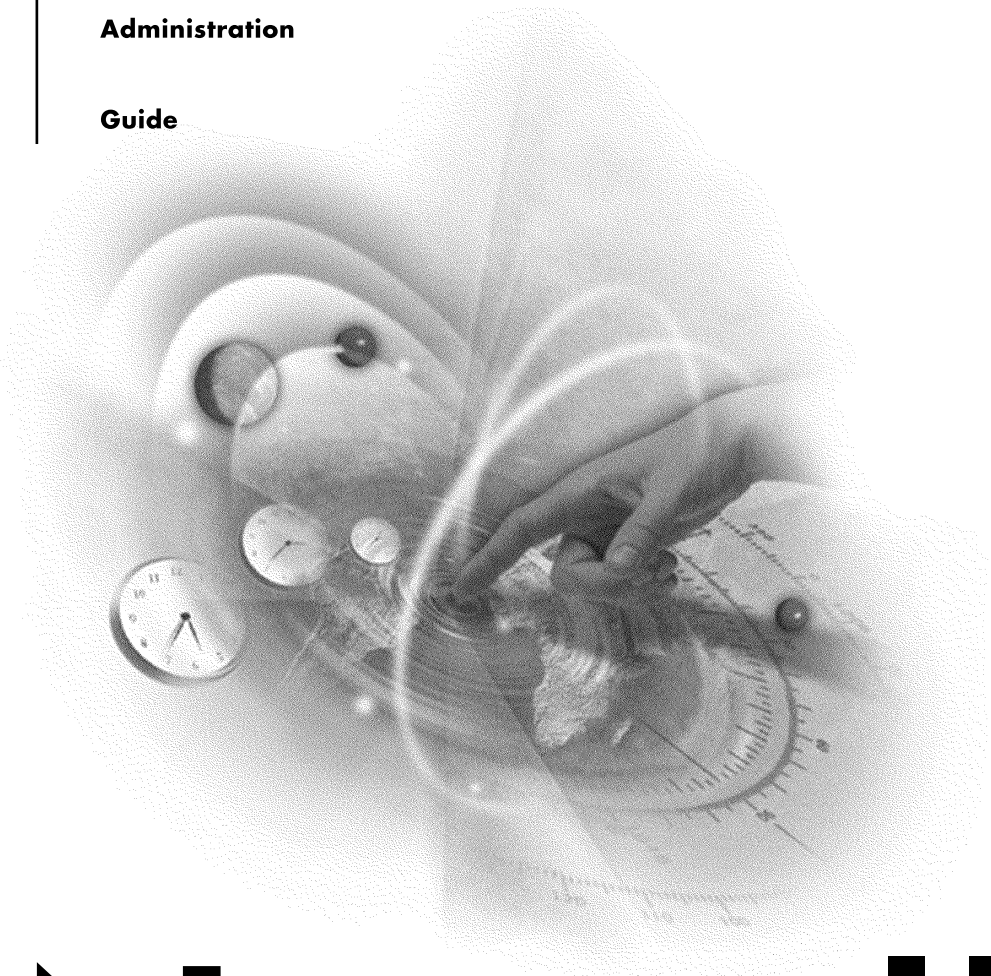
VERSION 1.0

Novell Modular Authentication Service

Installation and Administration Guide



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.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

U.S. Patent Nos. 5,818,936; 5,933,503. Patents Pending.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

100-004525-001 A
January 2000
100-004525-001 A

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

Novell Trademarks

ConsoleOne is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Client is a trademark of Novell, Inc.

Novell Directory Services and NDS are registered trademarks of Novell, Inc., in the United States and other countries.

Third-Party Trademarks

RSA and the RSA encryption engine logo are trademarks of RSA Security Inc.

All other third-party trademarks are the property of their respective owners.

