

# **Administration Guide**

## **Password Management 3.3.2**

April 30, 2012

## Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2010-2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.  
1800 South Novell Place  
Provo, UT 84606  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation/).

## Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

## Third-Party Materials

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

---

# Contents

<b>About This Guide</b>	<b>5</b>
<b>1 Overview</b>	<b>7</b>
1.1 Universal Password Background . . . . .	7
1.1.1 How Secure Is Universal Password? . . . . .	8
1.2 Universal Password . . . . .	9
1.3 Password Policies . . . . .	9
1.4 Password Self-Service . . . . .	10
1.5 Password Synchronization . . . . .	10
<b>2 Deploying Universal Password</b>	<b>11</b>
2.1 Step 1: Review the Services You Currently Use and Understand their Current Password Limitations . . . . .	11
2.2 Step 2: Identify Your Need for Universal Password . . . . .	13
2.3 Step 3: Make Sure Your Security Container Is Available . . . . .	13
2.4 Step 4: Verify That Your SDI Domain Key Servers Are Ready for Universal Password . . . . .	14
2.5 Step 5: Upgrade at Least One Server in the Replica Ring to eDirectory 8.7.3 or Later . . . . .	15
2.6 Step 6: Check the Tree for SDI Key Consistency . . . . .	16
2.7 Step 7: Enable Universal Password . . . . .	16
2.8 Step 8: Deploy Novell Client Software . . . . .	17
2.9 Backward Compatibility . . . . .	17
2.10 Password Administration . . . . .	19
2.11 Issues to Watch For . . . . .	20
<b>3 Managing Passwords by Using Password Policies</b>	<b>23</b>
3.1 Overview of Password Policy Features . . . . .	23
3.2 Planning for Password Policies . . . . .	24
3.2.1 Planning How to Assign Password Policies in the Tree . . . . .	24
3.2.2 Planning the Rules for Your Password Policies . . . . .	24
3.2.3 Planning Login and Change Password Methods for your Users . . . . .	25
3.3 Prerequisite Tasks for Using Password Policies . . . . .	28
3.3.1 Re-Creating Universal Password Assignments . . . . .	30
3.4 Creating Password Policies . . . . .	31
3.4.1 Advanced Password Rules . . . . .	31
3.4.2 Modifying Password Policies Outside of the Password Policies Interface . . . . .	42
3.4.3 Random Password Generation . . . . .	42
3.4.4 Universal Password Configuration Options . . . . .	43
3.5 Assigning Password Policies to Users . . . . .	46
3.6 Finding Out Which Policy a User Has . . . . .	47
3.7 Setting A User's Password . . . . .	48
3.8 Troubleshooting Password Policies . . . . .	48
3.8.1 iManager Self-Service Login Requires Full DN . . . . .	48
3.8.2 Errors Indicate a Password Policy Is Not Assigned to a User . . . . .	49
3.8.3 Using Challenge Response Questions . . . . .	49
3.8.4 Giving Access to Users in New Containers . . . . .	49
3.8.5 NMAS LDAP Transport Error . . . . .	49

<b>4</b>	<b>Password Self-Service</b>	<b>51</b>
4.1	Overview of Password Self-Service . . . . .	51
4.2	Prerequisites for Using Password Self-Service . . . . .	52
4.3	Managing Forgotten Passwords . . . . .	52
4.3.1	Enabling Forgotten Password . . . . .	53
4.3.2	Creating or Editing Challenge Sets . . . . .	54
4.3.3	Selecting a Forgotten Password Action . . . . .	57
4.3.4	Disabling Password Hint by Removing the Hint Gadget . . . . .	59
4.3.5	Configuring Forgotten Password Self-Service . . . . .	60
4.3.6	What Users See When They Forget Passwords . . . . .	64
4.4	Providing Users with Password Reset Self-Service . . . . .	67
4.5	Adding a Password Change Message . . . . .	67
4.6	Configuring E-Mail Notification for Password Self-Service . . . . .	68
4.6.1	Prerequisites . . . . .	69
4.6.2	Setting Up the SMTP Server to Send E-Mail Notification . . . . .	69
4.6.3	Setting Up E-Mail Templates for Notification . . . . .	70
4.7	Testing Password Self-Service . . . . .	70
4.8	Adding Password Self-Service to Your Company Portal . . . . .	71
4.8.1	Integrating Password Self-Service with Virtual Office . . . . .	72
4.8.2	Linking to Password Self-Service from a Company Portal . . . . .	73
4.8.3	Making Sure Users Have Configured Password Features . . . . .	76
4.9	Troubleshooting Password Self-Service . . . . .	76
<b>A</b>	<b>Security Considerations</b>	<b>77</b>

---

# About This Guide

This guide provides information on how to manage passwords on Novell systems. It includes instructions on how to deploy, configure, and manage Universal Password, password policies, and password self-service.

- ♦ Chapter 1, “Overview,” on page 7
- ♦ Chapter 2, “Deploying Universal Password,” on page 11
- ♦ Chapter 3, “Managing Passwords by Using Password Policies,” on page 23
- ♦ Chapter 4, “Password Self-Service,” on page 51

## Audience

This guide is written primarily for network administrators.

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

## Documentation Updates

For the most recent version of the *Password Management Administration Guide*, visit the [Password Management Documentation Web site \(http://www.novell.com/documentation/password\\_management33/index.html\)](http://www.novell.com/documentation/password_management33/index.html).



---

# 1 Overview

This section provides an overview of Universal Password, password policies, and password self-service.

- ♦ [Section 1.1, “Universal Password Background,” on page 7](#)
- ♦ [Section 1.2, “Universal Password,” on page 9](#)
- ♦ [Section 1.3, “Password Policies,” on page 9](#)
- ♦ [Section 1.4, “Password Self-Service,” on page 10](#)
- ♦ [Section 1.5, “Password Synchronization,” on page 10](#)

## 1.1 Universal Password Background

Universal Password is managed by the Secure Password Manager, a component of the Novell Modular Authentication Services (NMAS) module. The Secure Password Manager simplifies the management of password-based authentication schemes across a wide variety of Novell products as well as Novell partner products. The management tools expose only 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 an eDirectory 8.7.3 or later installation. 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:** Password Management 2.02, a plug-in for Novell eDirectory for iManager 2.x, is available for download at the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com). Minimum requirements are eDirectory 8.7.3 or later and iManager 2.02 or later. Information on how to download and install this plug-in is available on the download site.

---

Novell Client software supports the Universal Password. It also continues to support the NDS password for older systems in the network. After Universal Password has been configured and enabled for a user, the Novell Client has the capability of automatically upgrading/migrating the NDS password to the Universal Password.

## 1.1.1 How Secure Is Universal Password?

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

A Universal Password is protected by three levels of security:

- ♦ triple DES encryption of the password itself
- ♦ eDirectory rights
- ♦ file system rights

The Universal Password is encrypted by a triple DES, user-specific key. Both the Universal Password and the user key are stored in system attributes that only eDirectory can read. The user key (3DES) is stored encrypted with the tree key, and the tree key is protected by a unique Novell International Cryptographic Infrastructure (NICI) key on each machine. Note that neither the tree key nor the NICI key is stored within eDirectory. They are not stored with the data they protect.

The tree key is present on each machine within a tree, but each tree has a different tree key. So, data encrypted with the tree key can be recovered only on a machine within the same tree. Thus, while stored, the Universal Password is protected by three layers of encryption.

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

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

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

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

---

<b>Platform</b>	<b>Directories/Files</b>
Windows	<ul style="list-style-type: none"><li>♦ <code>\system32\novell\nici</code></li><li>♦ <code>\system32\</code> where the NICI DLL is installed</li></ul>
Linux/UNIX	<ul style="list-style-type: none"><li>♦ <code>/var/novell/nici</code></li><li>♦ <code>etc/nici.cfg</code></li><li>♦ <code>/usr/local/lib/libccs2.so</code> and the NICI shared libraries in the same directory</li></ul> <p>On LSB-compliant systems, the above mentioned directories and files as well as the following files:</p> <ul style="list-style-type: none"><li>♦ <code>/var/opt/novell/nici</code></li><li>♦ <code>etc/opt/novell</code></li><li>♦ <code>/opt/novell/lib</code></li></ul>

---



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

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

## 1.2 Universal Password

In the past, administrators have needed 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 nonreversible. 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 nds-cluster-config 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 is no longer supported by Novell. The enhanced password is the forerunner of Universal Password. It offers some password policy, but its design is not consistent with other passwords. It provides a one-way synchronization and it replaces the simple or NDS password.

Novell introduced Universal Password as a way to simplify the integration and management of different password and authentication systems into a coherent network.

Universal Password addresses these password problems by doing the following:

- ♦ Providing one password for all access to eDirectory.
- ♦ Enabling the use of extended characters in passwords.
- ♦ Enabling advanced password policy enforcement.
- ♦ Allowing synchronization of passwords from eDirectory to other systems.

Most features of password management require Universal Password to be enabled.

For detailed information, see [Chapter 2, “Deploying Universal Password,”](#) on page 11.

## 1.3 Password Policies

Universal Password provides the ability to create advanced password policies. A password policy is a collection of administrator-defined rules that specify the criteria for creating and replacing end user passwords. NMAS allows you to enforce password policies that you assign to users in Novell eDirectory.

You manage password policies by using iManager.

For more information, see [Chapter 3, “Managing Passwords by Using Password Policies,”](#) on page 23.

## 1.4 Password Self-Service

Password Self-Service enables users to do the following:

- ◆ Recover from forgotten passwords

This service reduces calls to the help desk when users forget passwords.

- ◆ Reset passwords

Users change their passwords while viewing the rules that you have specified in the password policy.

You manage the policy for password self-service by using iManager. Users access the password self-service features in several ways, including the Novell Client, the iManager portal, and the Identity Manager User Application.

The Password Self-Service features were removed from iManager 2.6 and later, so in order for users to use the self-service features, you must have a server running iManager 2.0.2. Users go to this server's portal ([https://www.my\\_iManager\\_server.com/nps](https://www.my_iManager_server.com/nps)) to access the self-service features.

For more information, see [Chapter 4, "Password Self-Service,"](#) on page 51.

## 1.5 Password Synchronization

Password synchronization across connected systems is a feature included with Novell Identity Manager 2.0 and later. It provides the following benefits:

- ◆ Bidirectional password synchronization
- ◆ Enforcement of Password Policies on connected systems
- ◆ E-mail notification when synchronization fails
- ◆ The ability to check password synchronization status for a user

For more information, see Chapter 3, "[Connected System Support for Password Synchronization](http://www.novell.com/documentation/idm401/idm_password_management/data/bo1o7xz.html)" in the *Novell Identity Manager 4.0.1 Password Management Guide* ([http://www.novell.com/documentation/idm401/idm\\_password\\_management/data/front.html](http://www.novell.com/documentation/idm401/idm_password_management/data/front.html)).

---

# 2 Deploying Universal Password

This section describes how to deploy and manage Universal Password.

Follow the instructions in sections 2.1 through 2.8 to deploy Universal Password:

- ◆ [Section 2.1, “Step 1: Review the Services You Currently Use and Understand their Current Password Limitations,” on page 11](#)
- ◆ [Section 2.2, “Step 2: Identify Your Need for Universal Password,” on page 13](#)
- ◆ [Section 2.3, “Step 3: Make Sure Your Security Container Is Available,” on page 13](#)
- ◆ [Section 2.4, “Step 4: Verify That Your SDI Domain Key Servers Are Ready for Universal Password,” on page 14](#)
- ◆ [Section 2.5, “Step 5: Upgrade at Least One Server in the Replica Ring to eDirectory 8.7.3 or Later,” on page 15](#)
- ◆ [Section 2.6, “Step 6: Check the Tree for SDI Key Consistency,” on page 16](#)
- ◆ [Section 2.7, “Step 7: Enable Universal Password,” on page 16](#)
- ◆ [Section 2.8, “Step 8: Deploy Novell Client Software,” on page 17](#)
- ◆ [Section 2.9, “Backward Compatibility,” on page 17](#)
- ◆ [Section 2.10, “Password Administration,” on page 19](#)
- ◆ [Section 2.11, “Issues to Watch For,” on page 20](#)

## 2.1 Step 1: Review the Services You Currently Use and Understand their Current Password Limitations

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

**Table 2-1** Password Limitations

Service	Description	Limitations
Novell Client for Windows* NT*/2000/XP versions earlier than 4.9 and Novell Client for Windows 95/98 versions earlier than 3.4.	The Novell Client software for file and print services. It uses the NDS password, which is based on the RSA public/private key system.	<ul style="list-style-type: none"><li>◆ Has limited support for passwords with extended characters</li><li>◆ Passwords are inaccessible from non-Novell systems</li><li>◆ Passwords are stored in a way that prevents extraction, thus disallowing interoperability with the simple password</li></ul>

<b>Service</b>	<b>Description</b>	<b>Limitations</b>
Windows Native Networking (CIFS) in NetWare 6 and NetWare 5.1 (NFAP add-on pack for NetWare 5.1)	Novell's CIFS server as part of the Native File Access Protocols. It allows Windows clients to access Novell services by using the built-in Windows Client Networking Services.	<ul style="list-style-type: none"> <li>◆ Uses a separately administered password called the simple password</li> <li>◆ Has no expiration or restriction capabilities for the simple password</li> <li>◆ Attempts to synchronize with NDS password but can get out of sync</li> </ul>
Macintosh Native Networking (AFP) in NetWare 6 and NetWare 5.1 (NFAP add-on pack for NetWare 5.1)	Novell's AFP server as part of the Native File Access Protocols. It allows Macintosh clients to access Novell services by using the built-in Macintosh Client Networking Services.	<ul style="list-style-type: none"> <li>◆ Uses a separately administered password called the simple password</li> <li>◆ Has no expiration or restriction capabilities for the simple password</li> <li>◆ Attempts to synchronize with the NDS password but can get out of sync</li> </ul>
nds-cluster-config	Novell's nds-cluster-config services allow a user to bind using a user name and password across a Secure Sockets Layer (SSL) connection.	<ul style="list-style-type: none"> <li>◆ Limited interoperability with Novell Client services (NDS password) for extended character or international versions</li> <li>◆ First tries the NDS password, then attempts to utilize the simple password if the bind is not a simple bind. If the bind is not a simple bind, the bind is using an encrypted password.</li> </ul>
nds-cluster-config User Import	Uses ICE or other tools to import users from foreign directories into eDirectory. Passwords are also brought in.	<ul style="list-style-type: none"> <li>◆ Passwords are imported into the simple password</li> <li>◆ Mutually exclusive of NFAP solutions (Windows and Macintosh Native File Access) if it is not a clear text password</li> <li>◆ Password is in its digested/hashed native format</li> </ul>
Web-Based Services	Novell Web-based services (Apache Web server) authentications. This includes eGuide, Novell Portal Services, and other Web-based applications.	<ul style="list-style-type: none"> <li>◆ Limited interoperability with Novell Client services (NDS password) for extended character or international versions</li> <li>◆ Not designed to check the simple password</li> </ul>
RADIUS Services	Novell RADIUS Authentication Services.	<ul style="list-style-type: none"> <li>◆ Limited interoperability with the Novell Client services (NDS password) for extended character or international versions</li> </ul>
NetWare Remote Manager	Novell's Web-based server health and management interface.	<ul style="list-style-type: none"> <li>◆ Limited interoperability with Novell Client services (NDS password) for extended character or international versions</li> <li>◆ Not designed to check the simple password</li> </ul>

Service	Description	Limitations
DirXML Password Synchronization for Windows 1.0 and DirXML Starter Pack	Enables synchronization of passwords for NT, Active Directory, and eDirectory accounts.	<ul style="list-style-type: none"> <li>eDirectory password changes made outside of the Novell Client are not synchronized. For example, an eDirectory password change made through eGuide would not be synchronized to Active Directory or NT.</li> </ul> <p>See “<a href="http://www.novell.com/documentation/ig/dirxmlstarterpack/jetset/data/aktnwz0.html">Sample Password Scenarios</a>” (<a href="http://www.novell.com/documentation/ig/dirxmlstarterpack/jetset/data/aktnwz0.html">http://www.novell.com/documentation/ig/dirxmlstarterpack/jetset/data/aktnwz0.html</a>) in the <i>DirXML Starter Pack Installation Guide</i> for detailed information about DirXML Password Synchronization for Windows.</p>

## 2.2 Step 2: Identify Your Need for Universal Password

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

- Do you currently use Native File Access and desire to enforce policies such as password expiration or password length?
- Do you use or plan to use Native File Access (Windows or Macintosh)?
- Do you plan to have international users access Novell Web-based services or use the Novell Client for Windows to access Novell file and print services?
- Do you plan to use Novell Identity Manager 2 or 3, with its enhanced password policy and password synchronization capabilities?

## 2.3 Step 3: Make Sure Your Security Container Is Available

NMAS relies on storing global policies to the eDirectory tree, which 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 the [Root] partition. 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.

eDirectory 8.8 provides security container caching. This feature caches the security container data on local servers so NMAS doesn't need to access the Security container with every attempted login. See the “[Security Object Caching](http://www.novell.com/documentation/edir88/edir88new/data/bwpla84.html)” (<http://www.novell.com/documentation/edir88/edir88new/data/bwpla84.html>) section in the *Novell eDirectory 8.8 SP7 Administration Guide* for more information.

With NMAS and eDirectory 8.8.x, 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.

---

**WARNING:** Because the Security container contains global policies, be careful where writable replicas are placed, because these servers can modify the overall security policies specified in the eDirectory tree. In order for users to log in with NMAS, replicas of the User objects and security container must be on the NMAS server.

---

For additional information, see [Novell TID3393169 \(http://www.novell.com/support/viewContent.do?externalId=3393169\)](http://www.novell.com/support/viewContent.do?externalId=3393169).

## 2.4 Step 4: Verify That Your SDI Domain Key Servers Are Ready for Universal Password

You must verify that the SDI Domain Key servers meet minimum configuration requirements and have consistent keys for distribution and use by other servers within the tree. These steps are crucial. If you don't follow them as outlined, you could cause serious password issues on your system when you turn on Universal Password.

We recommend that eDirectory 8.7.3 or later be installed on your SDI Domain Key servers.

- 1 At a Windows server command prompt, run `sdidiag.exe`.

`sdidiag.exe` ships with the Windows version of eDirectory 8.7.3 or later. The file is available as part of a security patch (`sdidiag22.exe`) associated with [Novell TID 2974092 \(http://support.novell.com/docs/Readmes/InfoDocument/2974092.html\)](http://support.novell.com/docs/Readmes/InfoDocument/2974092.html).

- 2 Log in as an Administrator by entering the server (full context), the tree name, the user name, and the password.
- 3 Check to make sure all your servers are using 168-bit keys.

Follow the instructions in [Novell TID 3364214 \(http://www.novell.com/support/viewContent.do?externalId=3364214\)](http://www.novell.com/support/viewContent.do?externalId=3364214) to ensure that this requirement is met.

- 4 Enter the command `CHECK -v >> installation folder\sdi notes.txt`.

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

- 5 If no problems are found, go to “[Step 5: Upgrade at Least One Server in the Replica Ring to eDirectory 8.7.3 or Later](#)” on page 15.

or

Follow the instructions written to the `installation folder\sdi notes.txt` file to resolve any configuration and key issues, then continue with [Step 6](#).

