NetIQ® Modular Authentication Services™ (NMAS) 8.8 SP8

Administration Guide

September 2013

Legal Notice

Contents

About this Book and the Library

The *Administration Guide* provides an overview of the NetIQ Modular Authentication Services (NMAS) technology and software. It includes instructions on how to install, configure, and manage NMAS.

For the most recent version of the *NetIQ Modular Authentication Services Administration Guide*, see the NetIQ eDirectory 8.8 online documentation Web site.

Intended Audience

The guide is intended for network administrators.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Describes how to configure and use XDASv2 to audit eDirectory and NetIQ Identity Manager.

Administration Guide

Describes how to manage and configure eDirectory.

These guides are available at NetIQ eDirectory 8.8 documentation Web site.

For information about the eDirectory management utility, see the *NetIQ iManager 2.7 Administration Guide*.

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 NMAS Overview

This section provides an overview of the NetIQ Modular Authentication Service (NMAS). NMAS 8.8.8 is part of eDirectory 8.8 SP8. For eDirectory 8.8 and later, NMAS is automatically installed when you install eDirectory. For more information about eDirectory 8.8 SP8, including supported platforms and installation instructions, see the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

1.1 NMAS Functionality

NMAS is designed to help you protect information on your network. In addition to the Password Management tool, NMAS brings together ways of authenticating to NetIQ eDirectory 8.7.3 or later networks. This helps to ensure that the people accessing your network resources are who they say they are.

1.1.1 NMAS Features

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

1. User Identification Phase (who are you?)
2. Authentication (Login) Phase (prove who you say you are)
3. Device Removal Detection Phase (are you still there?)

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

User Identification Phase

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

Authentication (Login) Phase

- "Password Authentication" on page 12
- "Physical Device Authentication" on page 12
- "Biometric Authentication" on page 13

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)

For more information on these login factors, see Section 1.1.2, "Login and Post-Login Methods and Sequences," on page 14.

Password Authentication

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

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

Universal Password is a way to simplify the integration and management of different password and authentication systems into a coherent network. For more information on Universal Password, see the *NetIQ Password Management 3.3.2 Administration Guide*.

Physical Device Authentication

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

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

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

  NetIQ provides the NetIQ Enhanced Smart Card login method for the use of smart cards. The NetIQ Enhanced Smart Card login method is provided as part of the Identity Assurance Client. For more information, see the *NetIQ Enhanced Smart Card Method 3.0 Installation and Administration Guide*.
- **One-Time Password (OTP) device:** An OTP device is a hand-held hardware device that generates a one-time password to authenticate its owner.
- **Proximity card:** A proximity card is a card worn by a person. This technology locks and unlocks a person's workstation based on the card's proximity to the workstation.

  NetIQ provides the pcProx login method, which supports RFID proximity cards. The pcProx login method is provided as part of the NetIQ SecureLogin product. For more information, see *NMAS Login Method and Login ID Snap-In for pcProx*.

Biometric Authentication

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

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

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

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

Device Removal Detection Phase

The user's session enters this phase after login is complete. Two methods are available:

- The Secure Workstation method, which is available with NetIQ SecureLogin. The user's session can be terminated when an authentication device (such as a smart card) is removed. This device need not be used in any of the other phases

  For more information on the Secure Workstation method, see the *NetIQ SecureLogin 7.0 SP3 Administration Guide*.
- The NetIQ Enhanced Smart Card login method also provides smart card removal detection. For more information on the NetIQ Enhanced Smart Card login method, see the *NetIQ Enhanced Smart Card Method Installation Guide*.

1.1.2 Login and Post-Login Methods and Sequences

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

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

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

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

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

1.1.3 Security Object Caching

The security container is created off the root partition when the first server is installed in the tree and holds information such as global data, security policies, and keys.

After universal password was introduced, whenever a user logged into eDirectory through NMAS, NMAS accessed the information in the security container to authenticate the login. When the partition having the security container was not present locally, NMAS accessed the server, which had this partition. This had an adverse impact on the performance of NMAS authentication. The situation was worse in the scenarios where the server containing the partition having the security container had to be accessed over WAN links.

To resolve this, with eDirectory 8.8, the security container data is cached onto the local server. Therefore, NMAS does not need to access the security container located on a different machine whenever a user logs in, it can easily access it locally. This increases the performance. Adding the partition having security container to local server improves the performance, but it might not be feasible in scenarios where there are too many servers.

If the actual data in the security container changes on the server containing the security container partition, the local cache is refreshed by a background process called backlinker. By default, backlinker runs every thirteen hours and it pulls the modified data from remote server. In case, the data needs to be synchronized immediately, you can schedule backlinker on the local server either through iMonitor, ndstrace on Linux, or ndscons on Windows. For more information, refer to the iMonitor online help or the ndstrace manpage.

The security object caching feature is enabled by default. If you do not want backlinker to cache any data, remove `CachedAttrsOnExtRef` from the NCP server object.

1.2 NMAS Software

NMAS is included as a bundled product with NetIQ eDirectory. The software image includes the following:

- NMAS server software
- Login methods software
- Support for multiple login methods per login sequence
- Support for graded authentication
- Universal Password

NMAS client software is available with the NetIQ Client for Windows and with NetIQ SecureLogin.

1.2.1 Server and Client Software Installation

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

The NMAS client software now ships with the NetIQ Client. For more information, refer to the NetIQ Client for Windows documentation.

