Novell Modular Authentication Service

2.02

www.novell.com

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.

Novell Modular Authentication Service (NMAS) software includes support for a number of login methods from third-party authentication developers. Refer to the PARTNERS.PDF file in the NMAS software 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.

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 No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,859; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,850,565; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,878,434; 5,884,304; 5,893,116; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,950,198; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,771; 5,991,810; 6,002,398; 6,014,667; 6,015,132; 6,016,499; 6,029,247; 6,047,289; 6,052,724; 6,061,743; 6,065,017; 6,094,672; 6,098,090; 6,105,062; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,192,365; 6,216,123; 6,219,652; 6,229,809. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell Modular Authentication Service Administration Guide
October 2001
103-000119-001

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.
NDS is a trademark of Novell, Inc.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
NMAS is a trademark of Novell, Inc.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Novell Certificate Server is a trademark of Novell, Inc.
Novell Client is a trademark of Novell, Inc.
Novell Directory Services is a trademark of Novell, Inc.
Novell, Yes, Tested & Approved is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

Preface

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

Documentation Conventions

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

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

1 NMAS Overview

This chapter provides an overview of Novell® Modular Authentication Service (NMAS™).

NMAS Functionality

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

NMAS is available in two different products: NMAS, which is the product that is bundled with other products, and NMAS Enterprise Edition, which is the product that is sold by itself.

This manual deals with NMAS Enterprise Edition and its functionality.

There are three key features of NMAS Enterprise Edition:

- Login factors
- Login methods and sequences
- Graded authentication

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.
- **Cleartext:** Cleartext (or plaintext) authentication sends the password over the wire in an unencrypted form. Aside from no authentication at all, this is the lowest form of user authentication from a security standpoint. 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:** 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 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:** 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 NDS.
- **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.
  - **X509 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 using an algorithm into 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.

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 NDS. For example, one post-login method is the Workstation Access method that 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 PARTNERS.PDF file on the NMAS CD-ROM for a list of authorized NMAS partners and a description of their methods.

Once 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 Enterprise Edition 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 NDS and file system access rights, which still need to be administered.

Graded authentication is managed from the Security Policy object in the Security container 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 Enterprise Edition 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 Enterprise Edition comes with eight security labels defined. The following table shows the pre-defined 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 NDS 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 which 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 Enterprise Edition 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 23.

NMAS Software

NMAS

NMAS is bundled with other Novell products, such as NetWare 6. It provides a limited set of NMAS functionality.

- Limited number of NMAS methods are available
- Single login method per login sequence
- No support for Graded Authentication
- No RADIUS

NMAS Enterprise Edition

NMAS Enterprise Edition is available for purchase on CD and includes the following:

- NMAS server and client software
- Login methods software

- Support for multiple login methods per login sequence
- Support for graded authentication
- ConsoleOne management utility snap-in
- RADIUS

Server and Client Software Installation

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

The NMAS server software is installed from a Windows client workstation. You must have Admin rights to the NDS 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 ConsoleOne snap-ins) are installed using the ConsoleOne utility. The client software is installed using a Windows installation program. Several currently supported login methods are available on the NMAS Enterprise Edition CD.

NMAS software includes support for a number of login methods from third-party authentication developers. Refer to the PARTNERS.PDF file in the NMAS software 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.

Novell encourages 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.

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 sequences, enrollment, and graded authentication.

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, 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.

Next Steps

- To install NMAS Enterprise Edition, see the file NMAS_INSTALL.PDF that ships with this CD or see the Quick Start in the NMAS product box.
- To set up login methods and sequences, see Chapter 2, "Setting Up Login and Post-Login Methods and Sequences," on page 17.
- To set up graded authentication, see Chapter 3, "Using Graded Authentication," on page 23.
- To log in using NMAS, see Chapter 4, "Logging In to the Network Using NMAS," on page 37.

2 Setting Up Login and Post-Login Methods and Sequences

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

Overview

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 Enterprise Edition includes several login methods on the product CD in the NMASMETHODS folder.

See the PARTNERS.PDF file in the NMAS software for a description of the login methods and specific installation instructions.

Installing a Login Method

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. Select New > Object.