Contents

Preface

Novell® Modular Authentication Service (NMAS) software provides additional login methods for users to authenticate to NDS®. These new login methods provide increased security in accessing network resources. NMAS must be installed on both a NetWare 5 server and on the Novell client workstation. Once NMAS in installed, the new login methods are installed and managed using ConsoleOne™.

This guide provides an overview of the NMAS technology and software. It also includes instructions on how to install, configure, and manage NMAS.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with the NMAS product.

To contact us, send e-mail to webdoc@novell.com, or send comments to:

Novell, Inc.
Product Documentation
MS PRV-C-231
122 East 1700 South
Provo, UT 84606-6194 USA
Fax (801) 861-3002

1 NMAS Overview

This section provides an overview of Novell® Modular Authentication Service (NMAS) functionality and describes the different features of the NMAS Starter Pack and the NMAS Enterprise Edition.

Two NMAS Products

As Novell continues to enhance and expand the services and functionality of Novell Directory Services® (NDS®), the methods for authenticating to NDS are also being enhanced and expanded. NMAS offers two different products that allow users to authenticate to NDS through additional login methods. The two products are NMAS Starter Pack and NMAS Enterprise Edition.

NMAS Starter Pack includes:

- NMAS client and server software
- Login methods software
- Support for one login method per login sequence
- ConsoleOne™ management utility snap-in

NMAS Enterprise Edition includes:

- NMAS client and server software
- Login methods software
- Support for multiple login methods per login sequence
- Support for graded authentication
- ConsoleOne managment utility snap-in

NMAS Server and Client Software

NMAS software is installed on a NetWare® 5 server and on Windows* client workstations. Two separate installation programs are used. The programs are located in their specific folders within the NMAS product.

The NMAS server software is installed from a Windows client workstation. You must have Admin rights to the [Root] of the NDS tree 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.

Login Methods

NMAS offers additional ways to securely authenticate to NDS. These new authentication modules are called login methods. In addition to the standard password-challenge-response authentication offered with NDS, NMAS provides login methods via:

- "Something you know" (password authentication)
- "Something you have" (physical device authentication)
- "Something you are" (biometric authentication)

NMAS-supported login methods include both authentication modules developed by Novell as well as by third parties. A summary of each of these login methods follows.

Password Authentication

Passwords ("something you know") are important authentication methods to networks. NMAS provides the standard NDS password login method as well as login methods common with LDAP, Internet browsers, and other directories. These include cleartext, SHA-1, and MD-5 login methods.

Standard NDS Password Authentication

Standard NDS password authentication uses a very secure password challenge response authentication method. Because of the increased security it offers, the standard NDS password authentication is slower than cleartext or SHA-1/MD5 authentication.

Cleartext

Cleartext (or plaintext) authentication is a process of sending a password over the wire in an unencrypted form. Aside from no authentication at all, from a security standpoint, this is the lowest form of user authentication. Because there is no encryption process, plaintext 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

Developed and published by the National Institute of Standards and Technology (NIST) in 1993 and 1995, the secure hash algorithm (SHA-1) is a popular method of network authentication based on a hash algorithm. 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 cleartext 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

Developed by Ron Rivest at MIT, this message-digest algorithm takes a message of arbitrary length and produces a 128-bit message digest (or hash) output. MD-5 was, at one time, the most widely used secure hash algorithm.

Physical Device Authentication

Another way that users can authenticate to the network is through a physical object that proves their identity (“something you have”). Third-party authentication developers have written authentication modules for NMAS for two types of physical devices: smart cards and tokens.

Smart Cards

A smart card is a plastic card, about the size of a credit card, that includes an embedded microchip that can store data and perform cryptographic functions. Depending on what is stored on the microchip, a smart card can be used for a variety of tasks.

With NMAS, a smart card can be used to establish an identity when authenticating to NDS. For example, the ActivCard Gold smart card lets users prove their identity by using their private key and an associated X.509 v3 user certificate that is stored on the smart card.

You can use Novell Certificate Server 2.0 to issue X.509 v3 user certificates for NDS authentication. The product is available for download at www.novell.com (http://www.novell.com).

