	Uses ICE or other tools to import users from foreign directories into eDirectory. Passwords are also brought in.	- Passwords are imported into the simple password system. - Mutually exclusive of NFAP solutions (Windows and Macintosh Native File Access) if not clear text password. - Password is in its encrypted native format
Web-Based Services	Novell Web-based services (Apache Web server) authentications. This includes eGuide, Novell Portal Services, and other Web-based applications.	- Limited interoperability with the Novell Client services (NDS password) for extended character or international versions - Not designed to check simple password
RADIUS Services	Novell RADIUS Authentication Services	- Limited interoperability with the Novell Client services (NDS password) for extended character or international versions
NetWare Remote Manager	Novell's Web-based server health and management interface.	- Limited interoperability with the Novell Client services (NDS password) for extended character or international versions - Not designed to check simple password
NDS for NT	Novell eDirectory™ Services for Microsoft Windows NT 4 Server domains.	- Uses a separate value for storing the NT password - Synchronized only with the NDS password by the Novell Client and the ConsoleOne® and NWAdmin snap-in tools
DirXML® Password Synchronization for Windows 1.0 and DirXML Starter Pack	Enables synchronization of passwords for NT, Active Directory*, and eDirectory accounts.	- eDirectory password changes made outside of the Novell Client will not be synchronized. For example, an eDirectory password change made through eGuide would not be synchronized to Active Directory or NT. See Sample Password Scenarios (http://www.novell.com/documentation/lg/dirxmlstarterpack/jetset/data/aktnwz0.html) for detailed information about DirXML Password Synchronization for Windows.

Step 2 - Identify Your Need for Universal Password

If you answer yes to any of the following questions, you should plan to deploy and use Universal Password:

- Do you currently use Native File Access and desire to enforce policies such as password expiration and/or password length?
- Do you use or plan to use Native File Access (Windows and/or Macintosh)?
- Do you plan to have international users access Novell Web-based services and/or use the Novell Client for Windows NT/2000/XP or the Novell Client for Windows 95/98 to access Novell file and print services?
- Do you plan to use Novell Nsure Identity Manager 2, powered by DirXML, with its enhanced password policy and password synchronization capabilities?
- Do you plan to use Nterprise Branch Office 2.0?

Step 3 - Make Sure Your Security Container is Available

NMAS relies on storage of policies that are global to the eDirectory tree. The eDirectory tree is effectively the security domain. The security policies must be available to all servers in the tree.

NMAS places the authentication policies and login method configuration data in the Security container that is created off of the [Root] in NetWare 5.1 or later eDirectory trees. This information must be readily accessible to all servers that are enabled for NMAS. The purpose of the Security container is to hold global policies that relate to security properties such as login, authentication, and key management.

With NMAS, we recommend that you create the Security container as a separate partition, and that the container be widely replicated. This partition should be replicated as a Read/Write partition only on those servers in your tree that are highly trusted.

NOTE: Because the Security container contains global policies, be careful where writable replicas are placed, because these 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 must be on the NMAS server.

For additional information, see Novell TID 10091343 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10091343.htm).

Step 4 - Verify That Your SDI Domain Key Servers Are Ready for Universal Password

1 Verify that the SDI Domain Key servers meet minimum configuration requirements and have consistent keys for distribution and use by other servers within the tree.

1a From a NetWare server console, load sdidiag.nlm.

From a Windows server, open a command prompt box and run sdidiag.exe.

NOTE: Sdidiag.nlm ships with NetWare 6.5 or later. Sdidiag.exe ships with the Windows version of eDirectory 8.7.3 or later. Both files are available as part of a security patch (sdidiag21.exe) associated with Novell TID 2966746 (http://support.novell.com/severlet/tidfinder/2966746).

1b Log in as an Administrator by entering the tree name, the server, the context, the user name, and the password.

1c Check to make sure all you servers are using 168 bit keys. Follow the instructions in Novell TID 10093969 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093969.htm) to ensure this requirement is met.

1d Enter the command `CHECK -v >> sys:system\sdinotes.txt`

The output to the screen will display the results of the `CHECK` command.

If no problems are found, go to "Step 5 - Upgrade At Least One Server in the Replica Ring to NetWare 6.5 or later or eDirectory 8.7.1 or later" on page 49.

or

If problems are found, follow the instructions written to the sys:system\sdinotes.txt file to resolve any configuration and key issues.