- 6 Verify that the SDI Domain Key Servers are running NICI 2.6.x or later.

The version must be 264xx.xx or later.

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

- ♦ Update the servers' NICI to version 2.6.x, which requires eDirectory 8.7.3 or later.

You can download NICI from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com). Select *NICI* from the Product or Technology drop-down list, then click *Search*.

- ◆ Update the SDI Domain Key servers to eDirectory 8.7.3 or later.
  - ◆ Remove the servers as SDI Domain Key Servers and add an eDirectory 8.7.3 or later server. See [Section 2.5, “Step 5: Upgrade at Least One Server in the Replica Ring to eDirectory 8.7.3 or Later,”](#) on page 15.
- 7 (Optional) After completing one of the options above, you might want to re-run the SDIDIAG CHECK command. See [Step 4](#).

For more information on using SDIDIAG, see [Novell TID 3364214 \(http://www.novell.com/support/viewContent.do?externalId=3364214\)](http://www.novell.com/support/viewContent.do?externalId=3364214).

## Adding or Removing an SDI Domain Key Server

To remove a server as an SDI Domain Key Server, complete the following procedure:

- 1 At a Windows server, open a command prompt box and run `sdidiag.exe`.  
`sdidiag.exe` ships with the Windows version of eDirectory 8.7.3 or later. The file is available as part of a security patch (`sdidiag22.exe`) associated with [Novell TID 2966746 \(http://support.novell.com/docs/Readmes/InfoDocument/2974092.html\)](http://support.novell.com/docs/Readmes/InfoDocument/2974092.html).
- 2 Log in as an administrator with management rights over the Security container and the W0.KAP.Security objects by entering the server (full context), the tree name, the user name, and the password.
- 3 Enter the command `RS -s servername`.  
 For example, if `server1` exists in container `PRV` in the organization `Novell` within the `Novell_Inc` tree, you would type `.server1.PRV.Novell.Novell_Inc` for the `servername`.

To add a server as an SDI Domain Key Server, complete the following procedure:

- 1 From a Windows server, open a command prompt box and run `sdidiag.exe`.
- 2 Log in as an Administrator by entering the server (full context), the tree name, the user name, and the password.
- 3 Enter the command `AS -s servername`.  
 For example, if `server1` exists in container `PRV` in the organization `Novell` within the `Novell_Inc` tree, you would type `.server1.PRV.Novell.Novell_Inc` for the `servername`.

## 2.5 Step 5: Upgrade at Least One Server in the Replica Ring to eDirectory 8.7.3 or Later

- 1 Identify the container that holds the User objects of those users who will be using Universal Password.
- 2 Find the partition that holds that container and the User objects.
- 3 Identify at least one server that holds a writable replica of the partition.
- 4 Upgrade that server to eDirectory 8.7.3 or later.

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

## 2.6 Step 6: Check the Tree for SDI Key Consistency

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

- 1 At a Windows server command prompt, run `sdidiag.exe`.
- 2 Enter the command `CHECK -v >> sys\system\sdi notes.txt -n container DN`.

For example, if user Bob exists in container USR in the organization Acme within the Acme\_Inc tree, you would type `.USR.Acme.Acme_Inc.` for the container distinguished name (DN).

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

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

- 3 If no problems are reported, you are ready to enable Universal Password. Go to “[Step 7: Enable Universal Password](#)” on page 16.

or

If problems are reported, follow the instructions in the `sdi notes.txt` file.

In most cases, you are prompted to run the command `RESYNC -T`. This command can be repeated any time NMA reports -1418 or -1460 errors during authentication with Universal Password.

For more information on SDIDIAG options and operations, refer to the following:

- ♦ [Novell TID 3364214](http://www.novell.com/support/viewContent.do?externalId=3364214) (<http://www.novell.com/support/viewContent.do?externalId=3364214>)
- ♦ [Novell TID 7005397](http://www.novell.com/support/viewContent.do?externalId=7005397) (<http://www.novell.com/support/viewContent.do?externalId=7005397>)

## 2.7 Step 7: Enable Universal Password

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

---

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

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

---



## 2.8 Step 8: Deploy Novell Client Software

You can deploy the Novell Client for Windows version 4.91, but the client does not take advantage of these services until you enable Universal Password on the server. For more information about enabling Universal Password, see “[Step 7: Enable Universal Password](#)” on page 16.

Once the Universal Password is enabled, the Novell Client 4.9.1 and later for Windows automatically starts using the Universal Password. Users see no differences in the client, except with case-sensitive passwords.

---

**NOTE:** Novell Client 4.9.1 includes the NMAS Client.

---

## 2.9 Backward Compatibility

Universal Password is designed to supply backward compatibility to existing services. By default, passwords changed with this service can be synchronized to the simple and NDS passwords on the User object. You can choose which passwords you want to have synchronized by using the Password Management plug-in. This way, Novell Client software earlier than the Novell Client for Windows version 4.9 or the Novell Client for Windows version 3.4, which don't take advantage of NMAS, have their passwords continue to function properly.

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

The Novell NetWare Storage Management Services (SMS) infrastructure is used for Novell and third-party backup and restore applications. Additionally, the Novell Server Consolidation utility, Distributed File Services Volume Move, and Server Migration utilities use SMS as their data management infrastructure. The system passwords used by these Novell and third-party products cannot contain extended characters if they are to function in a mixed environment.

---

**NOTE:** Refer to [Novell TID 3065822 \(http://www.novell.com/support/viewContent.do?externalId=3065822\)](http://www.novell.com/support/viewContent.do?externalId=3065822) to see which applications and services are Universal Password-capable, as well as which applications and services are extended character-capable. Many applications and services can use extended characters without Universal Password.

---

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

**Table 2-2** Behavior of Enabled Universal Password

---

Password Change Method	Passwords Changed
Novell Client software earlier than Novell Client for Windows NT/2000/XP version 4.9 or Novell Client for Windows 95/98 version 3.4 to any server version	NDS password only.

---

<b>Password Change Method</b>	<b>Passwords Changed</b>
Native File Access (Windows or Macintosh) on NetWare 5.1 or NetWare 6	Simple password and NDS password. The password change is successful only if the old NDS and simple passwords were in sync.
Native File Access (Windows or Macintosh) on NetWare 6.5	Universal, simple, and NDS passwords are changed. All are synchronized, even if old ones were out of sync, if the configuration allows for synchronization, and the password policy is configured to allow changes to NDS and simple passwords.
nds-cluster-config (standard) earlier than eDirectory 8.7.3	NDS password only.
nds-cluster-config (extended) earlier than eDirectory 8.7.3	Simple password or NDS password is changed. Extensions specify which password is changed. Simple password change results in a -1697 failure.
nds-cluster-config (standard) to NetWare 6.5 (or NetWare 5.1 or 6 running eDirectory 8.7.3)	Universal, simple, and NDS passwords are changed. All are synchronized even if old ones were out of sync, if the password policy is configured to allow changes to NDS and simple passwords.
nds-cluster-config (extended) to NetWare 6.5	Universal, simple, or NDS password changed. Extensions specify which password is changed. This only applies if the password policy is configured to allow changes to NDS and simple passwords.
NetWare Administrator (run on a workstation with a client earlier than version 4.9) to any User object in any container	NDS password only.
NetWare Administrator (run on a workstation with the version 4.9 client) to a User object in a container that has a R/W replica on a NetWare 6.5 server (or NetWare 5.1 or 6 running eDirectory 8.7.3)	(Untested and unsupported) Universal, simple, and NDS passwords are changed. All are synchronized even if old ones were out of sync.
ConsoleOne® (run on a workstation with a client earlier than version 4.9) to any User object in any container	There are separate change password pages for the NDS password and the simple password.
ConsoleOne (run on a workstation with the version 4.9 client) with the NMAS client installed and enabled to a User object in a container that has a R/W replica on a NetWare 6.5 server (or NetWare 5.1 or 6 running eDirectory 8.7.3)	Universal, simple, and NDS passwords are changed. All are synchronized even if old ones were out of sync (if the password policy is configured to allow changes to NDS and simple passwords).
ConsoleOne (run on a workstation with the version 4.9 client) to a User object in a container that has no R/W replicas on any NetWare 6.5 servers, or NetWare 5.1 or 6 with eDirectory 8.7.3 (only R/W replicas on NetWare 5.1 or NetWare 6 servers with eDirectory versions earlier than 8.7.3)	There are separate change password pages for the NDS password and the simple password.
Novell iManager 1.5 (NetWare 5.1 or NetWare 6 only) to any User object in any container	NDS password only.

Password Change Method	Passwords Changed
Novell iManager 2.0 (NetWare 6.5 only) to a User object in a container that has a R/W replica on a NetWare 6.5 server (or NetWare 5.1 or 6 running eDirectory 8.7.3)	Universal, simple, and NDS passwords are changed. All are synchronized even if old ones were out of sync, if the password policy is configured to allow changes to NDS and simple passwords.
Novell iManager 2.0 (NetWare 6.5 only) to a User object in a container that does not have any R/W replica on any NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 8.7.3	NDS password only.
Novell Remote Manager running on a NetWare 6.5 server to a User object in a container that has a R/W replica on a NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 8.7.3	Universal, simple, and NDS passwords are changed. All are synchronized, even if old ones were out of sync, if the password policy is configured to allow changes to NDS and simple passwords.
Novell Remote Manager running on a NetWare 6.5 server to a User object in a container that does not have a R/W replica on a NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 8.7.3	NDS password only.
Novell Remote Manager NDS change password running on a NetWare 5.1 or NetWare 6 server	NDS password only.
Novell Remote Manager simple password management (NetWare 5.1 and 6 only with Native File Access installed)	Simple password only.

## 2.10 Password Administration

You can use the following methods to administer Universal Password:

- ♦ **iManager (Recommended):** Administering passwords by using Novell iManager automatically sets the Universal Password to be synchronized to simple and NDS password values for backward compatibility. The NMAS task in iManager does allow for granular management of individual passwords and authentication methods that are installed and configured in the system.

In iManager using the Password Management plug-in, you can use password policies to specify how Universal Password is synchronized with NDS, simple, and distribution passwords. In addition, an iManager task is provided that lets an Administrator set a user's Universal Password.

- ♦ **ConsoleOne:** The *NDS Password* tab in ConsoleOne on a Windows workstation with the Novell Client for Windows version 4.9/4.91 installed, automatically sets the Universal Password and synchronizes other passwords for backward compatibility.
- ♦ **nds-cluster-config:** Changing passwords via `nds-cluster-config` on a NetWare 6.5 server also sets the Universal Password and synchronizes other passwords for backward compatibility.
- ♦ **Third-party Applications:** Third-party applications that are written to Novell Cross-Platform Libraries and that perform password management also set the Universal Password and synchronize other passwords if the newer libraries are installed on the Novell Client for Windows version 4.9/4.9.1 workstation or NetWare 6.5 server.

## 2.11 Issues to Watch For

- ◆ In a mixed environment of Novell Client software earlier than the Novell Client for Windows NT/2000/XP version 4.9 or the Novell Client for Windows 95/98 version 3.4 (including Native File Access servers on NetWare 5.1 and NetWare 6), if passwords are changed from those older systems, only the older values are changed, so the NDS or the simple password is out of synchronization with the Universal Password.

This might be an issue only for users who log in to their accounts from both older Novell Client workstations, earlier than Client for Windows NT/2000/XP version 4.9 or Novell Client for Windows 95/98 v3.4, and from newer Novell Client workstations, Novell Client for Windows NT/2000/XP version 4.9 or Novell Client for Windows 95/98 version 3.4. If so, the problem occurs only if users either use international characters in passwords or if they change the password from the older workstation.

---

**NOTE:** Novell Client has not yet been updated to work with the latest password-management features and Windows Server 2008 Password Policy policies.

---

- ◆ When you disable a user's NDS password, the NDS password is set to an arbitrary value that is unknown to the user. The following list describes how some login methods handle this change:
  - ◆ The simple password method is not disabled if the NDS password is disabled. The simple password method uses the Universal Password if it is enabled and available. Otherwise, it uses the simple password. If Universal Password is enabled but not set, then the simple password method sets the Universal Password with the simple password.
  - ◆ The enhanced password method is not disabled when the NDS password is disabled. The enhanced password does not use the Universal Password for login.
  - ◆ The NDS password method (Universal Password) is not disabled when the NDS password is disabled. The NDS password method uses the Universal Password if it is enabled and available. Otherwise, it uses the NDS password. If the Universal Password is enabled but not set, then the NDS Password method sets the Universal Password with the NDS password.
- ◆ A security enhancement was added to NMAS 2.3.4 regarding Universal Passwords changed by an administrator. It works the same way as the feature previously provided for NDS password. If an administrator changes a user's password, such as when creating a new user or in response to a help desk call, for security reasons the password is automatically expired if you have enabled the setting to expire passwords in the password policy. This is the *Number of days before password expires (0-365)* setting in the password policy under *Advanced Password Rules*. For this particular feature, the number of days is not important, but the setting must be enabled.

---

**NOTE:** With NMAS 3.1.3 and later, this behavior can be overwritten in the password policy by selecting the *Do not expire the user's password when the administrator sets the password* option.

---

- ◆ Prior to NMAS 3.1, NDS password settings are replaced when password policies are changed. If you create a password policy and enable Universal Password and enable Advanced Password Rules, the Advanced Password Rules are enforced instead of any existing password settings for NDS password. The legacy password settings are ignored. No merging or copying of previous settings is done automatically when you create password policies.

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

NMAS 3.1 and later replaces the NDS password setting on the user object with corresponding password policy settings. For example, if the number of grace logins for the user object is 4, and it is 5 for the password policy, when the user logs in or changes the password, the number of grace logins for the user object changes to 5.



---

# 3 Managing Passwords by Using Password Policies

You can use password policies to increase security by setting rules for how users create their passwords. You can also decrease help desk costs by providing users with self-service options for forgotten passwords and for resetting passwords.

The following is discussed in this section:

- ◆ [Section 3.1, “Overview of Password Policy Features,” on page 23](#)
- ◆ [Section 3.2, “Planning for Password Policies,” on page 24](#)
- ◆ [Section 3.3, “Prerequisite Tasks for Using Password Policies,” on page 28](#)
- ◆ [Section 3.4, “Creating Password Policies,” on page 31](#)
- ◆ [Section 3.5, “Assigning Password Policies to Users,” on page 46](#)
- ◆ [Section 3.6, “Finding Out Which Policy a User Has,” on page 47](#)
- ◆ [Section 3.7, “Setting A User's Password,” on page 48](#)
- ◆ [Section 3.8, “Troubleshooting Password Policies,” on page 48](#)

For information on Forgotten Password Self-Service and Reset Password Self-Service, see [Chapter 4, “Password Self-Service,” on page 51](#).

## 3.1 Overview of Password Policy Features

A password policy is a collection of administrator-defined rules that specify the criteria for creating and replacing end-user passwords. NMAS enables you to enforce password policies that you assign to users in Novell eDirectory.

Password policies can also include Forgotten Password Self-Service features, to reduce help desk calls for forgotten passwords. Another self-service feature is Reset Password Self-Service, which lets users change their passwords while viewing the rules the administrator has specified in the password policy. Users access these features through the Identity Manager User Application or iManager self-service console.

---

**NOTE:** The iManager self-service console is available only with iManager 2.0.2.

---

Using a password policy requires you to enable Universal Password for your users if you want to use advanced password rules, password synchronization, and many of the Forgotten Password features. For information on deploying Universal Password, see [Chapter 2, “Deploying Universal Password,” on page 11](#).

You create password policies by using the Password Policy Wizard. In iManager, click *Passwords > Password Policies > New*. For more information on creating password policies, see [Section 3.4, “Creating Password Policies,”](#) on page 31.

## 3.2 Planning for Password Policies

- ♦ [Section 3.2.1, “Planning How to Assign Password Policies in the Tree,”](#) on page 24
- ♦ [Section 3.2.2, “Planning the Rules for Your Password Policies,”](#) on page 24
- ♦ [Section 3.2.3, “Planning Login and Change Password Methods for your Users,”](#) on page 25

### 3.2.1 Planning How to Assign Password Policies in the Tree

We recommend that you assign a default policy to the whole tree and assign any other policies you use as high up in the tree as possible, to simplify administration.

NMAS determines which password policy is in effect for a user. See [Section 3.5, “Assigning Password Policies to Users,”](#) on page 46 for more information.

### 3.2.2 Planning the Rules for Your Password Policies

You can use the Advanced Password Rules in a password policy to enforce your business policies for passwords.

Keep in mind that the Novell Client (4.9 SP2), Identity Manager User Application, and the iManager self-service console (iManager 2.0.2 or later) display the password rules from the password policy. If your users will be changing their passwords through the LDAP server or on a connected system, you need to make the password rules readily available to users to help them be successful in creating a compliant password.

If you are using Identity Manager Password Synchronization, keep in mind that you must make sure that the users who are assigned password policies match with the users you want to participate in Password Synchronization for connected systems. Password policies are assigned with a tree-centric perspective. By contrast, Password Synchronization is set up per driver, on a per-server basis. To get the results you expect from Password Synchronization, make sure the users that are in a read/write or master replica on the server running the drivers for Password Synchronization match with the containers where you have assigned password policies with Universal Password enabled. Assigning a password policy to a partition root container ensures that all users in that container and subcontainers are assigned the password policy.

#### Advanced Password Rules

Advanced Password Rules let you define the following criteria for the Universal Password:

- ♦ The lifetime of a password: Password policies provide the same policy features eDirectory has offered in the past, so you can specify how often a password must be changed and whether it can be reused.
- ♦ What a password contains: You can require a combination of letters, numbers, uppercase or lowercase letters, and special characters. You can exclude passwords that you don't feel are secure, such as your company name. You can also require a certain number of characters in a password be “new,” unused in previous passwords, and configure the number of password policy violations allowed in a specified password.



To use Advanced Password Rules in a password policy, you must enable Universal Password. If you don't enable Universal Password for a policy, the password restrictions set for the NDS<sup>®</sup> password are enforced instead.

---

**NOTE:** When you create a password policy and enable Universal Password, the Advanced Password Rules are enforced, instead of any existing password settings for NDS Password. The legacy password settings are ignored. No merging or copying of previous settings is done automatically when you create password policies.

For example, if you have a setting for the number of grace logins that you use with the NDS Password, when you enable Universal Password you need to re-create the grace logins setting in the Advanced Password Rules in the password policy.

If you later disable Universal Password in the password policy, the existing password settings that you had are no longer ignored. They would be enforced for the NDS password.

NMAS 3.1 and later replaces the NDS password setting on the user object with corresponding password policy settings. For example, if the number of grace logins for the user object is 4, and it is 5 for the password policy, when the user logs in or changes the password, the number of grace logins for the user object changes to 5.

---

## Enforcing Policies

When you assign a password policy to users in the tree, any password changes going forward must comply with the Advanced Password Rules in that policy. In the portal (iManager 2.02 or later, Virtual Office, Identity Manager User Application, and eXtend Director), the password rules are displayed in the page where the user changes the password. In Novell Client 4.9 SP2 or later, the rules are also displayed. In both methods of access, a noncompliant password is rejected. NMAS is the application that enforces these rules.

You can specify in the policy that existing passwords are checked for compliance and users are required to change existing noncompliant passwords. A password is marked as expired when the check for compliance option is enabled and the password does not satisfy the password policy rules.

