NetIQ® Identity Manager
Password Management Guide

May 2024

Legal Notice

Copyright 2009 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/ (http://www.microfocus.com/about/legal/).

Contents

About this Book and the Library **5**

1 Understanding Password Management **7**

Universal Password and Distribution Password 8
Password Synchronization Flow 8
Supported Password Policy Syntax 9
Password Policy Enforcement 11
Password Policy Enforcement Notifications 11
Password Policy Assignments 11
Password Synchronization Status 12
Password Self-Service 12

2 Password Management Checklist **13**

Prerequisites 13
Synchronizing Passwords 13
Password Self-Service 14

3 Connected System Support for Password Synchronization **15**

Systems That Support Bidirectional Password Synchronization 15
Systems That Accept Passwords from Identity Manager 16
Systems That Don’t Accept or Provide Passwords By Default 17
Systems That Don’t Support Password Synchronization 17

4 Configuring Password Flow **19**

Verifying Password Synchronization Settings in iManager 19
Verifying Password Synchronization Settings in Designer 21

5 Configuring E-Mail Notification **25**

Prerequisites 26
Setting Up the SMTP Server to Send E-Mail Notification 26
Setting Up E-Mail Templates for Notification 28
Providing SMTP Authentication Information in Driver Policies 28
Adding Your Own Replacement Tags to E-Mail Notification Templates 30
Adding Replacement Tags to Password Synchronization E-Mail Notification Templates 31
Adding Replacement Tags to Forgotten Password E-Mail Notification Templates 36
Sending E-Mail Notifications to the Administrator 36
Localizing E-Mail Notification Templates 37

6 Checking the Password Synchronization Status for a User **39**

7 Troubleshooting Password Synchronization **41**

A Password Synchronization Scenarios **43**

Scenario 1: Using NDS Password to Synchronize between Two Identity Vaults 43
Advantages and Disadvantages of Scenario 1 44
Setting Up Scenario 1 44
Troubleshooting Scenario 1 45
Scenario 2: Using Universal Password to Synchronize Passwords 46
Advantages and Disadvantages of Scenario 2 47
Setting Up Scenario 2 47
Troubleshooting Scenario 2 52
Scenario 3: Synchronizing an Identity Vault and Connected Systems, with Identity Manager Updating the Distribution Password 56
Advantages and Disadvantages of Scenario 3 57
Setting Up Scenario 3 57
Troubleshooting Scenario 3 61
Scenario 4: Tunneling 65
Advantages and Disadvantages of Scenario 4 67
Setting Up Scenario 4 67
Troubleshooting Scenario 4 69
Scenario 5: Synchronizing Application Passwords to the Simple Password 70
Advantages and Disadvantages of Scenario 5 72
Setting Up Scenario 5 72

B Driver Configuration Policies **75**

Policies Required in the Publisher Command Transformation Set 75
Policies Required in the Publisher Input Transformation Policy Set 77
Policies Required in the Subscriber Command Transformation Policy Set 77
Policies Required in the Subscriber Output Transformation Policy Set 78

About this Book and the Library

The *Password Management Guide* contains information about managing passwords through Identity Manager.

Intended Audience

This book provides information for Identity Manager administrators, partners, and consultants.

Other Information in the Library

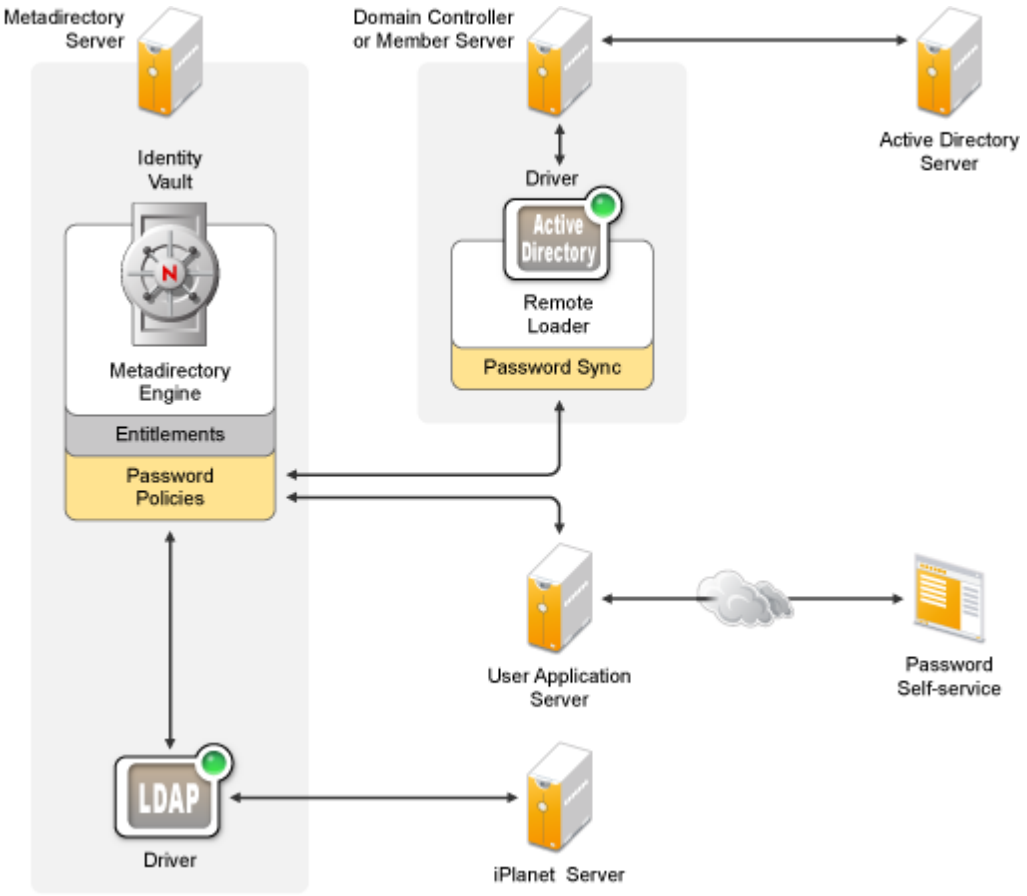
For more information about the library for Identity Manager, see the Identity Manager documentation website (https://www.netiq.com/documentation/identity-manager-49/).

1 Understanding Password Management

Identity Manager helps you manage user passwords across multiple accounts. You can synchronize passwords among systems, allow users to change their passwords, and enable users to recover from forgotten passwords.

In the following diagram, the Identity Manager system is configured to synchronize passwords for users who have Active Directory and SunOne accounts. In addition, password self-service is enabled through the Identity Manager User Application so that users can change their passwords and, if necessary, recover from forgotten passwords.

Figure 1-1 *Password Management with Identity Manager*



Identity Manager provides synchronization of passwords between the Identity Vault and connected systems. It also supports password self-service, which is the ability for users to change their own passwords and recover from forgotten passwords.