2 Verify that the SDI Domain Key Servers are Running NICI 2.4.2 or later

We recommend that NetWare 6.5 or later or eDirectory 8.7.1 or later be installed on your SDI Domain Key servers. However, this is not required. At a minimum, you need to install NICI 2.4.2 or later on these servers.

You can verify if NICI 2.4.2 is installed on these servers:

2a From the server console, execute the NetWare command `M NICISDI.NLM`.

The version must be 24212.98 or later.

If the version is earlier, you must do ONE of the following:

- Update the servers' NICI to version 2.4.2, which requires eDirectory 8.5.1 or later.

  NOTE: You can download NICI version 2.4.2 from the Novell Free Download site (http://download.novell.com). Select Novell International Cryptographic Infrastructure from the Choose a Product drop-down list, then click Submit Search. NICI 2.4.2 requires eDirectory 8.5.1 or later.

  Also, you must reinstall NICI 2.4.2 or later if you install an eDirectory upgrade after installing NICI. This issue will be resolved with the Consolidated Support Pack 10.

- Update the SDI Domain Key servers to NetWare 6.5 or later or eDirectory 8.7.1 or later.

- Remove the servers as SDI Domain Key Servers and add a server that meet these requirements.

  To remove a server as an SDI Domain Key Server:

  1. At the server console, load SDIDIAG.

  2. Log in as an Administrator that has management rights over the Security container and the W0.KAP.Security objects by entering the tree name, the server, the context, the user name, and the password.

  3. Enter the command **`RS -s`** ***`servername`***

  For example, if server1 exists in container PRV in the organization Novell within the Novell_Inc tree, you would type .server1.PRV.Novell.Novell_Inc. for the servername.

  To add a server as an SDI Domain Key Server:

  1. At the server console, load SDIDIAG.

  2. Log in as an Administrator by entering the Tree name, the Server, the Context, the User name, and the password.

3. Enter the command **`AS -s`** ***`servername`***

For example, if server1 exists in container PRV in the organization Novell within the Novell_Inc tree, you would type .server1.PRV.Novell.Novell_Inc. for the servername.

2b After completing one of the options above, you might want to rerun the SDIDIAG check command. See Step 1d on page 48.

NOTE: For more information on SDIDIAG, see Novell TID 10083939 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10083939.htm) and Novell TID 10088626 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088626.htm).

Step 5 - Upgrade At Least One Server in the Replica Ring to NetWare 6.5 or later or eDirectory 8.7.1 or later

1. Identify the container that holds the User objects of those users who will be using Universal Password.
2. Find the partition that holds that container and the User objects.
3. Identify at least one server that holds a writable replica of the partition.
4. Upgrade that server to NetWare 6.5 or later or eDirectory 8.7.1 or later.

You do not need to upgrade all servers in your tree in order to enable Universal Password, but we recommend that you eventually upgrade them all. Plan to upgrade the servers that hold writable replicas first, followed by those with read-only replicas or no replicas. This allows Universal Password support for services on all those servers.

NOTE: If you have LDAP and CIFS (Windows Native Networking) and/or AFP (Macintosh Native Networking) servers that you want to use Universal Password, you must upgrade those servers to NetWare 6.5.

Step 6 - Check the Container for SDI Key Consistency

Check to ensure that all instances of cryptographic keys are consistent throughout the tree. Sdidiag ensures that each server has the cryptographic keys necessary to securely communicate with the other servers in the tree.

1. From a NetWare server console, load sdidiag.nlm.

   From a Windows server, open a command prompt box and run sdidiag.exe.

2. Enter the command **`CHECK -v >> sys:system\sdinotes.txt -n`** ***`container DN`***

   For example, if user Bob exists in container USR in the organization Acme within the Acme_Inc tree, you would type .USR.Acme.Acme_Inc. for the container DN.

   This reports if there are any key consistency problems among the various servers and the Key Domain servers.

   The output to the screen displays the results of the **`CHECK`** command.

3. If no problems are reported, you are ready to enable Universal Password. Go to "Step 7 - Turn on Universal Password" on page 50.

   or

   If problems are reported, follow the instructions in the sdinotes.txt file.

