Novell
Password Management

3.0

www.novell.com

ADMINISTRATION GUIDE

October 13, 2005

Novell®

Legal Notices

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

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

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

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

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

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

Novell Trademarks

Third-Party Materials

Contents

About This Guide

This guide provides 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. It is written primarily for network administrators.

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_management/index.html).

Documentation Conventions

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

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

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Overview

1

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

1.1 Universal Password

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

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

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

  The limitations of the simple password are that no password policy (minimum length, expiration, etc.) is enforced. Also, by default, users do not have rights to change their own simple passwords.
- Enhanced Password: The enhanced password offers some password policy, but its design is not consistent with other passwords. It provides a one-way synchronization and it replaces the simple or NDS password.

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

Universal Password was created to address these password problems by

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

For detailed information, see Chapter 2, “Deploying Universal Password,” on page 11.

1.2 Password Policies

With the release of Universal Password, Novell introduced 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.

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

You manage password policies using iManager.

For more information, see Chapter 3, "Managing Passwords by Using Password Policies," on page 23.

1.3 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 using iManager. Users access the password self-service features using one of the following:

- iManager 2.02 portal
- Novell Client™
- Virtual Office
- eXtend Director

For more information, see Chapter 4, "Password Self-Service," on page 41.

1.4 Password Synchronization

Using Password Synchronization, you can also enforce password policies on connected systems, as explained in Chapter 5, "Password Synchronization across Connected Systems," on page 77.

Deploying Universal Password

2

This section decribes how to deploy and manage Universal Password.

2.1 Universal Password Background

Universal Password is managed by the Secure Password Manager (SPM), a component of the NMAS™ module (nmas.nlm on NetWare®). SPM simplifies the management of password-based authentication schemes across a wide variety of Novell® products as well as 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 the NetWare 6.5 or later and eDirectory™ 8.7.3 or later install; however, Universal Password is disabled by default. Because all APIs for authentication and setting passwords are moving to support Universal Password, all the existing management tools, when run on clients with these new libraries, automatically work with the Universal Password.

NOTE: Password Management 2.02 for Novell eDirectory for iManager 2.*x* is available for download at the Novell Free Download Site (http://download.novell.com). Minimum requirements are eDirectory 8.7.3 or later and iManager 2.02 or later.

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, Novell Client has the capability of automatically upgrading/migrating the NDS password to the Universal Password.

2.1.1 How Secure Is Universal Password?

Reversible encryption of Universal Password is required for convenient interoperation with other password systems. Administrators have to evaluate the costs and benefits of the system. Using a Univeral 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, and file system rights.

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

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

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

NetWare	%system32%\novell\nici
Windows	%system32%\novell\nici
	%system32% where the NICI DLL is installed
Linux/Unix	/var/novell/nici
	etc/nici.cfg
	/usr/locall/lib/libccs2.so and the NICI shared libraries in the same directory
	On LSB-compliant systems:
	The above mentioned directories and files as well as
	/var/opt/novell/nici
	etc/opt/novell
	/opt/novell/lib

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

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

2.2 Deployment Steps

Follow the steps below to deploy Universal Password:

2.2.1 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:

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. Uses the NDS® password, which is based on the RSA public/private key system.	• Has limited support for passwords with extended characters • Passwords are inaccessible from non-Novell systems • Passwords are stored in such a way as to prevent extraction, thus disallowing interoperability with the simple password
Windows Native Networking (CIFS) in NetWare 6 and NetWare 5.1 (NFAP add-on pack for NetWare 5.1)	Novell's CIFS server as part of the Native File Access Protocols. It allows Windows clients to access Novell services using the built-in Windows Client Networking Services.	• Uses a separately administered password called the simple password • Has no expiration or restriction capabilities for the simple password • Attempts to synchronize with NDS password but can get out of sync
Macintosh* Native Networking (AFP) in NetWare 6 and NetWare 5.1 (NFAP add-on pack for NetWare 5.1)	Novell's AFP server as part of the Native File Access Protocols. It allows Macintosh clients to access Novell services using the built-in Macintosh Client Networking Services.	• Uses a separately administered password called the simple password • Has no expiration or restriction capabilities for the simple password • Attempts to synchronize with the NDS password but can get out of sync
LDAP	Novell's LDAP services allow a user to bind using username and password across a Secure Sockets Layer (SSL) connection.	• Limited interoperability with Novell Client services (NDS password) for extended character or international versions • Attempts to utilize the simple password if bind is not a simple bind (that is, the bind is using an encrypted password)
LDAP User Import	Uses ICE or other tools to import users from foreign directories into eDirectory. Passwords are also brought in.	• Passwords are imported into the simple password system • Mutually exclusive of NFAP solutions (Windows and Macintosh Native File Access) if not clear text password • Password is in its encrypted native format
Web-Based Services	Novell Web-based services (Apache Web server) authentications. This includes eGuide, Novell Portal Services, and other Web-based applications.	• Limited interoperability with Novell Client services (NDS password) for extended character or international versions • Not designed to check the simple password
RADIUS Services	Novell RADIUS Authentication Services	• Limited interoperability with the Novell Client services (NDS password) for extended character or international versions

Service	Description	Limitations
NetWare Remote Manager	Novell's Web-based server health and management interface.	• Limited interoperability with Novell Client services (NDS password) for extended character or international versions • Not designed to check the simple password
NDS for NT	Novell eDirectory services for Microsoft Windows NT 4 Server domains.	• Uses a separate value for storing the NT password • Synchronized only with the NDS password by the Novell Client and the ConsoleOne® and NWAdmin snap-in tools
DirXML® Password Synchronization for Windows 1.0 and DirXML Starter Pack	Enables synchronization of passwords for NT, Active Directory, and eDirectory accounts.	• eDirectory password changes made outside of the Novell Client are not synchronized. For example, an eDirectory password change made through eGuide would not be synchronized to Active Directory or NT. See Sample Password Scenarios (http://www.novell.com/documentation/lg/dirxmlstarterpack/jetset/data/aktnwz0.html) for detailed information about DirXML Password Synchronization for Windows.

2.2.2 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 Novell Client for Windows to access Novell file and print services?
- Do you plan to use Novell Nsure® Identity Manager 2, powered by DirXML, with its enhanced password policy and password synchronization capabilities?
- Do you plan to use Nterprise™ Branch Office™ 2.0?

2.2.3 Step 3: Make Sure Your Security Container is Available

NMAS relies on storage of policies that are global 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 of 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.

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

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 must be on the NMAS server.

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

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

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

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

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

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

1b Log in as an Administrator by entering the server (full context), the tree name, the username, and the password.

1c Check to make sure all you servers are using 168 bit keys.

Follow the instructions in Novell TID 10093969 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093969.htm) to ensure this requirement is met.

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

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

If no problems are found, go to "Step 5: Upgrade at Least One Server in the Replica Ring to NetWare 6.5 or Later or eDirectory 8.7.3 or Later" on page 17.

If problems are found, follow the instructions written to the sys:system\sdinotes.txt file to resolve any configuration and key issues. Continue with Step 2.

2 Verify that the SDI Domain Key Servers are running NICI 2.6.*x* or later.

We recommend that NetWare 6.5 or later or eDirectory 8.7.3 or later be installed on your SDI Domain Key servers.

To find out if NICI 2.6.*x* is installed on these servers:

2a At the server console, enter the NetWare command `M NICISDI.NLM`.

The version must be 264*xx.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 Free Download site (http://download.novell.com). Select NICI from the Product or Technology drop-down list, then click Search. NICI 2.4.2 requires eDirectory 8.5.1 or later.
- Update the SDI Domain Key servers to NetWare 6.5 or later or eDirectory 8.7.3 or later.
- Remove the servers as SDI Domain Key Servers and add a NetWare 6.5 or eDirectory 8.7.3 or later server.

  To remove a server as an SDI Domain Key Server

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

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

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

  2. Log in as an administrator that has 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

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

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

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

  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.

2b (Optional) After completing one of the options above, you might want to rerun the SDIDIAG check command.

See Step 1d on page 15.

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

2.2.5 Step 5: Upgrade at Least One Server in the Replica Ring to NetWare 6.5 or Later or 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 NetWare 6.5 or later or 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 eventually upgrade them all. Plan to upgrade the servers that hold writable replicas first, followed by those with read-only replicas or no replicas. This allows Universal Password support for services on all those servers.

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

2.2.6 Step 6: Check the Container for SDI Key Consistency

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

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

   At a Windows server, open a command prompt box and run sdidiag.exe.
2. Enter the command `CHECK -v >> sys:system\sdinotes.txt -n` *`container DN`*.

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

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

   The output to the screen displays the results of the `CHECK` command.
3. If no problems are reported, you are ready to enable Universal Password. Go to "Step 7: Enable Universal Password" on page 18.

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

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

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

2.2.7 Step 7: Enable Universal Password

To turn on Universal Password, do the following:

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

2.2.8 Step 8: Deploy Novell Client Software

You can deploy the Novell Client for Windows version 4.9/4.9.1, but the client does not take advantage of these services until you enable Universal Password (see "Step 7: Enable Universal Password" on page 18).

The new Novell Client software automatically starts using the Universal Password. Users see no differences in the client, except with case-sensitive passwords.

NOTE: Novell Client 4.9 includes NMAS Client 2.7. Novell Client 4.9.1 includes NMAS Client 3.0.

2.3 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 using the Password Management plug-in). This way, NetWare 6 and 5.1 servers running Native File Access protocols for Windows and Apple* native workstations continue to have their passwords function properly. 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, also have their passwords continue to function properly.

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

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 of NetWare 4, 5, and 6 servers. However, when all servers are upgraded to NetWare 6.5, extended character passwords can be used.

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

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

Password Change Method	Passwords Synchronized
Novell Client software 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.
Native File Access (Windows or Macintosh) on NetWare 5.1 or NetWare 6	Simple password and NDS password. The password change is successful only if the old NDS and simple passwords were in sync.
Native File Access (Windows or Mac) on NetWare 6.5	Universal, simple, and NDS passwords are changed. All are synchronized, even if old ones were out of sync.
LDAP (standard) earlier than eDirectory 8.7.3	NDS password only.
LDAP (extended) earlier than eDirectory 8.7.3	Simple password or NDS password is changed (extensions specify which one).
LDAP (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.
LDAP (extended) to NetWare 6.5	Universal, simple, or NDS password changed (extensions specify which one).
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 5.1or 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 is a separate change password page for NDS password and simple password.

Password Change Method	Passwords Synchronized
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.
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 is a separate change password page for NDS password and simple password.
Novell iManager 1.5 (NetWare 5.1 or NetWare 6 only) to any User object in any container	NDS password only.
Novell iManager 2.0 (NetWare 6.5 only) to a User object in a container that has a R/W replica on a NetWare 6.5 server (or NetWare 5.1 or 6 running eDirectory 8.7.3)	Universal, simple, and NDS passwords are changed. All are synchronized even if old ones were out of sync.
Novell iManager 2.0 (NetWare 6.5 only) to a User object in a container that does not have any R/W replica on any NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 8.7.3	NDS password only.
NetWare Remote Manager running on a NetWare 6.5 server to a User object in a container that has a R/W replica on a NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 8.7.3	Universal, simple, and NDS passwords are changed. All are synchronized, even if old ones were out of sync.
NetWare Remote Manager running on a NetWare 6.5 server to a User object in a container that does not have a R/W replica on a NetWare 6.5 server, or NetWare 5.1 or 6 servers running eDirectory version 8.7.3	NDS password only.
NetWare Remote Manager NDS change password running on a NetWare 5.1 or NetWare 6 server	NDS password only.
NetWare Remote Manager simple password management (NetWare 5.1 and 6 only with Native File Access installed)	Simple password only.

2.4 Password Management

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.
- ConsoleOne: The NDS Password tab in ConsoleOne run on a NetWare 6.5 server, or on a Windows workstation with the Novell Client for Windows version 4.9/4.9.1 installed, automatically sets the Universal Password and synchronizes for backward compatibility.

- NWAdmin32: The same results should be seen when using NWAdmin32 as with ConsoleOne, although Novell has not tested this case.
- LDAP: Changing passwords via LDAP on a NetWare 6.5 server also sets the Universal Password and synchronizes the others 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 the others if the newer libraries are installed on the Novell Client for Windows version 4.9/4.9.1 workstation or NetWare 6.5 server.

NOTE: 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.

2.5 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, driving the NDS or the simple password 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 change the password from the older workstation.
- When you disable a user’s NDS password, the NDS password is set to an arbitrary value that is unknown to the user. The following 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 basically the same way as the feature previously provided for NDS Password. If an administrator changes a user's password, such as when creating a new user or in response to a help desk call, for security the password is automatically expired if you have enabled the setting to expire passwords in the Password Policy. The setting is named “Number of days before password expires (0-365)” 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.
- After implementing Universal Passwords, some applications fail to load

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

This has been resolved in NMAS 2.3.7 and later.

- NDS password settings are replaced by new password policies

  If 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 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.

Managing Passwords by Using Password Policies

3

Using password policies, you can 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:

- Overview of Password Policy Features (page 23)
- Planning for Password Policies (page 25)
- Prerequisite Tasks for Using Password Policies (page 28)
- Creating Password Policies (page 31)
- Assigning Password Policies to Users (page 36)
- Finding Out Which Policy a User Has (page 37)
- Setting A User's Password (page 38)
- Troubleshooting Password Policies (page 38)

For information on Forgotten Password Self-Service and Reset Password Self-Service, see Chapter 4, “Password Self-Service,” on page 41.

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 enduser passwords. NMAS™ enables you to enforce password policies that you assign to users in Novell® eDirectory™.

Password policies 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 iManager self-service console.

Most features of password management require Universal Password to be enabled. Ideally, you would also integrate the iManager self-service console into your existing company portal, if you have one, to give users easy access to Forgotten Password Self-Service and Reset Password Self-service. The iManager self-service console is available only with iManager 2.0.2.

You create Password Policies by using a wizard. In iManager, click Passwords > Password Policies > New.

Password Management lets you set the following:

- Universal Password (page 24)
- Advanced Password Rules (page 24)
- Enforcement of Policies in eDirectory (page 24)

3.1.1 Universal Password

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.

3.1.2 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, upper- or lowercase letters, and special characters. You can exclude passwords that you don’t feel are secure, such as your company name.

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

3.1.3 Enforcement of Policies in eDirectory

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, Virtual Office, 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, 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.

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 Planning for Password Policies

The following are discussed in this section:

- Planning How to Assign Password Policies in the Tree (page 25)
- Planning the Rules for Your Password Policies (page 25)
- Planning Login and Change Password Methods for your Users (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 36 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 only the Novell Client (4.9 SP2) and the iManager self-service console (iManager 2.0.2) 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 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.