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

1.2.2 Login Method Software and Partners

Software and Partners

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

NMAS software includes support for a number of login methods from third-party authentication developers. Refer to the NetIQ Partners Web site for a list of NetIQ partners.

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

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

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

Installing a Login Method

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

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

For more information on installing a login method, see Section 2.1, “Installing a Login Method,” on page 17.

1.2.3 Universal Password

Universal Password is a way to simplify the integration and management of different password and authentication systems into a coherent network. It provides one password for all access to eDirectory, enables the use of extended characters in passwords, enables advanced password policy enforcement, and allows synchronization of passwords from eDirectory to other systems.

For more information on Universal Password, see the *NetIQ Password Management 3.3.2 Administration Guide*.

1.2.4 iManager Management

You can manage NMAS by using iManager. NetIQ iManager is a Web-based utility for managing eDirectory. Specific property pages in iManager let you manage login methods, login sequences, enrollment, and graded authentication.

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

For more information about installing login methods, see Section 2.1, “Installing a Login Method,” on page 17.

1.3 What's Next

- To install and set up login methods and sequences, see Chapter 2, “Managing Login and Post-Login Methods and Sequences,” on page 17.
- To log in using NMAS, see Chapter 3, “Using NMAS to Log In to the Network,” on page 25.

2 Managing Login and Post-Login Methods and Sequences

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

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

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

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

See the NetIQ Partners Web site for a list of eDirectory partners. Some partners develop third-party login methods.

2.1 Installing a Login Method

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

- nmasinst utility (UNIX and Windows), which allows you to install login methods into eDirectory.
- NetIQ iManager (UNIX and Windows), which allows you to install login and post-login methods into eDirectory.

2.1.1 Using the nmasinst Utility to Install a Login Method

From the server console command line, enter:

```
nmasinst -addmethod admin.context treename config.txt_path [-h hostname[:port]] [-
w password|file:<filename>|env:<environment_variable>] [-checkversion]
```

- *admin.context*: The admin name and context.

- *treename*: The name of the eDirectory tree where you are installing the login method.
- *config.txt_ path* - The complete or relative path to the `config.txt` file of the login method. A `config.txt` file is provided with each login method.
- `[-h hostname[:port]]`: (Optional) The hostname and port of the server. Use this if eDirectory is not running on the default port. You can also specify the IP address. eDirectory 8.8 SP8 supports both IPv4 and IPv6 addresses. For example:
  - **IPv4:** `-h 127.0.0.1:8443`
  - **IPv6:** `-h [2001:db8::6]:8443`
- `[-w password|file:<filename>|env:<environment_variable>]`: This option allows you to specify the password using one of the following methods:
  - On the command line. For example: `-w n`
  - Through a file. For example: `-w file:/tmp/passwd`
  - Through an environment variable. For example: `-w env:PASSWD`
- `[-checkversion]`: This option reports an error if the installed method version is the same or newer than the method version being installed.

If the login method already exists, nmasinst updates it.

2.1.2 Using NetIQ iManager to Install a Login or Post-Login Method

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

2.2 Updating Login and Post-Login Methods

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

- Section 2.2.1, “Using the nmasinst Utility to Update a Login Method,” on page 18
- Section 2.2.2, “Using NetIQ iManager to Update a Login Method,” on page 18

2.2.1 Using the nmasinst Utility to Update a Login Method

Use the same procedure you used to install a login method with the nmasinst utility (see Section 2.1.1, “Using the nmasinst Utility to Install a Login Method,” on page 17). Include the path to the new `config.txt` file and the login method is updated.

2.2.2 Using NetIQ iManager to Update a Login Method

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

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

4 Click the login method you want to update.

5 On the login method property page, click **Update Method**.

6 Follow the update wizard to completion.

2.3 Managing Login Sequences

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

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

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

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

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

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

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

- "Creating a New Login Sequence by Using NetIQ iManager" on page 19
- "Modifying a Login Sequence" on page 20
- "Deleting a Login Sequence" on page 20

2.3.1 Creating a New Login Sequence by Using NetIQ iManager

1 Launch NetIQ iManager.

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

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

4 Click **New** and specify a name for the new login sequence.

All available methods are listed under **Available Login Methods** and **Available Post-Login Methods**.

5 Select the **Sequence Type** from the drop-down list.

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

6 Use the horizontal arrows to add each desired method to the sequence.

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

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

7 Click **Finish** to save the login sequence.

2.3.2 Modifying a Login Sequence

1 Launch NetIQ iManager.

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

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

4 Click a login sequence name.

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

5 Select an action:

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

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

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

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

6 Click **Apply** or **OK**.

2.3.3 Deleting a Login Sequence

1 Launch NetIQ iManager.

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

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

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

5 Click **Apply** or **OK**.

2.4 Authorizing Login Sequences for Users

2.4.1 Assigning Login Sequences

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

The attributes found with the User object supersede any attributes found with container, partition root, or login policy object. If a login sequence has been assigned to a partition root, that login sequence applies to all the users under that partition root only if a login sequence has not already been individually assigned to specific users.

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

2.4.2 Authorizing a Login Sequence

1. Launch NetIQ iManager.
2. Authenticate to the eDirectory tree as an administrator or a user with administrative rights.
3. On the **Roles and Tasks** menu, click **NMAS** > **NMAS Users**, select the user you want to authorize the login sequences for, then click the **NMAS** tab.
4. Authorize or de-authorize a login sequence for a user by selecting the login sequence and clicking **Authorize** or **De-authorize**.
5. Click **Apply** or **OK**.