The following sections introduce you to the concepts you need to understand to successfully implement password synchronization and password self-service:

- "Universal Password and Distribution Password" on page 8
- "Password Synchronization Flow" on page 8
- "Supported Password Policy Syntax" on page 9
- "Password Policy Enforcement" on page 11
- "Password Policy Enforcement Notifications" on page 11
- "Password Policy Assignments" on page 11
- "Password Synchronization Status" on page 12
- "Password Self-Service" on page 12

Universal Password and Distribution Password

Identity Manager requires Universal Password for both password synchronization and password self-service. Universal Password synchronizes the various passwords (Universal, NDS, Simple, and Distribution) stored in the Identity Vault and provides password policies that define the rules for creating and replacing passwords in the Identity Vault.

To control password synchronization between the Identity Vault and connected systems, Identity Manager uses the Distribution password. When a password is received from a connected system, it is stored as the Distribution password. When a password is sent to a connected system, the Distribution password is sent.

You can choose to synchronize the Distribution and Universal passwords or not synchronize them. If you synchronize the passwords, your Identity Vault passwords and connected system passwords will be the same. If you don't synchronize the passwords, your Identity Vault passwords will be different than your connected system passwords; in essence, you are "tunneling" passwords among connected systems without affecting the passwords (Universal, NDS, or Simple) in your Identity Vault.

Password Synchronization Flow

Identity Manager supports the following levels of password synchronization:

- **Bidirectional:** Identity Manager accepts passwords from a connected system and distributes passwords to the connected system. Users can change their passwords in the connected system or in the Identity Vault.

  Some connected systems can't provide the user's actual password, which means they don't support full bidirectional password synchronization. However, they can provide data (first name, last name, and so forth) that the connected system's driver policies use to create an initial password. After the initial password is created from connected system data, no more password information is sent from the connected system. Passwords flow only from the Identity Vault to the connected system.
- **To the connected system:** Identity Manager distributes passwords from the Identity Vault to the connected system only.

- **To the Identity Vault:** Identity Manager distributes passwords from the connected system to the Identity Vault only.

The connected system determines the level of support for password synchronization. Some systems, such as Microsoft Active Directory and NetIQ eDirectory, support bidirectional synchronization. Other systems support synchronization in one direction only. See Chapter 3, "Connected System Support for Password Synchronization," on page 15 for details.

Supported Password Policy Syntax

Identity Manager supports three password policy syntax options for creating and administrating password policies in iManager:

- **Use Microsoft complexity policy**
- **Use Microsoft Server 2008 Password Policy**
- **Use NetIQ syntax**

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

The following sections describe the default requirements for each password policy option.

Use Microsoft complexity policy

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

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

Use Microsoft Server 2008 Password Policy

This setting allows you to use the Microsoft Windows Server 2008 password policy complexity requirements. If you select this option for a policy, all users to which the policy is assigned must create passwords that meet the criteria of the Microsoft Windows Server 2008 Complexity Policy as implemented in Universal Password. The criteria include:

- Minimum password length is 6 characters, by default.
- Maximum password length is 512 characters.
- The password must contain at least one character from three of the five types of character, uppercase, lowercase, numeric, non-alphanumeric characters, and other characters:
  - Uppercase characters - all uppercase European-language characters, with diacritical marks, as well as Greek and Cyrillic characters.
  - Lowercase characters - all lowercase European-language characters, with diacritical marks, as well as Greek and Cyrillic characters.
  - Numeric characters - 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9.
  - Non-alphanumeric characters - any of the following special characters: ( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? / _.
  - Other characters - any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- The password cannot contain the full value of the CN user attribute for the eDirectory account. NMAS does not perform this check if the length of the attribute is less than three characters.
- The password cannot contain any word from the list of excluded passwords. NMAS does not perform this check if the length of the excluded password is less than three characters.
- The password cannot contain the full value or any part of the value of the `Full Name` attribute for the account, if the attribute contains at least three characters and is a single word. A part of the attribute value is defined as three or more consecutive characters delimited on both ends by the following characters: commas; periods; dashes; hyphens; underscores; spaces; pound signs; or tabs.
- The maximum number of complexity policy violations allowed in a password is 2 by default. You can configure the number of complexity violations allowed using the **Maximum number of complexity policy violations in password (0-5)** option.

Use NetIQ syntax

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

- Minimum password length is 4 characters, by default. You can configure the minimum password length in your environment using the **Minimum number of characters in password (1-512)** option.
- Maximum password length is 12 characters, by default. You can configure the maximum password length in your environment using the **Maximum number of characters in password (1-512)** option.

Password Policy Enforcement

Identity Manager can enforce password policies on incoming passwords from connected systems and on passwords set or changed through the User Application password self-service. If the new password does not comply, you can specify that Identity Manager not accept the password. This also means that passwords that don't comply with your policies are not distributed to other connected systems.

In addition, Identity Manager can enforce password policies on connected systems. If the password being published to the Identity Vault does not comply with rules in a policy, you can specify that Identity Manager not only does not accept the password for distribution, but actually resets the noncompliant password on the connected system by using the current Distribution password in the Identity Vault.

For example, you want to require passwords to include at least one numeric character. However, the connected system does not have the ability to enforce such a policy. You specify that Identity Manager resets passwords that flow from the connected system but do not comply with rules in the policy.

Password Policy Enforcement Notifications

Identity Manager enables you to automatically notify users via e-mail when a password change was not successful.

For example, you set Identity Manager to not accept incoming passwords from Active Directory when they don’t comply with your password policy. One policy rule specifies that the company name can’t be used as a password. A user changes his or her Active Directory password to include the company name. Identity Manager rejects the password and sends the user an e-mail message stating that the password change was not synchronized.

The User Application password self-service console lets you display the password policy rules so that users know how to create a compliant password. However, if you allow users to change their password through a connected system, the connected system is not able to display the policy.

If you want to avoid notifications caused by non-compliant passwords, you should require users to change the password only in the User Application, or at least make sure that the policy rules are well publicized.

Password Policy Assignments

Password policies are assigned with a tree-centric perspective, meaning that you assign them to the Identity Vault containers that hold the users to whom you want the policies applied. In contrast, password synchronization is set up per driver. Drivers are installed on a per-server basis and can manage only those users who are in a master or read/write replica on the server.

To get the results you expect from password synchronization, make sure that the user containers that have password policies required by a driver for password synchronization are in a master or read/write replica on the driver’s server. Assigning a password policy to a partition root container ensures that all users in that container and subcontainers are assigned the password policy.

Password Synchronization Status

Identity Manager enables you to query connected systems to check a user's password synchronization status. If the connected system supports the check password feature, you can find out whether passwords are synchronizing successfully.

For information on how to check passwords, see "Checking the Password Synchronization Status for a User" on page 39.

For a list of which systems support checking passwords, see "Connected System Support for Password Synchronization" on page 15.

Password Self-Service

Password self-service is provided through the Identity Manager User Application. The User Application Identity Self-Service lets users manage their passwords, including resetting and recovering from forgotten passwords.

2 Password Management Checklist

The following sections provide checklists for setting up password synchronization and password self-service. The prerequisites apply to both scenarios.

- "Prerequisites" on page 13
- "Synchronizing Passwords" on page 13
- "Password Self-Service" on page 14

Prerequisites

The following prerequisites must be met before starting the tasks in "Synchronizing Passwords" on page 13 or "Password Self-Service" on page 14.