You can also specify that when users authenticate through a portal, they are prompted to set up any Forgotten Password features you have enabled. This is called post-authentication services. For example, if you want users to create a Password Hint that can be e-mailed to them when they forget a password, you can use post-authentication services to prompt users to create a Password Hint at login time.

The post-authentication setting is the last option on the Forgotten Password property page.

### 3.2.3 Planning Login and Change Password Methods for your Users

There are several different ways a user can log in or change a password. For all of them, you need to upgrade your environment to eDirectory 8.7.3 or later with the associated LDAP server, NMAS 2.3 or later, and iManager 2.0.2 or later. For more information about upgrading to support Universal Password, see [Chapter 2, "Deploying Universal Password," on page 11](#).

This section explains the additional requirements for supporting Universal Password in each case:

- ♦ ["Novell Client" on page 26](#)
- ♦ ["Identity Manager User Application and iManager" on page 27](#)

- ◆ “Other Protocols” on page 27
- ◆ “Connected Systems” on page 27
- ◆ “Preventing Legacy Novell Clients from Changing Passwords” on page 27

## Novell Client

If you are using the Novell Client, upgrade it to version 4.9 SP2 or later.

Keep in mind that using the Novell Client is not required, because users can log in through the iManager self-service console or other company portals depending on your environment. Also, the Novell Client is no longer required for Password Synchronization on Active Directory.

The following table describes the differences between Novell Client versions in regard to Universal Password and gives suggestions for handling legacy Novell Clients.

**Table 3-1** *Universal Password with legacy Novell Clients*

Novell Client Version	Login	Change Password
Earlier than 4.9	Does not go through NMAS, so it does not support Universal Password. Instead, it logs in directly using the NDS password.	<p>Changes the NDS Password directly, instead of going through NMAS.</p> <p>If you are using Universal Password, this can mean that the NDS password and the Universal Password are not kept synchronized. To prevent this, you have three options:</p> <ul style="list-style-type: none"> <li>◆ Upgrade all the clients to version 4.9 or later.</li> <li>◆ Block legacy clients from changing passwords by using an attribute value on a container. With this solution, legacy clients can still log in, but they cannot change the password. Password changes must be done using a later Novell Client or iManager. See “Preventing Legacy Novell Clients from Changing Passwords” on page 27.</li> <li>◆ Use the password policy setting for <i>Remove the NDS Password when Setting Universal Password</i>. This is a drastic measure, because it prevents both login and password change through the NDS password.</li> </ul>
4.9	Supports Universal Password.	<p>Enforces password policy rules for Universal Password.</p> <p>If a user tries to create a password that is not compliant, the password change is rejected. However, the list of rules is not displayed to the user.</p>
4.9 SP2 or later	Supports Universal Password.	<p>Enforces password policy rules for Universal Password.</p> <p>In addition, it displays the rules to the users to help them create compliant passwords.</p>

## Identity Manager User Application and iManager

Identity Manager User Application and iManager provide Password Self-Service, so users can reset passwords and set up Forgotten Password Self-Service if the password policy provides it. For information about configuring Password Self-Service, see [Chapter 4, “Password Self-Service,”](#) on [page 51](#). Also ensure the following requirements are met:

- ♦ If you use iManager, make sure users have a browser that supports iManager 2.0.2 or later.

---

**NOTE:** As of version 2.6, Password Self-Service features are no longer included in iManager.

---

- ♦ We recommend that in your password policies you accept the default setting of *Synchronize NDS password when setting Universal Password*.
- ♦ Make sure you have the NMAS Simple Password login method installed. You can install it when you install eDirectory or you can manually install it afterward.

## Other Protocols

Make sure that eDirectory, LDAP server, NMAS, and iManager are upgraded to support Universal Password.

For information about using AFP, CIFS, and other protocols with Universal Password, see [Chapter 2, “Deploying Universal Password,”](#) on [page 11](#).

## Connected Systems

If you are using Identity Manager Password Synchronization, make sure the following requirements are met so that user password changes are successful:

- ♦ Any DirXML drivers for the system have been upgraded to Identity Manager format.
- ♦ The Identity Manager driver configuration includes the new Password Synchronization policies.
- ♦ The Password Synchronization settings should specify that Universal Password is to be used, as well as the Distribution Password if bidirectional Password Synchronization is desired.
- ♦ Password filters have been deployed on the connected system to capture passwords, if necessary.

For more information, see “[Connected System Support for Password Synchronization](http://www.novell.com/documentation/idm401/idm_password_management/data/bo1o7xz.html)” ([http://www.novell.com/documentation/idm401/idm\\_password\\_management/data/bo1o7xz.html](http://www.novell.com/documentation/idm401/idm_password_management/data/bo1o7xz.html)) in the *Novell Identity Manager 4.0.1 Password Management Guide* ([http://www.novell.com/documentation/idm401/idm\\_password\\_management/data/front.html](http://www.novell.com/documentation/idm401/idm_password_management/data/front.html)).

## Preventing Legacy Novell Clients from Changing Passwords

For versions of the Novell Client earlier than 4.9, login and password changes go directly to the NDS Password instead of through NMAS, so Universal Password is not supported.

If you are using Universal Password, using a legacy Novell Client to change passwords can create a problem called *password drift*, meaning that the NDS password and the Universal Password are not kept synchronized.

To prevent this issue, one option is to block password changes from Novell Clients earlier than version 4.9. This is done by using an eDirectory attribute on a partition root container, class, or object. The attributes are part of the schema in eDirectory 8.7.3 or later and are not supported on eDirectory 8.7.0 or earlier.

The method used by legacy Novell Clients to change the NDS password is called NDAP password management. The following list explains how you can use an attribute to disable NDAP password management at the partition level. You can still enable it per class or per object if necessary by using other attributes.

- ♦ **ndapPartitionPasswordMgmt:** For partition-level containers. If the attribute is not present or the value is not set at the partition level, then NDAP password management is enabled.

To disable NDAP password management, add this attribute to the partition and set it to 0. To enable it again, set the attribute to 1.

You can use the other attributes listed below to let classes or objects use NDAP password management even if it is disabled at the partition level. However, if NDAP password management is enabled at the partition level, then NDAP password management is enabled for all objects in that partition regardless of the class and entry level policies.

- ♦ **ndapClassPasswordMgmt:** For a class. If you add this attribute to a class definition, the class can use NDAP password management even if the partition-level policy specifies that it is disabled. The presence of this attribute is what enables NDAP password management. The value is not important.
- ♦ **ndapPasswordMgmt:** For a specific object. If you add this attribute to a specific object and set the value to 1, the object can use NDAP password management even if the partition or class specifies that it is disabled.

A setting of 0 disables NDAP password management, but only if it is also disabled at the partition level.

---

**IMPORTANT:** Remember that eDirectory 8.7.0 and earlier does not support this feature. If a tree exists with an eDirectory 8.7.3 or later server and an eDirectory 8.7.0 or earlier server, and the two servers share a partition, disabling NDAP password management on that partition has unreliable results. The 8.7.3 server enforces the setting, preventing legacy Novell Clients from changing the NDS password. However, the 8.7.0 server does not enforce the setting. If a user tries to change the NDS Password via the 8.7.0 server, the change succeeds.

---

## 3.3 Prerequisite Tasks for Using Password Policies

If you want to take advantage of all the features of password policies, you need to complete some steps to prepare your environment.

- 1 Upgrade your environment to support Universal Password.  
For more information, see [Chapter 2, “Deploying Universal Password,”](#) on page 11.
- 2 If you want to use the Microsoft Server 2008 Password Policy option, ensure that you upgrade to eDirectory 8.8 SP7, which includes NMAS 3.3.4.
- 3 Upgrade your client environment to support Universal Password.  
See [Section 3.2.3, “Planning Login and Change Password Methods for your Users,”](#) on page 25 and [Chapter 2, “Deploying Universal Password,”](#) on page 11.

- 4 If you have not run the iManager Configuration Wizard previously when you set up iManager, either as part of the iManager install or post-installation, you must run it. For information on how to run the iManager Configuration Wizard, see the “Role-Based Services” ([http://www.novell.com/documentation/imanager27/imanager\\_admin\\_275/data/am757mw.html](http://www.novell.com/documentation/imanager27/imanager_admin_275/data/am757mw.html)) section in the *Novell iManager 2.7.5 Administration Guide*.

---

**IMPORTANT:** After you run the iManager Configuration Wizard, iManager runs in RBS mode. This means that administrators do not see any tasks unless they have assigned themselves to specific roles. Make sure you assign administrators to roles to give them access to all the iManager tasks.

---

- 5 Install the Novell iManager Password Management plug-in.

This is available for download at the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com).

---

**IMPORTANT:** If you upgrade to the latest version of the Novell iManager Password Management plug-in without first upgrading eDirectory and then try to modify or create a password policy, iManager displays an error.

---

- 6 Make sure that SSL is configured between the iManager Web server and eDirectory, even if they are running on the same machine.

This is a requirement for NMAS 2.3 or later, and for [Step 7](#).

- 7 Make sure the LDAP Group-Server object in eDirectory is configured to require TLS for simple bind.

This is the default setting when you configure iManager. Requiring TLS for simple bind is strongly recommended for Password Self-Service functionality, and is required for using the iManager task *Passwords > Set Universal Password*.

If you are requiring TLS for simple bind, no additional configuration is needed for the LDAP SSL port.

---

**IMPORTANT:** If you choose not to require TLS for simple bind, this means that users are allowed to log in to the iManager self-service console by using a clear-text password.

You can use this option, but another step is required.

By default, the Password Self-Service functionality assumes that the LDAP SSL port is the one specified in the `System.DirectoryAddress` setting in the `PortalServlet.properties` file. If your LDAP SSL port is different, you must indicate the correct port by adding the following key pair to the `PortalServlet.properties` file:

```
LDAPSSLPort=your_port_number
```

For example, if you are running Tomcat, you would add this key pair in the `PortalServlet.properties` file in the `tomcat\webapps\nps\WEB_INF` directory.

---

- 8 To enable e-mail notification for Forgotten Password features, complete the steps in [Section 4.6, “Configuring E-Mail Notification for Password Self-Service,”](#) on page 68.

You must set up the SMTP server and customize the e-mail templates.

- 9 (NetWare 6.5 users only) If you have previously set up Universal Password for use with NetWare 6.5, complete the steps in [Section 3.3.1, “Re-Creating Universal Password Assignments,”](#) on page 30.

You are now ready to use all the features of password policies. Create policies as described in [Section 3.4, “Creating Password Policies,”](#) on page 31.

### 3.3.1 Re-Creating Universal Password Assignments

If you have previously set up Universal Password for use with NetWare 6.5, you must remove the old password policies and use the new plug-ins and password policies.

- ♦ The NMAS plug-ins that were used in NetWare 6.5 for Universal Password are no longer available. Instead, you use *Passwords > Password Policies*, which offers more features.
- ♦ The first time you use the *Password Policies* in the new plug-ins, you see three policy objects in the list that cannot be edited:
  - ♦ Universal Password On
  - ♦ Universal Password Off
  - ♦ Universal Password On - S

These objects were used for the NetWare 6.5 implementation of Universal Password. To take advantage of the additional benefits of password policies provided by Identity Manager, you need to remove them.

To remove the old policy objects and re-create your policies:

- 1 Decide where you want Universal Password enabled in your tree:
  - ♦ If you want it turned on for the same containers as when you set up Universal Password the first time with the NetWare 6.5 plug-ins, continue with [Step 2](#).
  - ♦ If you want it turned on everywhere in your tree, simply create a new password policy with Universal Password enabled and assign it to the Login Policy object. Then continue with [Step 4](#) to remove the old policies.

- 2 Find out where in the tree you had previously enabled Universal Password when you set it up using the plug-ins that shipped with NetWare 6.5.

This step is necessary because the plug-ins do not display where the assignments were made using the old plug-ins. Instead, you find them by searching the tree.

- 2a Search the tree for objects that have the `nspmPasswordPolicyDN` attribute populated with one of the following values:

- ♦ Universal Password On
- ♦ Universal Password On - S

- 2b Make a note of all the containers that are the results of the search. These are the containers where Universal Password is turned on.

- 3 If you want Universal Password assigned in the same containers where you had assigned it previously, create one or more new password policies with Universal Password enabled and assign them to the same containers.

Refer to the list of containers from [Step 2](#) to make sure your assignments match.

- 4 Go to *Passwords > Password Policies* and remove the policy objects that remain from the first NetWare 6.5 implementation:

- ♦ Universal Password Off
- ♦ Universal Password On
- ♦ Universal Password On - S

After removing the old policy objects, you can use new password policies to meet your password needs.

## 3.4 Creating Password Policies

Use the Password Policy Wizard in iManager to create new password policies.

See the online help for information about each step in the wizard, as well as the information in [Chapter 3, “Managing Passwords by Using Password Policies,”](#) on page 23 and in [Chapter 4, “Password Self-Service,”](#) on page 51.

- 1 Make sure you have completed the steps in [Section 3.3, “Prerequisite Tasks for Using Password Policies,”](#) on page 28.

These steps prepare you to use all the features of password policies.

- 2 In iManager, in the *Roles and Tasks* view, click *Passwords > Password Policies*.
- 3 Click *New* to create a new password policy.
- 4 Follow the steps in the wizard to create Advanced Password Rules, Universal Password Configuration Options, and Forgotten Password selections for the policy.
- 5 Assign the password policy to individuals, organizations, or your entire company, as necessary.
- 6 Review the settings for the new policy and click *Finish*, then click *Close* to close the wizard.

### 3.4.1 Advanced Password Rules

[Figure 3-1](#) shows the first section of the advanced password rules:

**Figure 3-1** Advanced Password Rules

**Password Policy Wizard**

**Step 3 of 8:** Add rules to the Password Policy

**Advanced Password Rules**

**Password Syntax**

- Use Microsoft complexity policy
- Use Microsoft Server 2008 Password Policy
- Use Novell syntax

**Change Password**

- Allow user to initiate password change
- Do not expire the user's password when the administrator sets the password
- Require unique passwords
  - Remove password from history list after:  Days (0-365)  
History list size:  Passwords (1-255)
  - Remove password from history list when the list is full.  
History list size:  Passwords (1-255)
- Number of characters different from current password and passwords from history (0-6)  Characters
- Number of passwords in history to be considered for character exclusion (0-10)  Passwords

**Password Lifetime**

- Number of days before password can be changed (0-365)  Days
- Number of days before password expires (0-365)  Days

<< Back   Next >>   Close   Finish

## Password Syntax

You can specify one of three password syntax options to use for a password policy:

- ◆ *Use Microsoft complexity policy*
- ◆ *Use Microsoft Server 2008 Password Policy*
- ◆ *Use Novell syntax*

---

**WARNING:** iManager allows you to create a policy using the Microsoft Server 2008 Password Policy type, regardless of the version of NMAS installed on your server. However, you must have NMAS 3.3.4 or later installed to use this option. If you have a previous version of NMAS installed, the new password policy does not function properly. NMAS 3.3.4 is included with eDirectory 8.8 SP7.

---

- ◆ *Use Microsoft complexity policy*

This setting allows you to use the Microsoft\* Complexity Policy requirements. Use this option if you must synchronize passwords between eDirectory and Microsoft Active Directory.

If you select this option for a policy, all users to which the policy is assigned must create passwords that meet the criteria of the Microsoft Complexity Policy as implemented in Universal Password. The criteria include:

- ◆ Minimum password length is 6 characters.
- ◆ Maximum password length is 128 characters.
- ◆ The password must contain at least one character from three of the four types of character, uppercase, lowercase, numeric, and special:
  - ◆ Uppercase characters - all uppercase characters in the Basic Latin and the Latin-1 character sets.
  - ◆ Lowercase characters - all lowercase characters in the Basic Latin and the Latin-1 character sets.
  - ◆ Numeric characters - 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9.
  - ◆ Special characters - all other characters.
- ◆ The values of the following user attributes can not be contained in the password: CN, Given Name, Surname, Full Name, and displayName.
- ◆ *Use Microsoft Server 2008 Password Policy*

This setting allows you to use the Microsoft\* Windows Server 2008 password policy complexity requirements. Use this option if you must synchronize passwords between eDirectory and Microsoft Active Directory.

If you select this option for a policy, all users to which the policy is assigned must create passwords that meet the criteria of the Microsoft Windows Server 2008 Complexity Policy as implemented in Universal Password. If you select this option, several options on the Advanced Password Rules page are set to meet the criteria of the Complexity Policy. The criteria include:

- ◆ Minimum password length is 6 characters, by default. You can configure the minimum password length in your environment using the *Minimum number of characters in password (1-512)* option. For more information about configuring the minimum number of characters, see [“Password Length” on page 38](#).
- ◆ Maximum password length is 512 characters.



- ◆ The password must contain at least one character from three of the five types of character, uppercase, lowercase, numeric, non-alphanumeric characters, and other characters:
  - ◆ Uppercase characters - all uppercase European-language characters, with diacritical marks, as well as Greek and Cyrillic characters.
  - ◆ Lowercase characters - all lowercase European-language characters, with diacritical marks, as well as Greek and Cyrillic characters.
  - ◆ Numeric characters - 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9.
  - ◆ Non-alphanumeric characters - any of the following special characters: ( ) ` ~ ! @ # \$ % ^ & \* - + = | \ { } [ ] : ; " ' < > , . ? / \_ .
  - ◆ Other characters - any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- ◆ The password cannot contain the full value of the CN user attribute for the eDirectory account. NMAS does not perform this check if the length of the attribute is less than three characters.
- ◆ The password cannot contain any word from the list of excluded passwords. NMAS does not perform this check if the length of the excluded password is less than three characters. For more information about excluding passwords, see [“Password Exclusions” on page 37](#).
- ◆ The password cannot contain the full value or any part of the value of the Full Name attribute for the account, if the attribute contains at least three characters and is a single word. A part of the attribute value is defined as three or more consecutive characters delimited on both ends by the following characters: commas; periods; dashes; hyphens; underscores; spaces; pound signs; or tabs.
- ◆ The maximum number of complexity policy violations allowed in a password is 2 by default. You can configure the number of complexity violations allowed using the *Maximum number of complexity policy violations in password (0-5)* option. For more information about configuring the maximum violations allowed, see [“Password Complexity Violations” on page 39](#).
- ◆ *Use Novell syntax*

This allows you to use the Novell syntax for the password policy. This option is selected by default. Standard settings for policies using Novell syntax include:

- ◆ Minimum password length is 4 characters, by default. You can configure the minimum password length in your environment using the *Minimum number of characters in password (1-512)* option. For more information about configuring the minimum number of characters, see [“Password Length” on page 38](#).
- ◆ Maximum password length is 12 characters, by default. You can configure the maximum password length in your environment using the *Maximum number of characters in password (1-512)* option. For more information about configuring the maximum number of characters, see [“Password Length” on page 38](#).

## Password Syntax Precedence

If you modify the attributes of a password policy using Directory Administration or LDAP, outside of the iManager Password Management plug-in interface, you may set up a conflict between one or more of the password policy types. For example, you could use LDAP to enable both the Microsoft complexity policy and Microsoft Windows 2008 Password Policy types for the same policy.

In the event of a conflict, eDirectory uses the following order of precedence:

- ◆ Microsoft Windows 2008 Password Policy
- ◆ Microsoft complexity policy
- ◆ Novell syntax

For more information about modifying password policies outside of the Password Management interface, see [“Modifying Password Policies Outside of the Password Policies Interface” on page 42](#).