2.5 Setting Default Login Sequences

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

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

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

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

For more information on how to assign login sequences, see "Assigning Login Sequences" on page 21.

2.6 Deleting a Login Method

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

NOTE: nmasinst does not have an option to remove NMAS methods. It must be done through iManager.

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

- “Removing the Login Method from Any Login Sequence” on page 22
- “Deleting the Login Method” on page 22

2.6.1 Removing the Login Method from Any Login Sequence

To use iManager to remove the login method for any login sequence:

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

When the login method has been removed from all login sequences, you can then delete it. See Section 2.6.2, “Deleting the Login Method,” on page 22.

2.6.2 Deleting the Login Method

To use iManager to delete the login method:

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

2.7 Deleting a Login Sequence

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

2.8 What's Next

- To log in using NMAS, see Chapter 3, “Using NMAS to Log In to the Network,” on page 25.

3 Using NMAS to Log In to the Network

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

3.1 Password Field

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

See the Novell Client For Windows documentation for more information on hiding the password field.

3.2 Advanced Login

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

   You can browse only if an eDirectory tree has been specified on the **eDirectory** tab.
4. Specify the desired user session clearance or browse the eDirectory tree for a complete and current list.

   By default, the **Clearance** field is disabled. To enable the **Clearance** field:

   4a Right-click the red N in the task bar.

   4b Click **Novell Client Properties** > **Location Profiles**.

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

   4d On the **NMAS** tab, select **Display Clearance Field**.

   4e Click **OK** three times.

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

5 Click **OK**.

3.3 Unlocking the Workstation

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

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

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

3.4 Capturing an NMAS Client Trace

Capturing an NMAS client trace can help in troubleshooting NMAS authentication problems. For more information, see TID # 3331372.

3.5 Viewing NMAS Clearance Status

1 Right-click the red N in the task bar.

2 Click **Novell Connections**.

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

3.6 Single Sign-on Tab

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

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

To configure the **Single Sign-on** tab:

1 Open the Novell Client Windows property page.

2 Click the **Single Sign-on** tab.

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

4 Click **OK**.

NOTE: Single Sign-on feature is available only on Windows XP.

4 History of NetIQ Passwords

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

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

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

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

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

Universal Password is managed by the Secure Password Manager, a component of the NMAS module. Secure Password Manager simplifies the management of password-based authentication schemes across a wide variety of NetIQ, Novell, and NetIQ partner products. The management tools only expose one password and do not expose all of the behind-the-scenes processing for backwards compatibility.

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

NOTE: The Password Management plug-in is available for download at the Novell Downloads Web site.

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

For NMAS 3.2*x* and earlier, when the NDS password is migrated to the Universal password, the password expiration time is recalculated from the current time plus the password expiration interval. For NMAS 3.3 and later, password expiration time is not updated when the NDS password is migrated to the Universal Password unless the “Verify whether existing passwords comply with the password policy (verification occurs on login)” password policy rule is set to “true”.

For more information about deploying and managing Universal Password, see the *NetIQ Password Management 3.3.2 Administration Guide*.

5 NMAS HOTP Method

The following sections contain information about the NMAS HOTP method:

5.1 Overview

HOTP is an HMAC-based one-time password (OTP) algorithm. An OTP is a password that is valid for only one login session or transaction. An OTP provides better performance than the traditional (static) passwords because there are less chances of security attacks associated with it. A potential intruder who records an OTP that has been used to log into a service or to conduct a transaction, cannot manipulate it because it has already been used once and is no longer valid.

Every OTP based authentication requires an OTP server and an OTP client (hardware/software token). Implementation of OTP based authentication in NMAS is based on the RFC 4226 standard. Traditionally, the NDS password that was individually presented to the server is now appended to the OTP to enhance the password based authentication by retaining all the client components and their user interface.

The authentication to eDirectory server is done through the HOTP feature by using LDAP-based login or NetWare Core Protocol (NCP)-based login.

5.1.1 LDAP-Based Login

Prerequisites

- Set the `NDSD_TRY_NMASLOGIN_FIRST` environment variable to true.

  For more information, refer to the “How to Make Your Password Case-Sensitive” section in the *NetIQ eDirectory 8.8 SP8 What’s New Guide*.

Login Method

An HOTP-enabled user can perform LDAP bind by concatenating the NDS password with the HOTP value.

For example,

```
ldapsearch -D cn=user1,o=novell -w secret40338314 -h 164.99.91.165 -p 389 -b
"o=novell" -s sub -LLL dn
```

5.1.2 NCP-Based Login

A HOTP-ready/enabled user can perform NCP login by concatenating the NDS Password with the HOTP value by using any of the following utilities:

- ndslogin

  For example,

  ```
  ndslogin user1.org -h org.com -p secret40338314
  ```

- iMonitor
- iManager (replace the existing `libnmasclnt.so` file in the iManager-installed location)

NOTE: iManager plug-ins that perform LDAP authentication will fail if used by HOTP-enabled users.

5.2 Prerequisites

- eDirectory 8.8 SP6 or later on all supported platforms of eDirectory 8.8.

  For more information on the supported platforms of eDirectory 8.8, refer to the *NetIQ eDirectory 8.8 SP8 Installation Guide*.

5.3 Installation

5.3.1 Server Installation

The HOTP server module is a part of the NMAS server component. The server module validates the OTP presented from the client.