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 (page 26)
- iManager 2.02 and Virtual Office (page 26)

- Other Protocols (page 27)
- Connected Systems (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 or NT.

The following table describes the differences between Novell Client versions in regard to Universal Password and gives suggestions for handling legacy 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.	Changes the NDS Password directly, instead of going through NMAS. If you are using Universal Password, this can create a problem called "password drift," meaning that the NDS Password and the Universal Password are not kept synchronized. To prevent this, you have three options: • Upgrade all the clients to version 4.9 or later. • Block legacy clients from changing passwords, 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 Client or iManager. See "Preventing Legacy Novell Clients from Changing Passwords" on page 27. • Use the Password Policy setting. Remove the NDS Password when Setting Universal Password. This is a rather drastic measure, because it prevents both login and password change using NDS Password.
4.9	Supports Universal Password.	Enforces password policy rules for Universal Password. 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.
4.9 SP2	Supports Universal Password.	Enforces password policy rules for Universal Password. In addition, it displays the rules to the users to help them create compliant passwords.

iManager 2.02 and Virtual Office

iManager 2.02 and Virtual Office provide Password Self-Service, so users can reset passwords and set up Forgotten Password Self-Service if the password policy provides it. The iManager self-service console is accessible to users on your iManager 2.02 server using a URL such as https://www.*servername*.com/nps (for example, https://www.myiManager.com/nps).

- Make sure users have a browser that supports iManager 2.0.2 or later.

- We recommend that in your password policies you select Synchronize NDS Password When Setting Universal Password. It is the default setting.
- 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

As noted earlier, 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.

❑ The DirXML® driver for the system has been upgraded to Identity Manager format.

❑ The DirXML driver configuration includes the new Password Synchronization Policies.

❑ The Password Synchronization settings specify that Universal Password should be used, and Distribution Password as well if bidirectional Password Synchronization is desired.

❑ Password filters have been deployed on the connected system to capture passwords, if necessary.

For more information, see the *Novell Nsure Identity Manager Administration Guide* (http://www.novell.com/documentation/dirxml20/admin/data/an4bz0u.html).

Preventing Legacy Novell Clients from Changing Passwords

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

If you are using Universal Password, using legacy Clients 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 Clients earlier than version 4.9. This is done 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 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, 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 is 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 eDir 8.7.3 or later server and an eDir 8.7.0 or earlier server, and the two servers share a partition, disabling NDAP password management on that partition will have unreliable results. The 8.7.3 server enforces the setting, preventing legacy Clients from changing the NDS Password; however, the 8.7.0 server does not enforce the setting. So 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. 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.
3. 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.

   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.
4. Install the Password Management plug-ins.

   This is available for download at the Novell Free Download Site (http://download.novell.com).
5. 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 6.
6. 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 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 keypair in the PortalServlet.properties file in the tomcat\webapps\nps\WEB_INF directory.

---

7. 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 64.

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

8. (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, “(NetWare 6.5 only) Re-Creating Universal Password Assignments,” on page 29.

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 (NetWare 6.5 only) Re-Creating Universal Password Assignments

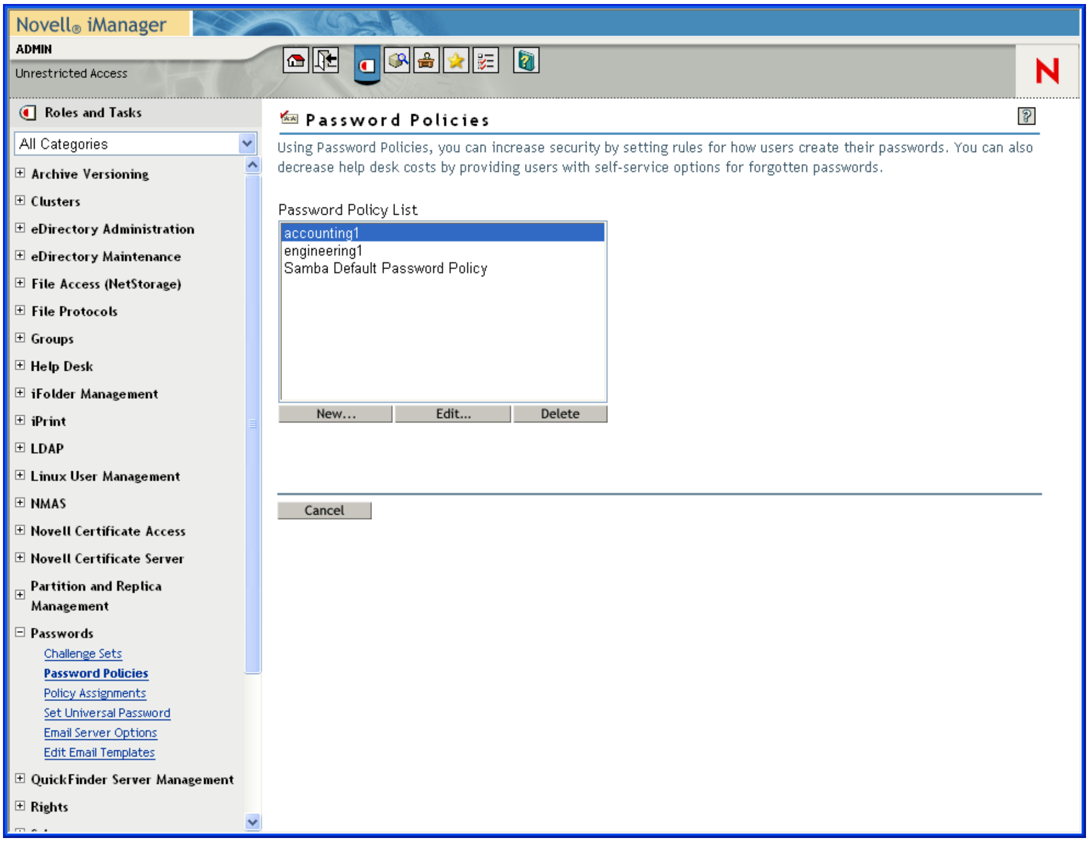
If you have previously set up Universal Password for use with NetWare 6.5, you must remove the old password policies and use the new plug-ins and password policies.

- The NMAS plugins 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 Passsword On
  - Universal Passsword Off
  - Universal Passsword 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.

  The following figure shows an example:

Description: Example of password policies from NetWare 6.5 use of Universal Password



Password Policies

Using Password Policies, you can 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.

Password Policy List

accounting1
engineering1
Samba Default Password Policy

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

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, click Passwords > Password Policies.

3 Click New to create a new password policy.

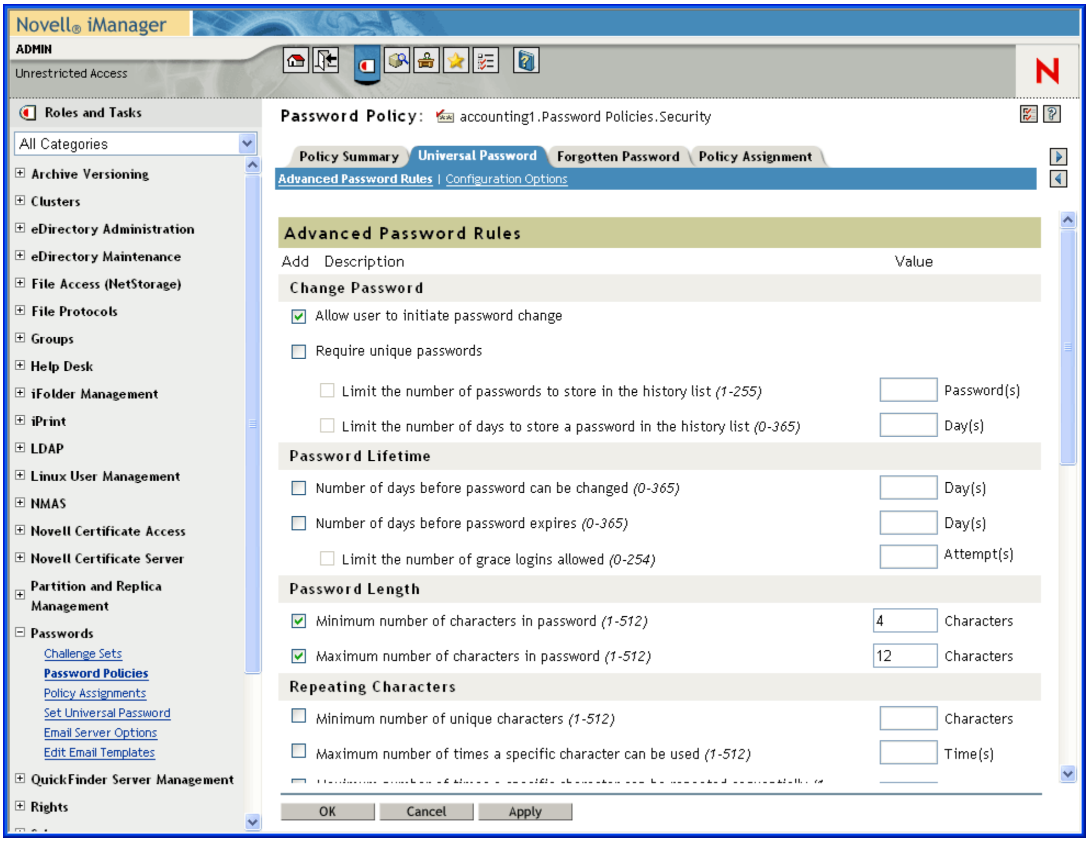
4 Follow the steps in the wizard to create Advanced Password Rules, Universal Password Configuration Options, and Forgotten Password selections for the policy.

See the online help for information about each step, 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 41.

3.4.1 Advanced Password Rules

The following figure shows an example of the advanced password rules:

Description: Advanced Password Rules interface



Password Policy: accounting1.Password Policies.Security

Advanced Password Rules

Add	Description	Value
	Change Password	
☑	Allow user to initiate password change	
□	Require unique passwords	
□	Limit the number of passwords to store in the history list *(1-255)*	Password(s)
□	Limit the number of days to store a password in the history list *(0-365)*	Day(s)
	Password Lifetime	
□	Number of days before password can be changed *(0-365)*	Day(s)
□	Number of days before password expires *(0-365)*	Day(s)
□	Limit the number of grace logins allowed *(0-254)*	Attempt(s)
	Password Length	
☑	Minimum number of characters in password *(1-512)*	4 Characters
☑	Maximum number of characters in password *(1-512)*	12 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)

- Change Password
    - Allow the user to initiate password change

      This allows the user to use the password self-service features (see Chapter 4, "Password Self-Service," on page 41).
    - Require unique passwords

      You can specify how unique passwords are enforced by using one or both of the following two values.
    - Limit the number of passwords to store in the history list (1-255)

      If you require unique passwords, you can 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, the password policy rejects the password and the user is prompted to specify a different one.
    - Limit the number of days to store a password in the history list (0-365)

      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 30 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.

- Password Lifetime
    - Number of days before the password can be changed (0-365)

      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. The password policy does not allow the Universal Password to be changed by the user before that time has elapsed.
    - Number of days before the password expires (0-365)

      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, described in the next item, the user can log in with the expired password the specified number of times.

      NOTE: A security enhancement was added to NMAS 2.3.4 regarding Universal Passwords changed by an administrator. It works in much the same way as the feature previously provided for NDS® Password. If an administrator changes a user's password, such as when creating a new user or in response to a help desk call, for security the password is automatically expired if you have enabled the setting to expire passwords in the password policy. For this particular feature, the number of days is not important, but this setting must be enabled.
    - Number of grace logins allowed after the password has expired (0-254)

      When the password expires, this value indicates how many times a user is allowed to log in to eDirectory 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.
- Password Length
    - Minimum number of characters in the password (1-512)
    - Maximum number of characters in the password (1-512)
- 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)
- Case sensitivity

  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 make your passwords case sensitive for all the clients that are upgraded to eDirectory 8.8. See the *eDirectory 8.8 Admininstration Guide* (http://www.novell.com/documentation/beta/edir88/index.html?page=/documentation/beta/edir88/edir88new/data/brix9ry.html#brix9ry) for more information.
    - Allow the password to be case sensitive
    - Minimum number of uppercase characters required in the password (1-512)

    - Maximum number of uppercase characters allowed in the password (1-512)
    - Minimum number of lowercase characters required in the password (1-512)
    - Maximum number of lowercase characters allowed in the password (1-512)
- Numeric characters
    - Allow numeric characters in the password
    - Disallow a numeric character as the first character
    - Disallow a numeric character as the last character
    - Minimum number of numerals in the password (1-512)
    - Maximum number of numerals in the password (1-512)
- Special characters

  Special characters are the characters that are not numbers (0-9) and are not alphabetic characters. (The alphabetic characters are a-z, A-Z, and alphabetic characters in the Latin-1 code page 850.)
    - Allow special characters in the password
    - Disallow a special character as the first character
    - Disallow a special character as the last character
    - Minimum number of special characters (1-512)
    - Maximum number of special characters (1-512)
- Password exclusions

  The passwords that you exclude are case insensitive, so if you specify the word “test” as a word that cannot be used as a password, then “Test” and “TEST” are also excluded.