   In most cases, you will be prompted to run the command **`RESYNC -T -n`** ***`container DN`***.

This command can be repeated any time NMAS reports -1418 or -1460 errors during authentication with Universal Password.

For more information on SDIDIAG options and operations, refer to Novell TID 10081773 (http://support.novell.com/servlet/tidfinder/10081773).

Step 7 - Turn on Universal Password

If you are using the Password Management plug-in, do the following:

1. Start Novell iManager.
2. Under Roles and Tasks > Passwords, click Password Policies.
3. Start the Password Policy Wizard by clicking New.
4. Provide a name for the policy and click Next.
5. Select Yes to enable Universal Password.
6. Complete the Password Policy Wizard.

IMPORTANT: If you assign a policy to a container that is the root of a partition, the policy assignment is inherited by all users in that partition, including users in subcontainers. To determine whether a container is a partition root, browse for the container and note whether a partition icon is displayed beside it.

If you assign a policy to a container that is not the root of a partition, the policy assignment is inherited only by users held in that specific container. It is not inherited by users that are held in subcontainers. If you want the policy to apply to all users below a container that is not a partition root, you must assign the policy to each subcontainer individually.

Step 8 - Deploy Novell Client Software

You can deploy the Novell Client for Windows NT/2000/XP version 4.9, Novell Client for Windows 95/98 version 3.4, or NMAS Client 2.2 or later prior to enabling Universal Password, but the client does not take advantage of these services until you enable Universal Password (see "Step 7 - Turn on Universal Password" on page 50). The new Novell Client software automatically starts using the Universal Password when it is turned on. Users will see no differences in the client, except with case-sensitive passwords.

NOTE: You must manually install Client NICI 2.6.1 for Windows or later and NMAS^{TM} Client 2.2 in order for Novell Client for Windows 95/98 to start using the Universal Password services.

Backwards Compatibility

Universal Password is designed to supply backwards compatibility to existing services. By default, passwords changed with this service will automatically be synchronized to the simple and NDS passwords on the User object (unless you specify otherwise using the Password Management plug-in). This way, NetWare 6 and 5.1 servers running Native File Access protocols for Windows and Apple* native workstations will continue to have their passwords function properly. Novell Client software prior to the Novell Client for Windows NT/2000/XP version 4.9 or the Novell Client for Windows 95/98 version 3.4 will also have their passwords continue to function properly.

The exception to this is the use of international characters in passwords. Because the character translations are different for older clients, the actual values will no longer match. Customers who have deployed Web-based or LDAP services and who use international passwords have already seen these problems and have been required to change passwords so they do not include international characters. We recommend that all servers be upgraded to NetWare 6.5 and all Novell Client software be upgraded in order for full, system-wide international passwords to function properly.

Novell's NetWare Storage Management Services™ (SMS) infrastructure is used for Novell and third-party backup and restore applications. Additionally, the Novell Server Consolidation utility, Distributed File Services Volume Move, and Server Migration utilities use SMS as their data management infrastructure. The system passwords used by these Novell and third-party products cannot contain extended characters if they are to function in a mixed environment of NetWare 4, 5, 6, and 6.5 servers. However, when all servers are upgraded to NetWare 6.5, extended character passwords can be used.

NOTE: Please refer to Novell TID 10083884 (http://support.novell.com/servlet/tidfinder/10083884). It shows which applications/services are Universal Password-capable, as well as which applications/services are extended character-capable. Many applications/services can use extended characters without Universal Password.

The following table shows the expected behavior of Universal Password when it interacts with older services.

Password Change Method	**Passwords Synchronized**
Novell Client software prior to Novell Client for Windows NT/2000/XP version 4.9 or Novell Client for Windows 95/98 version 3.4 to any server version	NDS password only.
Native File Access (Windows or Macintosh) on NetWare 5.1 or NetWare 6	Simple password and NDS password. The password change is successful only if the old NDS and simple passwords were in sync.
Native File Access (Windows or Mac) on NetWare 6.5	Universal, simple, and NDS passwords are changed. All are synchronized, even if old ones were out of sync.
LDAP (standard) prior to eDirectory 8.7.1	NDS password only.
LDAP (extended) prior to eDirectory 8.7.1	Simple password or NDS password is changed (extensions specify which one).
LDAP (standard) to NetWare 6.5 (or NetWare 5.1, 6 running eDirectory 8.7.1)	Universal, simple, and NDS passwords are changed. All are synchronized even if old ones were out of sync.
LDAP (extended) to NetWare 6.5	Universal, simple, or NDS password changed (extensions specify which one).