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 the challenge-response 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. If they don’t match, access is denied.

VASCO Data Security provides a module for NDS authentication using its Digipass token.

Time-Synchronous Authentication

RSA* Security Inc. uses 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, it grants the user access to the network.

RSA Security Inc. provides a module for NDS authentication using its SecurID token along with its ACE/Server authentication server.

Biometric Authentication

Another authentication technique supported by NDS is 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, wherever the data is to be analyzed, 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 using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Identicator, a division of Identix, provides a module for NDS authentication using its BioLogon 2.0 fingerprint authentication software.

SAFLINK Corporation provides three modules for NDS authentication using licensed biometric authentication technology for facial, fingerprint, and voice authentication.

Biometric authentication can be classified into two groups: static biometric authentication and dynamic biometric authentication.

Static Biometric Authentication

Static biometric authentication 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

Dynamic biometric authentication captures and verifies behavioral characteristics of an individual. Common dynamic biometric characteristics include voice or handwriting.

Login Method Installation

All NMAS login methods are installed using the ConsoleOne utility. To install login methods, see “Managing NMAS” on page 27.

Login Sequences

Login methods are assigned to users via a login sequence. A login sequence is an ordered set of one or more login methods. Users log in to the network using these defined login sequences. If the login sequence contains more than one login method, the methods are presented to the user in the order specified.

A login sequence has a sequence grade, which is the composite of all authentication grades of the methods in the sequence. For example, if a login sequence contains a password login method and a biometric login method, the login sequence would have a sequence grade of “Biometric & Password.”

IMPORTANT: In the NMAS Starter Pack, only one login method is allowed per login sequence. In the NMAS Enterprise Edition, users can have multiple login methods per login sequence.

Login sequences are managed through ConsoleOne. They are stored in the Login Policy object in the Security container. A sequence includes the methods and the order in which those methods execute during user authentication. To set up login sequences, see “Managing NMAS” on page 27.

Managing Authentication Sequences

Suppose your organization implements a login policy that requires users to log in using “something they are” and “something they know.” As the administrator, you decide to require each user to authenticate using the Identicator BioLogon method, along with a SHA-1 password method. You would first decide the sequence of login prompts (Identicator prompt first followed by SHA-1 password or vice versa) and then create the sequence in the Login Sequences property page.

NMAS lets you easily chain both Novell and third-party login methods as part of a login sequence. No collaborative engineering work between different companies is needed; NMAS does the collaboration. This makes it possible to create a sequence using, for example, the Identicator fingerprint reader, a Vasco token, and a standard NDS password.

Graded Authentication

IMPORTANT: Graded authentication is only available in the NMAS Enterprise Edition product.

The graded authentication feature of NMAS Enterprise Edition allows you to "grade," or control, users' authentication access based on their login method. This means that you can set access rights to NDS partitions or volumes based on how users log in and even from where they authenticate.

Graded authentication is based on the relationship between a user and an object, where an object is a network volume or partition. Graded authentication uses the following factors or characteristics to establish the user-object relationship and to determine the grade or level of authentication:

- Password—"something you know." It can also be a personal information number (PIN).
- Token—"something you hold." It can be a smart card or a certificate.
- Biometric—"something you are." It can be a thumbprint, retina scan, or some other human physical characteristic form of identification.

Each of these factors is a login method that can be used to authenticate to the network. With NMAS, you can also combine methods to create a multiple-factor authentication. Based on the login method used, the results can then be used to control access to the network.

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 like that contained in personnel files.
- Engineering handles restricted or confidential information like that contained in 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 may 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.

In the NetWare environment, NMAS replaces the physical key given to users with a clearance, which is also a security label that indicates what key is needed for access. NMAS also replaces the filing cabinet with NDS file system volumes and NDS partitions that are also assigned security labels. These security labels identify the filing cabinet lock type.