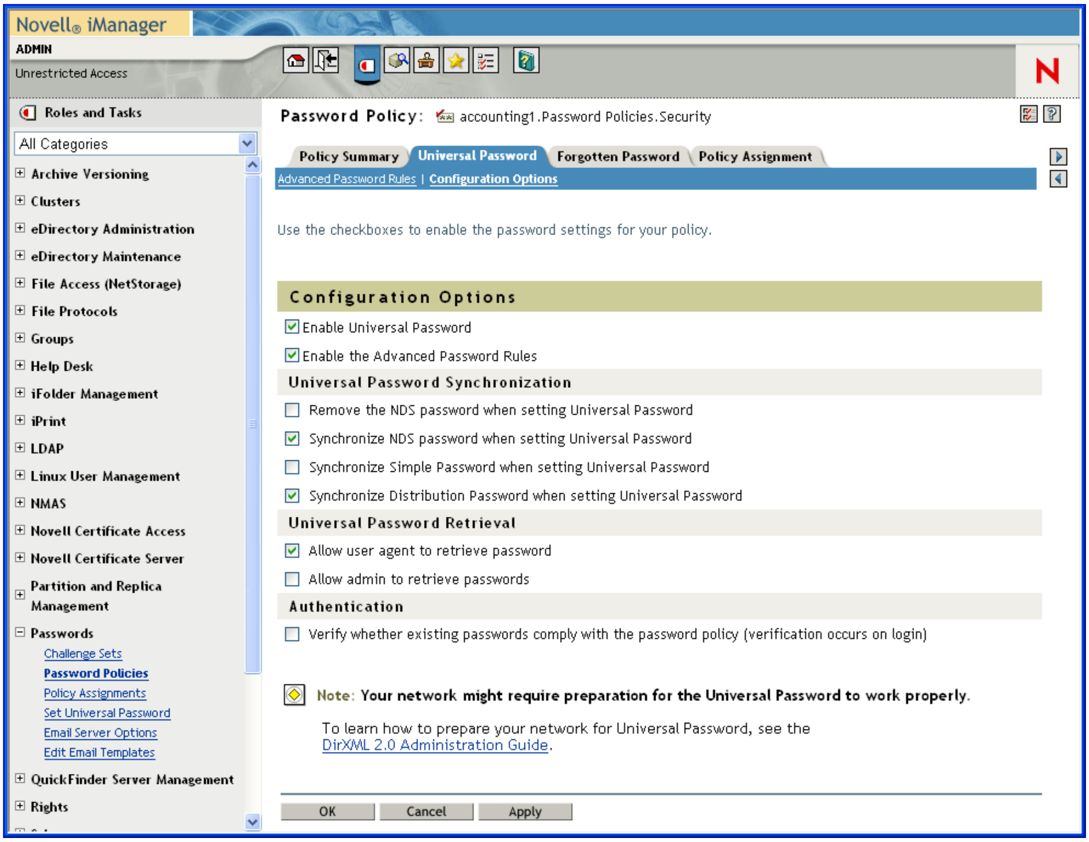
  At this time, the list of excluded passwords must be typed manually, one at a time. Also, you can exclude only specific words, not a pattern or an eDirectory attribute.

  TIP: 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.

3.4.2 Universal Password Configuration Options

The following figure shows an example of the advanced password rules:

Description: graphic



Password Policy: accounting1.Password Policies.Security

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 agent to retrieve password

□ Allow admin to retrieve passwords

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 DirXML 2.0 Administration Guide.

- 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.

  - Synchronize NDS password when setting Universal Password

    If this option is selected, setting the Universal Password in applications such as the Novell Client also changes the NDS 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 using ICE.

  - Synchronize Distribution Password when setting Universal Password

    Determines whether the DirXML® engine can retrieve or set a user's Universal Password in eDirectory.

- Universal Password Retrieval
  - Allow user agent 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 grayed out on the Forgotten Password page in the Password Policy.

  - Allow admin to retrieve passwords

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

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

    If this option is selected, when 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 (using the Login Policy object), specific partitions or containers, or specific users. We encourage you to set password policies as high up in the tree as you can, to simplify administration.

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

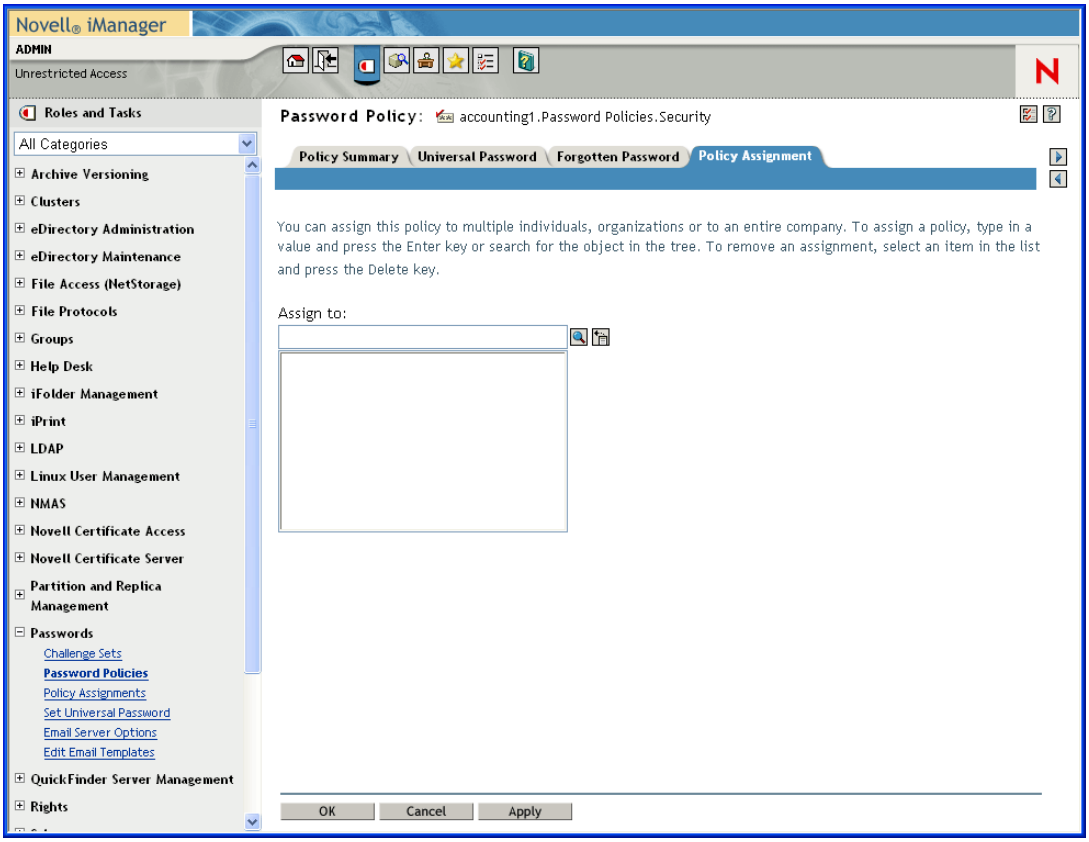
- A specific user

Only one policy is effective for a user at a time. Novell Modular Authentication Services (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 which 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:

Description: Assigning Password Policy to objects interface



Password Policy: accounting1.Password Policies.Security

You can assign this policy to multiple individuals, organizations or to an entire company. To assign a policy, type in a value and press the Enter key or search for the object in the tree. To remove an assignment, select an item in the list and press the Delete key.

Assign to:

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, go to iManager > Passwords > Policy Assignments.

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 36.

3.7 Setting A User's Password

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

1. In iManager, click Passwords > Set Universal Password.

   If the user has a password policy assigned and Universal Password enabled, you are allowed to change the password using this task.

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

   NOTE: If Universal Password is not enabled for a user, the Advanced Password Set task displays an error and the password is not changed. You must either assign a policy to the user and then return to this task, or change the user’s NDS password using the eDirectory Administration > Modify Object task.

2. Create a password for the user, making sure it is compliant with all password rules that are displayed.

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

3.8 Troubleshooting Password Policies

- iManager self-service login requiring 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/Portal configuration. You need to run the Portal Servlet Configuration Wizard (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.

- Errors about password policy 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 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 also 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 iManager install doesn't 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 6 on page 28.

- Using Challenge Response questions

  Make sure that you are using a browser that iManager 2.02 supports.

- Giving access to users in new containers

  When you set up iManager or one of Novell's portal products, such as exteNd™ Director™ Standard Edition, 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 Director Platform Edition Installation and Configuration Guide* (http://www.novell.com/documentation/lg/nedpe41/configure/data/ajhotzv.html#ajhotzv).~D

- 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.)
  - The LDAP Server Group object in eDirectory must be configured to require TLS on simple binds. You set this option by editing the LDAP Server object properties in iManager.

Password Self-Service

4

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

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

- iManager 2.0.2 portal
- Novell® Client™
- Virtual Office
- exteNd™ Director™

The following information is discussed in this section:

- Prerequisites for Using Password Self-Service (page 41)
- Managing Forgotten Passwords (page 42)
- Providing Users with Password Reset Self-Service (page 61)
- Adding a Password Change Message (page 63)
- Configuring E-Mail Notification for Password Self-Service (page 64)
- Test-Driving Password Self-Service (page 66)
- Adding Password Self-Service to Your Company Portal (page 67)
- Novell Client and Password Self-Service (page 74)
- Troubleshooting Password Self-Service (page 75)

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.

The Password Self-Service features were removed from iManager 2.5, so in order for users to use the self-service features, you must have a server running iManager 2.02. Users hit this server's portal (https://www.*my_iManager_server*.com/nps) to access the self-service features.

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) to access the self-service features. See Section 4.8.2, "Integrating Password Self-Service with Virtual Office," on page 70.

The Novell Client also takes advantage of Password Self-Service features. See Using Forgotten Password Self-Service in the *Novell Client for Windows Installation and Administration Guide* (http://www.novell.com/documentation/noclienu/noclienu/data/bxne05q.html).

Although users use iManager 2.02 as one way to use the Password Self-Service features, this section assumes that you are managing Password Self-Service using iManager 2.5 or later.

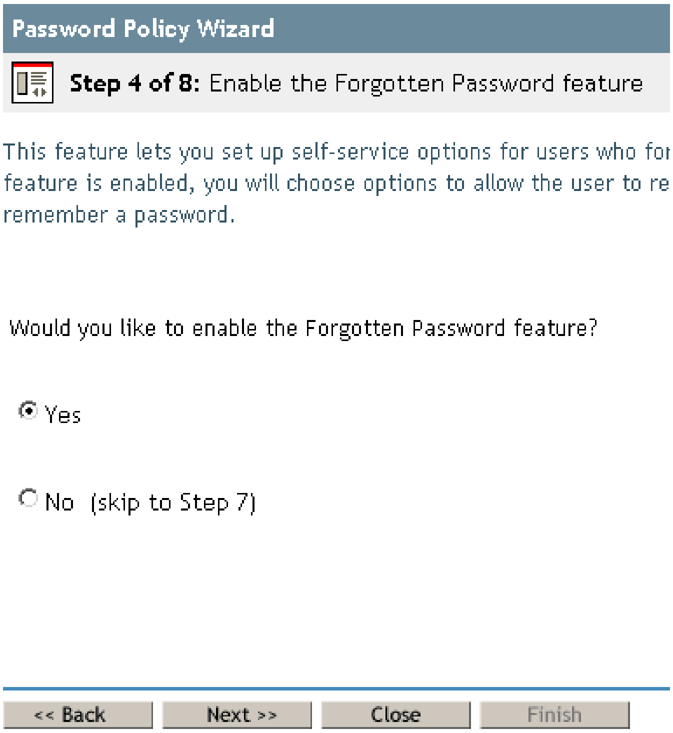
4.3 Managing Forgotten Passwords

The following sections describe how to manage forgotten passwords:

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.

Description: graphic



Password Policy Wizard

Step 4 of 8: Enable the Forgotten Password feature

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.

Would you like to enable the Forgotten Password feature?

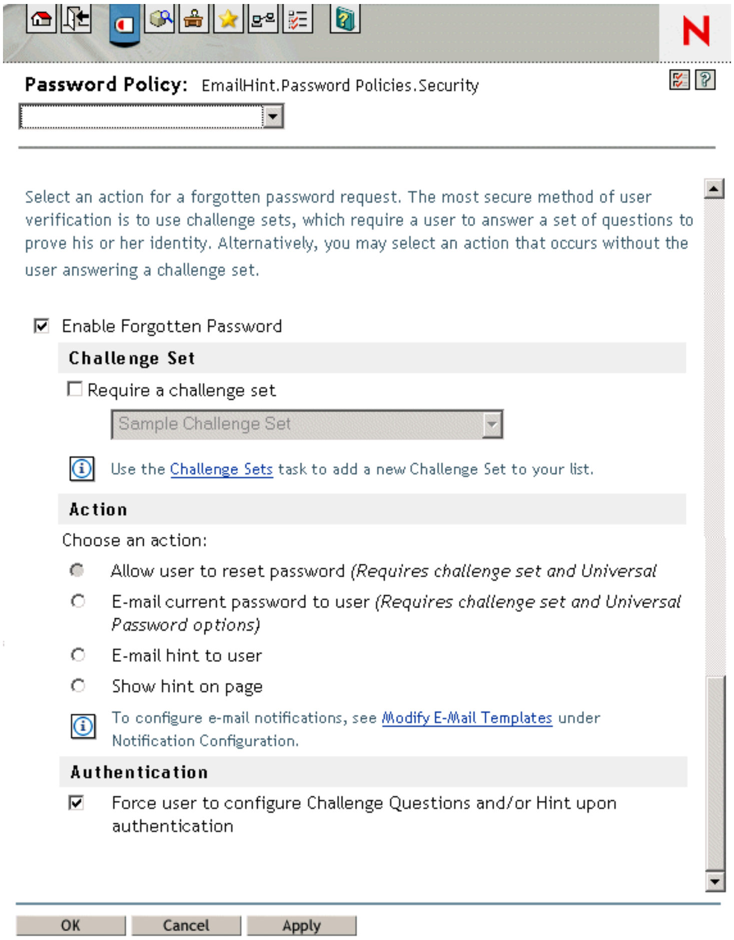
● Yes

○ No (skip to Step 7)

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

1. In iManager, click Passwords > Password Policies.
2. Select a password policy, then click Edit.

Description: Forgotten Password interface



Password Policy: EmailHint.Password Policies.Security

Select an action for a forgotten password request. The most secure method of user verification is to use challenge sets, which require a user to answer a set of questions to prove his or her identity. Alternatively, you may select an action that occurs without the user answering a challenge set.

☑ Enable Forgotten Password

Challenge Set

☐ Require a challenge set

Sample Challenge Set

Use the Challenge Sets task to add a new Challenge Set to your list.

Action

Choose an action:

○ Allow user to reset password *(Requires challenge set and Universal*

○ E-mail current password to user *(Requires challenge set and Universal Password options)*

○ E-mail hint to user

○ Show hint on page

To configure e-mail notifications, see Modify E-Mail Templates under Notification Configuration.

Authentication

☑ Force user to configure Challenge Questions and/or Hint upon authentication

3 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 users answer to prove thier 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.

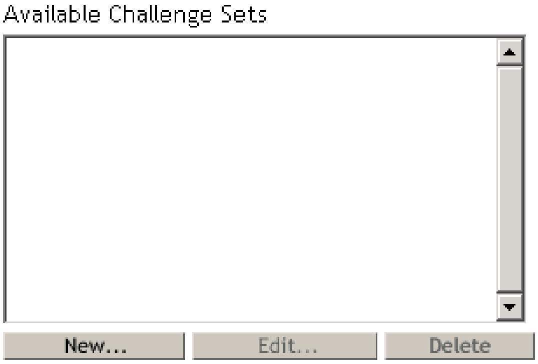
You can use challenge sets as part of providing Forgotten Password self-service for users. Requiring a user to answer challenge questions before receiving forgotten password help provides an additional level of security.

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 47.