## Change Password

- ◆ *Allow user to initiate password change*

This allows the user to use the password self-service features. This option is selected by default. For information about password self-service, see [Chapter 4, “Password Self-Service,” on page 51](#).

- ◆ *Do not expire the user’s password when the administrator sets the password*

This option requires the user to go and change his or her password. This feature allows you to override the default. The default behavior in eDirectory, when password expiration is set, is to expire the user’s password when the administrator sets the password.

- ◆ *Require unique passwords*

When this option is selected, the user is prevented from changing the password to one that is already in the history list. If a user tries to change the password and reuse one that is in the history list, the password policy rejects the password and the user is prompted to specify a different one.

You can specify how unique passwords are enforced by using one of the following two values:

- ◆ *Remove password from history list after a specified number of days (0-365) and a specified History list size (1-255).*

If you require unique passwords, you can specify how many days a previous password remains stored in the history list for comparison.

For example, if you specify a limit of 30 days, and the user’s previous password was “mountains99,” that password remains in the history list for 30 days. During that time, if the user tries to change his or her password and reuse “mountains99,” the password policy rejects that password, and the user is prompted to specify a different one. After the 30-day period, the old password is no longer stored for comparison, and the password policy allows it to be reused.

If you require unique passwords, you can also indicate how many passwords are stored in the history list for comparison. For example, if you specify 3, then the user’s previous three passwords are stored. If a user tries to change his or her password and reuse one that is in the history list before the number of days specified for removal from the history list, the password policy rejects the password, and the user is prompted to specify a different one.

---

## NOTE

- ◆ If the *Use Microsoft Server 2008 Password Policy* option is selected, the *Require unique passwords* option is also selected by default.
- ◆ If *Require unique passwords* is selected and you select *Remove password from history list after a specified number of days (0-365)* but don't specify a number of days, the password is on the history list for 8 times the value set in the *Number of days before password expires (0-365)* field, in the Password Lifetime section. If neither field has a value, the password is on the history list for 365 days.
- ◆ If you specify a password history list size and a number of days, and the number of passwords in the password history list size has been met, the user cannot change his or her password unless the password has expired. An administrator can change or set a user password even if the password list size has been met.
- ◆ After one or more passwords expire in the password history list, the list is no longer full, and a user is again able to change his or her password. This limitation is included to prevent users from changing their passwords so many times that a password is no longer included in the password history list, and they can re-use it.
- ◆ If a password history list size is not specified, the password history is never full.
- ◆ When comparing a specified password against previous passwords in the password history, eDirectory differs from Active Directory. If the size of the password history list is "N," Active Directory compares a specified password against "N" previous passwords. However, eDirectory compares a specified password against "N+1" previous passwords.

- 
- ◆ *Remove password from history list when the list is full* and the number of passwords reaches the specified *History list size (1-255)*.

If you require unique passwords, you can indicate how many passwords are stored in the history list for comparison. This option works on a first-in, first-out basis, where the oldest passwords are removed from the history list first. For example, when a user creates a new password that is not currently in the history list, the oldest password in the history list is removed if the history list is full.

---

## NOTE

- ◆ If the *Use Microsoft Server 2008 Password Policy* option is selected, the *Remove password from history list when the list is full* option is also selected by default. With the Microsoft Server 2008 syntax enabled, the *History list size* range is 0-24 passwords.
- ◆ If this option is selected, you should also select both the *Number of days before password can be changed* and *Number of days before password expires* options, with at least the minimum number of days for each.
- ◆ If you specify a password history list size of 0, NMAS only compares any new password created by a user against that user's current password.

- 
- ◆ *Number of characters different from current password and passwords from history (0-6)* and a specified number of characters

When this option is selected, the user must specify a password that includes at least as many "new" characters, characters unused in previous passwords, as specified in the setting. This option is selected by default.

You can specify how unique the unused characters must be by using the following value:

- ◆ *Number of passwords in history to be considered for character exclusion (0-10)* and a specified number of characters

If you require a certain number of unused characters for any new password, you can specify how many previous passwords to consider when checking a password for previously-used characters.

For example, if you specify a minimum of three new characters and specify that five previous passwords should be considered for character exclusion, and a user creates the new password "mountains99," that password must include at least three characters not in any of the previous five passwords. If the user's password two changes previous was "maintains99," only two characters different from the new password, the password policy rejects that password, and the user is prompted to specify a different one.

---

#### NOTE

- ◆ Both the *Number of characters different from current password and passwords from history (0-6)* and *Number of passwords in history to be considered for character exclusion (0-10)* options are selected by default. However, the values of both options are set to 0 by default.
  - ◆ If the value of the *Number of characters different from current password and passwords from history (0-6)* option is set to 0, the option is disabled.
  - ◆ If the value of the *Number of passwords in history to be considered for character exclusion (0-10)* option is set to 0, only the current password is considered when eDirectory checks for "new" characters.
- 

## Password Lifetime

- ◆ *Number of days before password can be changed (0-365)*

This option restricts the user from changing their Universal Password before the specified time has elapsed. For example, if this value is set to 30, a user must keep the same password for 30 days before he or she can change it.

- ◆ *Number of days before password expires (0-365)*

This option causes a user's password to expire after a specified time has elapsed. For example, if this value is set to 90, a user's password expires 90 days after it has been set. If grace logins are not enabled, the user cannot log in after a password has expired, and administrator assistance is needed to reset the password. However, if you enable grace logins, the user can log in with the expired password the specified number of times. Also, if you do not select the *Limit the number of grace logins allowed* option, unlimited grace logins are allowed.

---

## NOTE

- ◆ If the *Use Microsoft Server 2008 Password Policy* option is selected, the *Number of days before password can be changed* and *Number of days before password expires* options are also selected by default. With the Microsoft Server 2008 syntax enabled, the range for both options is 0-999 days.
- ◆ If an administrator changes a user's password, such as when creating a new user or in response to a help desk call, the password is automatically expired if you have enabled the setting to expire passwords in the password policy. For this particular feature, the number of days is not important, but this setting must be enabled. Selecting the *Do not expire the user's password when the administrator sets the password* option overrides this security enhancement.

---

- ◆ *Limit the number of grace logins allowed (0-254)*

When the password expires, this value indicates how many times a user is allowed to log in to eDirectory by using the expired password. If grace logins are not enabled, the user cannot log in after a password has expired, and he or she requires administrator assistance to reset the password. If the value is 1 or more, the user has a chance to log in additional times before being forced to change the password. However, if the user does not change the password before all the grace logins are used, he or she is locked out and is unable to log in to eDirectory. Also, if you have not selected the *Limit the number of grace logins allowed* option, unlimited grace logins are allowed.

## Password Exclusions

- ◆ *Exclude the following passwords*

This allows you to manually specify the passwords you want to exclude. You can use this option to exclude specific words or single characters, not a pattern or an eDirectory attribute. You can also exclude passwords containing a specific special character, including a \*, +, %, or space character. For example, if you add the character \* to the list of excluded passwords, a user who tried to specify the password "Pa55w0rd\*!" would receive an error saying that the specified password is invalid. This can be useful if you need to restrict users from specifying passwords containing special characters that cause issues with applications in your environment.

For NMAS 3.1.3 and later, the strings in the exclude list cannot be contained in the password, and the comparison is case-insensitive. For example, if "test" is in the exclude list, then the following cannot be passwords: Test, TEST, ltest, test1, and latest.

Keep in mind that password exclusions can be useful for a few words that you think would be security risks. Although an exclusion list feature is provided, it is not intended to be used for a long list of words, such as a dictionary. Long lists of excluded words can affect server performance. Instead of a long exclusion list to protect against "dictionary attacks" on passwords, we recommend that you use the Advanced Password Rules to require numbers to be included in the password.

- ◆ *Exclude passwords that match attribute values*

This allows you to select User object attributes that you want to exclude from being used as passwords. For example, if you add the Given Name attribute to the list, and the Given Name attribute contained the value of Frank, then neither frank, frank1, nor 1frank could be used as the password.

Use the plus and minus buttons to add and delete attribute values from the list.

---

**NOTE:** If the *Use Microsoft complexity policy* option is selected, the *Exclude passwords that match attribute values* option is also selected by default. With the Microsoft complexity policy syntax enabled, the list of attribute values to match is prepopulated with the following attributes: Common name; Display name; Full name; First name; and Last name.

---

**Figure 3-2** Advanced Password Rules Continued

**Password Policy Wizard**

**Step 3 of 8:** Add rules to the Password Policy

**Password Exclusions**

Exclude the following passwords Enter excluded password:

Exclude passwords that match attribute values.

**Password Length**

Minimum number of characters in password (1-512)  Characters

Maximum number of characters in password (1-512)  Characters

**Repeating Characters**

Minimum number of unique characters (1-512)  Characters

Maximum number of times a specific character can be used (1-512)  Time(s)

Maximum number of times a specific character can be repeated sequentially (1-512)  Time(s)

**Case Sensitive**

Allow the password to be case sensitive

Minimum number of upper case characters required in password (1-512)  Characters

Maximum number of upper case characters allowed in password (1-512)  Characters

Minimum number of lower case characters required in password (1-512)  Characters

<< Back   Next >>   Close   Finish

## Password Length

- ♦ *Minimum number of characters in password (1-512)*
- ♦ *Maximum number of characters in password (1-512)*

---

### NOTE

- ♦ The maximum length for any password created using NMA is 512 characters.
  - ♦ If the *Use Microsoft complexity policy* option is selected, neither the *Minimum number of characters in password* nor *Maximum number of characters in password* option is available.
  - ♦ If the *Use Microsoft Server 2008 Password Policy* option is selected, only the *Minimum number of characters in password* option is available. The option is selected by default.
  - ♦ If the *Use Novell syntax* option is selected, both the *Minimum number of characters in password* and *Maximum number of characters in password* options are also selected by default.
-

## Password Complexity Violations

- ♦ *Maximum number of complexity policy violations in password (0-5)*

This option allows you, as an administrator, to configure the number complexity policy violations you want to allow in passwords in your environment. By default, the Microsoft Server 2008 Password Policy requires that a password include at least one character from three of the five types of character, uppercase, lowercase, numeric, non-alphanumeric characters, and other characters. Therefore, the default number of violations allowed is 2. For more information on policy requirements for Microsoft Server 2008 Password Policy, see [“Password Syntax” on page 32](#).

However, if you want to make your password policy more or less restrictive, you can modify the default number of violations allowed. For example, if you change the default setting to 1, all passwords must include at least one character from four of the five character types listed above. If the setting is 4, passwords must include a character from only one of the five character types.

---

**NOTE:** The *Maximum number of complexity policy violations in password (0-5)* option is only available if you select the *Use Microsoft Server 2008 Password Policy* option. The option is selected by default.

---

## Repeating Characters

- ♦ *Minimum number of unique characters (1-512)*
- ♦ *Maximum number of times a specific character can be used (1-512)*
- ♦ *Maximum number of times a specific character can be repeated sequentially (1-512)*

---

**NOTE:** If either the *Use Microsoft complexity policy* or *Use Microsoft Server 2008 Password Policy* options is selected, the *Minimum number of unique characters*, *Maximum number of times a specific character can be used*, and *Maximum number of times a specific character can be repeated sequentially (1-512)* options are unavailable.

---

## Case Sensitive

In eDirectory 8.7.1 and 8.7.3, you needed to use the Novell Client for case sensitivity to work. In eDirectory 8.8 or later, you can use the *Allow the password to be case sensitive* option to make your passwords case sensitive for all the clients that are upgraded to eDirectory 8.8. See the [Novell eDirectory 8.8 SP7 Administration Guide \(http://www.novell.com/documentation/beta/edir88/edir88/data/a2iii88.html\)](http://www.novell.com/documentation/beta/edir88/edir88/data/a2iii88.html) for more information.

---

### NOTE

- ♦ NMAS does not currently support case sensitive password checking when using Unicode characters.
  - ♦ The *Allow the password to be case sensitive* option is only available if you select the *Use Novell syntax* option. The option is selected by default.
- 

The *Allow the password to be case sensitive* option is only available if you select the *Use Novell syntax* option. The option is selected by default.

With *Allow the password to be case sensitive* selected, you have four options:

- ◆ *Allow the password to be case sensitive*
  - ◆ *Minimum number of upper case characters required in the password (1-512)*
  - ◆ *Maximum number of upper case characters allowed in the password (1-512)*
  - ◆ *Minimum number of lower case characters required in the password (1-512)*
  - ◆ *Maximum number of lower case characters allowed in the password (1-512)*

When *Allow the password to be case sensitive* is not selected, the passwords are case insensitive, and you have two options:

- ◆ *Minimum number of alphabetic characters allowed in password (1-512)*
- ◆ *Maximum number of alphabetic characters allowed in password (1-512)*

---

**IMPORTANT:** Passwords are stored with case, and are synchronized between systems with case sensitivity, even though the *Allow passwords to be case sensitive* option is not selected. The case of password characters is ignored if the *Allow the password to be case sensitive* option is not selected.

---

**Figure 3-3** *Advanced Password Rules Final*

**Password Policy Wizard**

**Step 3 of 8:** Add rules to the Password Policy

**Numeric Characters**

- Allow numeric characters in password
  - Disallow numeric as first character
  - Disallow numeric as last character
  - Minimum number of numerals in password (1-512)  Characters
  - Maximum number of numerals in password (1-512)  Characters

**Non-alphanumeric Characters**

- Allow non-alphanumeric characters in the password
  - Disallow non-alphanumeric character as first character
  - Disallow non-alphanumeric character as last character
  - Minimum number of non-alphanumeric characters (1-512)  Characters
  - Maximum number of non-alphanumeric characters (1-512)  Characters
- Allow non-US ASCII characters

**Non-alphabetic Characters**

- Allow non-alphabetic characters in the password
  - Minimum number of non-alphabetic characters (1-512)  Characters
  - Maximum number of non-alphabetic characters (1-512)  Characters

<< Back    Next >>    Close    Finish

## Numeric Characters

- ◆ *Allow numeric characters in password*
  - ◆ *Disallow numeric as first character*



- ◆ *Disallow numeric as last character*
- ◆ *Minimum number of numerals in password (1-512)*
- ◆ *Maximum number of numerals in password (1-512)*

---

**NOTE:** The *Allow numeric characters in password* option is only available if you select the *Use Novell syntax* option. The option is selected by default.

---

## Non-alphanumeric Characters

Non-alphanumeric characters are characters that are not numbers (0-9) or alphabetic characters. Alphabetic characters are defined as a-z, A-Z, and alphabetic characters in the Latin-1 code page 850.

- ◆ *Allow non-alphanumeric characters in the password*
  - ◆ *Disallow non-alphanumeric character as first character*
  - ◆ *Disallow non-alphanumeric character as last character*
  - ◆ *Minimum number of non-alphanumeric characters (1-512)*
  - ◆ *Maximum number of non-alphanumeric characters (1-512)*
- ◆ *Allow non-US ASCII characters*

This option allows a password to include characters outside of the Basic Latin character set, also known as extended characters.

---

**NOTE:** The *Allow non-alphanumeric characters in the password* option is only available if you select the *Use Novell syntax* option. The option is selected by default.

---

## Non-alphabetic characters

Non-alphabetic characters are the characters that are not alphabetic characters. Alphabetic characters are defined as a-z, A-Z, and alphabetic characters in the Latin-1 code page 850.

- ◆ *Allow non-alphabetic characters in the password*
  - ◆ *Minimum number of non-alphabetic characters (1-512)*
  - ◆ *Maximum number of non-alphabetic characters (1-512)*

---

### NOTE

- ◆ The *Allow non-alphabetic characters in the password* option is only available if you select the *Use Novell syntax* option.
  - ◆ If you use the *Allow non-alphabetic characters in the password* option, ensure your policy does not unduly restrict possible passwords. For example, you can create a policy that requires multiple non-alphabetic characters or numerals but also *limits* the number of non-alphabetic characters allowed.
-

## 3.4.2 Modifying Password Policies Outside of the Password Policies Interface

In addition to creating, modifying, and assigning password policies using the iManager Password Management plug-in, you can modify policies outside of the Password Policies interface in one of the following ways:

- ♦ Modify the policy object directly using the Directory Administration interface.
- ♦ Modify the policy object directly using the `ldapmodify` command line tool.

However, it is not recommended that you manipulate password policies outside of the Password Policies interface, as this manipulation might cause issues in your environment if all attributes are not properly set. If you set multiple policy types for a single policy, for example, only the “highest” policy type in the order of precedence takes effect, and eDirectory ignores any policy rules for the “lower” policy types applied. For more information about password policy type precedence, see [“Password Syntax Precedence” on page 34](#).

In addition, if you change the type of a password policy from the Microsoft Server 2008 Password Policy type to the Microsoft complexity policy type without using the Password Policies interface, iManager does not delete the existing Microsoft Server 2008 Password Policy attribute (`nspmAD2K8Syntax`) in the policy object. Instead, iManager sets the value of the attribute to `False`. In this situation, eDirectory ignores all policies and rules set for either policy type.

Another issue can occur when you use LDAP to modify specific rules for a policy. If you modify a policy so that two rules conflict, eDirectory applies a rule that is selected or is set to `True` in the policy instead of a conflicting rule that is not selected or is set to `False`.

For example, you can create a policy and then modify that policy to both not allow numeric characters and allow non-alphabetic characters. Because the value of the `nspmNonAlphaCharactersAllowed` attribute is set to `True`, all non-alphabetic characters are allowed, including numeric characters, even though the `nspmNumericCharactersAllowed` is set to `False`.

## 3.4.3 Random Password Generation

Instead of specifying a particular password, users can also request a randomly-generated password. Randomly-generated passwords automatically conform to the complexity requirements and other restrictions of the password policy assigned to the user.

### Randomly-Generated Microsoft Server 2008 Passwords

Randomly-generated passwords for Microsoft Server 2008 Password Policy policies differ in the following ways from randomly-generated passwords using other password policy types:

- ♦ If a user is assigned a password policy that uses the Microsoft Server 2008 Password Policy type and requests a randomly-generated password, NMAS generates the password based on the number of password complexity violations allowed for the policy.
- ♦ If the number of password complexity violations allowed is set to the maximum value of 5, any randomly-generated password consists only of uppercase or lowercase alphabetic characters.

- ♦ If the configured password complexity requirements are extremely strict, even randomly-generated passwords may not be valid for the password policy.
- ♦ The maximum length of any randomly-generated Microsoft Server 2008 Password Policy password is 16 characters, unless the minimum length configured in the policy is more than 16 characters. If the minimum length is more than 16, the length of the generated password is the minimum length set in the policy. For example, if the minimum length of a password is set to 20 characters using a Microsoft Server 2008 policy, the randomly-generated password is always 20 characters long.

### **3.4.4 Universal Password Configuration Options**

The following figure shows an example of the Universal Password configuration options:

Figure 3-4 Configuration Options

Sample Password Policy.Password Policies.Security

Policy Summary **Universal Password** Forgotten Password Policy Assignment

Advanced Password Rules | **Configuration Options**

Use the checkboxes to enable the password settings for your policy.