   The New Object Wizard starts.

4. Select the SAS:NMAS Login Method class > click OK.

5. Specify the configuration file > click Next.

   The configuration file is located in the login method folder and is usually named CONFIG.TXT.

6. From the license agreement screen, click Accept > Next.

7. Accept the default method name or rename it > click Next.

8. Review the available modules for this method > click Next.

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

10. Review the installation summary > click OK.

11. If necessary, close and restart ConsoleOne to run the newly installed ConsoleOne snapins provided by the login method to configure the login and/or enroll users to use this login method.

Installing a Post-Login Method

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. Select New > Object.

   The New Object Wizard starts.

4. Select the sasPostLoginMethod class > click OK.

5. Specify the configuration file > click Next.

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

6. From the license agreement screen, click Accept > Next.

7. Accept the default method name or rename it > click Next.

8. Review the available modules for this method > click Finish.

9. Review the installation summary > click OK.
10. If necessary, close and restart ConsoleOne to run the newly installed ConsoleOne snapins provided by the login method to configure the login and/or enroll users to use this post-login method.

Updating a Login and Post-Login Method

When a login method vendor updates 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 General tab > click Update Method.
2. Specify the configuration file > click Next.

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

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

Creating a Login Sequence

Once login and post-login methods are installed, you must create login sequences in order for the methods to be used to log in to NDS®. You view, add, modify, or delete login sequences using ConsoleOne.

In NMAS Enterprise Edition, 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 on of the login methods validate the identity of the user for the login to be successful.

The post-login methods in a login sequence are all executed if the login is successful, regardless of the *And* and *Or*.

Once a sequence is created, users may be authorized to use the new sequence to log in to the network.

Adding a New Login Sequence

1. In ConsoleOne, select the Security container.
2. Right-click the Login Policy container > select Properties.
3. Click New Sequence.
4. Enter a name for the new login sequence > 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 will have to log in using every login method that makes up the login sequence. If you select Or, the user will only have 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.

Modifying a Login Sequence

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 have a post-login method selected.
   - 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.

Deleting a Login Sequence

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.

Authorizing Login Sequences for Users

You can restrict the login sequences each user can use by doing the following:

1. In ConsoleOne, right-click a User object > click Properties > click the Security tab > 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.

Setting Default Login Sequences

You can set a default login sequence so that a user or 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 > click Login Sequences.

2 Click 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 login without using a login sequence, this default login sequence will be attempted.

3 Click Apply or OK.

Next Steps

- To set up graded authentication, see Chapter 3, “Using Graded Authentication,” on page 23.
- To log in using NMAS, see Chapter 4, “Logging In to the Network Using NMAS,” on page 37.

3 Using Graded Authentication

This chapter describes how to set up graded authentication.

Overview

The graded authentication feature of NMAS™ Enterprise Edition allows you 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 NDS® 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 NDS 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 NDS attributes.
3. Assign clearances for each user who will be logging in to the network using NMAS. By default, all users have a clearance.

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

Key Graded Authentication Terms

Security Policy Object

The Security Policy object is the object in NDS 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 28.

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.

Integrity Categories

Integrity controls the modification or writing of information.

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

For more information, see "Defining User-Defined Categories (Closed User Groups)" on page 28.

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 NDS attribute. The security label is compared against a user's current clearance to determine what information the user can access.

NMAS Enterprise Edition comes with eight security labels defined. The following table shows the pre-defined 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 29.

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 27 and "Graded Authentication Rules" on page 27.

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 Enterprise Edition 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 pre-defined clearances and the security labels.

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

NA = No Access R = Read W = Write

For more information, see "Defining Clearances" on page 30.

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 27.

Graded Authentication Rules

IMPORTANT: 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.

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.
- The use of 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 Enterprise Edition. 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 NDS attribute or NetWare volumes. You can also assign clearances to User objects in your NDS 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 a security labels in addition to the three integrity and three secrecy categories (Biometric, Token, Password) that are pre-defined. For example, Biometric integrity and secrecy categories represent that access to an object is restricted to users logging in with a biometric method.