To create a challenge set:

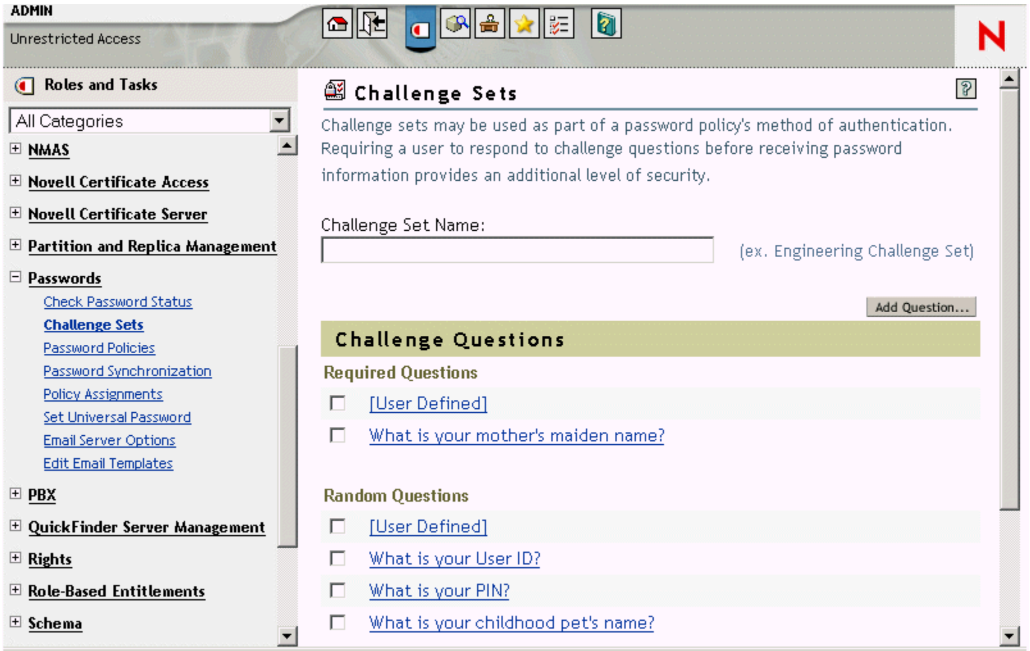
1 In iManager, click Passwords > Challenge Sets.

Description: graphic



2 Click New.

Description: graphic



Challenge Sets

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.

Challenge Set Name: (ex. Engineering Challenge Set)

Add Question...

Challenge Questions

Required Questions

- □ [User Defined]
- □ What is your mother's maiden name?

Random Questions

- □ [User Defined]
- □ What is your User ID?
- □ What is your PIN?
- □ What is your childhood pet's name?

3 Type a name in the Challenge Set Name field, 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.

Novell Modular Authentication Services (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.

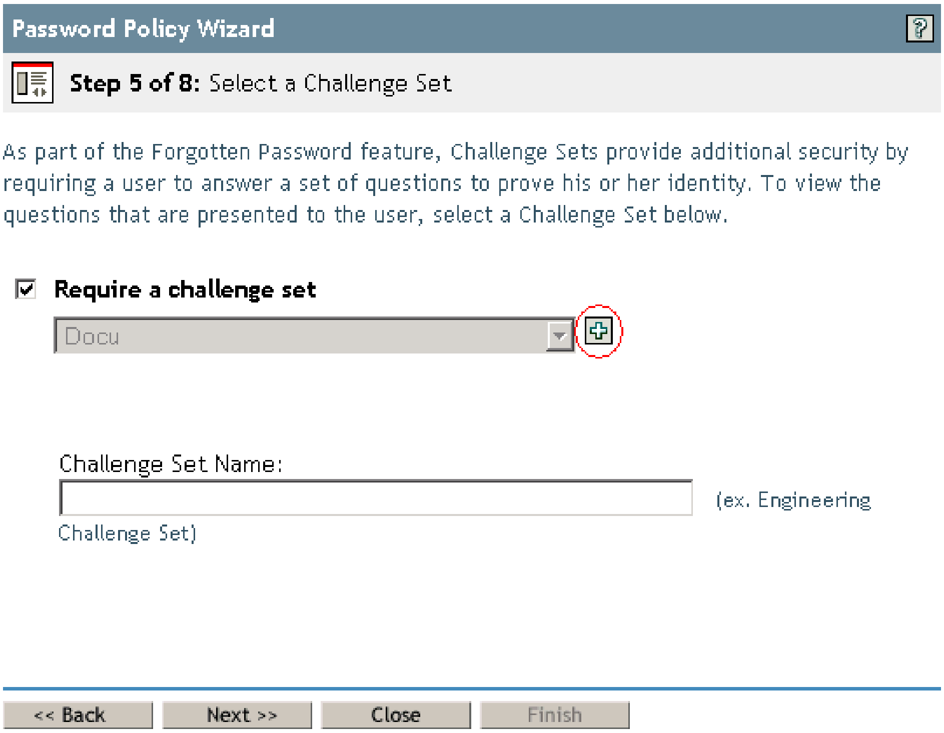
To create a challenge set while using the Password Policy Wizard:

1 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 the Add (plus sign icon) button.

Description: graphic



Password Policy Wizard

Step 5 of 8: Select a Challenge Set

As part of the Forgotten Password feature, Challenge Sets provide additional security by requiring a user to answer a set of questions to prove his or her identity. To view the questions that are presented to the user, select a Challenge Set below.

☑ **Require a challenge set**

Docu

Challenge Set Name: (ex. Engineering Challenge Set)

To use an existing challenge set, select it from the drop-down list.

4 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, then type the question.

5c Select whether the question is required or random.

5d Specify minimum and maximum characters required, then click OK

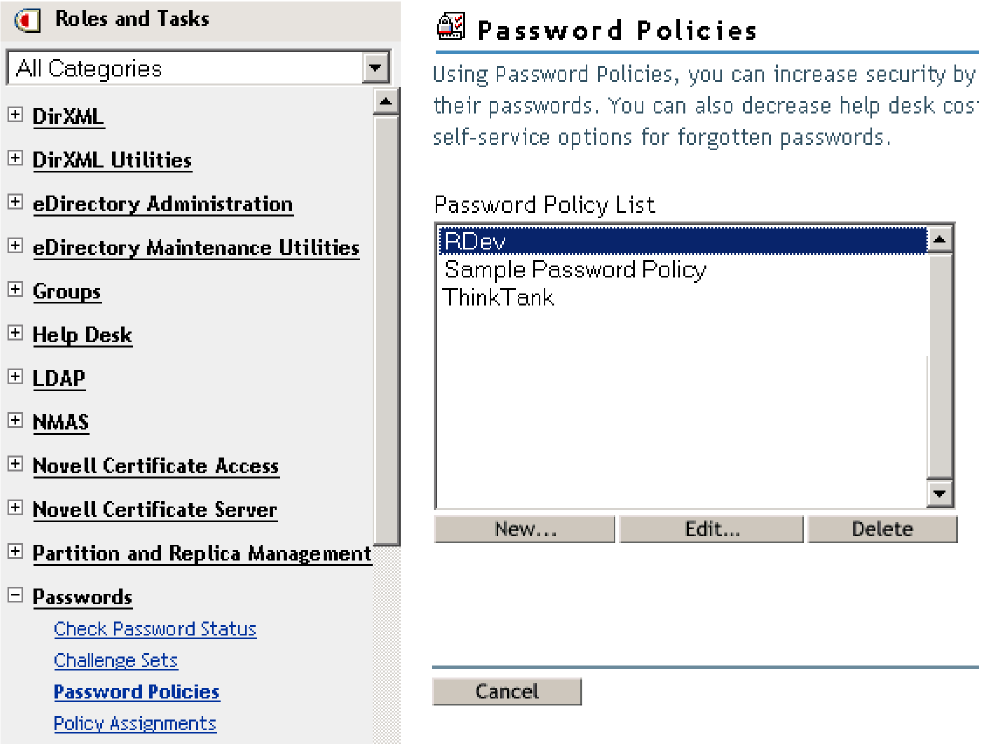
6 Specify the number of random question, then click Next.

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.

Description: graphic



Password Policies

Using Password Policies, you can increase security by their passwords. You can also decrease help desk cos self-service options for forgotten passwords.

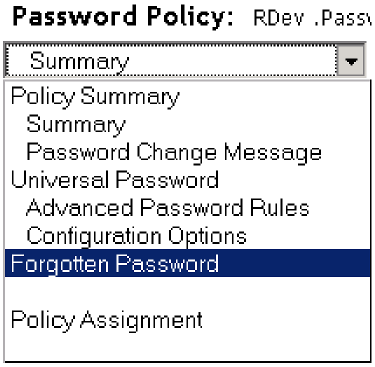
Password Policy List

RDev
Sample Password Policy
ThinkTank

2 Select a password policy, then click Edit.

3 From the Summary drop-down list, select Forgotten Password.

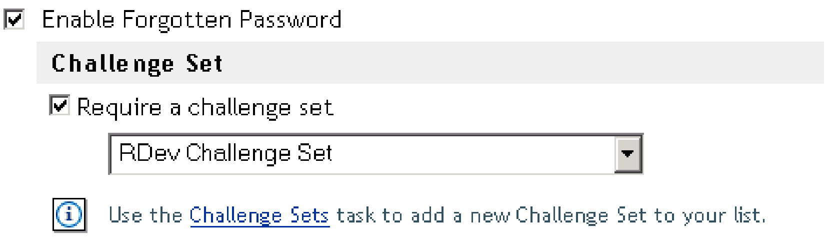
Description: graphic



Password Policy: RDev .Passv

4 Select Enable Forgotten Password > Require a Challenge Set.

Description: graphic



☑ Enable Forgotten Password

Challenge Set

☑ Require a challenge set

RDev Challenge Set

Use the Challenge Sets task to add a new Challenge Set to your list.

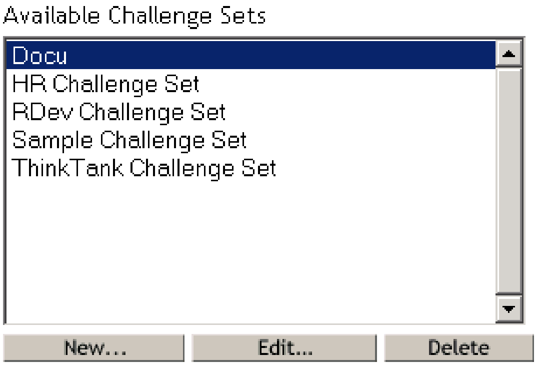
5 Select an existing challenge set from the drop-down list or create a new one.

To create a new one:

5a Click the Challenge Sets link.

5b In the Available Challenge Sets dialog box, click New.

Description: graphic



Available Challenge Sets

Docu
HR Challenge Set
RDev Challenge Set
Sample Challenge Set
ThinkTank Challenge Set

5c In the Challenge Sets dialox box, name the challenge set, select or add required or random questions, and then specify the number of random questions to ask.

5d Click OK.

6 Complete the remaining steps in the Password Policy Wizard.

4.3.3 Selecting a Forgotten Password Action

1 Enable Forgotten Password.

2 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, 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 64.

  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 64.

  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.

The Password Hint attribute (nsimHint) is publicly readable, to allow unauthenticated users who have forgotten a password to access their own hint. 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:

1. Allow access to the nsimHint attribute only on the LDAP server used for Password Self-Service.
2. Require that users answer challenge questions before receiving the password hint.
3. 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 63.

If you choose not to use password hint at all, 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 48.

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 Description: iManager Configuration icon.
2. Click Portal Platform Configuration > Gadgets.
3. From the list of gadgets, select Hint Setup.
4. Click Delete.

After deleting 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 (such as https://www.*servername*.com/nps) 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.

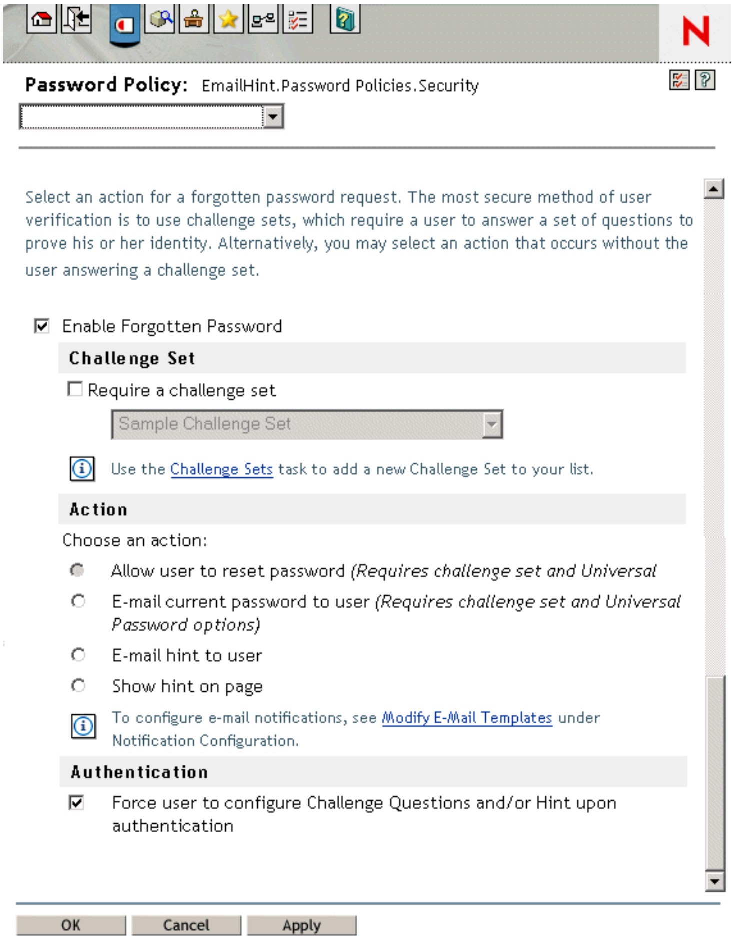
Prompting Users to Set Up Forgotten Password

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 using post-authentication services (pages displayed when users log in to the portal).

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

Description: Forgotten Password settings interface



Password Policy: EmailHint.Password Policies.Security

Select an action for a forgotten password request. The most secure method of user verification is to use challenge sets, which require a user to answer a set of questions to prove his or her identity. Alternatively, you may select an action that occurs without the user answering a challenge set.

☑ Enable Forgotten Password

Challenge Set

□ Require a challenge set

Sample Challenge Set

Use the Challenge Sets task to add a new Challenge Set to your list.

Action

Choose an action:

○ Allow user to reset password *(Requires challenge set and Universal*

○ E-mail current password to user *(Requires challenge set and Universal Password options)*

○ E-mail hint to user

○ Show hint on page

To configure e-mail notifications, see Modify E-Mail Templates under Notification Configuration.