Password Change Method	Passwords Synchronized
NetWare Administrator (run on a workstation with a client prior to version 4.9) to any user object in any container	NDS password only.
NetWare Administrator (run on a workstation with the version 4.9 client) to a User object in a container that has a R/W replica on a NetWare 6.5 server (or NetWare 5.1or 6 running eDirectory 87.1)	(Untested and unsupported) Universal, simple, and NDS passwords are changed. All are synchronized even if old ones were out of sync.
ConsoleOne (run on a workstation with a client prior to version 4.9) to any User object in any container	There is a separate change password page for NDS password and simple password.
ConsoleOne (run on a workstation with the version 4.9 client) to a User object in a container that has a R/W replica on a NetWare 6.5 server (or NetWare 5.1 or 6 running eDirectory 87.1)	Universal, simple and NDS passwords are changed. All are synchronized even if old ones were out of sync.
ConsoleOne (run on a workstation with the version 4.9 client) to a User object in a container that has no R/W replicas on any NetWare 6.5 servers, or NetWare 5.1 or 6 with eDirectory 87.1 (only R/W replicas on NetWare 5.1 or NetWare 6 servers with eDirectory versions older than 87.1)	There is a separate change password page for NDS password and simple password.
Novell iManager 1.5 (NetWare 5.1 or NetWare 6 only) to any user object in any container	NDS password only.
Novell iManager 2.0 (NetWare 6.5 only) to a User object in a container that has a R/W replica on a NetWare 6.5 server (or NetWare 5.1 or 6 running eDirectory 87.1)	Universal, simple and NDS passwords are changed. All are synchronized even if old ones were out of sync.
Novell iManager 2.0 (NetWare 6.5 only) to a User object in a container that does not have any R/W replica on any NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 87.1	NDS password only.
NetWare Remote Manager running on a NetWare 6.5 server to a User object in a container that has a R/W replica on a NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 87.1	Universal, simple, and NDS passwords are changed. All are synchronized, even if old ones were out of sync.
NetWare Remote Manager running on a NetWare 6.5 server to a User object in a container that does not have a R/W replica on a NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 87.1	NDS password only.
NetWare Remote Manager NDS change password running on a NetWare 5.1 or NetWare 6 server	NDS password only.
NetWare Remote Manager simple password management (NetWare 5.1 and 6 only with Native File Access installed)	Simple password only.

Password Management

You can use the following methods to administer Universal Password:

- iManager: Administering passwords by using Novell iManager automatically sets the Universal Password to be synchronized to simple and NDS password values for backwards compatibility. The NMAS task in iManager does allow for granular management of individual passwords and authentication methods that are installed and configured in the system.
- ConsoleOne: The NDS password tab in ConsoleOne run on a NetWare 6.5 server, or on a Windows workstation with the Novell Client for Windows NT/2000/XP version 4.9 or the Novell Client for Windows 95/98 version 3.4 installed automatically sets the Universal Password and synchronizes for backwards compatibility.
- NWAdmin32: The same results should be seen when using NWAdmin32 as with ConsoleOne, although Novell does not plan to test this case.
- LDAP: Changing passwords via LDAP on a NetWare 6.5 server also sets the Universal Password and synchronizes the others for backwards compatibility.
- Third-party Applications: Third-party applications that are written to Novell's Cross Platform Libraries and that perform password management will also set the Universal Password and synchronize the others if the newer libraries are installed on the Novell Client for Windows NT/2000/XP version 4.9 or the Novell Client for Windows 95/98 version 3.4 workstation or NetWare 6.5 server.

NOTE: If you are using the Password Management plug-in, you can use password policies to specify how Universal Password is synchronized with NDS, Simple, and Distribution Passwords. In addition, an iManager task is provided that lets an Administrator set a user’s Universal Password.