Once 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 > select either Secrecy Categories or Integrity Categories.
3. Click Add > type in 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 > select either Secrecy Categories or Integrity Categories.
3. Click on the category you want to rename > click Rename Category.
4. Enter the new name > click OK > click OK or Apply.

Defining Security Labels

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

Once 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 > Security Policy.
2. Click Define Labels.
3. Click New Label and type in 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. Type in the 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 a 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.

Once 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 > type in a name for the clearance.
4. Select a security label from the Read label drop-down list.

   This label will be 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 will be the Write label for this clearance. Note that 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 what Read and Write labels 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. Type in 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 will tell 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 what access the clearance has to the labeled object.

Assigning Security Labels to Network Resources

With NMAS Enterprise Edition, you can assign NetWare volumes and any NDS attribute a security label. Users that 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 clearances to NDS 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 > 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 that contained in personnel files.
- Engineering handles restricted or confidential information such as 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 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.

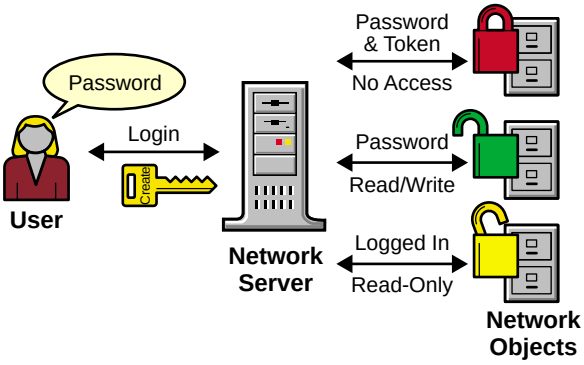
Graded authentication replaces the physical key given to users with a clearance. Also, NMAS replaces the filing cabinet with NetWare file system volumes that are also assigned security labels. These security labels replace the filing cabinet lock type.

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 33) 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).

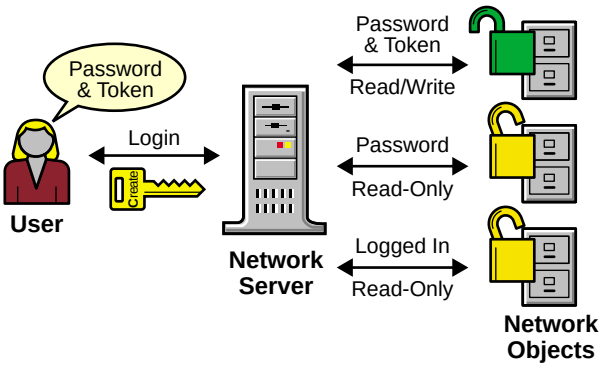
Figure 1 Single-Factor Authentication



The following would apply (as illustrated in Figure 2, “Multiple-Factor Authentication,” on page 34) 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 (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.

Next Steps

- To set up login methods and sequences, see Chapter 2, "Setting Up 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

Once NMAS™ Enterprise Edition is installed and graded authentication is configured, you are ready for users to log in to the network. This chapter describes some of the additional features of the login experience that you should communicate to your network users.

Additional information is available to help your network users understand the NMAS login process. You can print the NMAS_USER.PDF file on the *NMAS Enterprise Edition* CD-ROM 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 NDS® tree for a complete and current list.

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

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

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

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

4b Click Novell Client Properties > Location Profiles.

4c Select the desired profile > click Properties > Properties.

4d Check Display Clearance Field.

4e Click OK > OK > OK.

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 has changed. 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 their 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 NDS trees, the login sequence for any NDS tree may be used. The default is the first NDS tree.

Client Log File

You can create a client log file which 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 > click Properties.
4. Click the Services tab > select the Service and Server Instance > click Properties.
5. From the NMAS tab, click Log NMAS Client Activity > 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 Enterprise Edition, 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 only, a Single Sign-on (SSO) tab is available as a convenience for NMAS users authenticating via a biometric 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.

You can configure the Single Sign-on tab by doing the following:

1. Open the Novell Client Windows property page.
2. Click the Single Sign-on tab.
3. Check the Enable Single Sign-on box to enable this feature.
4. Click OK.