Authentication

☑ Force user to configure Challenge Questions and/or Hint upon authentication

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:

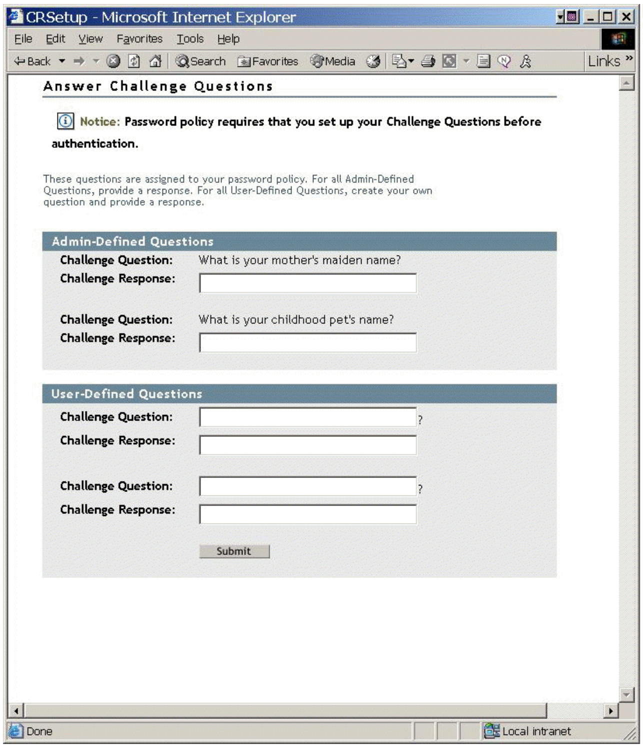
- "Post-Authentication" on page 50
- "In the Portal" on page 52

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 logs in through the portal (such as https://www.*servername*.com/nps). This is called post-authentication setup.

The following figure illustrates the Challenge Set setup, post-authentication.

Description: Post-authentication Challenge Set setup


CRSetup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
Done
Local intranet

Answer Challenge Questions

Notice: Password policy requires that you set up your Challenge Questions before authentication.

These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response.

Admin-Defined Questions

Challenge Question: What is your mother's maiden name?
Challenge Response:

Challenge Question: What is your childhood pet's name?
Challenge Response:

User-Defined Questions

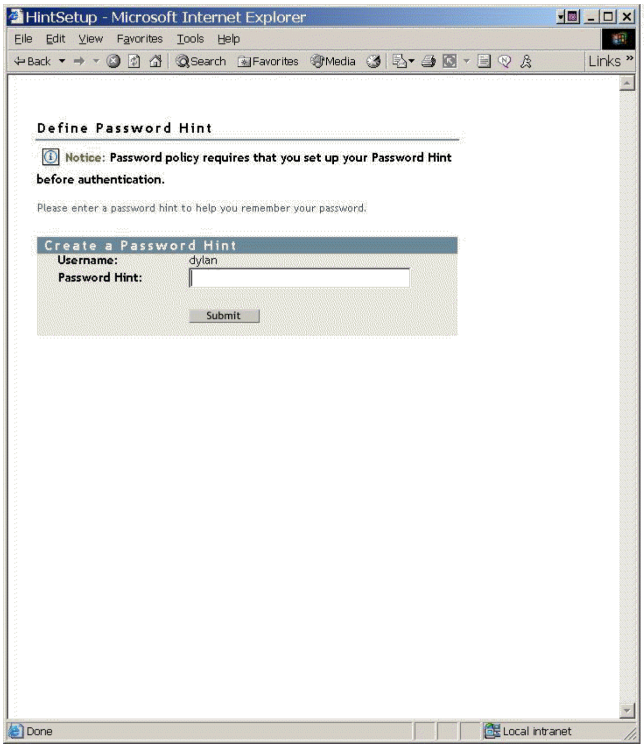
Challenge Question: ?
Challenge Response:

Challenge Question: ?
Challenge Response:

Submit

The following figure illustrates the Password Hint setup, post-authentication.

Description: Post-authentication Password Hint setup


HintSetup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
Done
Local intranet

Define Password Hint

Notice: Password policy requires that you set up your Password Hint before authentication.

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

Create a Password Hint

Username: dylan
Password Hint:

Submit

In the Portal

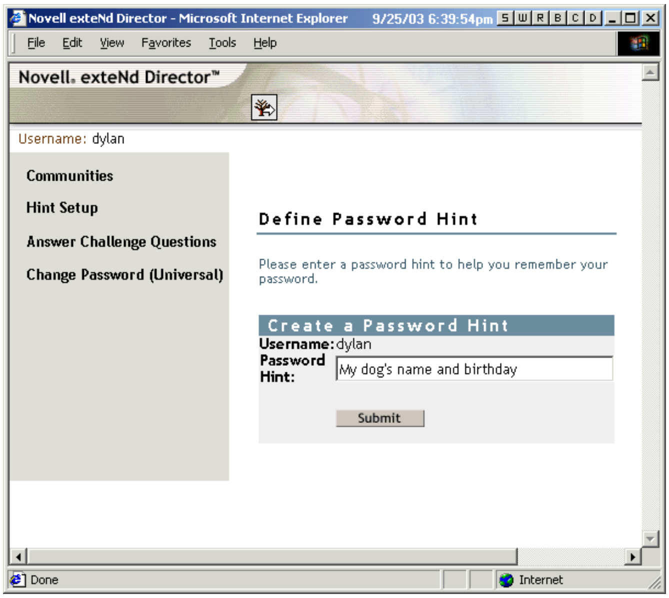
When users log in through the iManager portal, iManager gives them access to the gadgets for setting up or changing challenge sets and password hints for Forgotten Password Self-Service. This is the same place where users can initiate a password change. They can access the following gadgets here:

- 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.

The following figure shows the Hint Setup page:

Description: Hint Setup gadget in iManager self-service console



Username: dylan

Define Password Hint

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

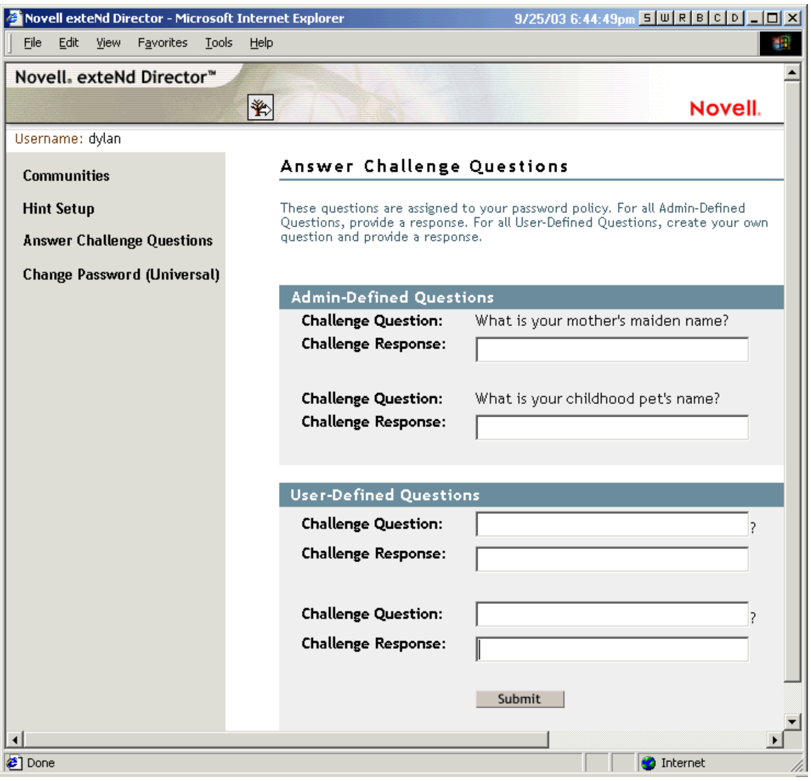
Create a Password Hint

Username: dylan

Password Hint: My dog's name and birthday

The following figure illustrates the Answer Challenge Questions page:

Description: Answer Challenge Questions gadget in iManager self-service console


Novell exteNd Director - Microsoft Internet Explorer
9/25/03 6:44:49pm
File Edit View Favorites Tools Help
Novell. exteNd Director™
Novell.
Communities
Hint Setup
Answer Challenge Questions
Change Password (Universal)
Submit
Done
Internet

Username: dylan

Answer Challenge Questions

These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response.

Admin-Defined Questions

Challenge Question: What is your mother's maiden name?
Challenge Response:

Challenge Question: What is your childhood pet's name?
Challenge Response:

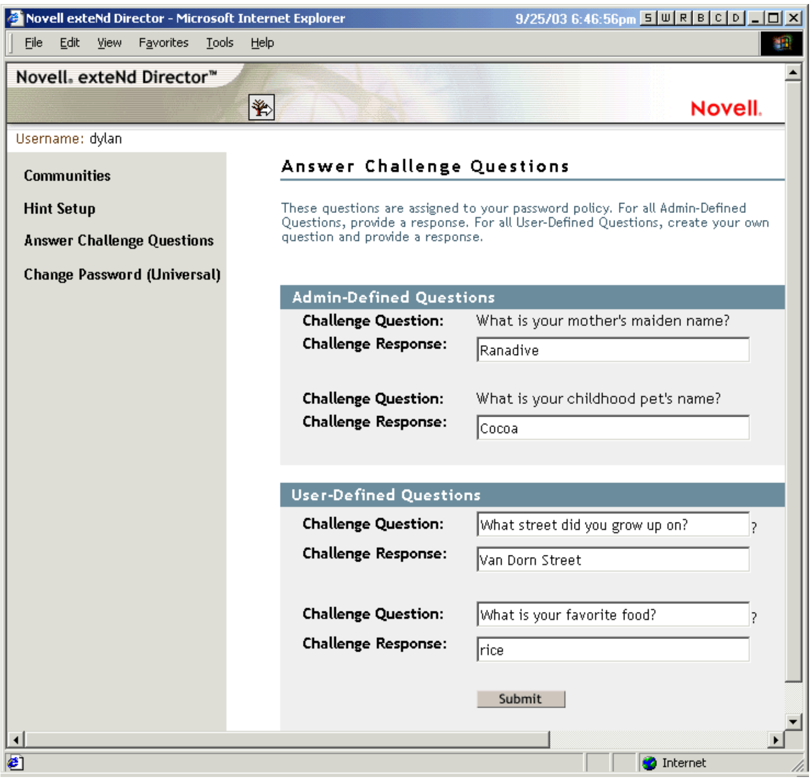
User-Defined Questions

Challenge Question: ?
Challenge Response:

Challenge Question: ?
Challenge Response:

The first questions listed in this example are administrator defined and the others are user defined. The user answers the administrator questions and creates both a question and answer for the user-defined questions, as in the following example:

Description: Answer Challenge Questions gadget in iManager self-service console, with questions answered


Novell exteNd Director - Microsoft Internet Explorer
9/25/03 6:46:56pm
File Edit View Favorites Tools Help
Novell. exteNd Director™
Novell.
Internet

Username: dylan

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

Answer Challenge Questions

These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response.

Admin-Defined Questions

Challenge Question: What is your mother's maiden name?
Challenge Response: Ranadive

Challenge Question: What is your childhood pet's name?
Challenge Response: Cocoa

User-Defined Questions

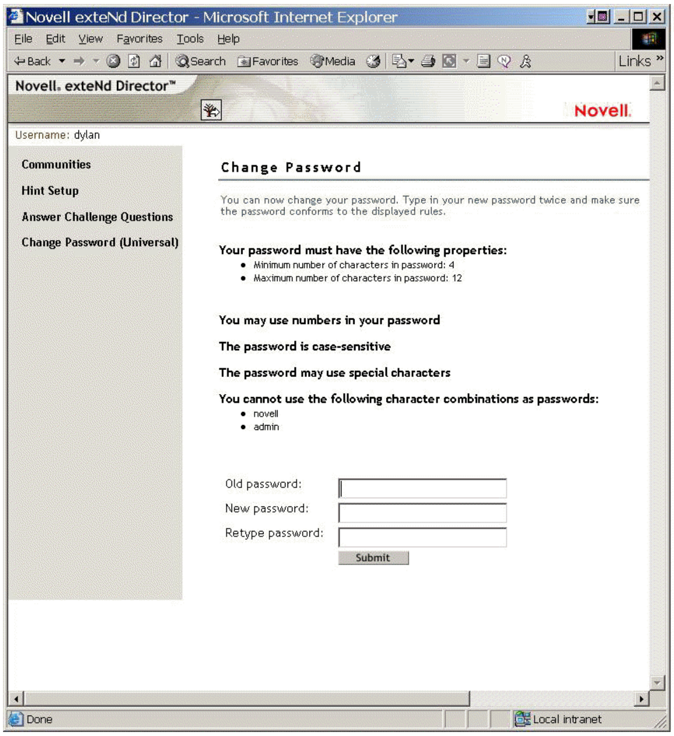
Challenge Question: What street did you grow up on??
Challenge Response: Van Dorn Street

Challenge Question: What is your favorite food??
Challenge Response: rice

Submit

The following figure illustrates the Change Password (Universal) page, which appears after the user successfully answers the challenge question:

Description: Change Password (Universal) gadget in iManager self-service console


Novell exteNd Director - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Novell. exteNd Director™
Novell.
Done
Local intranet

Username: dylan

Communities

Hint Setup

Answer Challenge Questions

Change Password (Universal)

Change Password

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:

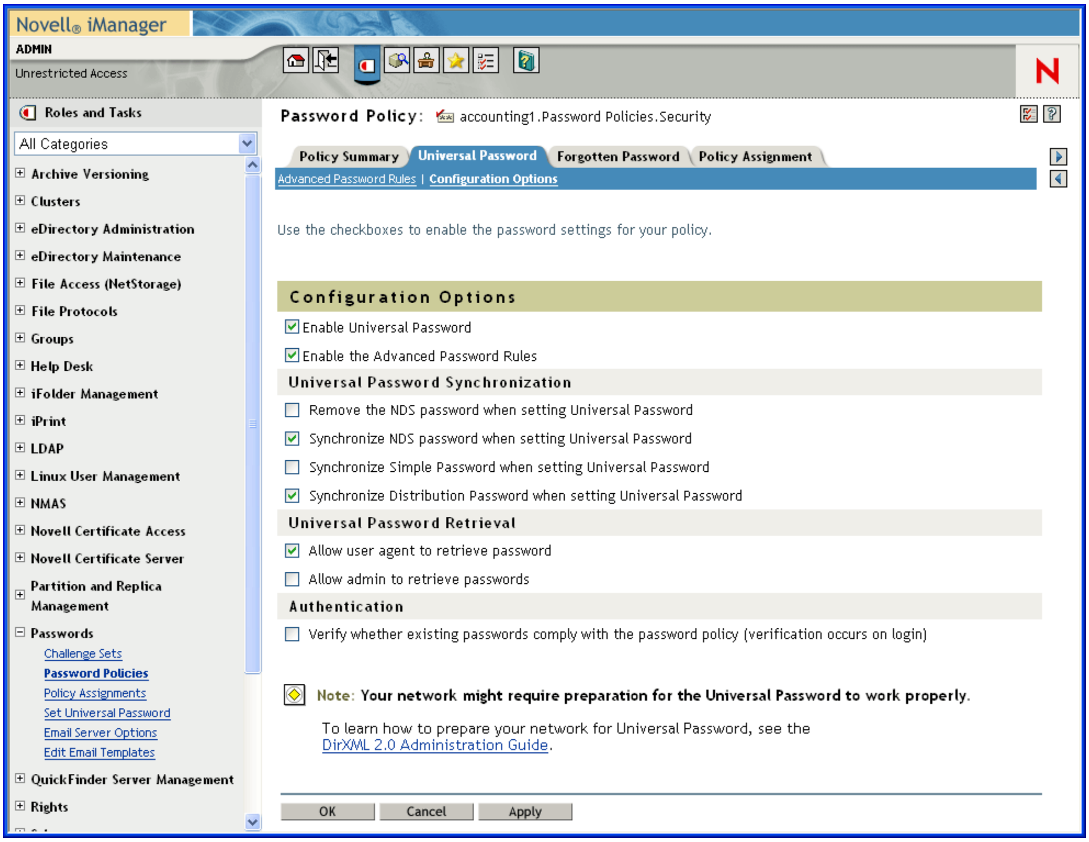
Submit

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 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:

Description: Interface for Universal Password configuration options



Password Policy: accounting1.Password Policies.Security

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 agent to retrieve password

☐ Allow admin to retrieve passwords

Authentication

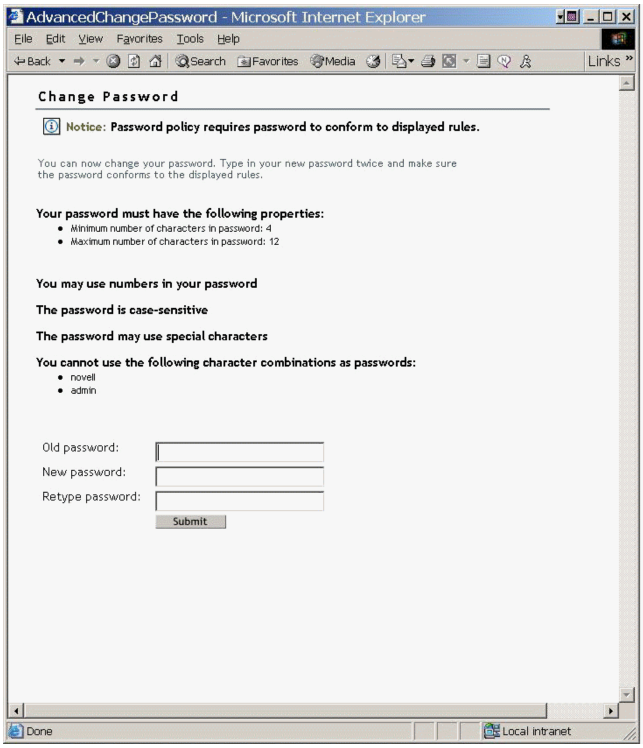
☐ Verify whether existing passwords comply with the password policy (verification occurs on login)

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 DirXML 2.0 Administration Guide.

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.

Description: Post-authentication Reset Password


AdvancedChangePassword - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
Done
Local intranet

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:

Submit

4.3.6 Turning Off the Forgotten Password Link

If you don't want the “Forgot your password?” link to appear in the portal, you can turn it off by using the following steps: ~D

1 In iManager, click the Configure icon Description: configure icon to enter the Administration gadget.

2 Click Portal Platform Configuration > Gadgets.

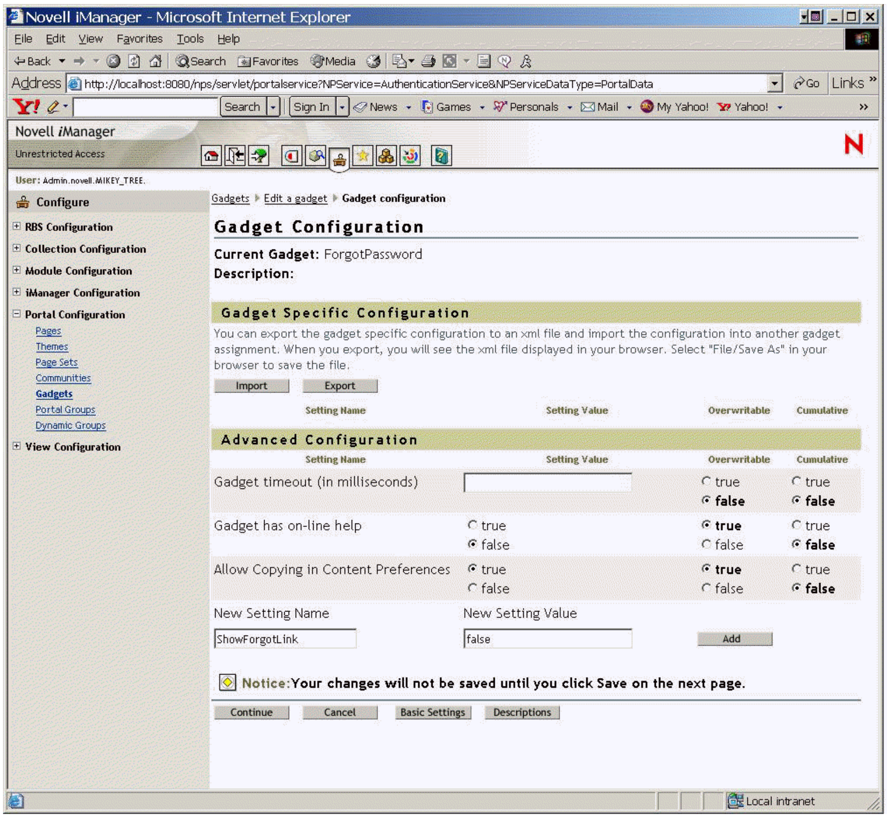
3 From the list of Gadgets, select the Forgot Password gadget.

4 Click Edit > Configuration > All Settings.

5 Add a keypair in the gadget settings, as shown in the following figure (New Setting Name/ Value under Advanced Configuration).

If this keypair does not exist at all in the gadget settings, the default behavior is True.

Description: Page for editing ForgottenPassword gadget


Novell iManager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:8080/nps/servlet/portalservice?NPService=AuthenticationService&NPServiceDataType=PortalData
Go Links
Search Sign In News Games Personals Mail My Yahoo! Yahoo!
Novell iManager
Unrestricted Access
User: Admin.novell.MIKEY_TREE.
Configure
RBS Configuration
Collection Configuration
Module Configuration
iManager Configuration
Portal Configuration
Pages
Themes
Page Sets
Communities
Gadgets
Portal Groups
Dynamic Groups
View Configuration
Gadgets ▸ Edit a gadget ▸ Gadget configuration
Import
Export
Add
Continue
Cancel
Basic Settings
Descriptions
Local intranet

Gadget Configuration

Current Gadget: ForgotPassword
Description:

Gadget Specific Configuration

You can export the gadget specific configuration to an xml file and import the configuration into another gadget assignment. When you export, you will see the xml file displayed in your browser. Select "File/Save As" in your browser to save the file.

Advanced Configuration

Setting Name	Setting Value	Overwritable	Cumulative
Gadget timeout (in milliseconds)		○ true ● false	○ true ● false
Gadget has on-line help	○ true ● false	● true ○ false	○ true ● false
Allow Copying in Content Preferences	● true ○ false	● true ○ false	○ true ● false

New Setting Name	New Setting Value
ShowForgotLink	false

Notice: Your changes will not be saved until you click Save on the next page.

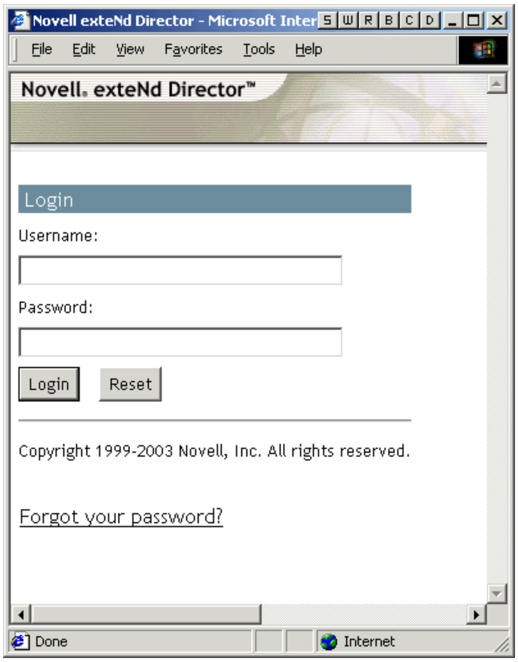
6 Click Continue > Save.

7 Restart the Web server so the change takes effect.

4.3.7 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 (such as https://www.*servername*.com/nps), as illustrated in the following figure.

Description: Login page showing "Forgot your password?" link


Novell exteNd Director - Microsoft Inter
File Edit View Favorites Tools Help
Novell. exteNd Director™
Login
Login
Reset
Done
Internet

Username:

Password:

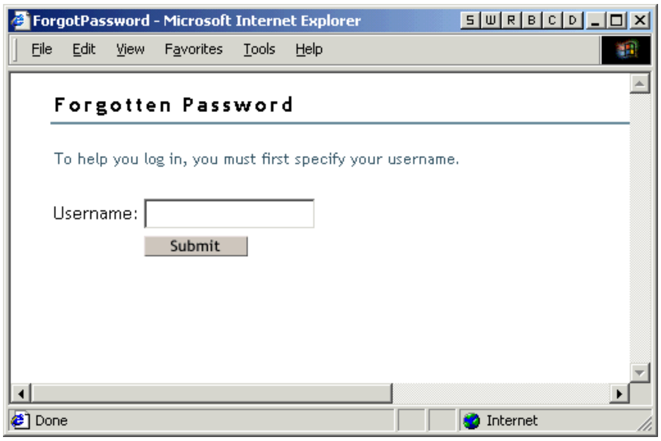
Copyright 1999-2003 Novell, Inc. All rights reserved.

Forgot your password?

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

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

Description: Forgotten Password page for entering username


ForgotPassword - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Submit
Done
Internet

Forgotten Password

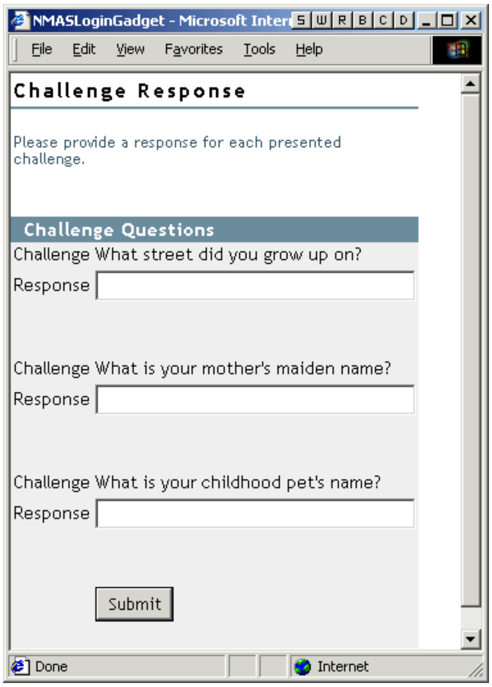
To help you log in, you must first specify your username.

Username:

After the username 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.

Description: Forgotten Password page for proving identity by answering challenge questions


NMASLoginGadget - Microsoft Inter
File Edit View Favorites Tools Help
Submit
Done
Internet

Challenge Response

Please provide a response for each presented challenge.

Challenge Questions

Challenge What street did you grow up on?

Response

Challenge What is your mother's maiden name?

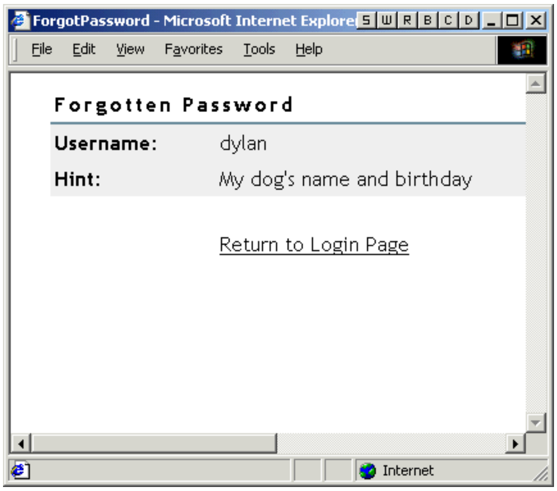
Response

Challenge What is your childhood pet's name?