- ❒ Make sure you have a functioning Identity Manager system in place. To do so, complete the tasks in the *NetIQ Identity Manager Install and Upgrade Guide for Linux*.
- ❒ Make sure you have reviewed Chapter 1, "Understanding Password Management," on page 7 and understand the concepts associated with password synchronization and password self-service.
- ❒ Deploy Universal Password. Universal Password coordinates the different types of Identity Vault passwords (simple, NDS, enhanced), enables synchronization of the passwords with connected systems, and supports password self-service.

Synchronizing Passwords

Complete the following tasks to set up password synchronization between the Identity Vault and a connected system. Repeat the tasks for each connected system with which you want to synchronize passwords.

- ❒ Verify that the driver supports password synchronization. For a list of supported drivers, see Chapter 3, "Connected System Support for Password Synchronization," on page 15.
- ❒ Make sure the driver is already installed and works with the connected system (except for password synchronization). For instructions, refer to the driver documentation on the Identity Manager Drivers documentation site.
- ❒ (Conditional) If you are using the Active Directory driver, install the password filters required to synchronize passwords. For instructions, see Setting Up Password Synchronization Filters in the NetIQ Driver for Active Directory Implementation Guide.
- ❒ (Conditional) If you are using the Linux and UNIX driver, install the password filters required to synchronize passwords. For instructions, see "Installing the PAM or LAM Module" in the *Identity Manager Driver for Linux and UNIX Implementation Guide*.

- ❒ Create a password policy that defines your business criteria for creating and replacing passwords. Assign the policy to the Identity Vault containers that hold the users to whom you want the policy applied. You can have more than one password policy if needed. For instructions, see "Managing Passwords by Using Password Policies" in the *NetIQ Password Management Administration Guide.*
- ❒ Make sure the driver's password synchronization settings support the correct flow of passwords between the Identity Vault and the connected system. For instructions, see Chapter 4, "Configuring Password Flow," on page 19.
- ❒ Set up e-mail notification so that users receive messages if their passwords are not successfully synchronized. For instructions, see Chapter 5, "Configuring E-Mail Notification," on page 25.

Password Self-Service

Complete the following tasks to set up password self-service.

- ❒ Install Identity Applications by following the installation checklist. For instructions, see *NetIQ Identity Manager Install and Upgrade Guide for Linux* or *NetIQ Identity Manager Install and Upgrade Guide for Windows*.
- ❒ (Conditional) By default, password self-service is available only within your firewall. If you want to make it available outside your firewall, you must set up a separate forgotten-password management `IDMPwdMgt.WAR` file and deploy it. For more information, see Understanding the Design Needs in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
- ❒ Set up the password self-service features (challenge response, forgotten password, password hints, and so forth).

3 Connected System Support for Password Synchronization

The level of support for password synchronization varies depending on the connected system. The following sections provide support information:

- "Systems That Support Bidirectional Password Synchronization" on page 15
- "Systems That Accept Passwords from Identity Manager" on page 16
- "Systems That Don't Accept or Provide Passwords By Default" on page 17
- "Systems That Don't Support Password Synchronization" on page 17

Systems That Support Bidirectional Password Synchronization

The following connected systems support bidirectional password synchronization. Bidirectional synchronization means that the connected system can provide the user's actual password to Identity Manager and can accept password changes from Identity Manager. This allows the password to be changed in either the Identity Vault or the connected system and then synchronized as needed.

Table 3-1 *Systems that Support Bidirectional Password Synchronization*

Connected System Driver	Subscriber Channel	Subscriber Channel	Subscriber Channel	Publisher Channel
	Application Can Accept Setting of Initial Password	**Application Can Accept Modification of Password**	**Application Supports Check Password**	**Application Can Provide (sync) Password**
Active Directory	Yes	Yes	Yes	Yes
eDirectory[1]	Yes	Yes	Yes	Yes
Linux and UNIX (NIS)	Yes	Yes	Yes	Yes

[1]Between Identity Vault trees, you can have bidirectional password synchronization for users even if Universal Password is not enabled for those users. See "Scenario 1: Using NDS Password to Synchronize between Two Identity Vaults" on page 43.

Systems That Accept Passwords from Identity Manager

The following connected systems can accept passwords from Identity Manager to some degree but cannot provide a user's actual password to Identity Manager.

Although they can't provide the user's actual password, they can be configured to create a password in the Identity Vault by using a policy on the Publisher channel. The password would be based on other user data in the connected system. The basic driver configurations provided for the connected systems include a default password based on the surname.

Table 3-2 *Systems That Accept Passwords from Identity Manager*

Connected System Driver	Subscriber Channel	Subscriber Channel	Subscriber Channel	Publisher Channel
	Application Can Accept Setting of Initial Password	**Application Can Accept Modification of Password**	**Application Supports Check Password**	**Application Can Provide (Sync) Password**
Groupwise	Yes	Yes	No	No[1]
JDBC	Yes[2]	No[3]	No	No[4]
LDAP	Yes[5]	Yes[5]	Yes	No
Lotus Notes	Yes	Yes[6]	Yes[7]	No
SAP User Management	Yes	Yes	No	No

[1]GroupWise supports two authentication methods:

- GroupWise provides its own authentication and maintains user passwords.
- GroupWise authenticates against eDirectory by using LDAP and does not maintain passwords.

  When you use this option, GroupWise ignores driver-synchronized passwords.

[2]The ability to set an initial password is available on all databases where the OS user account is distinct from the database user account, such as Oracle, MS SQL, MySQL, and Sybase.

[3]The Identity Manager Driver for JDBC can be used to modify a password on the connected system, but that feature is not demonstrated in the sample driver configuration.

[4]Passwords can be synchronized as data when stored in a table.

[5]If the target LDAP server allows setting the userpassword attribute.

[6]The Notes driver can accept a password modification and check passwords only for the **HTTPPassword** field in Lotus Notes.

Systems That Don’t Accept or Provide Passwords By Default

The following connected systems can’t accept passwords from Identity Manager or provide a user’s password to Identity Manager when using the basic driver configuration.

Although they can’t provide the user’s actual password, they can be configured to create a password in the Identity Vault by using a policy on the Publisher channel. The password would be based on other user data in the connected system. The basic driver configurations provided for the connected systems include a default password based on the surname.

Table 3-3 *Systems That Don’t Accept or Provide Passwords*

Connected System Driver	**Subscriber Channel**	**Subscriber Channel**	**Subscriber Channel**	**Publisher Channel**
	Application Can Accept Setting of Initial Password	**Application Can Accept Modification of Password**	**Application Supports Check Password**	**Application Can Provide (Sync) Password**
Delimited Text[1]	No	No	No	No
PeopleSoft 5.2	No	No	No	No
SAP HR	No	No	No	No

[1]The Identity Manager Driver for Delimited Text does not have features in the driver shim that directly support Password Synchronization. However, the driver can be configured to handle passwords, depending on the connected system you are synchronizing with.

Systems That Don’t Support Password Synchronization

The following connected systems are not intended to participate in password synchronization.