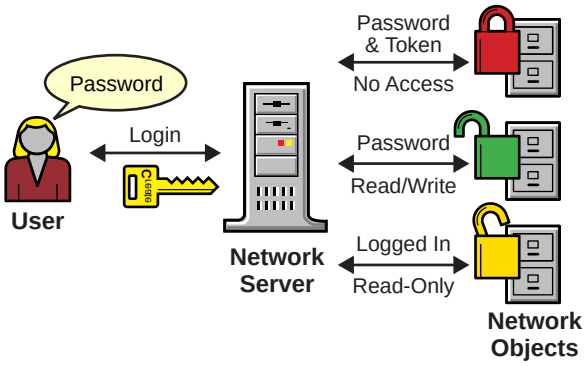
NOTE: The terminology used to specify the authentication level through the use of security labels is interchangeable. For example, for a user, biometric can be a security label, an authentication level, or a clearance (key). For a network volume or partition, biometric is a security label (lock).

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 security label that identifies the key that will be 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, typically only one clearance is used at login, and it is this clearance that determines what information can be unlocked. For example, a user logging in with an authentication grade of password would be using a single-factor authentication. This would allow the following:

- Read/Write access to other network areas labeled password
- No access to areas labeled password and token, since these levels are graded higher than password
- Read-Only access to any levels graded lower than password

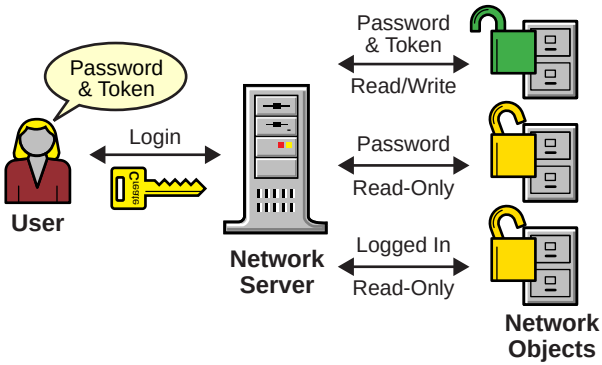
Figure 1 Single-Factor Authentication



A user logging in with a password and token would be using a multiple-factor authentication. This would allow the following:

- Read/Write access to other network areas labeled password and token
- Read-Only access to areas labeled password, since the password grade is lower than password and token
- Read-Only access to any levels graded lower than password and token

Figure 2 Multiple-Factor Authentication



While it may appear that a higher level of authentication automatically allows full access to all lower levels of authentication, this is not the case. Graded authentication allows Read/Write access at the same level, but Read-Only access at lower levels.

The purpose of this restriction is to prevent the unauthorized copying of information from higher levels of authentication to lower levels of authentication.

Graded Authentication Example

A user working in Human Resources with information classified as sensitive logs in with a password and token. The information that the user needs is on a network volume that is also labeled password and token. Since the user's login level and the volume label match, the user is able to read and write to and from the network volume.

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

The following table shows several departments within a company and how each department may classify its information. Security labels and authorization levels are assigned based on the information classification.

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

Since Sales has been assigned a Public information classification and since Sales information is freely accessible, a user only needs to be logged in to access Sales information.

However, users who work in Engineering need to use the standard NDS 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.

Summary of Rules, Authentication Levels, and Security Labels

The following rules apply to graded authentication in NMAS:

- Multiple-factor authentication is graded higher than single-factor authentication.
- If the session clearance is the same as the assigned security label, then access is read and write.
- If the session clearance is higher than the assigned security label, then access is read-only.

  For example, if a user has a session clearance of Password and Token and wants to access a 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 network volume assigned a Password or a Token security label.

  NOTE: Remember that 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 login authentication level.
- If the session clearance is lower than the assigned security label, then no access is allowed.