Issues to Watch For

- In a mixed environment of Novell Client software prior to the Novell Client for Windows NT/2000/XP version 4.9 or the Novell Client for Windows 95/98 version 3.4 (including Native File Access servers on NetWare 5.1 and NetWare 6), if passwords are changed from those older systems, only the older values will be changed, driving the NDS and/or the simple password out of synchronization with the Universal password. This might be an issue only for users who log in to their account from both older Novell Client workstations (prior to Client for Windows NT/2000/XP version 4.9 or Novell Client for Windows 95/98 v3.4) and from newer Novell Client workstations (Novell Client for Windows NT/2000/XP version 4.9 or Novell Client for Windows 95/98 version 3.4). If so, the problem will only occur if users are either using international characters in passwords or if they change the password from the older workstation.
- When you disable a user's NDS password, the NDS password is set to an arbitrary value that is unknown to the user. The following describes how some login methods handle this change.
    - The Simple Password method is not disabled if the NDS password is disabled. The Simple Password method uses the Universal Password if it is enabled and available. Otherwise, it uses the simple password. If Universal Password is enabled but not set, then the Simple Password method sets the Universal Password with the simple password.
    - The Enhanced Password method is not disabled when the NDS password is disabled. The enhanced password does not use the Universal Password for login. However, it can be configured to set the Universal Password, if the Universal Password is enabled, when the user changes the enhanced password.

    - The NDS Password method is not disabled when the NDS password is disabled. The NDS Password method will use the Universal Password if it is enabled and available. Otherwise, it will use the NDS password. If the Universal Password is enabled but not set, then the NDS Password method will set the Universal Password with the NDS password.

- A security enhancement was added to NMAS 2.3.4 regarding Universal Passwords changed by an administrator. It works basically the same way as the feature previously provided for NDS Password. If an administrator changes a user's password, such as when creating a new user or in response to a help desk call, for security the password is automatically expired if you have enabled the setting to expire passwords in the Password Policy. The setting in the Password Policy is in Advanced Password Rules, named "Number of days before password expires (0-365)." For this particular feature, the number of days is not important, but the setting must be enabled.

- After Implementing Universal Passwords, Some Applications Fail to Load

  After implementing UP, NDPS, ZEN, NILE (SSL connections), and SLPDA may not work. This is an application problem; the auto-generated passwords created by these applications violate password policies.

  The workaround is described in TID 10092957, and a patch will soon be available.

- NDS Password Settings Are Replaced by New Password Policies

  If you create a Password Policy (currently only possible using Identity Manager 2) and enable Universal Password, the Advanced Password Rules are enforced instead of any existing password settings for NDS Password. The legacy password settings are ignored. No merging or copying of previous settings is done automatically when you create Password Policies.

  For example, if you had a setting for the number of grace logins that you were using with the NDS Password, when you enable Universal Password you need to re-create the grace logins setting in the Advanced Password Rules in the Password Policy.

7 Troubleshooting

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

Installation Issues

1. The NMAS Server Install deletes the files securityservices.jar and securityservicesres.jar within the respective ConsoleOne® lib\security and resources\security directories.
2. If you are upgrading your Certificate Server from a version prior to 2.0 as part of your installation of NMAS, you will need to re-export any trusted root certificates you will use with the Advanced x.509 method.
3. When installing NMAS server to Windows NT or 2000, a dialog box might pop up informing you that it is necessary for NMAS to shut down eDirectory. After you click OK in this dialog box, the installation might fail.

   If this happens, restart the NMAS server installation. When the dialog box appears again, you need to manually shut down eDirectory. Do this by going into Control Panel and clicking eDirectory. Select the ds.dlm file (Novell Directory Services) and click Stop. After the directory services have been stopped, you can return to the dialog box, click OK, and the installation will continue properly.
4. We strongly recommended that you upgrade all previous versions of NMAS to this version on all servers.
5. 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.
6. If you install Client32™ after you have installed the NMAS client, the NMAS tab will not appear on the Client32 login screen.
7. If the target server goes down during the NMAS Server Installation, or if there are network communication problems sufficient to cause the install to fail, it is possible that one of the installation programs, launch.exe, is still loaded, and needs to be unloaded manually.

   Symptom: When you launch the install again, the NMAS Server Components check box is dimmed and not selectable.