Download the latest patch from the Novell Download site. Install the patch and extend the schema.

After extending the schema, the following attributes are available on the NMAS HOTP server:

- `sasOTPCounter` (per user attribute)
- `sasOTPEnabled` (per user/immediate parent container/partition root/Login Policy object)
- `sasOTPDigits` (per user/immediate parent container/partition root/Login Policy object)
- `asOTPLookAheadWindow` (tree wide set at the Login Policy object)
- `sasOTPResync` (9 per user attribute)

5.3.2 Client Installation

To login through the HOTP enabled user, the client needs the latest `libnmasclnt.so` file that contains the HOTP information needed to enable the HOTP method. Download the latest `libnmasclnt.so` file from the Novell Download site. To enable the HOTP method, the clients do not need any changes because the changes are available in the NMAS patch file.

NOTE: The HOTP client installation is only available for Linux 32-bit and 64-bit platforms.

5.3.3 Obtaining and Using nmashotpconf Utility

The nmashotpconf utility is a configuration utility that configures the OTP attributes on the eDirectory server.

NOTE: The HOTP utility is available only for the Linux 32-bit and 64-bit platforms.

To execute the `nmashotpconf` utility, perform the following steps:

1. Obtain the `nmasotpconf` utility and specify the directory where you unzipped the `NMAS HOTP` utility.

   The unzipped file contains the `linux` and `linux_x64` directories for the 32-bit and 64-bit Linux machines.

   The `linux` and `linux_x64` directories contain the `nmashotpconf` executable and `libnmasext.so` files.
2. Go to the `linux/final` directory on a Linux 32-bit machine, else go to the `linux_x64/final` directory on a Linux 64-bit machine.
3. Download the trusted root certificate and store it locally.

   For more information, see Exporting a Trusted Root or Public Key Certificate.

   For usage,

```
nmashotpconf -h <host_name> [-p <ssl_port>] -D <login_dn> [-w <password>]
 -e <trusted_cert> -t <cert_type> [-r <resync_window>] [-y
 <user_resync_window>] [-u <hotp_dn> [-o <hotp_options>] [-d digits] [-c
 <counter>] [-s <secret> -f <secret_format>]]
```

Option	Description
host_name	Specifies the LDAP server name or the IP address of the server.
ssl_port	Specifies the SSL port on the LDAP server. The default value is 636.
login_dn	Specifies the DN for the user.
password	Specifies the password for the user DN.
trusted_cert	Specifies the trusted root certificate file.
cert_type	Specifies the trusted root certificate encoding type. For example, DER means der-encoded file, and B64 means b64-encoded file.
encoded file digits	Specifies the number of digits used as the HOTP value. **NOTE:** This setting is applicable to all the users in the tree.

Option	Description
resync_window	Specifies the counter re-synchronization look-ahead window.
user_resync_window	Specifies the counter user re-synchronization look-ahead window.
hotp_dn	Specifies the target DN for which you are configuring the HOTP attributes. To configure the HOTP at the tree level, enable/disable HOTP at the tree level, or configure digits at tree level, then specify the DN as `cn=Login Policy,cn=Security`.
hotp_options	Enables or disables the HOTP for the hotp_dn option. Specify ENABLE to enable the HOTP, and DISABLE to disable HOTP.
counter	Specifies the HOTP counter value. The vaild range of the counter value is between 0 and 2147483647. The counter value is set through the hotp_dn option.
hotp_dn secret	Specifies the OATH HOTP secret. For example, the raw byte value of secret in the hexadecimal format is 31323334353637383930313233343536373839 30, or the corresponding ASCII/Extended ASCII string is 12345678901234567890.
secret_format	Specifies the format of the OATH HOTP secret. ◆ **STRING:** This format is used for an ASCII/Extended ASCII string. For example, 12345678901234567890. ◆ **RAW:** This format is used for raw byte values in a hexadecimal format. For example, 31323334353637383930313233343536373839 30, where hexadecimal value of the first character is 31, the value of the second character is 32, and so on.

5.4 Resynchronization of the Counter

The counter value of the server is incremented only after successful HOTP authentication, and the counter on the token is incremented every time a new HOTP is requested by the user. The counter values on the server and the counter on the token might be out of synchronization.

To address this, you should have a tree-wide look-ahead or a resynchronization window setting in place. If the server finds that the received HOTP does not correspond to the server counter value, the server can recalculate the next few HOTP values that are within the resynchronization window, and check them against the received HOTP. If there is a match, authentication succeeds and the server counter is set to the counter value that corresponds to the matched HOTP.

For successful authentication the server counter is set to the next counter value at which the authentication succeeds.

The tree-wide resynchronization window setting should be as low as possible in order to restrict the space of possible solutions for an attacker trying to recreate the HOTP values.

If the mismatch between the client and server counters is beyond the tree-wide resynchronization window setting, resynchronization can be achieved by temporarily setting a user-specific resynchronization window to a large value and then attempting an HOTP-based authentication.

The nmashotpconf utility should be used for configuring HOTP-based authentication. For more information, read the Configuration section.

5.5 Configuration

To provision an eDirectory user for an HOTP-based authentication, do the following configuration settings according to the RFC 4226 standard.