A special clearance called Multilevel Administration provides read and write access to all security labels simultaneously. This clearance should be reserved for network administrators. The Multilevel Administration clearance has the master key that has Read/Write access to all cabinets. This user is trusted to not make unauthorized copies from higher to lower.

The following table shows the session clearance and security labels currently employed by NMAS.

Session Clearance/Security Labels	Authentication and Access Requirements
Biometric & Password & Token	Authentication and access requires a physical attribute, a password, and a token.
Biometric & Password	Authentication and access requires a physical attribute and a password.
Biometric & Token	Authentication and access requires a physical attribute and a token.
Password & Token	Authentication and access requires a password and a token.
Biometric	Authentication and access requires a physical attribute.
Password	Authentication and access requires a password.
Token	Authentication and access requires a physical attribute and a password.
Logged In	A login defined by the network administrator that provides network access without using any NMAS methods.
Multilevel Administration	Authentication allows read and write access to all security labels simultaneously.

The following figure summarizes the relationships between the authentication level/security label and the read/write permissions.

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

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

ConsoleOne Management

NMAS is managed through a ConsoleOne snap-in module. ConsoleOne is the Java* authored, GUI-based framework for managing NDS. Specific ConsoleOne property pages let you manage login methods, the login sequence of the login methods, and the security grade (graded authentication) associated with the methods.

During the installation of the snap-in module, NMAS extends the NDS schema and creates new objects in the Security container in the NDS tree. These new objects are the Authorized Login Methods container and Login Policy objects. All login methods are stored and managed in the Authorized 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.

IMPORTANT: Run ConsoleOne locally on a client workstation to administer NMAS.

2 Installing NMAS Starter Pack

This section provides information on how to install the Novell® Modular Authentication Service (NMAS) Starter Pack software.

Installation Overview

The NMAS installation adds a set of containers, objects, and attributes to the NDS® tree to support NMAS. NMAS software is installed on a NetWare® 5 server and on Windows* client workstations. Two separate installation programs are used. The programs are located in their specific folders within the NMAS product.

The NMAS server software is installed from a Windows client workstation. You must have Admin rights to the [Root] of the NDS tree to install the NMAS server product.

The NMAS client software must be installed on each client workstation on which you want to use the NMAS login methods.

Installing NMAS Server Software

Before you begin the installation, make sure that your NetWare 5 environment meets all of the listed prerequisites. There are multiple files to download and install before you can install the NMAS Starter Pack software.

NetWare 5.*x* Server Prerequisites

IMPORTANT: NMAS will not operate in NetWare networks running NetWare versions earlier than 4.10.

- ❑ Make sure you have administrative rights to [Root] on the NetWare 5 server where NMAS will be installed.
- ❑ If you are using NetWare 5.0, download (http://support.novell.com/cgi-bin/search/tidfinder.cgi?2953759) and install NetWare 5 Support Pack 3.
- ❑ Download (http://webapps.novell.com/cgi-bin/custom/corp/esd/vrtlbox.pl?NOVELL_PID=87000377.01d) and install NDS eDirectory Upgrade on NetWare.
- ❑ Download (http://www.novell.com/corp/security/) and install the server software of Novell International Cryptographic Infrastructure (NICI) version 1.5.1.
- ❑ Download (http://webapps.novell.com/cgi-bin/custom/corp/esd/vrtlbox.pl?NOVELL_PID=87000386.01b) and install Novell Certificate Server 2.0.

Server Installation Instructions

1. If you haven't already done so, download (http://www.novell.com/corp/security/) and expand the NMAS Starter Pack software.
2. From the NMASSERVER directory, run INSTALL.EXE.
3. Follow the on-screen instructions.
4. Install and configure login methods and sequences as described in "Managing NMAS" on page 27.

Installing NMAS Client Software

Before you begin the installation, make sure that your Windows client workstations meet all of the listed prerequisites. There are additional files to download and install before you can install the NMAS Starter Pack software.

The NMAS client software must be installed on each client workstation on which you want to use the NMAS login methods.