Table 3-4 *Systems That Don’t Support Password Synchronization*

Connected System Driver	**Subscriber Channel**	**Subscriber Channel**	**Subscriber Channel**	**Publisher Channel**
	Application Can Accept Setting of Initial Password	**Application Can Accept Modification of Password**	**Application Supports Check Password**	**Application Can Provide (sync) Password**
Avaya PBX	No	No	No	No
Entitlements Service	No	No	No	No
LoopBack Service	No	No	No	No

Connected System Driver	Subscriber Channel	Subscriber Channel	Subscriber Channel	Publisher Channel
	Application Can Accept Setting of Initial Password	**Application Can Accept Modification of Password**	**Application Supports Check Password**	**Application Can Provide (sync) Password**
Manual Task Service	No	No	No	No
Null Service	No	No	No	No
WorkOrder	No	No	No	No

4 Configuring Password Flow

To ensure that passwords flow between the Identity Vault and the connected system the way you expect them to, you should verify the password synchronization settings for the connected system's driver are configured properly.

- "Verifying Password Synchronization Settings in iManager" on page 19
- "Verifying Password Synchronization Settings in Designer" on page 21

Verifying Password Synchronization Settings in iManager

1 In iManager, open the properties page for the driver whose password settings you want to check:

   1a Click to display the Identity Manager Administration page.

   1b In the **Administration** list, click **Identity Manager Overview**.

   1c On the **Driver Sets** tab, locate the driver set that contains the driver whose settings you want to check. If the driver set is not listed on the **Driver Sets** tab, use the **Search In** field to search for and display the driver set.

   1d Click the driver set to open the Driver Set Overview page.

   1e Click the driver to display the Driver Overview page.

   1f Click the upper right corner of the driver to display the **Actions** menu, then click **Edit properties**.

2 Navigate to **Roles and Tasks > Password Synchronization** tab to see the password synchronization options.

The settings that are enabled and disabled vary depending on the driver. Only those settings for features supported by the driver are available (not dimmed).

3 Verify that the settings are configured properly.

Identity Manager accepts passwords (Publisher Channel): If this option is enabled, Identity Manager allows passwords to flow from the connected system into the Identity Vault. Disabling this option means that no `<password>` elements are allowed to flow to Identity Manager. They are stripped out of the XML by a password synchronization policy on the Publisher channel.

This setting applies to user passwords that are provided by the connected system itself, and password values that are created by a policy on the Publisher channel.

If this option is enabled but the Distribution Password option below it is disabled, a `<password>` value coming from the connected system is written directly to the Universal password in the Identity Vault. If the user's password policy does not enable Universal Password, the password is written to the NDS password.

Use Distribution Password for password synchronization: This setting is available only if the **Identity Manager accepts passwords (Publisher Channel)** setting is enabled.

If this option is enabled, a password value coming from the connected system is written to the Distribution password. The Distribution password is reversible, which means that it can be retrieved from the Identity Vault data store for password synchronization. It is used by Identity Manager for bidirectional password synchronization with connected systems. For Identity Manager to distribute passwords from this system to other systems, this option must be enabled.

Accept password only if it complies with user's Password Policy: This setting is available only if the **Use Distribution Password for password synchronization** setting is enabled.

If this option is selected, Identity Manager does not write a password from this connected system to the Distribution password in the Identity Vault or publish it to connected systems unless the password complies with the user's password policy.

If a password does not comply, enable the **Reset the user's password to the Distribution Password** setting to reset the user's password on the connected system. This allows you to enforce the password policy on the connected system as well as in your Identity Vault. If you do not select this option, user passwords can become out-of-sync on connected systems. However, you need to consider the connected system's password policies when deciding whether to use this option. Some connected systems might not allow the reset because they don't allow you to repeat passwords.

By using the **Notify the user of password synchronization failure via e-mail setting**, you can inform users when a password fails to be set or reset. Notification is especially helpful for this option. If the user changes to a password that is allowed by the connected system but rejected by Identity Manager because of the password policy, the user won't know that the password has been reset until the user receives a notification or tries to log in to the connected system with the old password.

Always accept password; ignore Password Policies: This setting is available only if the **Use Distribution Password for password synchronization** setting is enabled.

If you select this option, Identity Manager does not enforce the user's password policy for this connected system. Identity Manager writes the password from this connected system to the Distribution password in the Identity Vault and distributes it to other connected systems regardless of password policy compliance.

Application accepts passwords (Subscriber Channel): If you enable this option, the driver sends passwords from the Identity Vault to this connected system. This also means that if a user changes the password on a different connected system that is publishing passwords to the Distribution password in the Identity Vault, the password is changed on this connected system.

By default, the Distribution password is the same as the Universal password in the Identity Vault, so changes to the Universal password made in the Identity Vault are also sent to the connected system.

Notify the user of password synchronization failure via e-mail: If you enable this option, e-mail is sent to the user if a password is not synchronized, set, or reset. The e-mail that is sent to the user is based on an e-mail template. This template is provided by the Password Synchronization application. However, for the template to work, you must customize it and specify an e-mail server to send the notification messages. For instructions, see Chapter 5, "Configuring E-Mail Notification," on page 25.

4 When you are finished, click **OK** to save your changes.

The settings are saved as Global Configuration Values. You can view them on the Identity Manager > Global Config Values page.

Verifying Password Synchronization Settings in Designer

1 In Designer, open your project.

2 In the Modeler, right-click the icon for the driver whose settings you want to check, then click **Password Synchronization** to display the Password Synchronization Options dialog box.

The settings that are enabled and disabled vary depending on the driver. Only those settings for features supported by the driver are available (not dimmed).

3 Verify that the settings are configured properly.

Identity Manager accepts passwords (Publisher Channel): If this option is enabled, Identity Manager allows passwords to flow from the connected system into the Identity Vault. Disabling this option means that no `<password>` elements are allowed to flow to Identity Manager. They are stripped out of the XML by a password synchronization policy on the Publisher channel.

This setting applies to user passwords that are provided by the connected system itself, and password values that are created by a policy on the Publisher channel.

If this option is enabled but the Distribution Password option below it is disabled, a `<password>` value coming from the connected system is written directly to the Universal password in the Identity Vault. If the user's password policy does not enable Universal Password, the password is written to the NDS password.

Use Distribution Password for password synchronization: This setting is available only if the **Identity Manager accepts passwords (Publisher Channel)** setting is enabled.

If this option is enabled, a password value coming from the connected system is written to the Distribution password. The Distribution password is reversible, which means that it can be retrieved from the Identity Vault data store for password synchronization. It is used by Identity Manager for bidirectional password synchronization with connected systems. For Identity Manager to distribute passwords from this system to other systems, this option must be enabled.

Accept password only if it complies with user's Password Policy: This setting is available only if the **Use Distribution Password for password synchronization** setting is enabled.

If this option is selected, Identity Manager does not write a password from this connected system to the Distribution password in the Identity Vault or publish it to connected systems unless the password complies with the user's password policy.

If a password does not comply, enable the **Reset the user's password to the Distribution Password** setting to reset the user's password on the connected system. This allows you to enforce the password policy on the connected system as well as in your Identity Vault. If you do not select this option, user passwords can become out-of-sync on connected systems. However, you need to consider the connected system's password policies when deciding whether to use this option. Some connected systems might not allow the reset because they don't allow you to repeat passwords.