- Enable HOTP on the user/container/partition root/Login Policy object in the same order of precedence.
- Set the HOTP-shared secret key and counter on the user. These two settings together determine the HOTP value.
- Configure the number of digits in HOTP values on the user/ container/partition root/Login Policy object.The valid range of digits is from 6 to 9.
- Set the resynchronization windows as follows:
  - Set the tree-wide resynchronization window at the Login Policy object.
  - Set the user-specific resynchronization window at the user level. This is needed only when the client and server are out of sync.

Examples:

- To configure a secret and a counter on the user object, run the following command:

```
./nmashotpconf -h 164.99.91.165  -p 636 -D cn=admin,o=novell -w novell   -e   /
var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -c 0
-s   31323334353637383930313233343536373839 30 -f  RAW
```

- To enable the OTP for a user object, run the following command:

```
./nmashotpconf -h 164.99.91.165  -p 636 -D cn=admin,o=novell -w novell   -e   /
var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -o
ENABLE
```

- To disable the OTP for a user object, run the following command:

```
./nmashotpconf -h 164.99.91.165  -p 636 -D cn=admin,o=novell -w novell   -e   /
var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -o
DISABLE
```

  Similarly, you can enable or disable the OTP for a container/partition or a root/Login Policy object.

- To configure an OTP digit for a user object, run the following command:

```
./nmashotpconf -h 164.99.91.165  -p 636 -D cn=admin,o=novell -w novell   -e /
var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -d 6
```

  Similarly, you can set the OTP digit for a parent container/partition root/ Login Policy object.

- To configure the user resyncronization window, run the following command:

```
./nmashotpconf -h 164.99.91.165  -p 636 -D cn=admin,o=novell -w novell   -y 5 -
e   /var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell
```

- To configure the counter re-synchronization look ahead window, run the following command:

```
./nmashotpconf -h 164.99.91.165 -p 636 -D cn=admin,o=novell -w novell   -r 6
```

5.6 Known Issues

5.6.1 ndsconfig add fails for an HOTP enabled administrative user

For HOTP enabled users, the OTP digit is used for authentication. The ndsconfig utility uses the same OTP digit for subsequent authentication, which causes the ndsconfig add to fail. Similarly, ndsconfig upgrade also fails.

To work around this issue, do not enable HOTP for the user through which you are performing ndsconfig add/ upgrade.

5.6.2 Login through HOTP-enabled user to a read-only replica fails

If you perform LDAP login through the HOTP-enabled user by sending a request to the read-only replica, the LDAP chaining does not happen. The read-only replica does not forward the request to the server where the actual user resides. The replica fails giving an illegal replica type error.

5.6.3 nmashotpconf utility cannot modify the user resynchronization window

If the value of the user resynchronization window is already set (say 2) and its value is changed by using the nmashotpconf utility, it displays the following error:

```
ldap_modify_ext_s on HOTP DN failed: error code=19: Constraint violation
```

One of the reasons for the error could be using a combination of the **-o** (the OTP enable or disable option), **-d** (OTP digit), **-c** (otpcouter) and **-y** (user_resync_window) options for modifying the user resynchronization value.

6 Other Administrative Tasks

This section describes other administrative tasks for NMAS™:

6.1 Using the Policy Refresh Rate Command

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

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

The policy refresh rate command has the following syntax:

```
nmas RefreshRate minutes
```

where *minutes* is the number of minutes between each attempt to check if the cached NMAS login policy needs to be updated.

For information on how the policy refresh rate command can be invoked for each NMAS Server platform, see Section 6.4, “Invoking NMAS Commands,” on page 39.

6.2 Using the LoginInfo Command

With NMAS 3.2 or later, you can turn off automatic updating of certain user object login attributes by using the `LoginInfo <numb>` command. You might want to do this manually if automatically updating attributes causes problems. The following sections further explain this functionality:

- Section 6.2.3, “Using the LoginInfo Command to Control LoginInfo Attributes When Attributes are Updated,” on page 36
- Section 6.2.4, “Using the sasUpdateLoginInfo and sasUpdateLoginTimeInterval Attribute,” on page 37

6.2.1 NMAS Login for LDAP Bind

In order to make your passwords case-sensitive, you must enable the NMAS login for LDAP Bind. For information on how to do this, see the “How to Make Your Password Case-Sensitive” section section in the *NetIQ eDirectory 8.8 SP8 What's New Guide*.

When the NMAS login is enabled for LDAP Bind, eDirectory automatically updates user object login attributes after the user has authenticated. The following is a non-exhaustive list of login attributes that are updated:

- Login Time
- Network Address
- Last Login Time

6.2.2 Problems Caused by Automatically Updating User Object Login Attributes

The automatic updating of user object login attributes can lead to the following problems:

- High utilization
- Unresponsiveness
- Client time-outs seen on busy authentication servers, especially in LDAP environments

If you are experiencing these problems, you might want to regulate when the login attributes are updated. For information on how to do this, see Section 6.2.3, “Using the LoginInfo Command to Control LoginInfo Attributes When Attributes are Updated,” on page 36.

6.2.3 Using the LoginInfo Command to Control LoginInfo Attributes When Attributes are Updated

To control when login attributes are updated, execute the `nmas LoginInfo <num>` command.

The value for `<num>` is as follows:

- **0 or off:** Do not update any login attributes.
- **1:** Only update attributes that are required by intruder detection.
- **2:** Update all login attributes except unused user password policy attributes.
- **3 or on:** Update all login attributes.

For information on how to invoke the LoginInfo command for each NMAS Server platform, see Section 6.4, “Invoking NMAS Commands,” on page 39.