5 Configuring and Managing NMAS on UNIX

NMAS Server Components on UNIX

The server components of NMAS are shipped along with Novell eDirectory on Unix. The NMAS Server Components that come along with Novell eDirectory on Unix Servers provide server-side support for following methods of logging in to eDirectory:

- **Default eDirectory Login Method:**Standard eDirectory login method for users from Windows clients.
- **Simple Password Methods:** Provide support for users to have SHA-1, MD5, or Clear text passwords and to log in to eDirectory using those passwords from Windows clients.
- **X509 method:** To log in to eDirectory using X509 certificates from Windows clients.

In addition, NMAS provides support for mutual authentication between a user and an eDirectory server using certificates through LDAP (with SSL) connection.

About the nmasconfig Utility

Use this utility for login sequence management, login method management, and Simple Password management, apart from configuring and unconfiguring the NMAS server.

When this utility is used with arguments, it validates them and prompts for the password of the user who has administrative rights.

If the utilility is used without arguments, nmasconfig displays a description of the utility and available options.

Four modes of operation are available:

1. config
2. method
3. sequence
4. passwd

Only one of the modes of operation needs to be selected.

This section discusses the following topics:

- Configuring the NMAS Server (page 42)
- Login Method Management (page 44)
- Login Sequence Management (page 45)
- Managing Simple Passwords (page 47)

Table 1 The nmasconfig Utility General Parameters

nmasconfig Parameter	Description
-t	Refers to the name of the eDirectory tree on which NMAS has to be configured. This is an optional parameter. By default, this is taken from the tree name of the current server, read from nds.conf file.
-h *host name*:[*port*]	Refers to the hostname and, optionally, the eDirectory port. By default, this is taken from the hostname of the current server and the default eDirectory port

Configuring the NMAS Server

The config mode of the nmasconfig utility lets you configure or remove the configuration of the NMAS server. To use this mode to configure the server, ensure that you have administrative rights.

Configuring the NMAS Server

To configure the NMAS server, enter the following command:

nmasconfig config [**-t** *treename*] [**-h** *hostname*[:*port*]] **-c -a** *adminname*

Table 2 The nmasconfig Utility Configure Parameters

Configure Parameter	Description
-c	Configures NMAS.
-d	Removes NMAS configuration.
-a	Refers to the fully distinguished name of the eDirectory administrator with supervisor rights to the security container. The fully distinguished name of the administrator should be specified in the typeless, dot-delimited form without the tree name. This parameter is required.

Example: To configure NMAS in the tree ACME running on the same host, enter the following command.

nmasconfig config **-t** *acme* **-c -a** *admin.company*

Unconfiguring the NMAS Server

To remove the NMAS server configuration, enter the following command:

nmasconfig config [**-t** *treename*] [**-h** *hostname*[:*port*]] **-d -a** *adminname*

Example: To remove the configuration of NMAS in the tree ACME, enter the following command:

nmasconfig config -t *acme* -d -a *admin.company*

NOTE: For NMAS configuration or unconfiguration to take effect, restart the Novell eDirectory server.

Login Method Management

Use the method mode of the nmasconfig utility to install a new login method or upgrade an existing login method to the tree. It can also be used to remove an existing login method

Installing a New Login Method

To install a new login method or upgrade an existing login method to the tree, enter the following command:

`nmasconfig method` [general options] **`-i | -U -f`** *path-to-config.txt* **`-a`** *admin_name*

Table 3 The nmasconfig Utility Method Parameters

Method Parameter	Description
-i	Installs a new method. This also creates a login sequence which contains only this login method.
-u	Upgrades NMAS configuration.
-r	Removes an existing method from the tree. This also removes the sequence with only this login method, created during this method install.
-a	Refers to the fully distinguished name of the eDirectory administrator with supervisor rights to the context in which the server object and Directory services are to be created. The fully distinguished name of the administrator should be specified in the typeless dot delimited form without the tree name. This parameter is required.
-f	Refers to the absolute or relative path, including the filename, to the config.txt file for the method that needs to be installed. This text file is located in the NMAS methods directory on the install CD. This is a required parameter if either the -i or -U options are specified.