By using the **Notify the user of password synchronization failure via e-mail setting**, you can inform users when a password fails to be set or reset. Notification is especially helpful for this option. If the user changes to a password that is allowed by the connected system but rejected by Identity Manager because of the password policy, the user won't know that the password has been reset until the user receives a notification or tries to log in to the connected system with the old password.

Always accept password; ignore Password Policies: This setting is available only if the **Use Distribution Password for password synchronization** setting is enabled.

If you select this option, Identity Manager does not enforce the user's password policy for this connected system. Identity Manager writes the password from this connected system to the Distribution password in the Identity Vault and distributes it to other connected systems regardless of password policy compliance.

The application accepts passwords (Subscriber Channel): If you enable this option, the driver sends passwords from the Identity Vault to this connected system. This also means that if a user changes the password on a different connected system that is publishing passwords to the Distribution password in the Identity Vault, the password is changed on this connected system.

By default, the Distribution password is the same as the Universal password in the Identity Vault, so changes to the Universal password made in the Identity Vault are also sent to the connected system.

Notify the user of password synchronization failure via e-mail: If you enable this option, e-mail is sent to the user if a password is not synchronized, set, or reset. The e-mail that is sent to the user is based on an e-mail template. This template is provided by the Password Synchronization application. However, for the template to work, you must customize it and specify an e-mail server to send the notification messages. For instructions, see Chapter 5, "Configuring E-Mail Notification," on page 25.

4 When you are finished, click **OK** to save your changes.

The settings are saved as Global Configuration Values. You can view them on the Identity Manager > Global Config Values page.

5 Configuring E-Mail Notification

iManager tasks enable you to specify the e-mail server and customize the templates for e-mail notifications.

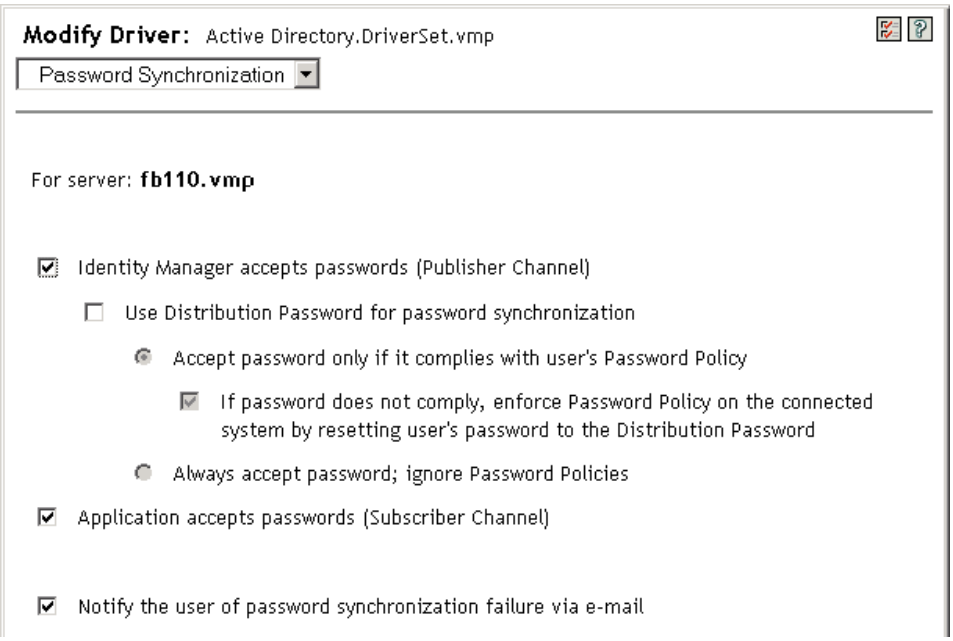
E-mail templates are provided to allow Password Synchronization and Password Self-Service to send automated e-mails to users.

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

You control whether e-mail messages are sent, based on your choices in iManager. 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-mailing a password to the user, or e-mailing a password hint to the user. See "Managing Forgotten Passwords" in the *Password Management 3.3 Administration Guide*.

When you select **Notify the user of password synchronization failure via e-mail**, Password Synchronization is configured to send e-mail for failed password sync operations only, and only for the drivers you specify.

Figure 5-1 *Configuring Password Synchronization*



In addition, you need to make sure that the SMTP authentication information is included in the driver policies.

- "Prerequisites" on page 26
- "Setting Up the SMTP Server to Send E-Mail Notification" on page 26
- "Setting Up E-Mail Templates for Notification" on page 28
- "Providing SMTP Authentication Information in Driver Policies" on page 28
- "Adding Your Own Replacement Tags to E-Mail Notification Templates" on page 30
- "Sending E-Mail Notifications to the Administrator" on page 36
- "Localizing E-Mail Notification Templates" on page 37

Prerequisites

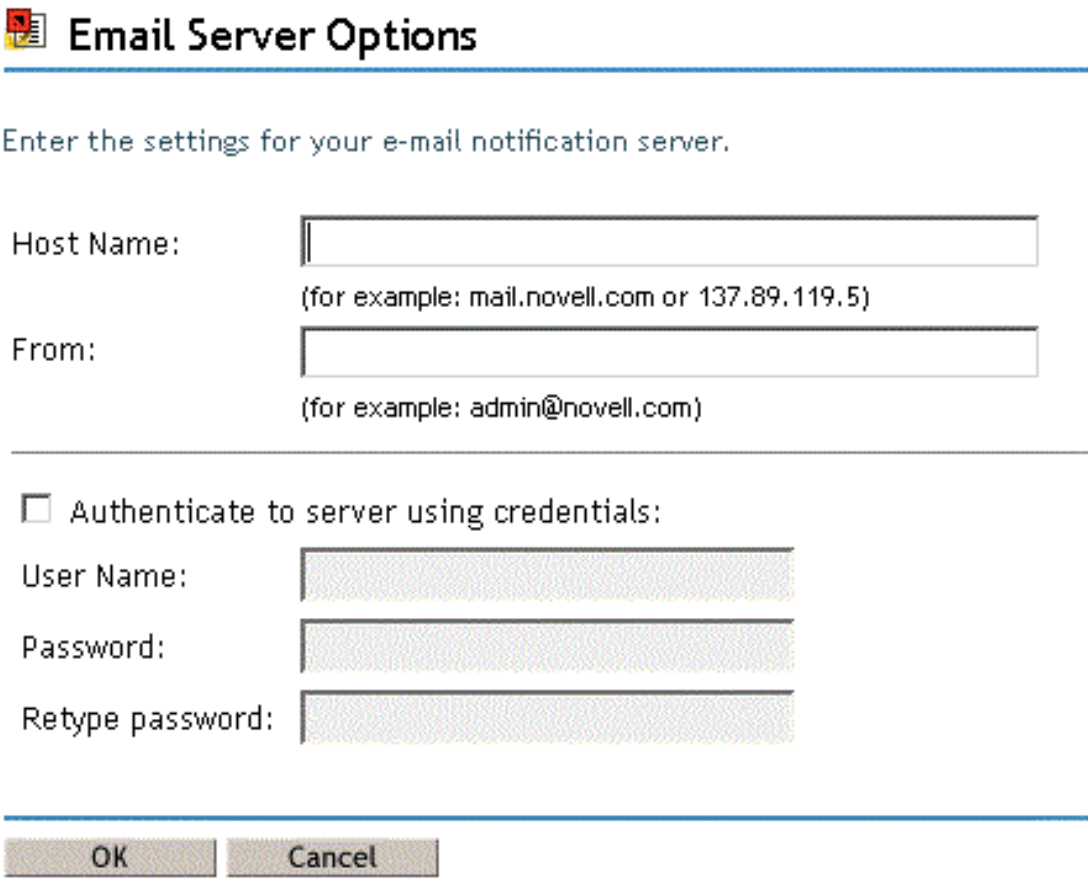
- ❒ Make sure that your Identity Vault users have the Internet EMail Address attribute populated.
- ❒ If you are using e-mail notifications for Password Synchronization, make sure that the Password Synchronization driver policies contain the password for the SMTP server. See "Providing SMTP Authentication Information in Driver Policies" on page 28.
- ❒ If you are concerned that some users might not have the e-mail address populated, or if you want an e-mail record of all failure notifications, consider choosing a password administrator account that all e-mail notifications are sent to, in addition to the user.