### Configuration Options

- Enable Universal Password
- Enable the Advanced Password Rules

### Universal Password Synchronization

- Remove the NDS password when setting Universal Password
- Synchronize NDS password when setting Universal Password
- Synchronize Simple Password when setting Universal Password
- Synchronize Distribution Password when setting Universal Password

### Universal Password Retrieval

- Allow user to retrieve password
- Allow admin to retrieve passwords
- Allow the following to retrieve passwords

Insert...   Remove
<input type="checkbox"/> DN
No objects can retrieve the password - Select Insert!

### Authentication

- Verify whether existing passwords comply with the password policy (verification occurs on login)

**Note:** Your network might require preparation for the Universal Password to work properly.

To learn how to prepare your network for Universal Password, see the [Password Management Administration Guide](#).

OK Cancel Apply Refresh

- ◆ *Enable Universal Password*

Enables Universal Password for this policy. You must enable Universal Password if you want to use the other password policy features.

- ◆ *Enable the Advanced Password Rules*

Enables the Advanced Password Rules found on the Advanced Password Rules page for this policy. These advanced password rules help secure your environment by giving you control over password lifetime and what the password can contain.

- ◆ *Universal Password Synchronization*

- ◆ *Remove the NDS password when setting Universal Password*

If this option is selected, the NDS password is disabled when the Universal Password is set. Also, when the NDS password is set, the NDS password hash is set to a random value that is not known except to eDirectory. There might or might not be a password that could be hashed to the random value.

- ◆ *Synchronize NDS password when setting Universal Password*

If this option is selected, and the Universal Password is set, the NDS password is set at the same time and with the same password.

- ◆ *Synchronize Simple Password when setting Universal Password*

Provided solely for backward compatibility with NetWare 6.0 servers that contain AFP/CIFS users. If you have NetWare 6.0 servers in the tree that contain AFP/CIFS users, you should select this option.

---

**NOTE:** The setting of this option does not affect your ability to import user passwords by using ICE.

---

If this option is selected, and the Universal Password is set, the Simple Password is set at the same time and uses the same password.

- ◆ *Synchronize Distribution Password when setting Universal Password*

Determines whether the Identity Manager Metadirectory engine can retrieve or set a user's Universal Password in eDirectory.

If this option is selected, and the Universal Password is set, the Distribution Password is set at the same time and uses the same password.

The Distribution Password can be used with Identity Manager to perform password synchronization to connected systems. This option also allows the Metadirectory engine to retrieve a user's Universal Password in eDirectory.

- ◆ *Universal Password Retrieval*

- ◆ *Allow user to retrieve password*

Determines whether the Forgotten Password Self-Service feature can retrieve a password on behalf of a user, so that the password can be e-mailed to the user. If this option is not selected, the corresponding feature is dimmed on the Forgotten Password page in the Password Policy.

This option allows users to retrieve their own passwords by using NMAS LDAP extensions.

- ◆ *Allow admin to retrieve passwords*

Lets you retrieve users' passwords by using a third-party product or service that uses this functionality.

This option is not recommended with NMAS 3.2 and later. Instead, you should use the *Allow the following to retrieve passwords* option to assign password read rights to specific objects, such as the SAMBA or freeRADIUS service objects, that need this ability to perform their functions.

If *Allow admin to retrieve passwords* is selected, then users that have write privileges on the target object's ACL attribute can retrieve the target object's password.

- ◆ *Allow the following to retrieve passwords*

Lets you insert an object that has the ability to retrieve passwords.

- ◆ *Authentication*

- ◆ *Verify whether existing passwords comply with the password policy (verification occurs on login)*

If this option is selected, and users log in through iManager or the iManager self-service console, their existing passwords are checked to make sure they comply with the Advanced Password Rules in the users' password policy. If an existing password does not comply, users are required to change it.

## 3.5 Assigning Password Policies to Users

You can assign a password policy to users in eDirectory by assigning the policy to the whole tree by using the Login Policy object, to specific partitions or containers, or to specific users. We encourage you to set password policies as high up in the tree as you can, to simplify administration.

---

**IMPORTANT:** Assigning a password policy to an entire eDirectory tree or to a container in a tree that contains a very large number of users (tens of thousands) in subcontainers can cause iManager and the iManager plug-in to hang.

In this case, you might want to consider individually assigning password policies to lower-level containers in order to control the number of users for each password policy assignment.

---

A policy is not in effect until you assign it to one or more objects. You can assign a password policy to the following objects:

- ◆ Login Policy object

We recommend that you create a default password policy for all users in the tree. You do this by creating a policy and assigning it to the Login Policy object. The Login Policy object is located in the Security container just below the root of the tree.

- ◆ A container that is a partition root

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

- ◆ A container that is not a partition root

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

- ◆ A specific user

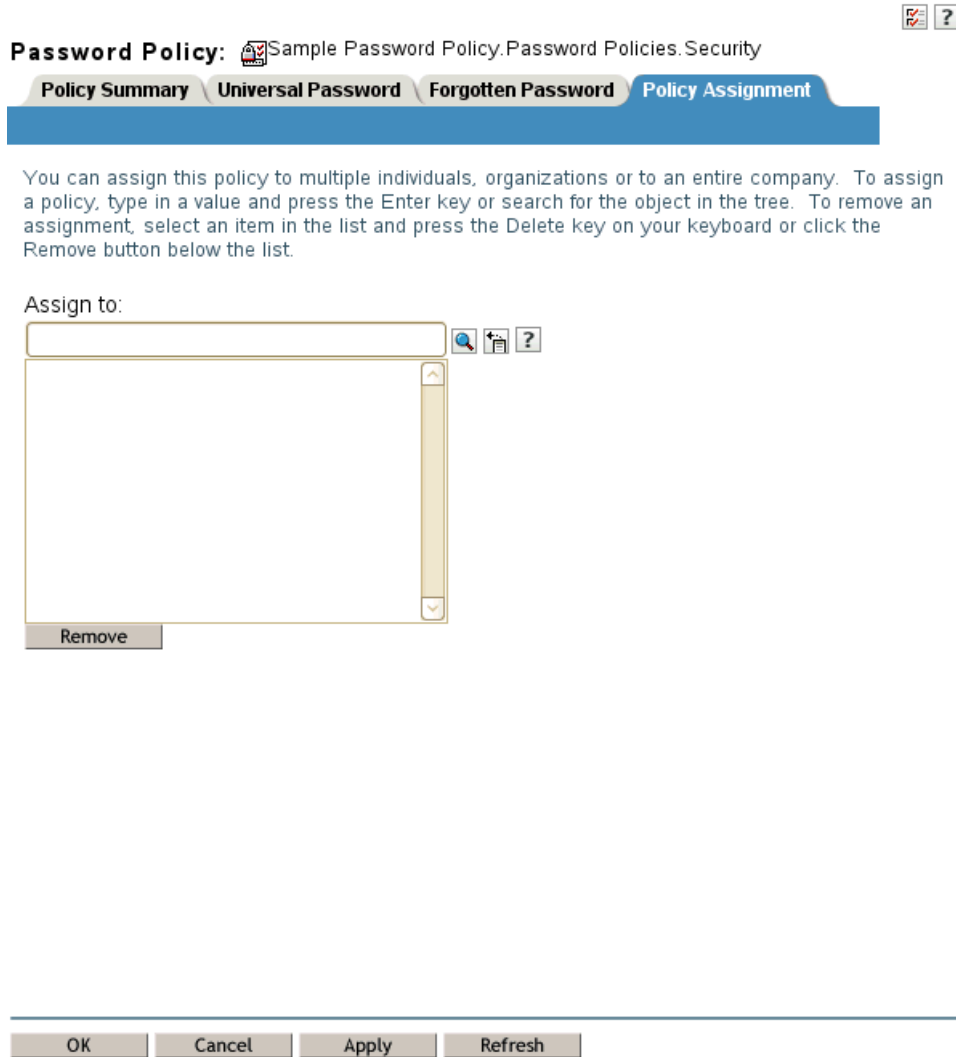
Only one policy is effective for a user at a time. NMAS determines which policy is effective for a user by looking for policies in the following order and applying the first one it finds.

1. **Specific user assignment:** If a password policy has been assigned specifically to the user, that policy is applied.
2. **Container:** If the user has no specific assignment, NMAS applies the policy that is assigned to the container that holds the user.
3. **Partition root container:** If no policy is assigned to the user or to the container directly above the user, the policy assigned to the partition root container is applied.

- 4. Login Policy object:** If no policy is assigned to the user or other containers, the policy assigned to the Login Policy object is applied. It is the default policy for all users in the tree.

The following figure shows an example of the property page where you specify which object password policy is assigned to:

**Figure 3-5** Assigning Password Policy to Objects



## 3.6 Finding Out Which Policy a User Has

Only one policy is in effect for a user at a time. To find out which policy is in effect for a particular user or container:

- 1 In iManager, in the *Roles and Tasks* view, click *Passwords > View Policy Assignments*.
- 2 Browse to and select the desired user.
- 3 Click *OK*.

If there are multiple policies in the tree, NMAS determines which policy to apply to a user as described in [Section 3.5, "Assigning Password Policies to Users,"](#) on page 46.

## 3.7 Setting A User's Password

Administrators or help desk personnel can set a user's Universal Password by using a task in iManager. The task shows the password rules for the password policy that is in effect for the user.

- 1 In iManager, in the *Roles and Tasks* view, click *Passwords > Set Universal Password*.
- 2 Browse to and select the desired user.
- 3 Click *OK*.

If the user has a password policy assigned and Universal Password enabled, you can change the password by using this task.

If the Advanced Password Rules are enabled in the policy, you see a list of rules that must be followed.

If Universal Password is not enabled for a user, iManager displays an error. You must either assign a policy to the user and then return to this task or change the user's NDS password by using the *eDirectory Administration > Modify Object* task.

- 4 Create a password for the user, making sure it is compliant with all password rules that are displayed.
- 5 Click *OK*.

The Universal Password is changed for the user.

If Password Synchronization is set up in your environment, the user's new password is distributed to the connected systems that are configured to accept it.

---

**NOTE:** If an administrator changes a user's password, such as when creating a new user or in response to a help desk call, the password is automatically expired if you have enabled the setting to expire passwords in the password policy. The setting, named *Number of days before password expires*, is in Advanced Password Rules. For this particular feature, the number of days is not important, but the setting must be enabled.

The *Do not expire the user's password when the administrator sets the password* option overrides this feature.

---

## 3.8 Troubleshooting Password Policies

- ♦ [Section 3.8.1, "iManager Self-Service Login Requires Full DN," on page 48](#)
- ♦ [Section 3.8.2, "Errors Indicate a Password Policy Is Not Assigned to a User," on page 49](#)
- ♦ [Section 3.8.3, "Using Challenge Response Questions," on page 49](#)
- ♦ [Section 3.8.4, "Giving Access to Users in New Containers," on page 49](#)
- ♦ [Section 3.8.5, "NMAPS LDAP Transport Error," on page 49](#)

### 3.8.1 iManager Self-Service Login Requires Full DN

If you have to type a full DN at the login prompt, the user object probably does not reside under the container specified during iManager or Portal configuration. You need to run the Portal Servlet Configuration Wizard ([http://your\\_iManager\\_server/nps/servlet/](http://your_iManager_server/nps/servlet/)), and specify additional login containers for the contextless login. The Forgotten Password feature also uses this setting to resolve a user's DN.



## 3.8.2 Errors Indicate a Password Policy Is Not Assigned to a User

If you see an error saying that a password policy is not assigned to a user from the Set Universal Password task, and you know that the user does have a password policy assigned, SSL might be the issue. To diagnose and resolve SSL issues, perform the following tasks:

- ♦ To help confirm that SSL configuration is the problem, use the View Policy Assignment task to check the policy for that user. If the View Policy Assignment task displays an NMAS Transport error, this can be an indicator that SSL is not configured properly.
- ♦ Make sure that SSL is configured correctly between the Web server running iManager and the primary eDirectory tree. Confirm that you have a certificate configured between the Web server and eDirectory.

This can be a problem if you are running iManager on Windows 2000 machine with IIS as the Web server, because the iManager installation does not automatically configure the certificate for you in that scenario.

- ♦ If you are not requiring TLS for simple bind, you must make sure you indicate the correct LDAP SSL port, as explained in the note in [Step 7 on page 29](#).

## 3.8.3 Using Challenge Response Questions

Make sure that you are using a supported browser for iManager.

## 3.8.4 Giving Access to Users in New Containers

When you set up iManager or one of Novell's portal products, such as Novell's UserApp™, you specify the portal users container. Usually you specify a container at a high level in the tree, so that all users in the tree can access portal features. If all your users are below that container, then all users have access to Forgotten Password and Reset Password Self-Service.

If you later create a container with users outside the portal users' container, and these users can't access Forgotten Password and Reset Password features, you'll need to specifically assign rights to the following gadgets for that new container: Challenge Response Setup, Change Universal Password, and Hint Setup.

For instructions on adding new users to the portal users' container, see "Portal User" in the Novell exteNd documentation (<http://www.novell.com/documentation/extend5/>).

## 3.8.5 NMAS LDAP Transport Error

If you are installing Identity Manager in a multiserver environment and use some of the Password Management plug-ins in iManager, you might see an error that begins with NMAS LDAP Transport Error.

One common cause of this error is that the `PortalServlet.properties` file is pointing to an LDAP server that does not have the NMAS extensions that are needed for Identity Manager. Open the `PortalServlet.properties` file and make sure the address for the LDAP server is the same server where you installed Identity Manager.

Other possible causes:

- ♦ The LDAP server is not running.

- ♦ SSL is not configured for LDAP between the iManager server running the plug-ins and the LDAP server.
- ♦ When logging in to other trees with iManager to manage remote Identity Manager DirXML servers, you might encounter errors if you use the server name instead of the IP address for the remote server.
- ♦ The trusted root certificate of the tree you authenticate to must be imported as a trusted certificate onto the Web server. You can use `keytool .exe` to export the certificate to the Web server. If you install eGuide, the certificate is exported to the Web server during the configuration process.

---

# 4 Password Self-Service

This section provides information on setting up and managing Password Self-Service.

- ◆ Section 4.1, “Overview of Password Self-Service,” on page 51
- ◆ Section 4.2, “Prerequisites for Using Password Self-Service,” on page 52
- ◆ Section 4.3, “Managing Forgotten Passwords,” on page 52
- ◆ Section 4.4, “Providing Users with Password Reset Self-Service,” on page 67
- ◆ Section 4.5, “Adding a Password Change Message,” on page 67
- ◆ Section 4.6, “Configuring E-Mail Notification for Password Self-Service,” on page 68
- ◆ Section 4.7, “Testing Password Self-Service,” on page 70
- ◆ Section 4.8, “Adding Password Self-Service to Your Company Portal,” on page 71
- ◆ Section 4.9, “Troubleshooting Password Self-Service,” on page 76

## 4.1 Overview of Password Self-Service

You can reduce help desk costs by setting up self-service so users can recover from forgotten passwords or reset their passwords while viewing the rules you have specified in the password policy.

You manage the policy for Password Self-Service by using one of the following:

- ◆ iManager

Most of this chapter describes how to manage password self-service using iManager.

- ◆ Identity Manager User Application

For information on managing password self-service with the Identity Manager User Application, see “Using the Identity Self-Service Tab” in the *Novell Identity Manager Roles Based Provisioning Module 4.0.1 User Application User Guide* (<http://www.novell.com/documentation/idm401/ugpro/data/ugpropartidentity.html>).

Users access the Password Self-Service features by using one of the following:

- ◆ iManager 2.0.2 portal

The Password Self-Service features were removed from iManager 2.6 and later, so in order for users to use the self-service features, you must have a server running iManager 2.0.2. Users go to this server's portal ([https://www.my\\_iManager\\_server.com/nps](https://www.my_iManager_server.com/nps) by default) to access the self-service features.

- ◆ Identity Manager User Application portlet

For information on using password self-service with Identity Manager User Application, see “Using the Identity Self-Service Tab” in the *Novell Identity Manager Roles Based Provisioning Module 4.0.1 User Application User Guide* (<http://www.novell.com/documentation/idm401/ugpro/data/ugpropartidentity.html>).

- ◆ Novell Client

For information on using password self-service with the Novell Client, see “Using Forgotten Password Self-Service” in the *Novell Client for Windows Administration Guide* ([http://www.novell.com/documentation/windows\\_client/windows\\_client\\_admin/data/bxne05q.html](http://www.novell.com/documentation/windows_client/windows_client_admin/data/bxne05q.html)).

- ◆ Virtual Office

Virtual Office is no longer supported by Novell. For information on using password self-service with Virtual Office, see the *Novell Open Enterprise Server Virtual Office Configuration Guide* (<http://www.novell.com/documentation/oes/virtualoffice/data/am0ogoi.html>).

## 4.2 Prerequisites for Using Password Self-Service

Review the information in Chapter 3, “Managing Passwords by Using Password Policies,” on page 23 and meet the prerequisites in Section 3.3, “Prerequisite Tasks for Using Password Policies,” on page 28.

Although you can use some Password Self-Service features without deploying Universal Password, we recommend that you prepare your environment and turn on Universal Password so you can use all the features of password policies.

You can also set up the Password Self-Service features in Virtual Office. Users use the Virtual Office portal ([https://www.my\\_iManager\\_server.com/vo](https://www.my_iManager_server.com/vo) by default) to access the self-service features. See “Integrating Password Self-Service with Virtual Office” on page 72.

The Novell Client also takes advantage of Password Self-Service features. See “Using Forgotten Password Self-Service” in the *Novell Client for Windows Administration Guide* ([http://www.novell.com/documentation/windows\\_client/windows\\_client\\_admin/data/bxne05q.html](http://www.novell.com/documentation/windows_client/windows_client_admin/data/bxne05q.html)).

Although users can use iManager 2.0.2 as one way to use the Password Self-Service features, this section assumes that you are managing Password Self-Service by using iManager 2.5 or later.

## 4.3 Managing Forgotten Passwords

The following sections describe how to manage forgotten passwords using iManager.

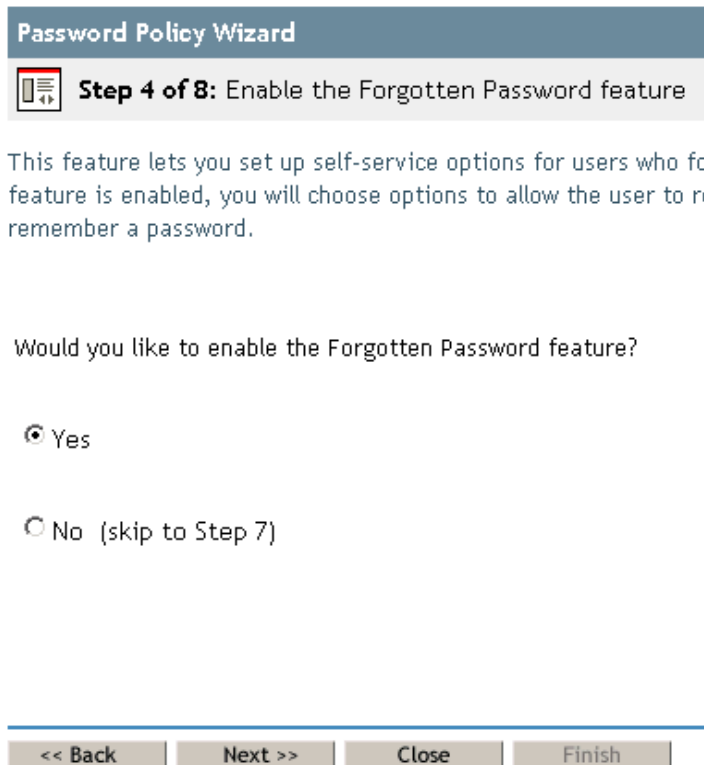
For information on managing forgotten passwords by using the Identity Manager User Application, see “Password Management Configuration” in the *Novell Identity Manager 4.0.1 User Application Administration Guide* (<http://www.novell.com/documentation/idm401/agpro/data/b6mixux.html>).