   Solution: Kill the launch.exe process by pressing Ctrl+Alt+Delete and selecting Task List. On the Processes tab, select launch.exe, then click End Process.
8. You must have the NICI Client installed on each client workstation that will run ConsoleOne and NMAS software.
9. If you do not restart the server after installing NMAS and you try to reset passwords, you will receive an error message.

Login Method and Sequence Issues

1. The NMAS client's install option for disconnected operations is not recommended and supports only the NDS® Password method.
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. You must have grace logins set to at least two. If it is set to one, the login will not work.
4. With ConsoleOne installed on a NetWare® server, when you install Login Methods under some configurations you might see a Failed status in the ConsoleOne Snap-ins field of the Login Method Installation Summary screen. If this occurs, the new snap-ins for that method did not install properly and you need to run snapininstall.exe in the \ConsoleOne directory or the NMAS software image.

   NOTE: snapininstall.exe installs only the snap-ins for NMAS Management, EnhancedPassword, SimplePassword, and WorkstationAccess.
5. If a login method's 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.
6. Snap-ins for managing the Enhanced Password login method can be installed into ConsoleOne by executing \nmas\consoleone\snapininstall.exe.
7. Two password methods, such as Simple and Enhanced, cannot be used in an AND sequence if the Novell Client™ is set to display the password field, which it is by default.
8. 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 simple 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.

Compatibility Issues

1. If the Single Sign-on 2.1 is installed on the client, the password field for the initial login screen is enabled. The user can remove the password field from the initial login screen by using the following steps:
   a. Select Novell Client Properties from the red N in the taskbar.
   b. Click the Location Profiles tab.
   c. Select the desired Location Profile.
   d. Click Properties.
   e. Click the NMAS tab.
   f. Uncheck Display Password Field by Default.
   g. Click OK three times.
2. The following instructions describe how to enable the version of Single Sign-on that ships with NMAS.
   a. Open Novell Client Properties by right-clicking the red N located in the taskbar.
   b. Click the Single Sign-on tab.

c. Check the Enable Single Sign-on box.

d. Click the Advanced Login tab.

e. Uncheck the Suppress Single Sign-on for This Login box.

f. Click OK.

Administration Issues

1. 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.
2. Updating ConsoleOne from 1.2d to 1.3.6 does not update the products.dat file on the NetWare server.
3. NMAS does not support AIX 4.3.3.
4. The simple password is used for various authentication services in NetWare 6.5. 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.
5. 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.
6. When a user logs in to a tree other than the preferred tree using the client, the client incorrectly queries the preferred tree to find the User object. If a user object with the same name exists in the preferred tree, the client uses that User object, which results in the login failing with a -601 error (No Such Object). This is because the wrong tree was used. This issue will be resolved in the next release of the client.

A eDirectory Considerations with NMAS

You need to make certain Novell® eDirectory™ considerations when configuring and managing NMAS™. This section describes some of these situations.

- "Setting Up a Security Container As a Separate Partition" on page 59
- "Merging Trees with Multiple Security Containers" on page 59

Setting Up a Security Container As a Separate Partition

NMAS relies on storage of policies that are global to the eDirectory tree. The eDirectory tree is effectively the security domain. The security policies must be available to all servers in the tree.

NMAS places the authentication policies and login method configuration data in the Security container that is created off of the [Root] in NetWare® 5.1 or later eDirectory trees. This information must be readily accessible to all servers that are enabled for NMAS. The purpose of the Security container is to hold global policies that relate to security properties such as login, authentication, and key management.

With NMAS, we recommend that you create the Security container as a separate partition, and that the container be widely replicated. This partition should be replicated as a Read/Write partition only on those servers in your tree that are highly trusted.

NOTE: Because the Security container contains global policies, be careful where writable replicas are placed, because these 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 must be on the NMAS server.

Merging Trees with Multiple Security Containers

Special considerations need to be made when merging eDirectory trees where a Security container has been installed in one or both of the trees. Make sure that this is something you really want to do—this procedure has the potential to be a very time-consuming and laborious task.

IMPORTANT: These instructions are complete for trees with Novell Certificate Server™ 2.21 and earlier, Novell Single Sign-on 2.*x*, and NMAS 2.*x*.

1. In ConsoleOne®, identify the trees that will be merged.
2. Identify which tree will be the source tree and which tree will be the target tree.