  This e-mail address should be in the **To** field of the Identity Manager script policy. For more information, see "Sending E-Mail Notifications to the Administrator" on page 36.
- ❒ If eDirectory and Identity Manager are on a UNIX server, the server must hold a replica of the e-mail template objects.

  These objects are located in the Security container, at the root. This means that the server needs a replica of the root partition.

Setting Up the SMTP Server to Send E-Mail Notification

1. In iManager, select **Passwords** > **Email Server Options**.



2 Specify the following information:

- The host name
- This field holds the information that you want to appear in the From field of the e-mail message.

  For example, mail.novell.com, mail.novell.com:2525, 192.99.90.66 or 192.99.90.66:2525

  NOTE: The host name (in Email Server configuration option) has enhanced to support the custom SMTP server port besides the default option of configuring SMTP server.

- The username and password for authenticating to the server, if necessary.

3 Click **OK**.

4 If you are using Password Synchronization with your Identity Manager drivers and want to use the e-mail notification feature, you must also do the following:

4a If your SMTP server requires authentication before sending e-mail, make sure that the driver policies contain the password. See "Providing SMTP Authentication Information in Driver Policies" on page 28 for instructions.

Specifying the authentication information in the Email Server Options page in Step 2 is sufficient for Forgotten Password notifications, but not for Password Synchronization notifications.

4b Restart Identity Manager drivers that need to be updated with the changes.

The driver reads the templates and SMTP server information only at startup time.

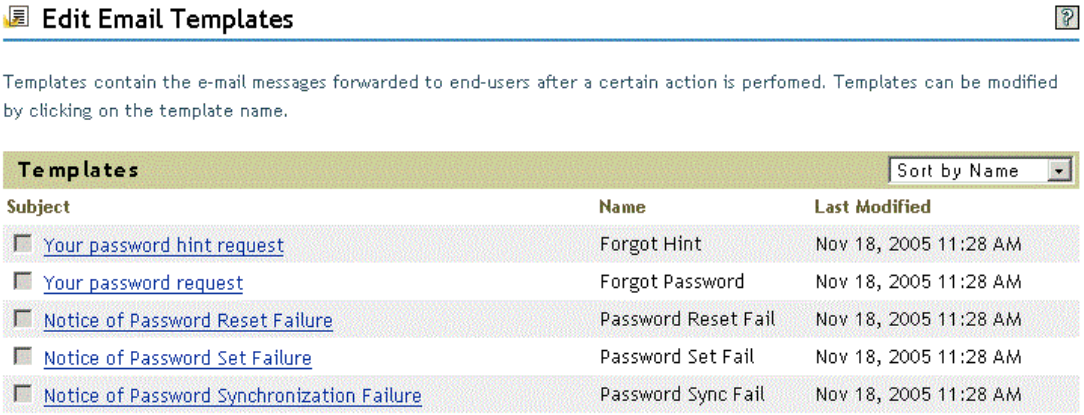
5 Customize the e-mail templates as described in "Setting Up E-Mail Templates for Notification" on page 28.

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.

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, select **Passwords** > **Email Templates**.



2 Edit the templates as desired.

Keep in mind that if you want to add any replacement tags, some additional tasks might be required. Follow the instructions in "Adding Your Own Replacement Tags to E-Mail Notification Templates" on page 30.

3 Restart Identity Manager drivers that need to be updated with the changes.

The driver reads the templates and SMTP server information only at startup time.

Providing SMTP Authentication Information in Driver Policies

You specify the username and password for the SMTP server in "Setting Up the SMTP Server to Send E-Mail Notification" on page 26. For Forgotten Password e-mail notifications, this is sufficient.

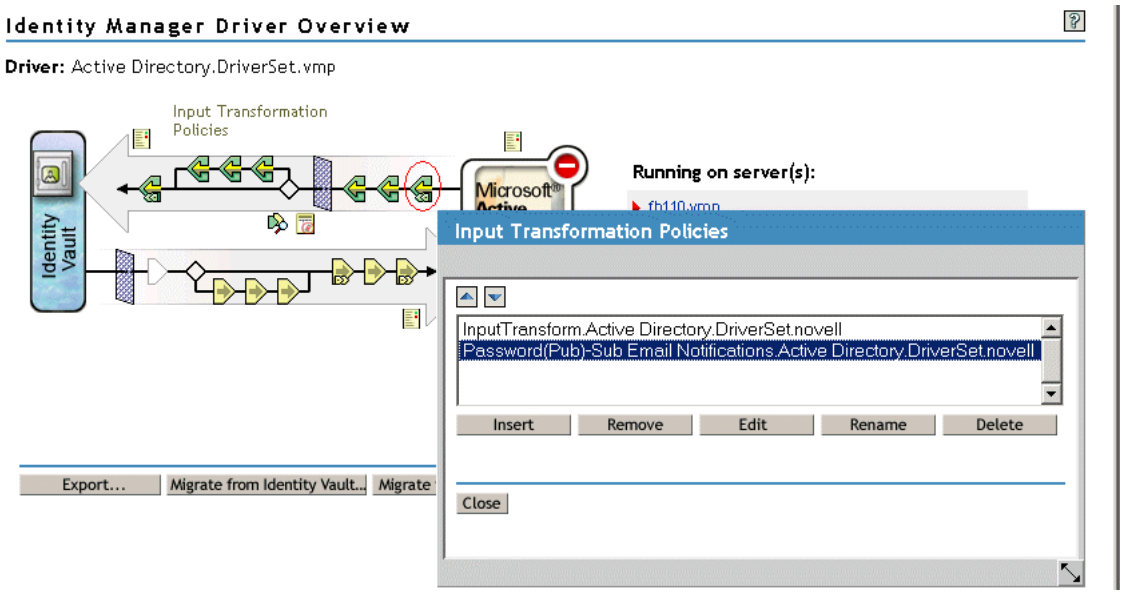
However, for Password Synchronization e-mail notifications, you also need to include the password in the driver policies. The Identity Manager engine can access the username, but not the passwords. The driver policy must provide it.