- ◆ Section 4.3.1, “Enabling Forgotten Password,” on page 53
- ◆ Section 4.3.2, “Creating or Editing Challenge Sets,” on page 54
- ◆ Section 4.3.3, “Selecting a Forgotten Password Action,” on page 57
- ◆ Section 4.3.4, “Disabling Password Hint by Removing the Hint Gadget,” on page 59
- ◆ Section 4.3.5, “Configuring Forgotten Password Self-Service,” on page 60
- ◆ Section 4.3.6, “What Users See When They Forget Passwords,” on page 64

## 4.3.1 Enabling Forgotten Password

To enable users to recover from a forgotten password without contacting the help desk, enable the Forgotten Password feature. As the following figure illustrates, you encounter this option while using the Password Policy Wizard to create a password policy. For more information on the Password Policy Wizard, see [“To create a challenge set while using the Password Policy Wizard:” on page 56](#)

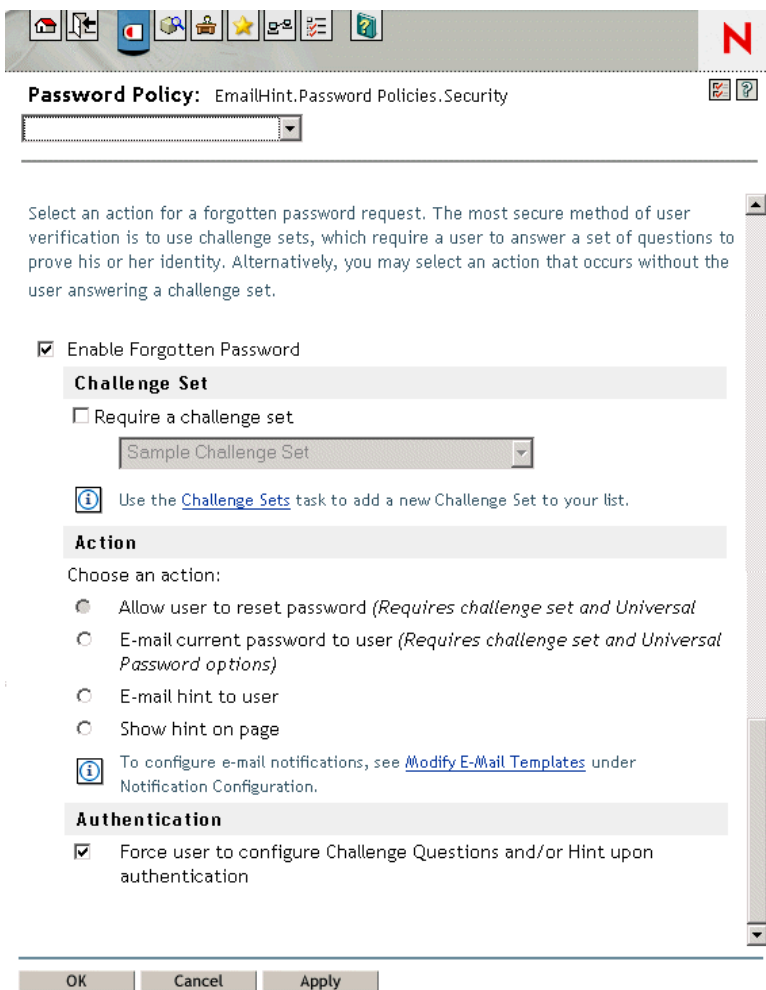
**Figure 4-1** Enable Forgotten Password



The screenshot shows a wizard window titled "Password Policy Wizard". Below the title bar, there is a progress indicator showing a list of steps with the current step highlighted. The text reads "Step 4 of 8: Enable the Forgotten Password feature". Below this, there is a paragraph of text: "This feature lets you set up self-service options for users who for feature is enabled, you will choose options to allow the user to re remember a password." Below the text is a question: "Would you like to enable the Forgotten Password feature?". There are two radio button options: "Yes" (which is selected) and "No (skip to Step 7)". At the bottom of the window, there are four buttons: "<< Back", "Next >>", "Close", and "Finish".

You can also enable Forgotten Password on an existing password policy:

- 1 In iManager, click *Passwords* > *Password Policies*.
- 2 Click the name of the policy.
- 3 Click the *Forgotten Password* tab.



- 4 Select *Enable Forgotten Password*, select or create a challenge set, specify an action, select the *Authentication* option, then click *OK*.

## 4.3.2 Creating or Editing Challenge Sets

A challenge set is a set of questions that a user answers to prove his or her identity, instead of using a password. The challenge set is assigned to a password policy and is used as part of a password policy's method of authentication. Users' answers to these challenge questions are case insensitive.

You can use challenge sets as part of providing Forgotten Password self-service for users. Requiring a user to answer challenge questions before receiving forgotten password help provides an additional level of security.

When you create a password policy, you can enable Forgotten Password self-service so that users can get help without calling the help desk. To make self-service more secure, you can create a challenge set and specify that users must answer the challenge set questions before obtaining forgotten password help. You also specify what action takes place to help users after they answer the questions, such as displaying a password hint to the user. These self-service features are available to users through Novell iManager. Your choices are explained in [Section 4.3.3, "Selecting a Forgotten Password Action," on page 57](#).

## To create a challenge set:

- 1 In iManager, click *Passwords > Challenge Sets*.
- 2 Click *New*.

The screenshot shows the Novell iManager interface. The left sidebar contains a tree view with categories like Roles and Tasks, Credential Provisioning, Directory Administration, eDirectory Maintenance, Groups, Help Desk, Identity Manager, Identity Manager Utilities, iManager Demonstrations, Partitions and Replicas, Passwords, PBX, Provisioning Configuration, Rights, Role-Based Entitlements, Schema, Users, Workflow Administration, and Work Orders. The 'Passwords' category is expanded, showing sub-links for Check Password Status, Challenge Sets, Password Policies, Password Synchronization, View Policy Assignments, Set Universal Password, Email Server Options, and Edit Email Templates. The 'Challenge Sets' link is selected. The main content area is titled 'Challenge Sets' and contains a description: 'Challenge sets may be used as part of a password policy's method of authentication. Requiring a user to respond to challenge questions before receiving password information provides an additional level of security.' Below this are two text input fields: 'Challenge set name:' (with a hint '(ex. Engineering Challenge Set)') and 'Create in container:' (with the value 'Password Policies.Security'). There is an 'Add Question...' button. The 'Required Questions' section has a header and a list of questions with checkboxes: '[User Defined]', 'What is your mother's maiden name?'. The 'Random Questions' section also has a header and a list of questions with checkboxes: '[User Defined]', 'What is your User ID?', 'What is your PIN?', 'What is your childhood pet's name?'. At the bottom, there is a dropdown menu set to '1' with the text 'Number of random questions to ask user when password is forgotten'. 'OK' and 'Cancel' buttons are at the very bottom.

- 3 Type a name in the *Challenge set name* field, select a container for the challenge set to be created in, then select or create challenge questions.

To select a default question in the challenge set, select its check box.

To edit a question or the number of characters (minimum or maximum) allowed for responses, click the question.

To create a question and add it to the challenge set, click *Add Question*.

**User Defined:** If you select this option, users can create their own challenge question.

NMAS stores a user's user-defined questions and responses in Novell eDirectory.

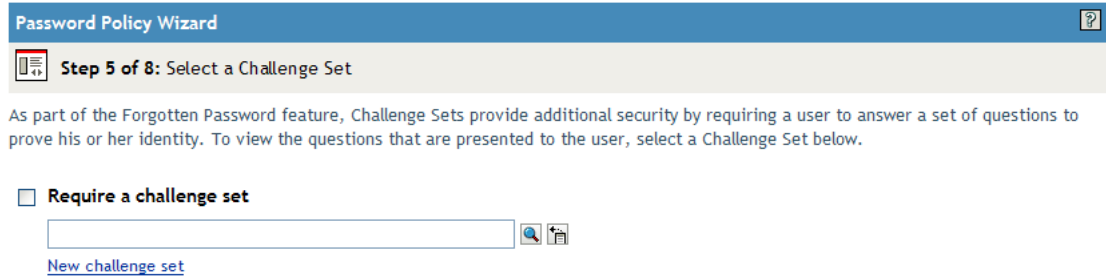
**Required Questions:** Questions in this list always appear when a user uses Password Self-Service.

**Random Questions:** Questions in this list appear only once as a complete set, when the user sets up Forgotten Password by answering the challenge set questions for the first time. When the user later needs to use Forgotten Password, only a few of the questions are presented for the user to answer. The number of random questions that appear depends on the number that you specify.

- 4 Click *OK*.

## To create a challenge set while using the Password Policy Wizard:

- 1 In iManager, launch the Wizard by clicking *Passwords > Password Polices > New*.
- 2 In Step 4, click *Yes* to enable Forgotten Password.
- 3 In Step 5, select *Require a Challenge Set* and then click *New challenge set*.



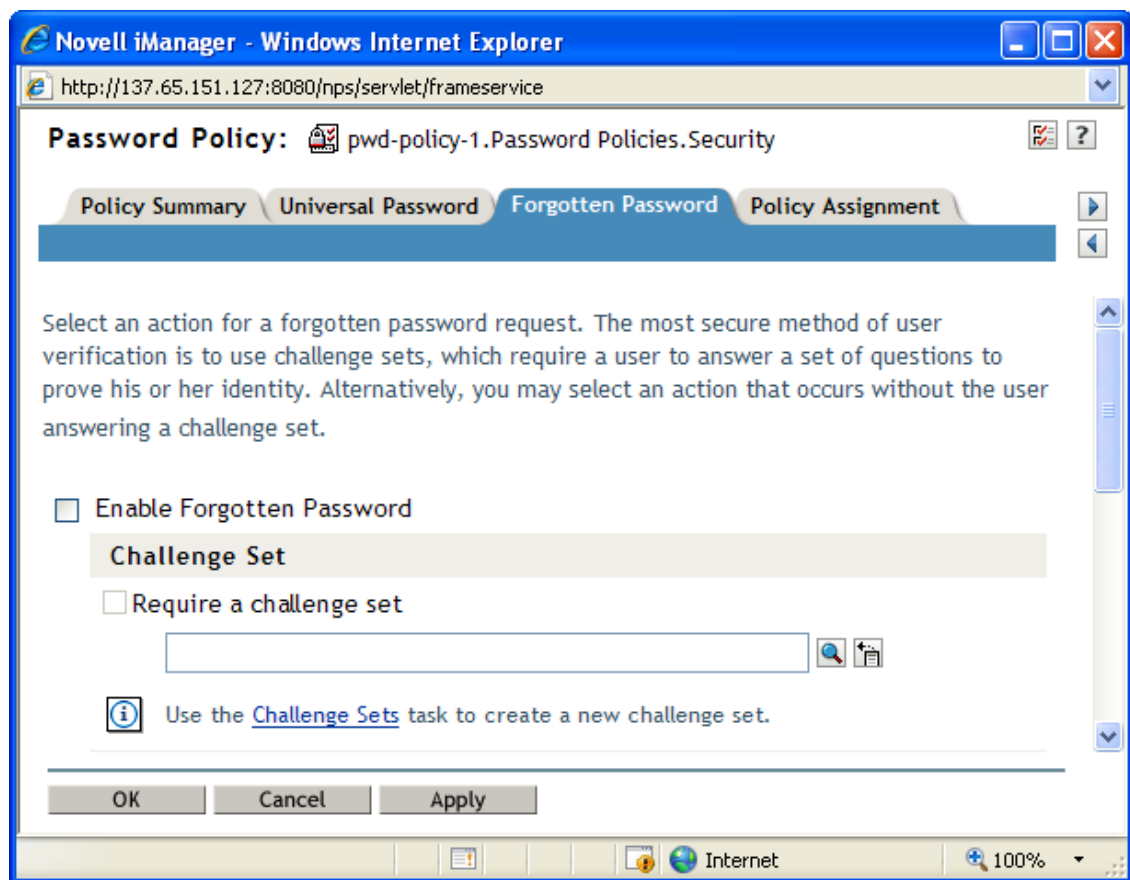
To use an existing challenge set, browse for and select it.

- 4 Specify the container you want the challenge set created in. Type a name in the *Challenge Set Name* field, then click *Next*.
- 5 Select or create required or random challenge questions.  
If you don't want to create new questions, select existing ones.  
To enable users to add their own questions, select *User Defined*.  
To create a new question:
  - 5a Click *Add Question*.
  - 5b Select *Administrator Defines the Question*, click *Add*, specify a language from the drop-down menu, type the question, then click *OK*.
  - 5c Select whether the question is required or random.
  - 5d Specify minimum and maximum characters required, then click *OK*
- 6 Specify the number of random question, then click *Next*.
- 7 Complete the remaining steps in the Password Policy Wizard.

## To create a challenge set for an existing password policy:

- 1 In iManager, click *Passwords > Password Policies*.
- 2 Click the name of a policy.
- 3 Click the *Forgotten Password* tab.
- 4 Select *Enable Forgotten Password > Require a Challenge Set*.





- 5 Browse for and select an existing challenge set or create a new one and then select the new one.  
To create a new one:
  - 5a Click the *Challenge Sets* link.
  - 5b In the Challenge Sets dialog box, click *New*.
  - 5c In the Challenge Sets dialog box, name the challenge set, specify a container to create the challenge set in, select or add required or random questions, then specify the number of random questions to ask.
  - 5d Click *OK*.

### 4.3.3 Selecting a Forgotten Password Action

- 1 In iManager, click *Passwords > Password Policies*.
- 2 Click the name of the policy.
- 3 Click the *Forgotten Password* tab.
- 4 Select the *Enable Forgotten Password* checkbox.
- 5 Select an action.
  - ♦ **Allow User to Reset Password:** After answering the challenge set questions to prove his or her identity, the user is allowed to change to a new password. Because the user has authenticated through answering the challenge questions, the user is allowed to change the

password without being required to provide the old password. To use this option, you must require a challenge set, and the user must have previously set up Forgotten Password in the iManager portal by answering the challenge set questions.

- ♦ **E-mail Current Password to User:** After answering the challenge set questions to prove his or her identity, the user receives the current password in an e-mail. To use this option, you must do the following:
  - ♦ Enable Universal Password for the policy. It is found in *Configuration Options* under *Universal Password*.
  - ♦ Enable the *Allow User to Retrieve Password* option, found in *Configuration Options* under *Universal Password*.
  - ♦ Set up e-mail notification as described in [Section 4.6, “Configuring E-Mail Notification for Password Self-Service,”](#) on page 68.

Also, the user must have previously set up Forgotten Password in iManager by answering the challenge set questions.

- ♦ **E-mail Hint to User:** The user receives the password hint in an e-mail. To use this option, you must set up e-mail notification as described in [Section 4.6, “Configuring E-Mail Notification for Password Self-Service,”](#) on page 68.

Also, the user must have previously set up Forgotten Password in iManager by providing a password hint.

- ♦ **Show Hint on Page:** The user is shown the password hint in the iManager portal. To use this option, the user must have previously set up Forgotten Password in iManager by providing a password hint.

## Password Hints

If you specify a Forgotten Password action that requires password hint, the user can enter a hint that is a reminder of the password.

- ♦ [“Password Hint”](#) on page 58
- ♦ [“Secure Hint”](#) on page 59

## Password Hint

The Password Hint attribute (`nsimHint`) is publicly readable, to allow unauthenticated users who have forgotten a password to access their own hints. Password hints can significantly reduce help desk calls.

For security, password hints are checked to make sure they do not contain the user's actual password. However, a user could still create a password hint that gives too much information about the password.

To increase security when using password hints:

- ♦ Allow access to the `nsimHint` attribute only on the `nds-cluster-config` server used for Password Self-Service.
- ♦ Remind users to create password hints that only they would understand. The Password Change Message in the password policy is one way to do that. See [Section 4.5, “Adding a Password Change Message,”](#) on page 67.

## Secure Hint

The Secure Hint attribute (`nsimPasswordReminder`) is more secure because it is not publicly readable. It requires the user to answer challenge questions before the hint is displayed.

The challenge/response requirement is set in the Forgotten Password section of the Password Policy properties.

If you choose not to use a password hint, make sure you don't use it in any of the password policies. To prevent password hints from being set, you can go a step further and remove the Hint Setup gadget completely, as described in [Section 4.3.4, “Disabling Password Hint by Removing the Hint Gadget,” on page 59.](#)


### 4.3.4 Disabling Password Hint by Removing the Hint Gadget

Password Hint is one method of helping users remember a password as part of Forgotten Password Self-Service. In the password policy, the Forgotten Password actions that use Password Hint are named E-mail Hint to User and Show Hint on Page.

For Password Hint to be useful to a user who has forgotten a password, unauthenticated users must have public access to the Password Hint attribute (`nsimHint`). Although Password Self-Service checks the password hint to make sure that the user has not included the actual password within the hint, you might still consider this public access to be a security issue.

If you don't want to use password hints, choose a different option for the Forgotten Password action in the password policy.

If you prefer to, you can remove the Hint Setup gadget completely. After installing the Identity Manager plug-ins for iManager, use the Configure view to remove the Hint Setup gadget by doing the following:

- 1 In iManager, click the *Configure* icon .
- 2 Click *Portal Platform Configuration > Gadgets*.
- 3 From the list of gadgets, select *Hint Setup*.
- 4 Click *Delete*.

After you delete the gadget, Hint Setup is no longer available to the user. The post-authentication services query for the existing gadgets before adding them to the delegation list. Regardless of what the policy states for post-authentication services, if the gadget does not exist, the service is not presented to the user by the post-authentication services or in the iManager portal.

After you delete the Hint gadget, make sure you don't select *E-mail Hint* or *Display Hint* as the forgotten password action in the password policy.