6.2.4 Using the sasUpdateLoginInfo and sasUpdateLoginTimeInterval Attribute

The `sasUpdateLoginInfo` attribute controls the updates of `LoginInfo` attributes.

The `sasUpdateLoginTimeInterval` attribute controls the update of the `Login Time` attribute of a user for a specified interval.

IMPORTANT: The Update Login Time Interval feature is available with eDirectory 8.8 SP7 Patch 3 and later. To enable this feature, a new attribute, `sasUpdateLoginTimeInterval`, is added to the NMAS schema. To use this feature with eDirectory 8.8 SP7 Patch 3, you must extend the `nmas.sch` file from the eDirectory schema. For more information, see Manually Extending the Schema in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

The `sasUpdateLoginInfo` attribute can have the following values:

- **0 or off:** Do not update any login attributes.
- **1:** Only update attributes that are required by intruder detection.
- **2:** Update all login attributes except unused user password policy attributes.
- **3 or on:** Update all login attributes.

The `sasUpdateLoginTimeInterval` attribute can have values from 0 to 1440 minutes (that is, one day).

- If the value is 0, the `Login Time` and `Last Login Time` attributes are updated for every successful login.
- If the value is between **1** and **1440** minutes, the `Login Time` attribute is updated after the specified interval. The Last Login Time attribute will not be updated.

NOTE: The `Login Time` attribute is not updated on consecutive successful logins during the interval. However, if there is a login failure during the interval followed by successful login, the `Login Time` attribute will be updated. The interval time from the successful login is counted.

The `sasUpdateLoginTimeInterval` attribute is effective only if the `sasUpdateLoginInfo` attribute value is set to 2 or 3.

The attributes can be specified for the following objects in the order of precedence (user having the highest precedence).

- User
- Container of the user
- Partition root
- Login Policy

If the `sasUpdateLoginInfo` and `sasUpdateLoginTimeInterval` are set on the Login Policy object, the setting becomes effective after the next policy refresh cycle. If the attributes are not set for the user, container, partition root, or Login Policy, the value set on a server using command line is used to maintain backward compatibility.

Following is an example to set the attribute values on the eDirectory server:

```
#cat nmas.config (The nmas.config file must be in the same directory as the dib
directory.)
nmas LoginInfo 2
nmas UpdateLoginTimeInterval 30
```

To set attributes value at the partition root:

1. To add the attributes to the Tree, go to **iManager** > **Schema** > **Add Attribute** > **Tree Root.**
2. Use the arrow to move the required attribute from **Available optional attribute** list to **Optional attribute** list.

To set the values of the attribute at partition root, run the `ldapmodify` command and the following commands at the command line or using an `ldif` file:

```
dn:T=< tree name>
changetype:modify
add:sasUpdateLoginTimeInterval
sasUpdateLoginTimeInterval:35

dn:T=< tree name>
changetype:modify
add:sasUpdateLoginInfo
sasUpdateLoginInfo: 2
```

You can edit the `sasUpdateLoginInfo` or `sasUpdateLoginTimeInterval` attribute values for user, container, and Login Policy objects using iManager or an `ldif` file.

Example:

```
#cat changesasUpdateLoginInfo.ldif
dn: cn=user1,o=org
change type: modify
replace: sasUpdateLoginInfo
sasUpdateLoginInfo: 1

#cat changesasUpdateLoginTimeInterval.ldif
dn: cn=user1,o=org
changetype: modify
replace: sasUpdateLoginTimeInterval
sasUpdateLoginTimeInterval: 60
```

The setting disables the update of `Login Time` attribute of user1 for 60 minutes from the previous update of the attribute.

To specify the `sasUpdateLoginInfo` and `sasUpdateLoginTimeInterval` attributes from iManager:

1. In NetIQ iManager, click the **Roles and Tasks** button 
2. Click **Directory Administration** > **Modify Object**.
3. Specify the name and context of a container or login policy object, then click **OK**.
4. On the **General** tab, select **Other** and then select **sasUpdateLoginTimeInterval** from **Unvalued Attributes** list.
5. Use the arrow button to move **sasUpdateLoginTimeInterval** from **Unvalued Attributes** list to the **Valued Attributes** list, then click **Apply**.

6.3 Setting Up NDSD_TRY_NMASLOGIN_FIRST

You must set `NDSD_TRY_NMASLOGIN_FIRST` to true to enable the NMAS login. This environment variable is available in eDirectory 8.8 and later versions. `NDSD_TRY_NMASLOGIN_FIRST` acts as a switch to enable or disable the NMAS-based login for LDAP authentication.

NOTE: NMAS-based login is slower compared to the traditional eDirectory login.

For more information on setting up `NDSD_TRY_NMASLOGIN_FIRST`, refer to the "How to Make Your Password Case-Sensitive" section in the *NetIQ eDirectory 8.8 SP8 What's New Guide*.

6.4 Invoking NMAS Commands

How you invoke an NMAS command differs depending on what platform you are running. The following platforms are supported:

- Section 6.4.1, "Windows," on page 39
- Section 6.4.2, "Linux," on page 39

6.4.1 Windows

When NMAS is started, it processes the commands in the `nmas.cfg` file. The `nmas.cfg` file must be in the same directory as the `dib` files, which are usually in `c:/novell/nds/dibfiles`.

or

After NMAS has been started, use the following procedure:

1. In the NetIQ eDirectory Services console, select `nmas.dlm`.
2. Type the command in the **Startup Parameters** field.
3. Click **Configure**.