Response

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

Description: Forgotten Password page, displaying a password hint


ForgotPassword - Microsoft Internet Explore
File Edit View Favorites Tools Help
Return to Login Page
Internet

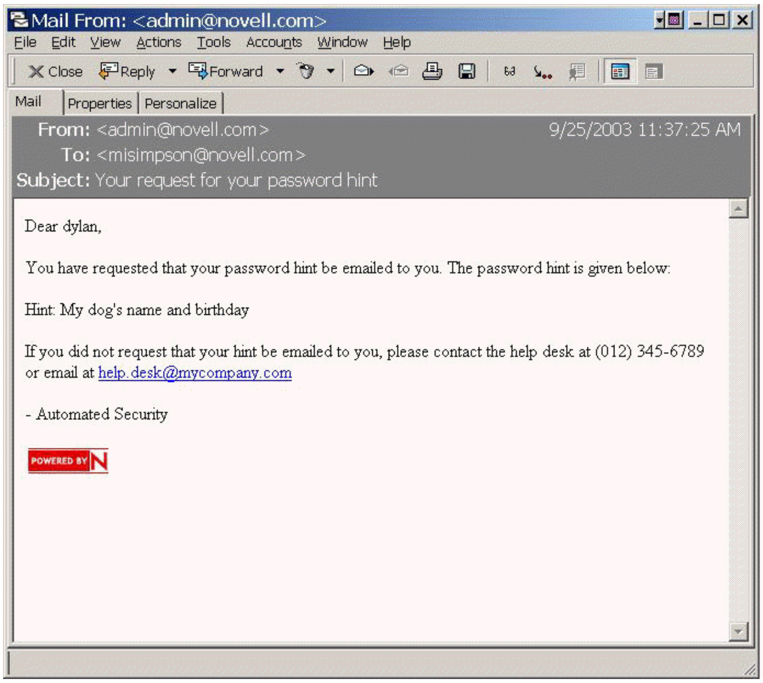
Forgotten Password

Username: dylan

Hint: My dog's name and birthday

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:

Description: Sample e-mail containing user's password hint


Mail From: <admin@novell.com>
File Edit View Actions Tools Accounts Window Help
Close Reply Forward
Mail Properties Personalize

From: <admin@novell.com> 9/25/2003 11:37:25 AM
To: <misimpson@novell.com>
Subject: Your request for your password hint

Dear dylan,

You have requested that your password hint be emailed to you. The password hint is given below:

Hint: My dog's name and birthday

If you did not request that your hint be emailed to you, please contact the help desk at (012) 345-6789 or email at help.desk@mycompany.com

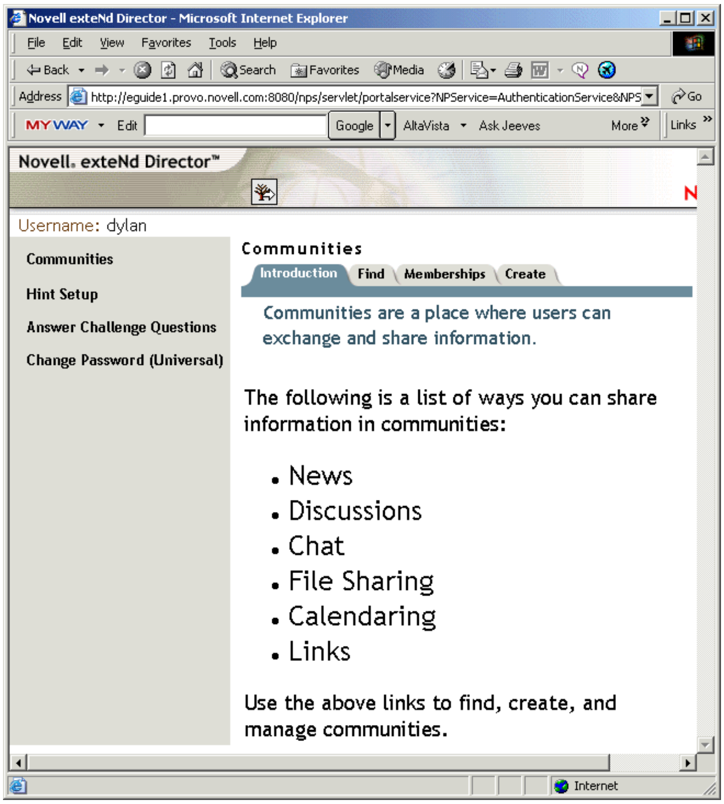
- Automated Security

4.4 Providing Users with Password Reset Self-Service

Using the iManager portal, users can reset their passwords while viewing the Advanced Password Rules. They do this by using the Change Password (Universal) gadget.

The following figure illustrates what users see when they log in to the iManager portal on your iManager Web server, using a URL like https://www.*servername*.com/nps.

Description: The iManager self-service console


Novell exteNd Director - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://eguide1.provo.novell.com:8080/nps/servlet/portalservice?NPService=AuthenticationService&NPS
Go
MY WAY Edit Google AltaVista Ask Jeeves More Links
Novell. exteNd Director™
Internet

Username: dylan

Communities

Hint Setup

Answer Challenge Questions

Change Password (Universal)

Communities

Introduction | Find | Memberships | Create

Communities are a place where users can exchange and share information.

The following is a list of ways you can share information in communities:

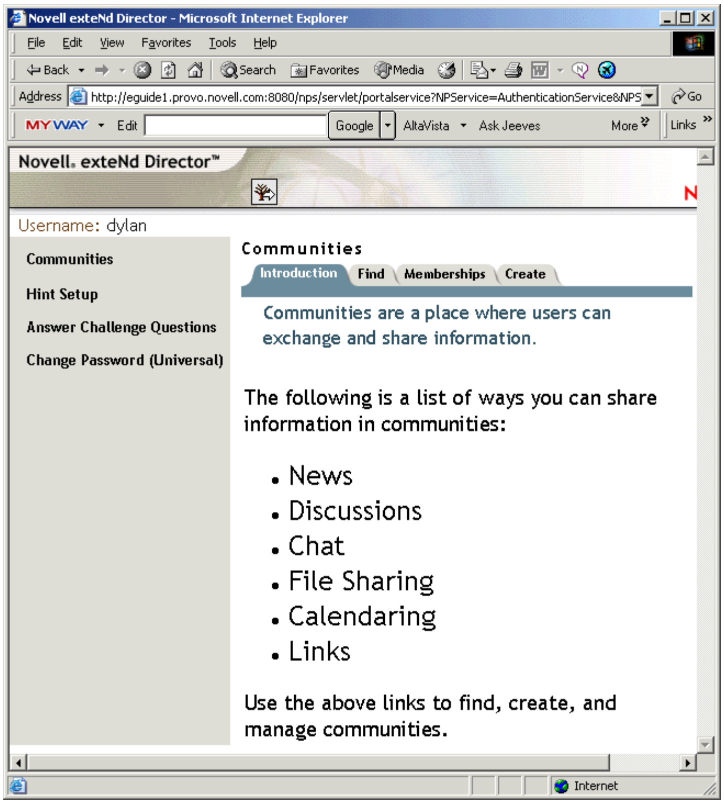
- News
- Discussions
- Chat
- File Sharing
- Calendaring
- Links

Use the above links to find, create, and manage communities.

Users can reset their passwords in the iManager portal, accessed using a URL such as https://www.*servername*.com/nps. For example, https://www.myiManager.com/nps.

The following is an example of the iManager portal after login:

Description: iManager self-service console


Novell exteNd Director - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://eguide1.provo.novell.com:8080/nps/servlet/portalservice?NPService=AuthenticationService&NPS
Go
MY WAY Edit Google AltaVista Ask Jeeves More Links
Novell. exteNd Director™
Communities
Hint Setup
Answer Challenge Questions
Change Password (Universal)
Introduction Find Memberships Create
Internet

Username: dylan

Communities

Communities are a place where users can exchange and share information.

The following is a list of ways you can share information in communities:

- News
- Discussions
- Chat
- File Sharing
- Calendaring
- Links

Use the above links to find, create, and manage communities.

4.5 Adding a Password Change Message

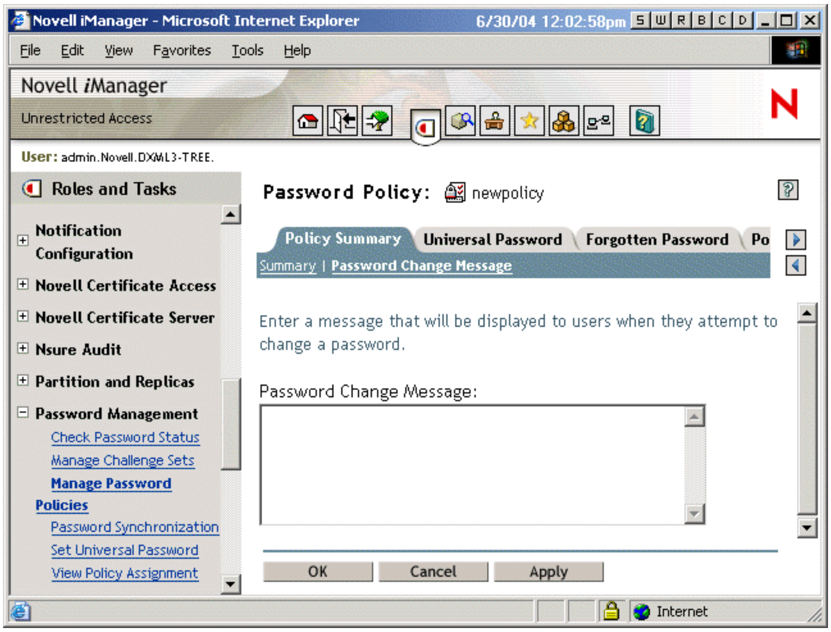
Although users can change their passwords whenever they choose to, they typically use the same passwords as long as possible. To increase security, you can use a password policy to require them to change it. That policy can contain a Password Change Message and the password rules. Whenever users change 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 password policy you want to add a message to, then click Edit.
3. Click Policy Summary > Password Change Message.

   The following page appears:

Description: Password Change Message page



User: admin.Novell.DXML3-TREE.

Password Policy: newpolicy

Enter a message that will be displayed to users when they attempt to change a password.

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; 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 65
- Section 4.6.2, “Setting Up the SMTP Server to Send E-Mail Notification,” on page 65

- “Setting Up E-Mail Templates for Notification” on page 66

4.6.1 Prerequisites

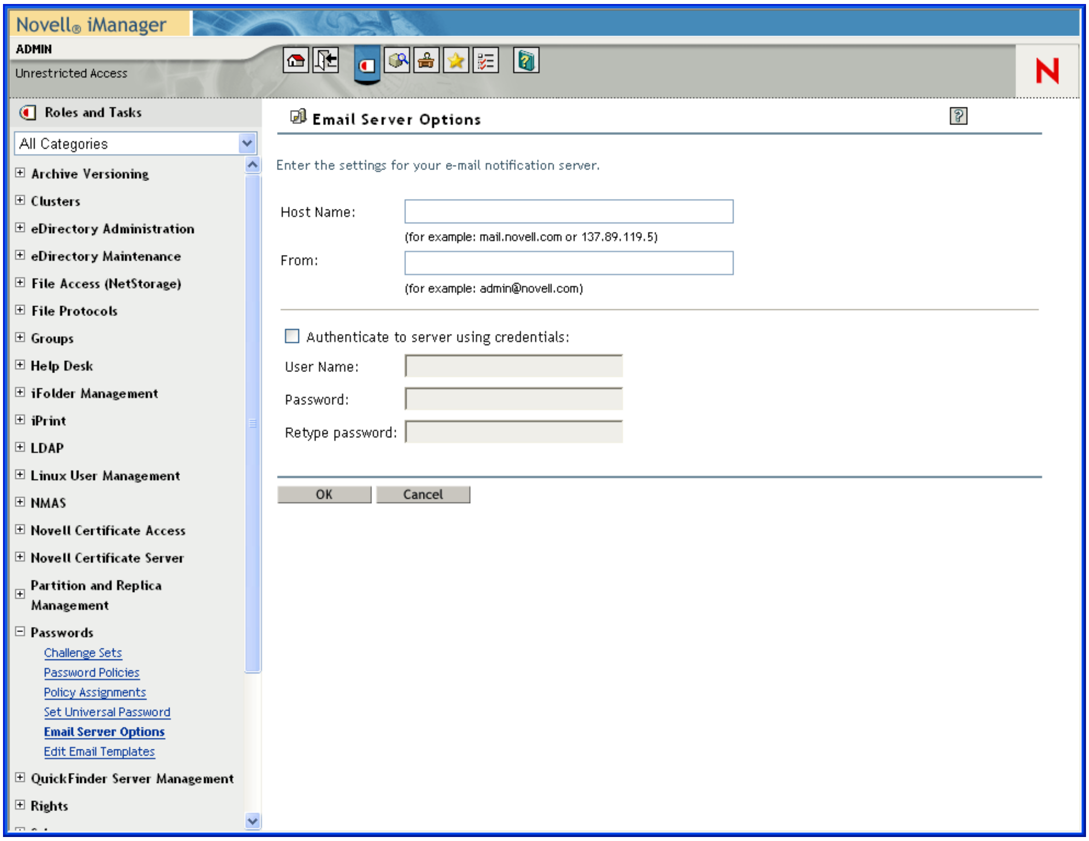
❑ Make sure that your eDirectory users have the Internet EMail Address attribute populated.

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:

Description: Configure SMTP server interface



Email Server Options

Enter the settings for your e-mail notification server.

Host Name:

(for example: mail.novell.com or 137.89.119.5)

From:

(for example: admin@novell.com)

☐ Authenticate to server using credentials:

User Name:

Password:

Retype password:

2 Specify the following information:

- Hostname
- Name you want to appear in the From field of the e-mail message (such as “Administrator”)
- Username and password for authenticating to the server (if necessary)

3 Click Close.

4 Customize the e-mail templates as described in “Setting Up E-Mail Templates for Notification” on page 66.

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.

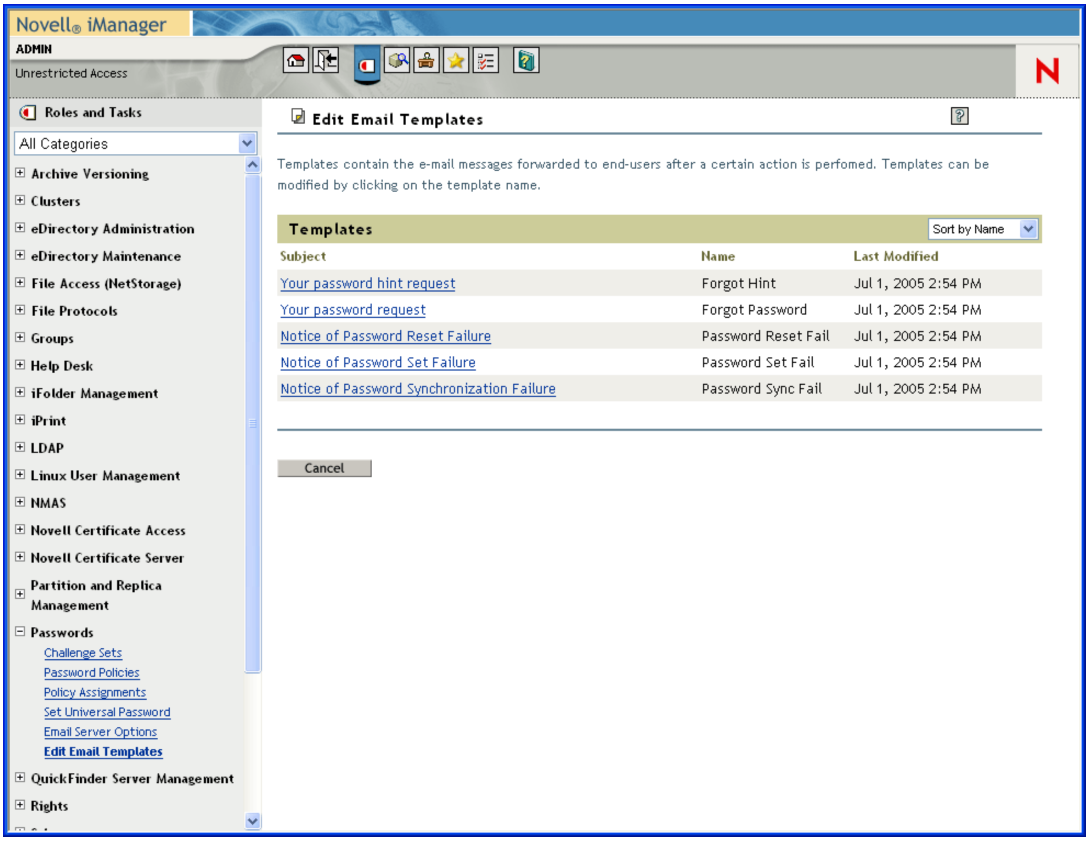
4.6.3 Setting Up E-Mail Templates for Notification

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

1. In iManager, click Passwords > Edit E-mail Templates.

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

Description: List of e-mail templates in iManager



Templates contain the e-mail messages forwarded to end-users after a certain action is perfomed. Templates can be modified by clicking on the template name.