Windows Client Workstation Prerequisites

- ❑ Make sure your workstation has a Pentium Pro 200 processor or equivalent and a minimum of 64 MB of RAM.
- ❑ Make sure your workstation is running Windows 95 Release B or later; Windows 98, or Windows NT* 4.0 with Service Pack 3 or later.
- ❑ Download (http://www.novell.com/download/#Clients - Network) and install the latest Novell Client™ for Windows software.
- ❑ Download (http://www.novell.com/corp/security/) and install the client software of Novell International Cryptographic Infrastructure (NICI) version 1.5.1.

Client Installation Instructions

1. If you haven't already done so, download (http://www.novell.com/corp/security/) and expand the NMAS Starter Pack software.
2. From the NMASCLIENT directory, run CLIENTSETUP.EXE.
3. Follow the on-screen instructions.

3 Managing NMAS

This section describes basic management functions for Novell® Modular Authentication Service (NMAS).

Once NMAS is installed, you need to install the desired login methods. You also need to create login sequences so users can authenticate to the network using the login methods. You should also configure NMAS and NDS® partitions.

If you are using the NMAS Enterprise Edition, you also might want to set up access controls and graded authentication.

Installing a Login Method

By default, the NDS password authentication method is installed. If you want to use additional login methods provided by Novell and other vendors, the methods need to be downloaded. You also might need additional hardware, depending on which login method you want to use. See the Novell Security Services (http://www.novell.com/corp/security/) Web site or the third-party vendor Web sites for more information.

When you have the necessary hardware and software, additional authentication methods can be installed using a wizard in ConsoleOne™.

IMPORTANT: Run ConsoleOne locally on a client workstation to administer NMAS.

1. In the Security container, select the Authorized Login Methods container.
2. Select the Create New Object option.
3. Follow the on-screen instructions.
4. Close and restart ConsoleOne.

Creating a Login Sequence

Once login methods are installed, you need to create login sequences in order for the methods to be used to authenticate to NDS. You view, add, modify, or delete login sequences using ConsoleOne.

In the NMAS Starter Pack, only one login method is allowed per login sequence. In the NMAS Enterprise Edition, you can set up multiple login methods per login sequence.

When multiple methods are selected for a sequence, they are executed in the order of selection, but they can be reordered if necessary. Once a login sequence is created, it becomes available when the user logs into the network.

IMPORTANT: Run ConsoleOne locally on a client workstation to administer NMAS.

Add a New Login Sequence

To add a new login sequence:

1. Open ConsoleOne.
2. Select the Security container.
3. Right-click the login policy container.
4. Select Properties.
5. Select New Sequence.
6. Enter a name for the new login sequence, then click OK to continue.

   All available methods will be listed under Available Methods.
7. Double-click each method you want to add to the sequence.

   Use the horizontal arrows to add a method. If you are using multiple methods, use the vertical arrows to change the execution order.
8. Click OK when you are finished.

Modify a Login Sequence

To modify a login sequence:

1. In the Security container, right-click the Login Policy container and selct Properties.
2. Select a login sequence from the Defined Login Sequences drop-down list (Alt+S). The Sequence Grade and Login Sequence for the selected method will display. All of the available login methods will display in the Available Methods list.
3. Choose your action:
   - To add or remove login methods from the sequence, use the left- and right-arrows. Since the NMAS Starter Pack only allows for one login method per login sequence, the right-arrow will be disabled if a login method is already selected.
   - To change the sequence order of the login methods, use the up- and down-arrows.
   - To add a new login sequence, click New Sequence, enter the sequence name, add the methods, and defien the login sequence order.
   - To delete a sequence, select the sequence from the Defined Login Sequences list and click Delete Sequence.
   - To exit without saving changes, click Cancel.