6.4.2 Linux

When NMAS is started, it processes the commands in the `nmas.config` file. The `nmas.config` file must be in the same directory as the `dib` directory. For example, if the `.dib` directory path is `/var/opt/novell/eDirectory/data/dib`, then the `nmas.config` file path is `/var/opt/novell/eDirectory/data/nmas.config`.

6.5 Setting the Delay Time for Failed Login Attempts

1. Install the NMAS plug-in into iManager.

   The NMAS plug-in can be downloaded from the Novell Download site
2. In iManager, on the **Roles and Tasks** menu, click **Directory Administration > Modify Object**.
3. Browse for and select the Login Policy object, then click **OK**.
4. Click the **NMAS** tab, then click **Settings**.
5. Type the number of seconds you want the login screen to be delayed between failed login attempts, then click **OK**.

6.6 Using DSTrace

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

For information on how to capture an NMAS client trace, see TID # 3331372.

For information on how to capture an NMAS server trace, see TID # 3815371.

6.7 Disabling and Uninstalling the NMAS Client

To disable the NMAS Client:

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

To uninstall the NMAS Client, use the Add/Remove Programs option of the Windows Control Panel.

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

6.8 Disabling NMAS on the Server

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

On Windows with NetIQ eDirectory

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

On Linux

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

6.9 Auditing NMAS Events

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

- NetIQ Audit Secure Logging Server

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

Windows: `novell\nds`

Linux: `/opt/novell/eDirectory/lib/nds-schema` (relative to where eDirectory is installed)

For information on installing and managing NetIQ Audit, see the NetIQ Audit online documentation.

- NetIQ Sentinel

  For information on installing and managing NetIQ Sentinel, see the NetIQ Sentinel online documentation.

With either product, you also need to enable NMAS Audit by using the NMAS 3.3 or later plug-in for iManager.

1. Install the NMAS 3.3 or later plug-in into iManager.

   You can download the NMAS 3.3 or later plug-in from the Novell Download site
2. In iManager, on the **Roles and Tasks** menu, click **Directory Administration > Modify Object**.
3. Browse for and select the Login Policy object, then click **OK**.
4. Click the **NMAS** tab, then click **Settings**.
5. Click the box next to **Enable auditing**, then click **OK**.

6.9.1 Using External Certificates with NetIQ Audit

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

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

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

- Linux/UNIX: `/etc`
- Windows: the return from GetWindowsDirectory (typically `c:\windows`)

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

6.9.2 Using XDASv2 for Auditing NMAS Events

NMAS events can be audited using XDASv2.

1. Install the NMAS 3.3 or later plug-in into iManager.

   You can download the NMAS 3.3 or later plug-in from the Novell Download site
2. In iManager, on the **Roles and Tasks** menu, click **Directory Administration > Modify Object**.
3. Browse for and select the Login Policy object, then click **OK**.
4. Click the **NMAS** tab, then click **Settings**.
5. Click the box next to **Enable auditing**, then click **OK**.

When NMAS auditing is enabled, if both Platform Agent and XDASv2 modules are installed and configured, NMAS logs events to both Platform Agent and XDASv2. For detailed installation and configuration instructions on XDASv2, refer to the *NetIQ XDASv2 Administration Guide*.

7 Troubleshooting

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

7.1 NMAS Error Codes

A complete list of NMAS error codes can be found in the NMAS NDK.

7.2 Installation Issues

- When upgrading NMAS on a UNIX platform, you might be prompted to replace `libspmdclnt.so`. If this happens, answer Yes.
- If you uninstall the Novell Client, you must uninstall and reinstall the NMAS Client if it is used by another application.
- We strongly recommended that you upgrade NMAS to the latest version on all servers.
- You must have NMAS installed on a server that holds a writable replica of the user’s object in order for the user to use NMAS.
- You must have the Novell International Cryptographic Infrastructure (NICI) Client installed on each client workstation that will run the NMAS software.
- If you do not restart the server after installing NMAS and you try to reset passwords, you receive an error message.
- You should keep the login method up to date. The eDirectory UNIX/Linux and OES/Linux installs might not provide a way to upgrade the method.
- The `nmasinst` utility does not work on AIX. Therefore, use iManager as described in Section 2.1.2, “Using NetIQ iManager to Install a Login or Post-Login Method,” on page 18 or use other platforms, as described in Section 2.1.1, “Using the nmasinst Utility to Install a Login Method,” on page 17.

7.3 Login Method and Sequence Issues

- For products to use NMAS login methods properly, at least one NMAS 2.3 or later server in the eDirectory partition needs to hold a R/W replica of the User objects that will be using NMAS.
- Not all login or post-login methods use the initial password field when they are activated. If you are prompted to enter a password, you can ignore the password field and close it.
- Two password methods, such as Simple and NDS, cannot be used in an AND sequence if the Novell Client is set to display the password field, which is the default.

7.4 Administration Issues

- You must give explicit rights to users with graded authentication. Inherited rights do not work. For example, an administrator's Supervisor right is defined at the [Root] container. Rights for the administrator are not defined in the Volume object. If the administrator changes the volume's security label from Logged In to any other security label, the administrator cannot get the appropriate rights. The administrator must assign explicit rights to the volume, directories, or files in the volume.
- If Universal Password is enabled and you attempt to set the simple password, a -1697 error message is returned.
- eDirectory 8.7.3 utilities like DSBackup (ndsbackup), DSRepair (ndsrepair), and DSMerge (ndsmerge) work with NDS passwords alone but do not work with NMAS Simple password. eDirectory 8.8 uses Universal Password.