Method Parameter	Description
-m	Refers to the name of the NMAS method object that needs to be removed from the tree. If there are spaces or special characters in the method object name, then the name should be within quotes (" "). This is a required parameter if the -r option is specified.

Example: To install a new method to the tree running on the current server, enter the following command:

`nmasconfig method -i -f` *./SimplePassword/config.txt* **`-a`** *admin.company*

Removing an Existing Login Method

To remove an existing login method, enter the following command:

`nmasconfig method` [general options] **`-r -m`** *methodname* **`-a`** *admin_name*

Example: To remove an existing login method from the tree running on the current server, enter the following command:

`nmasconfig method -t` *ACME* **`-r -m`** "*X.509 Certificate*" **`-a`** *admin.company*

IMPORTANT: You only need to specify one of these options: -i, -U, or -r.

Login Sequence Management

Use the sequence mode of the nmasconfig utility to manage the login sequence.

To manage the login sequence, enter the following command:

`nmasconfig sequence` [general options] **`-D`** *user_name* **`-a`** *admin_name*

Table 4 The nmasconfig Utility Sequence Parameters

Sequence Parameter	Description
-D	Refers to the distinguished name of the user object for which sequence management is to be done. The user's distinguished name should be specified in the typeless, dot-delimited form without the tree name. This is a required parameter.
-a	Refers to the distinguished name of the user object with supervisor rights to the context in which the previously specified user object is to be modified. The admin DN should be specified in the typeless, dot-delimited form without the tree name. This is a required parameter.

Example: To manage the authorized and default sequences of the user named user1 in tree ACME, enter the following command:

`nmasconfig sequence -t` *ACME* **`-D`** *user1.finance.company* **`-a`** *admin.company*

The sequence management option generates a menu of options.

Table 5 The Sequence Management Menu Options

Sequence Management Options	Description
(a) Authorize a method	Authorizes a sequence present in the "Available Login Sequences" list.
(b) Remove an authorized method	Removes an existing authorized login sequence from the "Authorized Login Sequences" list.
(c) Change default login sequence	Sets the default login sequence for the user from the "Authorized Login Sequences" list.
(d) Commit current changes and exit	Commits the changes to eDirectory and exits the sequence management menu.
(e) Quit without saving	Quits the sequence management menu without saving the changes.

Managing Simple Passwords

Use the passwd mode of nmasconfig utility to set simple passwords.

To set the simple password for a specified user in the tree, enter the following command:

nmasconfig passwd [general options] [**-H** *hash_type*] [**-a** *admin_name*] **-D** *user_name*

Table 6 The nmasconfig Utility Password Parameters

Password Parameter	Description
-H	Refers to the hashing format in which the simple password for the user needs to be stored in eDirectory. The valid values are "sha," "md5," or "clear." By default, simple password hash type is "clear."
-a	Refers to the distinguished name of the user object with supervisor rights to the context in which the specified user object's simple password is to be modified. The administrator's fully distinguished name should be specified in the typeless, dot-delimited form without the tree name.
-D	Refers to the distinguished name of the user object for which simple password change is to be done. The user DN should be specified in the typeless, dot-delimited form without the tree name. This is a required parameter.

Example 1: If you are an admin and are changing another user's simple password, enter the following command:

nmasconfig passwd -**a** *admin.company* **-D** *user1.finance.company*

Example 2: If you are modifying your own simple password, enter the following command:

nmasconfig passwd -**D** *user1.finance.company*

A NDS Considerations with NMAS

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

Setting Up a Security Container As a Separate Partition

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® 5.1 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, 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 NDS 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 NDS 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 when 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 Secret Store 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 Secret Store.

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

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.

NOTE: Any certificates signed by the Organizational CA of the source tree will become nonusable 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.

HINT: If you are uncertain about the identify of the signing CA for any Key Material object, reference 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 NDS 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.

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.

   HINT: 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 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, notate 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 notated 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, or NMAS, NetWare 5.1 or later, or NDS 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 then 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

NDS trees are merged using the DSMERGE utility. For more information, refer to the DSMERGE documentation (http://www.novell.com/documentation/lg/nds73/docui/index.html#../maintenu/data/hpqtpzmg.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.