## 4.3.5 Configuring Forgotten Password Self-Service

Clicking the *Forgot your password?* link when logging in to the portal (<https://www.servername.com/nps> by default) does not work for the user unless the following conditions are met:

- ♦ The administrator has set up a password policy with Forgotten Password enabled.
- ♦ The user has set up challenge questions or a password hint, if either of them is specified in the Forgotten Password setting.
- ♦ [“Prompting Users to Set Up Forgotten Password” on page 60](#)
- ♦ [“User Setup for Forgotten Password” on page 61](#)
- ♦ [“Requiring Existing Passwords to Comply” on page 62](#)

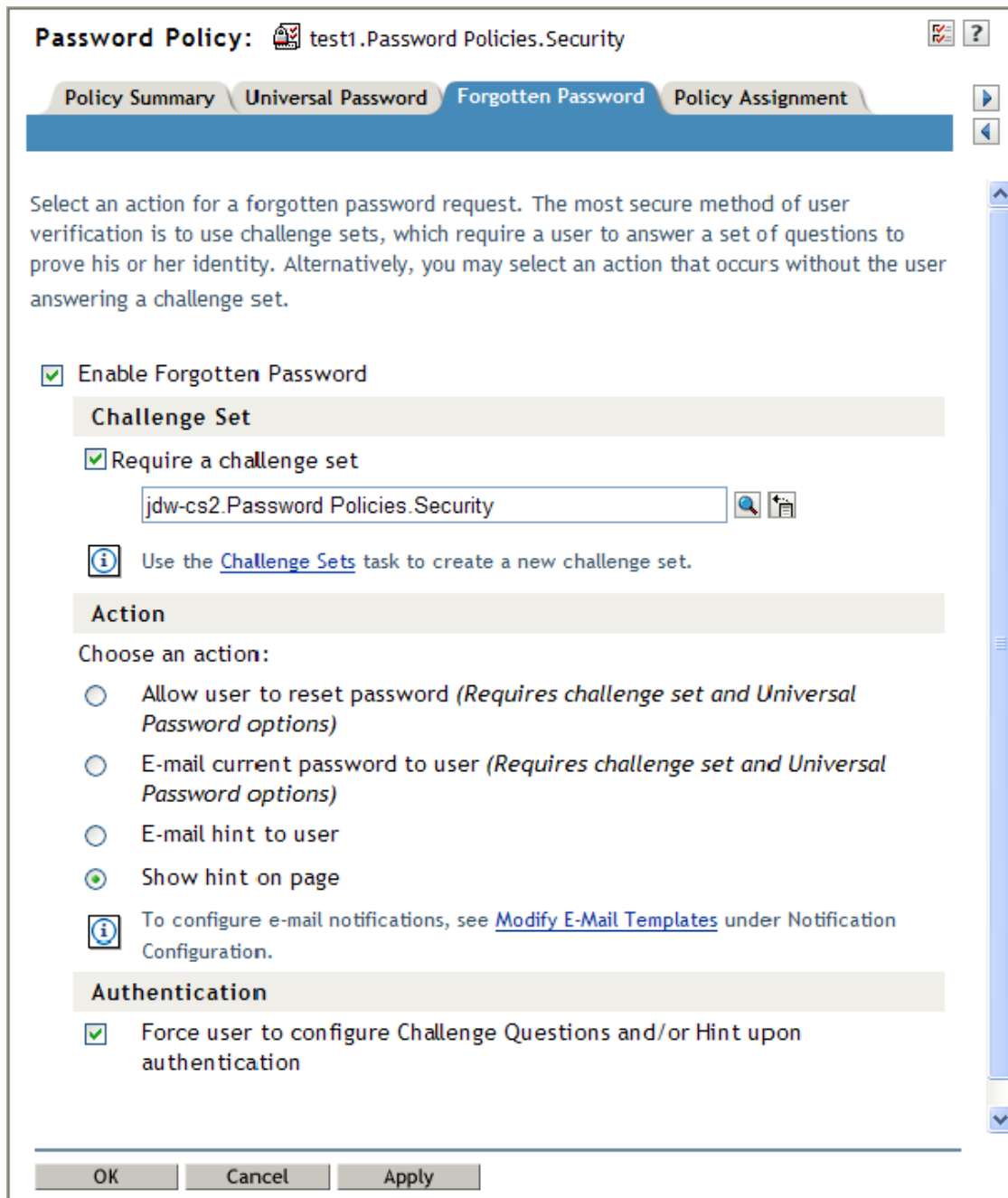
### Prompting Users to Set Up Forgotten Password

For some Forgotten Password actions, the user must do some setup before using the Forgotten Password self-service. For example, if the password policy specifies that a challenge set is used to allow a user to prove identity, and if the forgotten password action is to e-mail a password hint to the user, the user must first answer challenge-set questions and create a password hint before being able to use Forgotten Password Self-Service.

Users can initiate setting up these features in the portal, or you can require that users set them up by using post-authentication services, which are pages displayed when users log in to the portal.

To prompt users to set up these features at login time, select the *Force users to configure Challenge Questions and/or Hint upon authentication* option in the Password Policies interface at the bottom of the Forgotten Password page. This is selected by default when you create a policy.

Figure 4-2 Password Policy



To let users set up Forgotten Password at a time of their choice, you need to give them the URL for the portal, such as `https://www.my_iManager_server.com/nps`.

## User Setup for Forgotten Password

There are two ways the user's part of the configuration can be accomplished:

- ♦ “Post-Authentication” on page 62
- ♦ “In the Portal” on page 62

## Post-Authentication

The administrator can require the user to set up Forgotten Password features after a successful login by selecting the *Forgotten Password* option to force the user to configure challenge questions or a hint upon authentication. If this option is selected, but a user does not have questions or a hint set up, Forgotten Password configuration gadgets are displayed to the user the next time he or she logs in through the portal (<https://www.servername.com/nps> by default). This is called post-authentication setup.

## In the Portal

When users log in through the iManager portal, iManager gives them access to the gadgets for setting up or changing challenge sets and password hints for Forgotten Password Self-Service. This is the same place where users can initiate a password change. They can access the following gadgets here:

- ◆ Hint Setup
- ◆ Answer Challenge Questions
- ◆ Change Password (Universal)

The user can initiate changing these at any time. But if a hint or challenge set is not required for the user's password policy, the user cannot set them up. The page displays a message indicating that the options are not accessible.

To see specific examples of how these user options look in each application (iManager 2.02 portal, User Application portlet, Novell Client, and Virtual Office), refer to the documentation for each application as outlined in [Section 4.1, "Overview of Password Self-Service,"](#) on page 51.

## Requiring Existing Passwords to Comply

If you create or change a password policy, you can require users to change existing passwords that don't comply the next time they log in through the portal.

To do this, set an option in the password policy by using the *Universal Password* tab under *Configuration Options*. The option is called *Verify whether existing passwords comply with the password policy (verification occurs on login)*. By default, this option is turned off when you create a new password policy. The following figure illustrates the page where you set this option:

Figure 4-3 Requiring Existing Passwords to Comply

The screenshot shows the 'Configuration Options' tab of the 'Sample Password Policy' configuration window. The window title is 'Password Policy: Sample Password Policy.Password Policies.Security'. The 'Configuration Options' section is highlighted in green and contains the following settings:

- Enable Universal Password
- Enable the Advanced Password Rules

The 'Universal Password Synchronization' section is highlighted in grey and contains the following settings:

- Remove the NDS password when setting Universal Password
- Synchronize NDS password when setting Universal Password
- Synchronize Simple Password when setting Universal Password
- Synchronize Distribution Password when setting Universal Password

The 'Universal Password Retrieval' section is highlighted in grey and contains the following settings:

- Allow user to retrieve password
- Allow admin to retrieve passwords
- Allow the following to retrieve passwords

Below the 'Allow the following to retrieve passwords' option is a list box with the following content:

- Insert... | Remove
- DN

Below the list box is the text: 'No objects can retrieve the password - Select Insert'

The 'Authentication' section is highlighted in grey and contains the following setting:

- Verify whether existing passwords comply with the password policy (verification occurs on login)

A note is displayed with a yellow diamond icon:

**Note:** Your network might require preparation for the Universal Password to work properly.

To learn how to prepare your network for Universal Password, see the [Password Management Administration Guide](#).

At the bottom of the dialog box are four buttons: OK, Cancel, Apply, and Refresh.

If this option is set, the next time users log in through the portal, their passwords are checked for compliance with the password policy. If the password does not comply, a page similar to the following is displayed, and the user is not allowed to log in without changing the password.

Figure 4-4 Change Password

**Change Password**

**Notice:** Password policy requires password to conform to displayed rules.

You can now change your password. Type in your new password twice and make sure the password conforms to the displayed rules.

**Your password must have the following properties:**

- Minimum number of characters in password: 4
- Maximum number of characters in password: 12

**You may use numbers in your password**

**The password is case-sensitive**

**The password may use special characters**

**You cannot use the following character combinations as passwords:**

- novell
- admin

Old password:

New password:

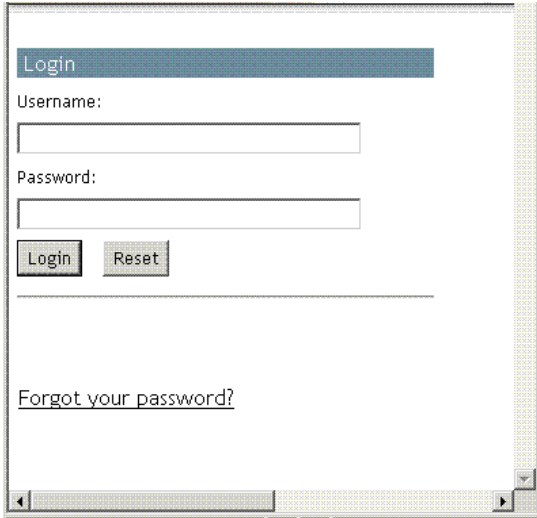
Retype password:

### 4.3.6 What Users See When They Forget Passwords

After you have installed the iManager plug-ins that shipped with Identity Manager, the *Forgotten Password* link shows up in the iManager portal (<https://www.servername.com/nps> by default), as illustrated in the following figure.



**Figure 4-5** *Forgotten Password in iManager*



A similar link is displayed when authenticating through Virtual Office and the Novell Client.

If a user clicks this link, the following page is displayed, asking for the user name:

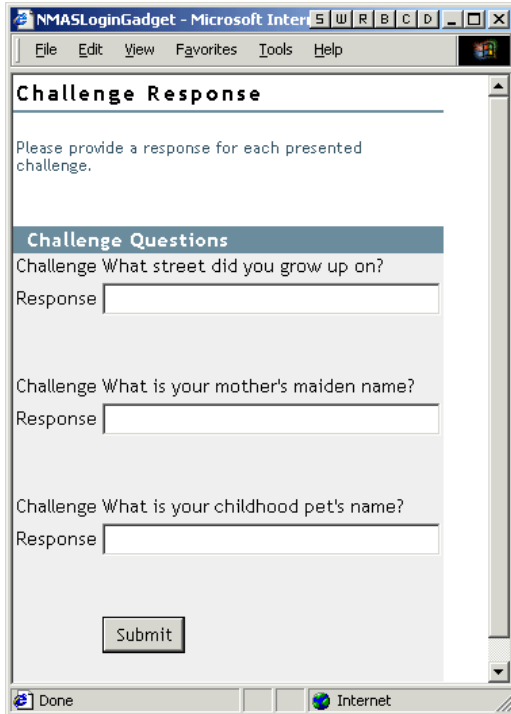
**Figure 4-6** *Forgotten Password in Virtual Office and Novell Client*



After the user name is entered, the Forgotten Password settings determine what the user sees.

For example, if the administrator specified in the password policy that a challenge set is used, a page similar to the following is displayed. The user must then answer challenge set questions to prove his or her identity.

**Figure 4-7** Forgotten Password Challenge Questions



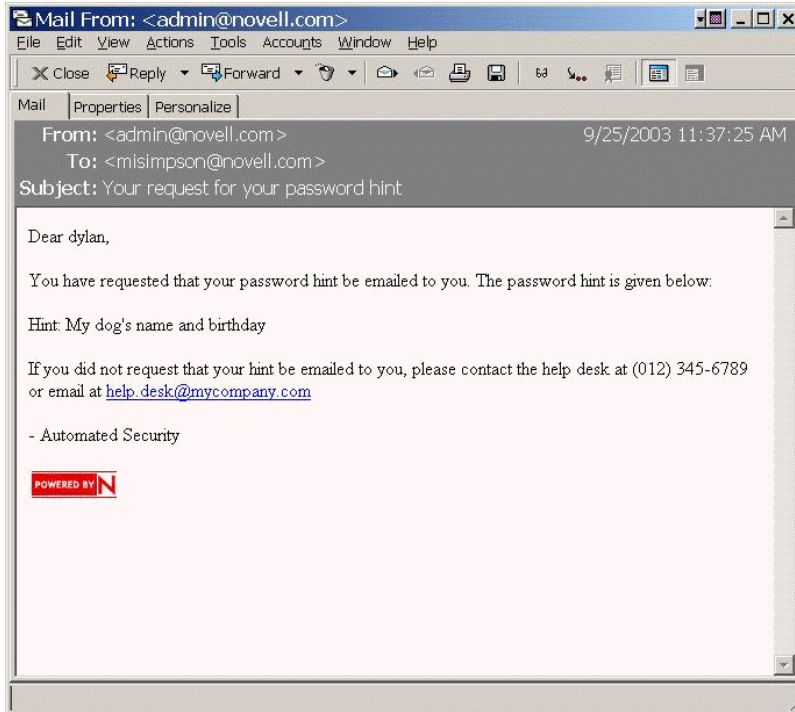
If the Administrator specified that the Forgotten Password action is *Show Hint on Page*, a page similar to the following is displayed:

**Figure 4-8** Forgotten Password Hint



If the Administrator specified that the Forgotten Password action is *E-mail Current Password to User* or *E-mail Hint to User*, a message is displayed saying that the password or hint has been e-mailed. The user receives an e-mail similar to the following:

**Figure 4-9** Password Hint E-Mail



## 4.4 Providing Users with Password Reset Self-Service

You can set up the password policy to allow users to reset their own passwords. How this is exposed to the user depends on which application they use to accomplish this task. See [Section 4.1, "Overview of Password Self-Service," on page 51](#) for documentation links to the different applications.

## 4.5 Adding a Password Change Message

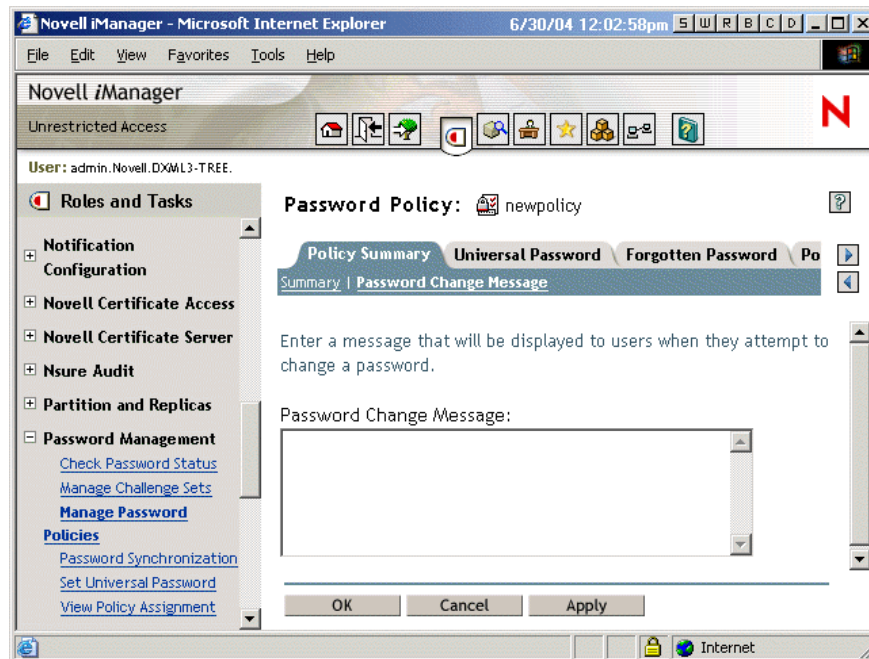
Although users can change their passwords whenever they choose to, they typically use the same passwords as long as possible. To increase security, you can use a password policy to require them to change it. That policy can contain a Password Change Message and the password rules. Whenever users change a password, they see this message along with the rules.

To edit the password policy and create this message:

- 1 In iManager, click *Passwords > Password Policies*.
- 2 Click the name of the password policy you want to add a message to.
- 3 Click *Policy Summary > Password Change Message*.

The following page appears:

Figure 4-10 Password Change Message



- 4 Type the message you want users to see, then click *OK*.

## 4.6 Configuring E-Mail Notification for Password Self-Service

The iManager role named Notification Configuration lets you specify the e-mail server and customize the templates for e-mail notifications.

E-mail templates are provided to allow Password Synchronization and Password Self-Service to send automated e-mails to users.

You don't create the templates. Instead, they are provided by the application that uses them. The e-mail templates are Template objects in eDirectory, and they are placed in the Security container, usually found at the root of your tree. Although they are eDirectory objects, you should edit them only through the iManager interface.

This is a modular framework. As new applications are added that use e-mail templates, the templates can be installed along with the applications that use them.

Identity Manager provides templates for Password Synchronization and Forgotten Password notifications. You control whether e-mail messages are sent, based on your choices in the iManager interface.

For Forgotten Password, e-mail notifications are sent only if you choose to use one of the Forgotten Password actions that causes an e-mail to be sent: e-mail password to user or e-mail password hint to user.

The following information is discussed in this section:

- ♦ [Section 4.6.1, "Prerequisites," on page 69](#)
- ♦ [Section 4.6.2, "Setting Up the SMTP Server to Send E-Mail Notification," on page 69](#)
- ♦ [Section 4.6.3, "Setting Up E-Mail Templates for Notification," on page 70](#)

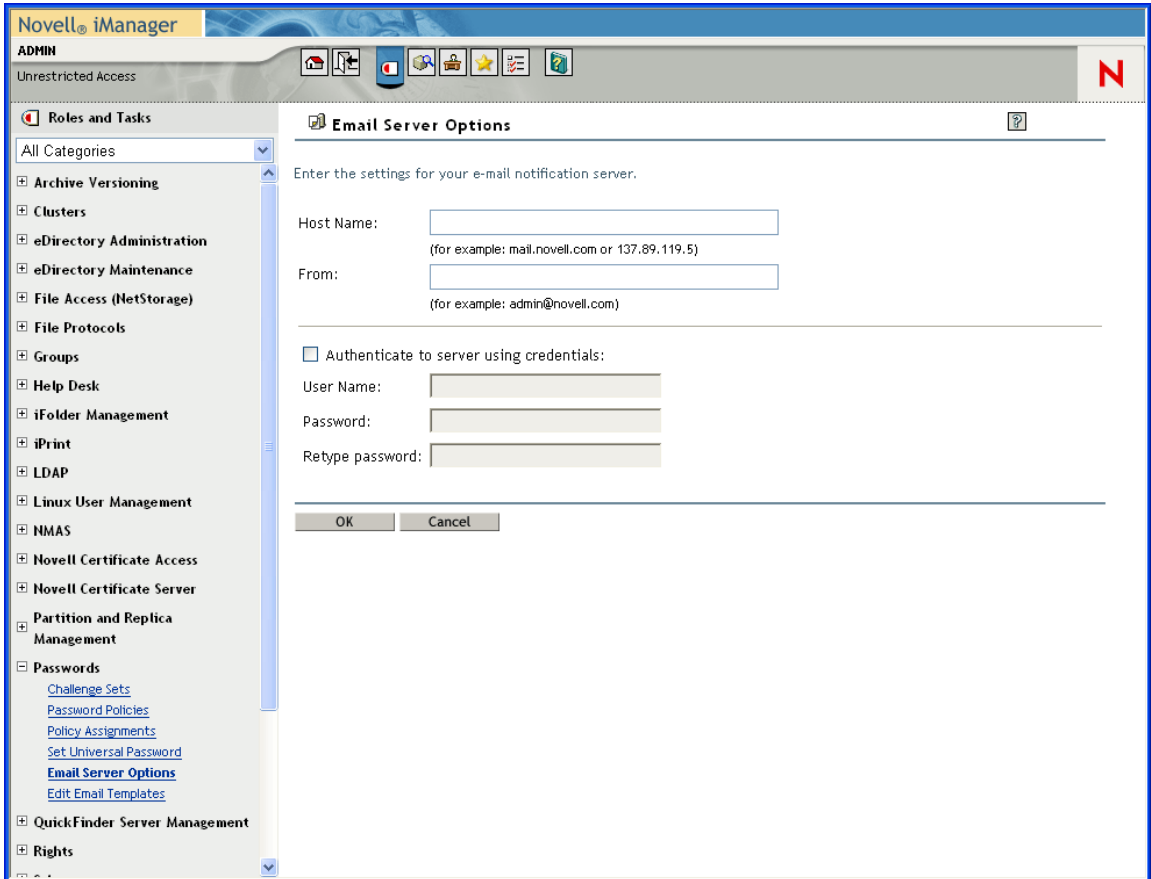
## 4.6.1 Prerequisites

- ◆ Make sure that your eDirectory users have the Internet EMail Address attribute populated.