   Keep in mind these security considerations for the source and target trees:

   - Any certificates signed by the source tree's Organizational CA must be deleted.
   - The source tree's Organizational CA must be deleted.
   - All user secrets stored in Novell SecretStore® on the source tree must be deleted.
   - All NMAS login methods in the source tree must be deleted and reinstalled in the target tree.

- All NMAS users that were in the source tree must be re-enrolled when the trees are merged.
- All users and servers that were in the source tree must have new certificates created for them when the trees are merged.
- All users that were in the source tree must have their secrets reinstalled into their SecretStore.

If neither the source tree nor the target tree has a container named Security under the [Root] of the tree, or if only one of the trees has the Security container, no further action is required. Otherwise, continue with the remaining procedures in this section.

Product-Specific Operations to Perform Prior to Tree Merge

- "Novell Certificate Server" on page 60
- "Novell Single Sign-on" on page 61
- "NMAS" on page 61
- "Novell Security Domain Infrastructure" on page 62
- "Other Security-Specific Operations" on page 62

Novell Certificate Server

If Novell Certificate Server (previously known as Public Key Infrastructure Services, or PKIS) has been installed on any server in the source tree, you should complete the following steps.

NOTE: Depending on how the product was used, the objects and items referred to might or might not be present. If the objects and items referred to in a given step are not present in the source tree, you can skip the step.

1 Any Trusted Root certificates in the source tree should be installed in the target tree.

Trusted Root certificates are stored in Trusted Root objects, which are contained by Trusted Root containers. Trusted Root containers can be created anywhere within the tree; however, only the Trusted Root certificates that are in the Trusted Root containers within the Security container must be moved manually from the source tree to the target tree.

2 Install the Trusted Root certificates in the target tree.

2a Pick a Trusted Root container in the Security container in the source tree.

2b Create a Trusted Root container in the Security container of the target tree with the exact name used in the source tree (Step 2a).

2c In the source tree, open a Trusted Root object in the selected Trusted Root container and export the certificate.

IMPORTANT: Remember the location and filename you choose; you will use them in the next step.

2d In the target tree, create a Trusted Root object in the container that you created in Step 2b. Specify the same name as the source tree and, when prompted for the certificate, specify the file that you created in Step 2c.

2e Delete the Trusted Root object in the source tree.

2f Repeat Step 2c through Step 2e until all Trusted Root objects in the selected Trust Root container have been installed into the target tree.

2g Delete the Trusted Root container in the source tree.

2h Continue Step 2a through Step 2f until all Trusted Root containers have been deleted in the source tree.

3 Delete the Organizational CA in the source tree.

The Organizational CA object is in the Security container.

IMPORTANT: Any certificates signed by the Organizational CA of the source tree will become unusable following this step. This includes server certificates and user certificates that have been signed by the Organizational CA of the source tree.

4 Delete every Key Material object (KMO) in the source tree that has a certificate signed by the Organizational CA of the source tree.

Key Material objects in the source tree with certificates signed by other CAs will continue to be valid and do not need to be deleted.

TIP: If you are uncertain about the identity of the signing CA for any Key Material object, look at the Trusted Root Certificate section of the Certificates tab in the Key Material object property page.

5 Delete all user certificates in the source tree that have been signed by the Organizational CA of the source tree.

NOTE: If users in the source tree have already exported their certificates and private keys, those exported certificates and keys will continue to be usable. Private keys and certificates that are still in eDirectory will no longer be usable after you perform Step 3.

For each user with certificates, open the properties of the User object. Under the Certificates section of the Security tab, a table lists all the certificates for the user. All of those certificates with the Organizational CA as the issuer must be deleted.

NOTE: User certificates will be present in the source tree only if Novell Certificate Server 2.0 or later has been installed on the server that hosts the Organizational CA in the source tree.

Novell Single Sign-on

If Novell Single Sign-on has been installed on any server in the source tree, you should delete all Novell Single Sign-on secrets for users in the source tree.

For every user using Novell Single Sign-on in the source tree, open the properties of the User object. All of the user’s secrets will be listed under the SecretStore section of the Security tab. Delete all listed secrets.

NOTE: Depending on how the product was used, the objects and items referred to might or might not be present. If the objects and items referred to are not present in the source tree, you can skip this step.