Templates

Subject	Name	Last Modified
Your password hint request	Forgot Hint	Jul 1, 2005 2:54 PM
Your password request	Forgot Password	Jul 1, 2005 2:54 PM
Notice of Password Reset Failure	Password Reset Fail	Jul 1, 2005 2:54 PM
Notice of Password Set Failure	Password Set Fail	Jul 1, 2005 2:54 PM
Notice of Password Synchronization Failure	Password Sync Fail	Jul 1, 2005 2:54 PM

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 Test-Driving 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:

   - 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 (a 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 Log in to Virtual Office as a user with the password policy assigned and verify that you are taken through the post-authentication steps of answering the challenge question and setting a hint.

4 Return to the iManager portal login page again and click Forgot your password?

5 With the user ID for the same user, verify that the challenge questions are correctly presented and that answering them correctly executes the correct action (display hint, allow user to reset password, etc.).

6 Return to the iManager portal login page again and click Forgot your password?

7 Enter the User ID for the user who does not have a password policy assigned and verify that the appropriate errors are given, advising the user that Forgotten Password functionality is not available to him.

What is the process for a forotten password? The user goes to the server portal and selects the Forgot Password? link. They imput their userid, they then are prompted for their mother's maiden name. If they imput this information correctly they are then given a hint about their password. They then can put the correct password into their NetWare client and complete logging into the tree.

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 2.02 server.

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

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 DirXML® 2 plug-ins and are also available separately from download.novell.com.	Follow the steps in • Section 3.3, "Prerequisite Tasks for Using Password Policies," on page 28. • All procedures in Chapter 4, "Password Self-Service," on page 41 (except for Section 4.8, "Adding Password Self-Service to Your Company Portal," on page 67, which is not necessary for iManager 2.02.)

Product	Support for Password Self-Service	Procedure
exteNd Director Standard Edition 4.1 with Support Pack 1	You can integrate the features. This version of exteNd Director supports Password Self-Service features if you install the necessary Novell portal modules (.npm files). To support the features, you must have Support Pack 1 or later.	Section 4.8.1, “Integrating Password Self-Service with exteNd Director 4.1,” on page 69
Virtual Office, provided with NetWare 6.5 Support Pack 2, running on an iManager server	You can integrate the features. 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.	Section 4.8.2, “Integrating Password Self-Service with Virtual Office,” on page 70
exteNd Director 5	You must link to the features. Because exteNd Director 5 is based on portlets and Password Self-Service is based on Novell portal modules (NPMs), you can't use the Password Self-Service features directly in another product. To use this product with Password Self-Service, create links from your company portal to the end user password features on an iManager server.	Section 4.8.3, “Linking to Password Self-Service from a Company Portal,” on page 70
Novell Portal Services (NPS) versions earlier than 4.1	You must link to the features. 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 ForgottenPassword.npm. To use this product with Password Self-Service, create links from your company portal to the end-user password features on an iManager server.	Section 4.8.3, “Linking to Password Self-Service from a Company Portal,” on page 70
Third-party products	You must link to the features. Because third-party products don't run Novell portal modules, you can't use the Password Self-Service features directly in another product. 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.	Section 4.8.3, “Linking to Password Self-Service from a Company Portal,” on page 70

4.8.1 Integrating Password Self-Service with exteNd Director 4.1

If you are using exteNd Director Standard Edition 4.1 with Support Pack 1 for a company portal, you can add the Forgotten Password module to your portal like any other Novell portal module. This module provides the same features that are available when using it on iManager 2.0.2:

- New portal user tasks for Password Self-Service:
  - Hint Setup
  - Answer Challenge Questions
  - Change Password (Universal)
- Forgotten Password Self-Service (accessed from the Forgot your password? link on the portal login page)
- Post-authentication features to prompt users to change noncompliant passwords or update Forgotten Password items such as the hint or challenge questions

To add these features:

1 Make sure you have installed Support Pack 1.

It includes enhancements that are necessary for the ForgottenPassword.npm.

2 Make sure that SSL is configured between the exteNd Director Web server and eDirectory, even if they are running on the same machine.

This is a requirement of NMAS 2.3 or later.

3 To ensure security for the Forgotten Password gadgets, check your LDAP SSL port number.

If you are using an LDAP SSL port other than 636, you must add the following key pair into the PortalServlet.properties file:

LDAPSSLPort=*your_port_number*

For example, if your Web server is running Active Directory, you need to make this change because Active Directory uses port 636. If you are running Tomcat, change the setting in the PortalServlet.properties file in the tomcat\webapps\nps\WEB_INF directory.

This setting takes higher precedence than the default value of 636 if that value exists in the file.

4 After changing the setting, restart the Web server.

5 Make sure all the eDirectory users in the portal users container have rights to self for the Hint attribute 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.

However, 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:

5a Go to http:\\download.novell.com.

5b Fill in the following fields:

- **Search By:** Product
- **Choose a Product:** Nsure® Identity Manager

5c Download the item named 2.0 Password Management Plug-in for iManager 2.0.*x*.

5d Follow the instructions in the nsimhintreadme.txt file.

If users do not have rights to self for 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).
```

6 (Conditional) If you have not installed Identity Manager on the server that holds eDirectory and NMAS, install the Challenge Response Login Method for NMAS.

This Login Method is installed automatically with Identity Manager and is provided as part of the eDirectory 8.7.3 product.

One way to install a Login Method is on Windows, using the Method Installer:

6a Locate the MethodInstaller.exe file in the \nmas\NmasMethods\ directory of the eDirectory CD.

6b Run the executable on a workstation and select the Challenge Response method.

6c Accept the agreement and the defaults for the Login Sequence.

The method is added to the Authorized Login Methods.Security.*tree_name* container.

For more information on installing a Login Method, including installing on UNIX, see "Installing a Login Method" (http://www.novell.com/documentation/lg/nmas23/admin/data/a49tuwk.html#a49tuwk) in the *NMAS 2.3 Administration Guide* (http://www.novell.com/documentation/lg/nmas23).

7 Add the following modules to exteNd Director:

- ForgottenPassword.npm
- nmasclient.npm

They are included with the DirXML product distribution.

For instructions on adding a module, see the *Novell exteNd Director Standard Edition Installation and Configuration Guide* (http://www.novell.com/documentation/lg/nedse41/configure/data/ajhotzv.html).

4.8.2 Integrating Password Self-Service with Virtual Office

Virtual Office supports all the features of Password Self-Service in NetWare 6.5 Support Pack 2 or later, OES for Linux, and OES for NetWare.

For instructions, see the *Virtual Office Configuration Guide* (http://www.novell.com/documentation/oes/virtualoffice/data/am0ogoi.html).

4.8.3 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 the table in Section 4.8, "Adding Password Self-Service to Your Company Portal," on page 67), 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 DirXML 2 plug-ins and are available separately by downloading the 2.0 Password Management Plug-in for iManager 2.0.*x* from http:\\download.novell.com.

The one feature that is not easy to incorporate is post-authentication services, which prompts users to update their passwords to comply with password policies and prompts them to set up Forgotten Password Self-Service according to the password policy, such as creating a password hint. To make sure that users have compliant passwords and are set up to use Forgotten Password Self-Service, you need to make sure that users log in to the iManager portal at least once to create compliant passwords and complete the password management setup, and then again whenever you make changes to Password Policies.

Complete the tasks in these sections:

- "Prerequisites" on page 71
- "Linking to Forgotten Password Self-Service" on page 71
- "Linking to User Password Management Tasks" on page 72
- "Returning Self-Service Users to the Company Portal" on page 73
- Section 4.8.4, "Making Sure Users Have Configured Password Features," on page 74

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

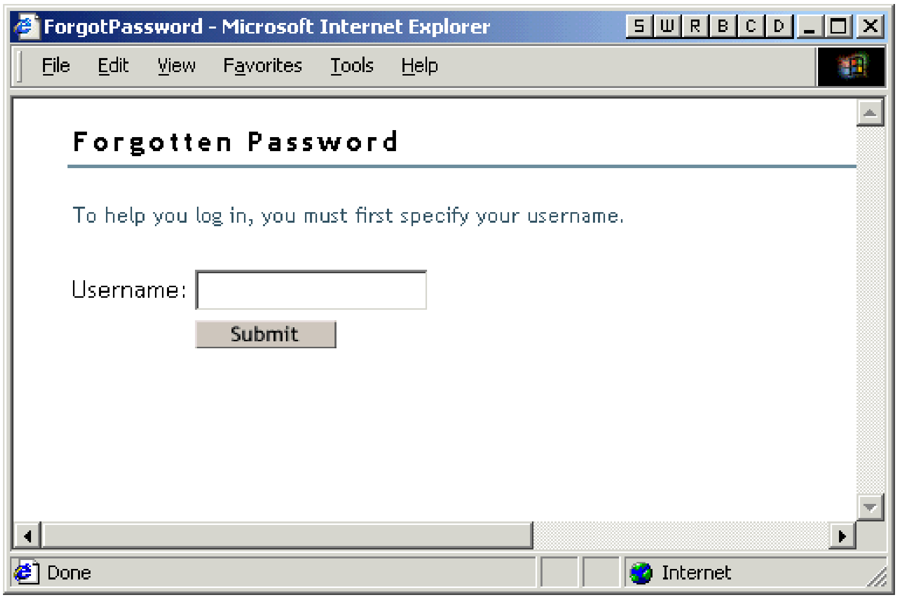
To give users access to Forgotten Password Self-Service from your company portal, you can link to that service on a separate iManager Web server.

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.

Description: Forgotten Password page for entering username



ForgotPassword - Microsoft Internet Explorer
File Edit View Favorites Tools Help

Forgotten Password

To help you log in, you must first specify your username.

Username:

2 Complete the steps in "Returning Self-Service Users to the Company Portal" on page 73.

Linking to User Password Management Tasks

1 Make sure all the eDirectory users in the portal users container have rights to self for the Hint attribute, 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:** Nsure 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 self for 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.

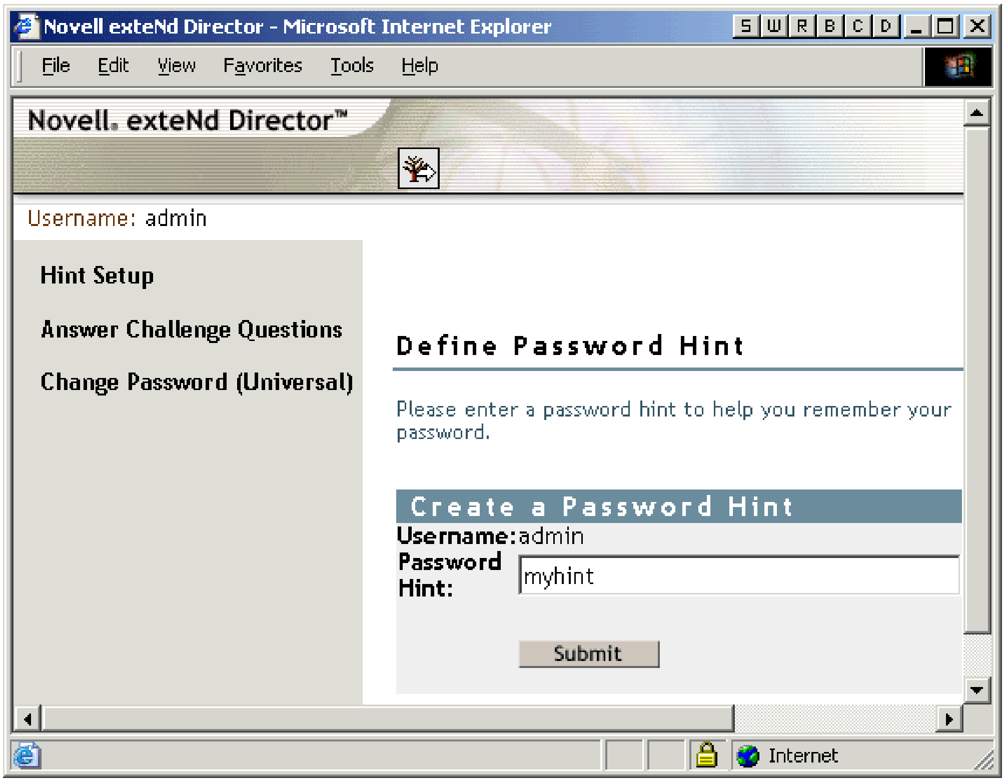
You can create a Manage Passwords link from the company portal and link to https://*other_iManager_server*/nps. This link would provide access to the Password Management end user tasks:

- 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:

Description: Forgotten Password page for entering username


Novell exteNd Director - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Novell. exteNd Director™
Hint Setup
Answer Challenge Questions
Change Password (Universal)
Submit
Internet

Username: admin

Define Password Hint

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

Create a Password Hint

Username: admin

Password Hint: myhint

3 Complete the steps in "Returning Self-Service Users to the Company Portal" on page 73.

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 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.xsl 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.

4.8.4 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 72, which requires users to log in to the iManager portal.

4.9 Novell Client and Password Self-Service

For information on using password self-service with the Novell Client, see Using Forgotten Password Self-Service in the *Novell Client for Windows Installation and Administration Guide* (http://www.novell.com/documentation/noclienu/noclienu/data/bxne05q.html).

4.10 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. But 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.

5 Password Synchronization across Connected Systems

Password synchronization across connected systems is a feature included with Novell® Identity Manager 2.*x*. 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 the *Novell Nsure Identity Manager Administration Guide* (http://www.novell.com/documentation/dirxml20/admin/data/an4bz0u.html).