You must complete this procedure if the following conditions exist:

- The SMTP server is secured and requires authentication before sending e-mail.
- You are using Identity Manager Password Synchronization with an Identity Manager driver
- In the Password Synchronization settings for the driver, you have selected **Notify the user of password synchronization failure via e-mail**.

To add the SMTP server password to the driver policy:

1. In iManager, select **Identity Manager** > **Identity Manager Overview.**
2. Search for the driver sets, or browse and select a container that holds the driver set.
3. In the Identity Manager Driver Overview, click the icon for the driver.
4. Select an Input Transformation icon or an Output Transformation icon.

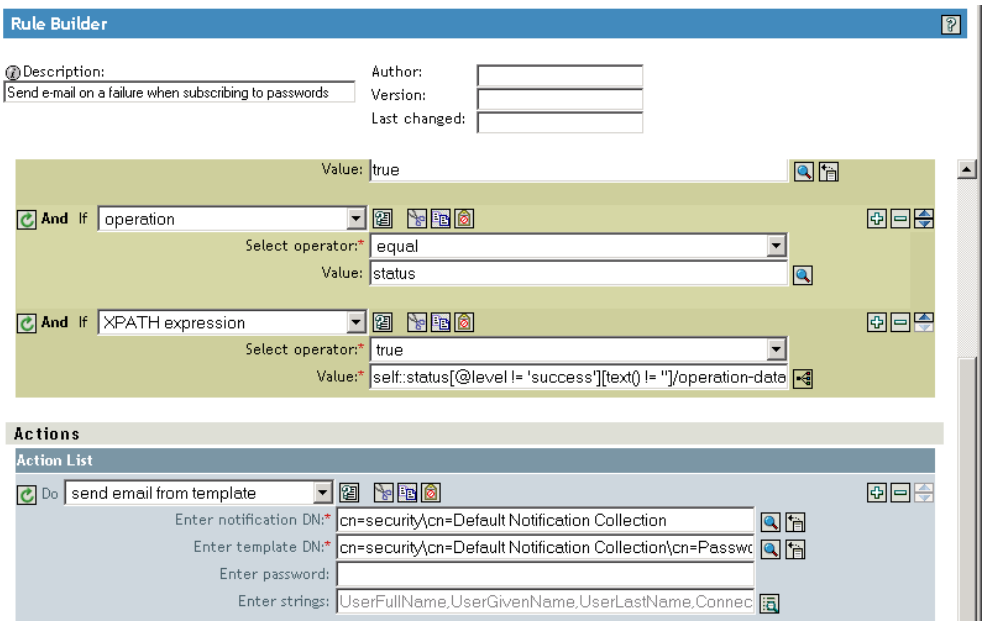


5. Select a policy, then click **Edit**.
6. Click a rule.
7. Specify the password for the SMTP server in the rules that include Do Send E-mail from Template actions.

   For example, if you are using the sample driver configurations, the following Password Synchronization policies need to be modified.

Policy Set	Policy Name	Rule Name
Input Transformation	Password(Pub)-Sub Email Notifications	◆ Send e-mail on a failure when subscribing to passwords ◆ Send e-mail on failure to reset the connected system password by using the Identity Manager data store password
Output Transformation	Password(Sub)-Pub Email Notifications	◆ Send e-mail for a failed publish password operation

The following figure shows an example of a Do Send E-mail from Template action that requires the password.



The password is obfuscated when it is stored in the Identity Vault.

8 Select the rule, then click **OK**.

Adding Your Own Replacement Tags to E-Mail Notification Templates

The e-mail notification templates have some tags defined by default, to help you personalize the message for the user. You can also add your own tags.

Your ability to add tags is dependent on the application that is using the e-mail template.

- "Adding Replacement Tags to Password Synchronization E-Mail Notification Templates" on page 31
- "Adding Replacement Tags to Forgotten Password E-Mail Notification Templates" on page 36

Adding Replacement Tags to Password Synchronization E-Mail Notification Templates

You can add replacement tags to the e-mail notification templates for Password Synchronization, but these tags don't work unless you also define them in every password synchronization policy rule that refers to the e-mail notification template. When using a DoSendEmailFromTemplate action, all replacement tags declared within the template must be defined as child arg-strings elements of the action.

For example, Identity Manager provides default replacement tags that are included with the e-mail notification templates. Identity Manager also provides default password synchronization policies in the driver configurations. Each default tag provided with the e-mail template is also defined in each rule of the password synchronization policy that uses that e-mail template.

For example, the UserGivenName tag is one of the default tags defined in the e-mail template named Password Set Fail. A policy rule named **Send e-mail on a failure when subscribing to passwords** refers to that e-mail template in a DoSendEmailFromTemplate action. This rule is used in a policy to notify to a user when a password fails to synchronize. The same UserGivenName tag is defined as an arg-string element in that rule.

Like this example, each new tag you add must be defined in both the e-mail template and the policy rules that refer to the e-mail template, so that the Identity Manager engine knows how to insert the correct data in place of the replacement tag when sending the e-mail to the user.

You can refer to the tags in the Identity Manager driver configurations that shipped with Identity Manager as examples.

Keep in mind the following guidelines:

- The items called replacement tags in the e-mail templates are called tokens in the context of Policy Builder.
- You should use Policy Builder to make it easier to define the argument strings for the replacement tags, as explained in the steps in this section.
- The tags you add might be defined to be any of the following:
  - Any Source or Destination attribute for the user

    Unlike adding tags for the e-mail templates for Forgotten Password, simply adding a tag that has the same name as an attribute on the User object in the Identity Vault does not cause the tag to work. As with all tags used in password synchronization e-mail notification templates, you must also define the tag in the policy that is referring to the e-mail template.
  - A global configuration value
  - An XPATH expression

  This is in contrast to tags for the e-mail templates for Forgotten Password, which are limited to eDirectory user attributes.
- Unlike adding tags for the e-mail templates for Forgotten Password (which require you to use the exact name of an eDirectory user attribute), you can name the replacement tags any name you choose, as long as it matches the name used to define the tag in the policies that reference the e-mail template.

To define the tags in a policy, find all the policies that refer to the e-mail notification template, and use Policy Builder to add the tags to them. In each policy, edit each rule that refers to the template.

One way to make sure that you find all the policies that refer to the e-mail notification templates is to export your driver configurations, then search the XML for a do-send-e-mail action that has the template equal to the name of the e-mail notification template.