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

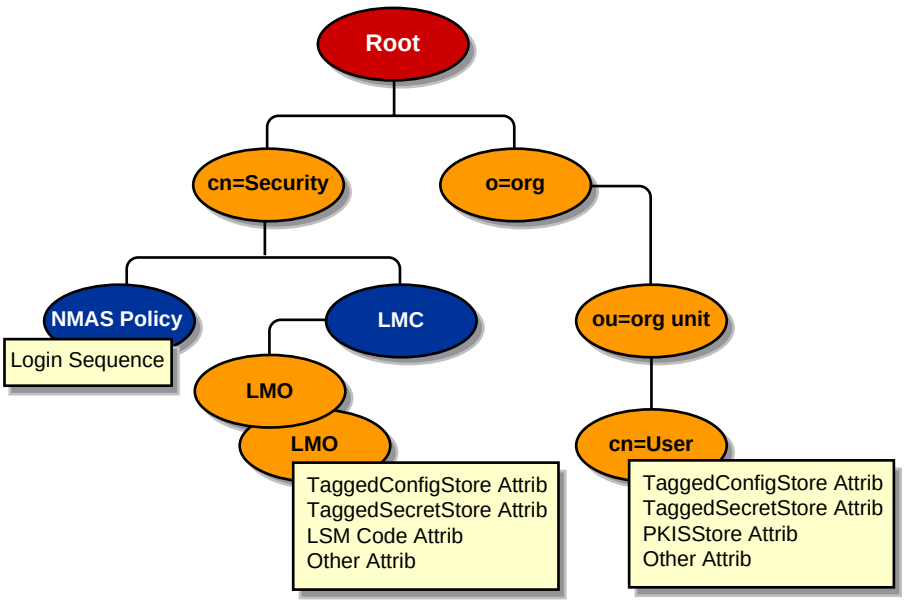
Configuring NMAS and NDS Partitions

NMAS relies on the storage of policies that are global to the NDS tree. The NDS 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 NDS 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, it is recommended that you create the security container as a separate partition, and that the container be widely replicated. This partition should only be replicated as a Read/Write partition on those servers that are highly trusted in your tree.

Figure 3 NMAS and NDS objects



NOTE: Since the security container will contain global policies, be careful where writable replicas are placed, as these servers can modify the overall security policies specified in the NDS tree. In order for users to log in with NMAS, replicas of the user objects must be on the NMAS server.

Setting Access Controls (Enterprise Edition Only)

Access controls are the grades or levels of authentication assigned to a user or a network object. A user can be assigned multiple authorized clearances, but only one grade can be assigned as the default clearance level.

Assigning multiple grades of authentication falls under the heading of authorized login levels. Whatever grade is assigned at login falls under the heading of the default login level.

Set the Authorized and Default Session Clearance

To set the authorized and default login levels for a user:

1. Open ConsoleOne.
2. Select an NDS tree and context.
3. Right-click the user that you want to set login levels for.
4. Select Properties.
5. Check the check boxes under Authorized Login Levels that you want for the user.
6. Select a default login level for the user from the Default Login Level drop-down list.
7. Click OK to finish.

Assign Security Labels

You can assign security labels to NDS partitions and NetWare volumes. A security label is a graded authentication level.

To assign a security label to a NDS partition:

1. Open ConsoleOne.
2. Right-click a partition.
3. Click Properties.

4. Select a security label from the Browse NDS Objects drop-down list.
5. Select a security label from the Read NDS Attributes drop-down list, then click OK to finish.

To assign a security label to a NetWare volume:

1. Open ConsoleOne.
2. Right-click a volume.
3. Click Properties.
4. Select a security label from the Security Label drop-down list.
5. Click OK to finish.

Using Multilevel Administration (Enterprise Edition Only)

Multilevel administration is generally reserved for network administrators or those users who require multiple levels of security access simultaneously.

To assign multiple security levels simultaneously to a user:

1. Open ConsoleOne.
2. Right-click a user from a selected NDS tree.
3. Click Properties.
4. Check the Multilevel Administration check box, then click OK to finish.