  For information on Universal Password, see the *NetIQ Password Management 3.3.2 Administration Guide* (https://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html).
- Clicking **OK** or switching between tabs when creating or renaming a label always creates or renames the label even if you respond **No** to the **Save Changes made for Labels?** prompt. You must click the **Cancel** button to cancel any changes. After a label is created, it cannot be deleted. However, you can rename it to an unused name, such as `Unused_x`.
- When you use XDAS auditing for NMAS, the DN format of the following events is not generated in the LDAP notation.
  - 00290035 SASL Mechanism Result
  - 00290061 Set Login Configuration
  - 00290062 Get Login Configuration
  - 00290064 Set Login Secret

NOTE: The ID (for example, 00290035 or 00290061) specifies the NMAS event ID as mentioned in the `lsc` file. The NMAS event ID is part of the `subEvent` field in the XDAS format.

A Security Considerations

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

A.1 Partner Login Methods

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

A.2 Login Policies

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

- Using the policy refresh rate command to check if the cached password policy needs to be refreshed on defined intervals instead of during each login causes a delay in the application of login policy changes.
- The `LoginInfo` command can be used to disable updating login-related attributes during login. These attributes include the intruder detection attributes. Disabling the update of these login-related attributes improves login performance. However, disabling the update of these attributes might lessen the security of the system.
- With NMAS 3.3 and later, the intruder detection policy can be set on the user object's direct container or on the user object's partition root. NMAS checks the parent container first for an intruder detection policy. If no policy is found, then the partition root is checked for an intruder detection policy.

A.3 NMASInst

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

Although nmasinst provides an option to specify the password on the command line, it is not recommended because the password could be compromised. With NMAS 8.8.8, nmasinst allows you to retrieve a password from either file or an environment variable.

A.4 Universal Password

- Because the Security container contains global policies, you should be careful where you place writable replicas. Some servers can modify the overall security policies specified in the eDirectory tree. In order for users to log in with NMAS, replicas of the User objects and security container must be on the NMAS server.
- If a Password policy is assigned to a container that is not a partition root, that policy is only effective for the user objects in the container, and not for user objects in subcontainers.
- If a Password policy is assigned to a container that is a partition root, that policy is effective for all users in the partition that do not have these values assigned to the user object or to the object's parent container.
- If a Password policy is assigned to a Login policy, that policy is effective for all users in the tree that do not have these values assigned to the user object, to the object's parent container, or to the object's partition root.
- When the NDS Password is migrated to the Universal Password during a user login, the password expiration time might be changed in the following circumstances:

  NOTE: This section only applies to NMAS 3.2*x* and earlier. For NMAS 3.3 and later, password expiration time is not updated when the NDS password is migrated to the Universal Password unless the "Verify whether existing passwords comply with the password policy (verification occurs on login)" password policy rule is set to "true".

  - If the password expiration time (calculated by adding the time that the NDS Password was set with the Password policy password expiration interval) is sooner than the user's current password expiration, the password expiration time is set to the calculated value.
  - If the password policy does not have a password expiration interval, the user's password expiration time attribute is removed.

- Password policies can be configured to allow the user or a password administrator to read the Universal Password by using documented NMAS LDAP extensions. These options should not be enabled unless required for your specific installation. If you require user passwords to be readable, you should configure the Password policy to only allow selected users to read the passwords.
- You should configure a password policy to synchronize to the Distribution Password only if Identity Manager Password Synchronization is being used to synchronize passwords between connected systems.

  For more information on sychronizing passwords between connected systems using Identity Manager Password Synchronization, see the *NetIQ Identity Manager 4.0.2 Password Management Guide*.
- You should only configure a password policy to synchronize to the Simple Password only if:
  - You have servers that hold a writable replica of user objects
  - Users access those servers using Native File Access Protocols such as CIFS and AFP.
- When advanced password rules are enabled for a password policy, the legacy password rules on the User object are ignored, and are updated to match the password policy rules when users change their passwords or log in.
- The password exclusion rules (password history, excluded passwords, and disallowed attribute vales) are not enforced when NMAS is used to generate random passwords.
- When selecting password rules, you should balance the requirements for hard-to-guess passwords with hard-to-remember passwords.
- When an administrator specifies that the NDS Password is to be removed, the result is that the NDS Password Hash is set to a random value that is unknown to anyone but eDirectory. There might or might not be a password value that could be hashed to that random value.
- XML Password Complexity
  - If there are duplicate rule tags, the most restrictive rule is used (others are ignored) for checking passwords against the policy and for random password generation.
  - The `ViolationsAllowed` and `NumberOfCharactersToEvaluate` rule set attributes are ignored for random password generation.
  - Only the first policy in an XML policy is used for random password generation.

For additional information on Universal Password security, see the *NetIQ Password Management 3.3.2 Administration Guide*.

A.5 SDI Key

You should make the Security Domain Infrastructure (SDI) key, also known as the tree key, a Triple DES key (3DES). The SDI key can be checked and upgraded by using the SDIDiag utility. See the "Step 4: Verify that Your SDI Domain Key Servers Are Ready for Universal Password" section in the *NetIQ Password Management 3.3.2 Administration Guide*.