NMAS

If NMAS has been installed on any server in the source tree, you should complete the following steps.

NOTE: Depending on how the product was used, the objects and items referred to might or might not be present. If the objects and items referred to are not present in the source tree, you can skip the step.

1 In the target tree, install any NMAS login methods that were in the source tree but not in the target tree.

TIP: To ensure that all of the necessary client and server login components are properly installed in the target tree, we recommend that you install all new login methods using original Novell or vendor-supplied sources.

Although methods *can* be reinstalled from existing server files, establishing a clean installation from Novell or vendor-supplied packages is typically simpler and more reliable.

2 To ensure that the previously established login sequences in the source tree are available in the target tree, migrate the desired login sequences.

2a In ConsoleOne, select the Security container in the source tree.

2b Right-click the Login Policy object > select Properties.

2c For each login sequence listed in the Defined Login Sequences drop-down list, note the Login Methods used (listed in the right pane).

2d Select the Security container in the target tree and replicate the login sequences using the same login methods note in Step 2c.

2e Click OK when you are finished.

3 Delete NMAS login security attributes in the source tree.

3a In the Security container of the source tree, delete the Login Policy object.

3b In the Authorized Login Methods container of the source tree, delete all login methods.

3c Delete the Authorized Login Methods container in the source tree.

3d In the Authorized Post-Login Methods container of the source tree, delete all login methods.

3e Delete the Authorized Post-Login Methods container in the source tree.

Novell Security Domain Infrastructure

If Novell Certificate Server 2.x or later, Novell Single Sign-on, NMAS, NetWare 5.1 or later, or eDirectory eDirectory 8.5 or later has been installed on any server in the source tree, the Novell Security Domain Infrastructure (SDI) will be installed. If SDI has been installed, you should complete the following steps.

NOTE: Depending on how the product was used, the objects and items referred to might or might not be present. If the objects and items referred to are not present in the source tree, you can skip the step.

1 Delete the W0 object and the KAP container in the source tree.

The KAP container is in the Security container. The W0 object is in the KAP container.

2 On all servers in the source tree, delete the Security Domain Infrastructure (SDI) keys by deleting the sys:\system\nici\nicisdi.key file.

IMPORTANT: Make sure that you delete this file on *all* servers in the source tree.

Other Security-Specific Operations

If a Security container exists in the source tree, delete the Security container before you merge the trees.

Performing the Tree Merge

eDirectory trees are merged using the DSMERGE utility. For more information, refer to the DSMERGE documentation (http://www.novell.com/documentation/lg/nds73/index.html?maintenu/data/hqcrag0y.html).

Product-Specific Operations to Perform after the Tree Merge

Novell Security Domain Infrastructure

If the W0 object existed in the target tree before the merge, the Security Domain Infrastructure (SDI) keys used by the servers that formerly resided in the target tree must be installed in the servers that formerly resided in the source tree.

The easiest way to accomplish this is to install Novell Certificate Server 2.0 or later on all servers formerly in the source tree that held SDI keys (the sys:\system\nici\nicisdi.key file). This should be done even if the Novell Certificate Server has already been installed on the server.

If the W0 object did not exist in the target tree before the merge but did exist in the source tree, the SDI must be reinstalled in the resulting tree.

The easiest way to accomplish this is to install Novell Certificate Server 2.0 or later on the servers in the resulting tree. Novell Certificate Server must be installed on the servers formerly in the source tree that held SDI keys (the sys:\system\nici\nicisdi.key file). It can also be installed on other servers in the resulting tree.

Novell Certificate Server

If you are using Novell Certificate Server: After the tree merge, reissue certificates for servers and users that were formerly in the source tree, as necessary.

NOTE: We recommend that you install Novell Certificate Server 2.0 or later on all servers that hold a replica of the partition containing a User object.

In order to issue a certificate for a server, Novell Certificate Server 2.0 or later must be installed.

Novell Certificate Server 2.0 or later must be installed on the server that hosts the Organizational CA.

Novell Single Sign-on

If you are using Novell Single Sign-on: After the tree merge, re-create SecretStore secrets for users that were formerly in the source tree, as necessary.

NMAS

If you are using NMAS: After the tree merge, re-enroll NMAS users that were formerly in the source tree, as necessary.