## 4.6.2 Setting Up the SMTP Server to Send E-Mail Notification

- 1 In iManager, click *Passwords > E-mail Server Options*.

The following page appears:



The screenshot shows the Novell iManager interface. The title bar reads 'Novell iManager' and 'ADMIN'. Below the title bar, there is a navigation pane on the left with a tree view containing categories like 'Roles and Tasks', 'Archive Versioning', 'Clusters', 'eDirectory Administration', 'eDirectory Maintenance', 'File Access (NetStorage)', 'File Protocols', 'Groups', 'Help Desk', 'iFolder Management', 'iPrint', 'LDAP', 'Linux User Management', 'NMAS', 'Novell Certificate Access', 'Novell Certificate Server', 'Partition and Replica Management', 'Passwords', 'QuickFinder Server Management', and 'Rights'. The 'Email Server Options' page is displayed in the main area. It has a header 'Email Server Options' with a help icon. Below the header, it says 'Enter the settings for your e-mail notification server.' There are four input fields: 'Host Name:' with a text box and a note '(for example: mail.novell.com or 137.89.119.5)'; 'From:' with a text box and a note '(for example: admin@novell.com)'; 'Authenticate to server using credentials:' with a checkbox; 'User Name:' with a text box; 'Password:' with a text box; and 'Retype password:' with a text box. At the bottom, there are 'OK' and 'Cancel' buttons.

- 2 Specify the following information:

- ◆ Hostname
- ◆ Name you want to appear in the From field of the e-mail message, such as "Administrator"
- ◆ User name and password for authenticating to the server, if necessary

- 3 Click *OK*.

- 4 Customize the e-mail templates as described in ["Setting Up E-Mail Templates for Notification"](#) on page 70.

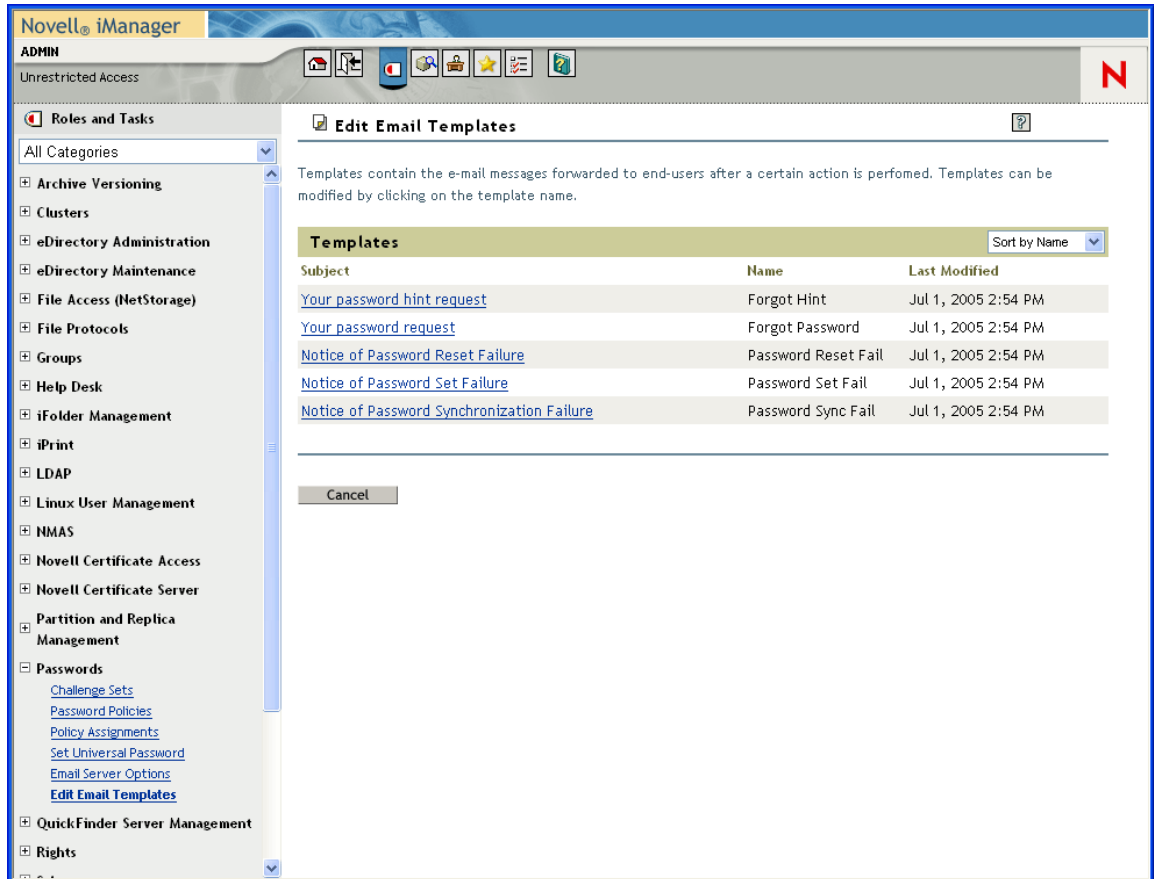
After the e-mail server is set up, e-mail messages can be sent by the applications that use them, if you are using the features that cause messages to be sent.

## 4.6.3 Setting Up E-Mail Templates for Notification

You can customize these templates with your own text. The name of the template indicates what it is used for. Email templates offer language support.

- 1 In iManager, click *Passwords > Edit Email Templates*.

A list of templates appears, as in the following example:



- 2 Edit the templates as desired.

Keep in mind that if you want to add any replacement tags, some additional tasks might be required.

## 4.7 Testing Password Self-Service

To verify that the features are set up correctly, complete the following as part of testing Password Self-Service:

- 1 Create a policy with the following characteristics. For information on how to accomplish this, see, [“Creating or Editing Challenge Sets” on page 54](#).
  - ◆ Enable Forgotten Password
  - ◆ Require Challenge Set

- ◆ Select the option to verify that the challenge response and hint are configured on login
  - ◆ Assign the password policy to a container with at least one user you can use to test with. This user is the user who has the e-mail address indicated on the User object in the Internet EMail Address attribute.
- 2 Make sure you have another user to test with who does not have a password policy assigned.
  - 3 To test password self-service, use the Identity Manager User Application. For information on how to do this, see *“Using the Identity Self-Service Tab” in the Novell Identity Manager Roles Based Provisioning Module 4.0.1 User Application User Guide* (<http://www.novell.com/documentation/idm401/ugpro/?page=/documentation/idm401/ugpro/data/ugpropartidentity.html>).
- For Windows users, test password self-service using the Novell Client. For information on how to do this, see *“Using Forgotten Password Self-Service” in the Novell Client for Windows Administration Guide* ([http://www.novell.com/documentation/windows\\_client/windows\\_client\\_admin/data/bxne05q.html](http://www.novell.com/documentation/windows_client/windows_client_admin/data/bxne05q.html)).

## 4.8 Adding Password Self-Service to Your Company Portal

Most of the procedures in the [Password Self-Service](#) section assume that you are using the Password Self-Service features on an iManager 2.0.2 server, which is the last version of iManager to support password self-service. If you have a version of iManager later than 2.0.2, you can only perform password self-service through Novell’s User Application. For more information on performing password self-service using Novell’s User Application, see *“Using the Identity Self-Service Tab” in the Novell Identity Manager Roles Based Provisioning Module 4.0.1 User Application User Guide* (<http://www.novell.com/documentation/idm401/ugpro/data/ugpropartidentity.html>).

Refer to the following table for instructions on how Password Self-Service features can be used with portal products, including products other than iManager.

**Table 4-1** Password Self-Service Features and Portal Products

Product	Support for Password Self-Service	Procedure
iManager 2.0.2	You can integrate the features.  This product supports Password Self-Service features if you install the password management plug-ins. These plug-ins are included with the Identity Manager 3 and are also available separately from <a href="http://download.novell.com">download.novell.com</a> .	Follow the steps in <ul style="list-style-type: none"> <li>◆ <a href="#">Section 3.3, “Prerequisite Tasks for Using Password Policies,” on page 28.</a></li> <li>◆ All procedures in <a href="#">“Password Self-Service” on page 51</a>, except for <a href="#">“Adding Password Self-Service to Your Company Portal” on page 71</a>, which is not necessary for iManager 2.02.</li> </ul>
Identity Manager User Application	User application allows users to perform password self-service tasks.	See Chapter 2, <a href="#">“Using the Identity Self-Service Tab” in the <i>Novell Identity Manager Roles Based Provisioning Module 4.0.1 User Application User Guide</i></a> ( <a href="http://www.novell.com/documentation/idm401/ugpro/data/ugpropartidentity.html">http://www.novell.com/documentation/idm401/ugpro/data/ugpropartidentity.html</a> ).

Product	Support for Password Self-Service	Procedure
Virtual Office, provided with NetWare 6.5 Support Pack 2, running on an iManager server	<p>You can integrate the features.</p> <p>You can use the Password Self-Service features on the same NetWare server used for Virtual Office and iManager by installing the plug-ins and completing some additional steps.</p>	<p><a href="#">Section 4.8.1, "Integrating Password Self-Service with Virtual Office," on page 72</a></p>
Novell Portal Services (NPS) versions earlier than 4.1	<p>You must link to the features.</p> <p>Although these legacy NPS products run Novell portal modules (NPMs), they don't have some of the enhancements that are required for the Password Self-Service features of the <code>ForgottenPassword.npm</code>.</p> <p>To use this product with Password Self-Service, create links from your company portal to the end-user password features on an iManager server.</p>	<p><a href="#">Section 4.8.2, "Linking to Password Self-Service from a Company Portal," on page 73</a></p>
Third-party products	<p>You must link to the features.</p> <p>Because third-party products don't run Novell portal modules, you can't use the Password Self-Service features directly in another product.</p> <p>To use third-party products with Password Self-Service, create links from your company portal to the end user password features on an iManager server.</p>	<p><a href="#">"Linking to Password Self-Service from a Company Portal" on page 73</a></p>

## 4.8.1 Integrating Password Self-Service with Virtual Office

Virtual Office supports all the features of Password Self-Service in NetWare 6.5 Support Pack 2 and later, and with OES 1 Linux. Virtual Office is not supported on OES 2 Linux.

For instructions, see the [Novell Open Enterprise Server Virtual Office Configuration Guide \(http://www.novell.com/documentation/oes/virtualoffice/data/am0ogoi.html\)](http://www.novell.com/documentation/oes/virtualoffice/data/am0ogoi.html).



## 4.8.2 Linking to Password Self-Service from a Company Portal

For products that can't provide the Password Self-Service features by running the `ForgottenPassword.npm`, as noted in [Table 4-1 on page 71](#), you can use the Password Self-Service features by creating another iManager server with the password management plug-ins installed and then linking from your portal home page to the iManager portal on the other server, such as `https://iManager_server_IP_address/nps`.

The password management plug-ins are included with the Identity Manager plug-ins and are available separately by downloading the Password Administration Plug-in for iManager 2.x from <http://download.novell.com>.

Complete the tasks in these sections:

- ♦ [“Prerequisites” on page 73](#)
- ♦ [“Linking to Forgotten Password Self-Service” on page 73](#)
- ♦ [“Linking to User Password Management Tasks” on page 74](#)
- ♦ [“Returning Self-Service Users to the Company Portal” on page 75](#)
- ♦ [“Making Sure Users Have Configured Password Features” on page 76](#)

### Prerequisites

The iManager server and the tree you are using must be prepared as follows:

- ♦ Meet the prerequisites described in [Section 3.3, “Prerequisite Tasks for Using Password Policies,” on page 28](#)
- ♦ Make sure you have set up password policies for your eDirectory users

### Linking to Forgotten Password Self-Service

To give users access to Forgotten Password Self-Service from your company portal, you can link to that service on a separate iManager Web server.

- 1 Create a link such as “Forgot your password?” on the login page for your company portal and point it to the following URL on your iManager Web server:

```
http://iManager_server_IP_address/nps/servlet/  
fullpageservice?NPService=ForgotPassword&nextState=getUserID
```

This URL takes users to the following page, where they begin the Forgotten Password process.



- 2 To customize the return page to go to the login page for your company portal, complete the steps in [“Returning Self-Service Users to the Company Portal”](#) on page 75.

## Linking to User Password Management Tasks

- 1 Make sure all the eDirectory users in the portal users container have rights to the Hint attribute, which is named nsimHint.

When you install the DirXML plug-ins on an iManager Web server, this step is automatically completed for the tree that iManager is configured for.

If you are pointing to a different tree, you must complete this step manually.

A utility is provided to help you do this, which you can download and run by doing the following:

- 1a Go to <http://download.novell.com>.
- 1b Fill in the following fields:
  - ♦ **Search By:** Product
  - ♦ **Choose a Product:** Novell Identity Manager
- 1c Download the item named 2.0 Password Management Plug-in for iManager 2.0.x.
- 1d Follow the instructions in the `nsimhintreadme.txt` file.

If users do not have rights to the nsimHint attribute, they get an error like the following when they try to create a hint:

“Could not write user hint” (Task could not be completed).

- 2 Provide users with a link from your company portal to the password management tasks.

You can create a *Manage Passwords* link from the company portal and link to `https://other_iManager_server/nps`. This link would provide access to the Password Management end user tasks:

- ♦ Hint Setup

- ◆ Answer Challenge Questions
- ◆ Change Password (Universal)

A user who clicks on the link would first need to log in and then would see a page like the following example:

Username: admin

**Hint Setup**

**Answer Challenge Questions**

**Change Password (Universal)**

**Define Password Hint**

Please enter a password hint to help you remember your password.

**Create a Password Hint**

Username: admin

Password

Hint: myhint

Submit

- 3 Complete the steps in [“Returning Self-Service Users to the Company Portal”](#) on page 75.

## Returning Self-Service Users to the Company Portal

The Password Self-Service features include scenarios in which users are provided with a link that lets them return to the login page. For example, when a user changes a password by using the Forgotten Password Self-Service, a page is displayed with the message Your password has been successfully changed. Click here to return to login page.

If you point from your company portal to Password Self-Service on a separate iManager server, you might want to customize the default return page so that users are returned to the login page for your company portal when they complete password tasks. By default, clicking the button returns the user to a page on the iManager Web server.

A link to return to the login page is provided in these three places:

- ◆ The page where a user can set a new password
- ◆ The page displayed after a user successfully changes a password
- ◆ The page where a user views a hint

To customize the return page to go to the login page for your company portal:

- 1 On the iManager Web server you are using for Forgotten Password Self-Service, locate the following directory:

```
\tomcat\webapps\nps\portal\modules\ForgottenPassword\skins\default\devices\default
```

- 2 Locate the following file in that directory:

```
forgottenpassword.xsl
```

- 3 Edit the `forgottenpassword.xml` file to customize the default return page.

Replace the code

```
href="{LoginURL}"
```

with a hard-coded URL such as

```
href="(http:\\www.your_company_portal_home_page.com)"
```

You need to make this change in three places in the file.

- 4 Stop and restart Tomcat on the iManager server.

The Return to Login Page links now redirect users to your company's portal login page.

### 4.8.3 Making Sure Users Have Configured Password Features

When users log in to the iManager portal at `https://iManager_server_IP_address/nps`, they are prompted to take action through a series of post-authentication pages if conditions such as the following are true:

- ♦ The user password doesn't comply with Advanced Password Rules in the password policy
- ♦ The password policy requires Challenge Questions when using Forgotten Password Self-Service and the user has not configured these questions
- ♦ The password policy is using Forgotten Password with Display Password Hint as the action and the user has not created a hint

For example, these prompts are necessary to make sure that the user can use Forgotten Password Self-Service. If the password policy requires users to answer Challenge Questions and the user has never configured them initially, the user can't access Forgotten Password Self-Service. If the user has not created a password hint, the user can't retrieve it to help in remembering the password.

Because other portal products won't automatically provide the post-authentication features, you need to make sure that users log in to the iManager portal at least once to create compliant passwords and complete password management setup, and then again whenever you make changes to Password Policies.

This can be done by making sure that users go to a Manage Passwords link you provide as described in [“Linking to User Password Management Tasks” on page 74](#), which requires users to log in to the iManager portal.

## 4.9 Troubleshooting Password Self-Service

- ♦ To use Challenge Response questions, make sure that you are using a browser that iManager 2.02 supports.
- ♦ If you don't have SSL set up properly, you won't be able to log in to iManager or the portal. If you can log in successfully to iManager and you are requiring TLS for Simple Bind, SSL is set up properly and you can rule out SSL-related issues when troubleshooting Password Self-Service.

---

# A Security Considerations

Reversible encryption of Universal Password is required for convenient interoperability with other password systems. Administrators must evaluate the costs and benefits of the system. Using a Universal Password stored in eDirectory might be more secure or convenient than attempting to manage several passwords.

A Universal Password in eDirectory is protected by three levels of security: triple DES encryption of the password itself, eDirectory rights, and file system rights.

- ◆ The Universal Password is encrypted by a triple DES, user-specific key. Both the Universal Password and the user key are stored in system attributes that only eDirectory can read. The user key (3DES) is stored encrypted with the tree key, and the tree key is protected by a unique NICKI key on each machine. Note that neither the tree key nor the NICKI key is stored within eDirectory. They are not stored with the data they protect. The tree key is present on each machine within a tree, but each tree has a different tree key, so data encrypted with the tree key can be recovered only on a machine within the same tree. Thus, while stored, the Universal Password is protected by three layers of encryption.
- ◆ Each key is also secured via eDirectory rights. Only administrators with the Supervisor right or the users themselves have the rights to change Universal Passwords.

---

**NOTE:** The password policy can be configured to allow Universal Password to be read by administrators and for users to read their own passwords through using NICKI/nds-cluster-config extensions. This is not enabled by default.

---

- ◆ File system rights ensure that only a user with the proper rights can access keys.

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

- ◆ Make sure that the following directories and files are secure:

---

Windows	\system32\novell\nici  \system32\ where the NICI DLL is installed
Linux/Unix	/var/novell/nici  etc/nici.cfg  /usr/local/lib/libccs2.so and the NICI shared libraries in the same directory  On LSB-compliant systems, make sure the following directories are also secure:  /var/opt/novell/nici  etc/opt/novell  /opt/novell/lib

---

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

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

For security consideration relating to password management, see the *Novell Modular Authentication Services 3.3 Administration Guide* (<http://www.novell.com/documentation/nmas33/admin/data/a20gkue.html>).