1 In iManager, select **Identity Manager** > **Identity Manager Overview**.

2 Select the driver set that contains the driver with the policy you want to edit.

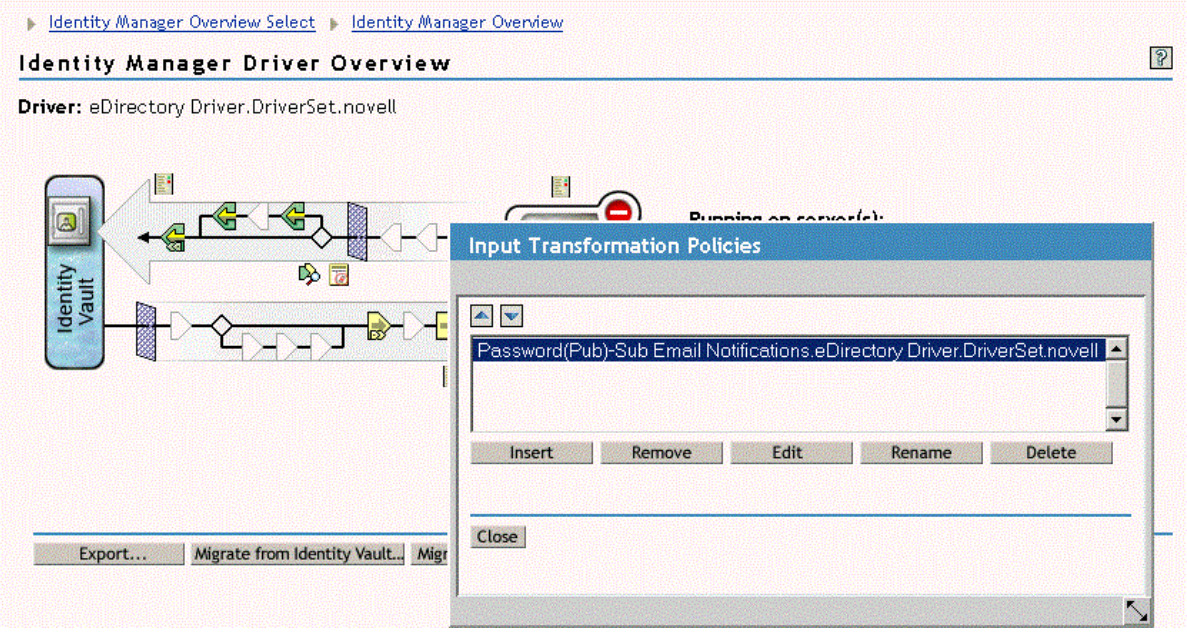
3 Click the icon for the driver that has the policy you want to edit.

4 On the Publisher or Subscriber channel, click the set of policies that contains the policy you want to edit.

   For example, the driver configuration for the eDirectory driver that ships with Identity Manager contains a policy in the Input Transformation policy set that references both password synchronization e-mail notification templates.

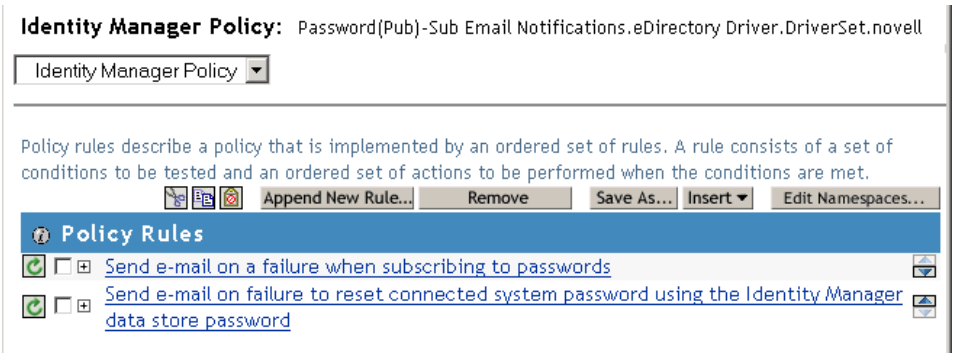
5 Click the policy, then click **Edit**.

   The following figure illustrates how to edit the Password(Pub)-Sub Email Notifications policy for the eDirectory driver:

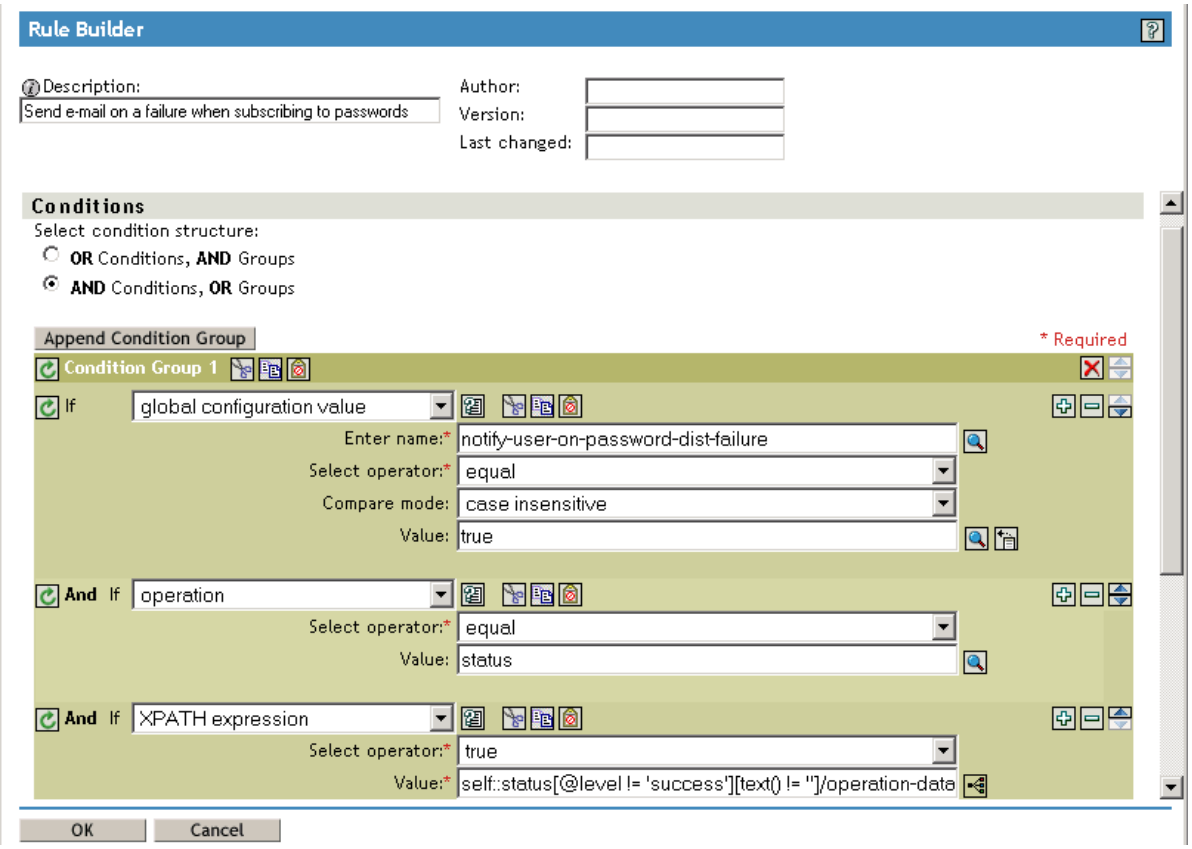


6 In the list of rules that opens, click the rule that refers to the e-mail notification template.

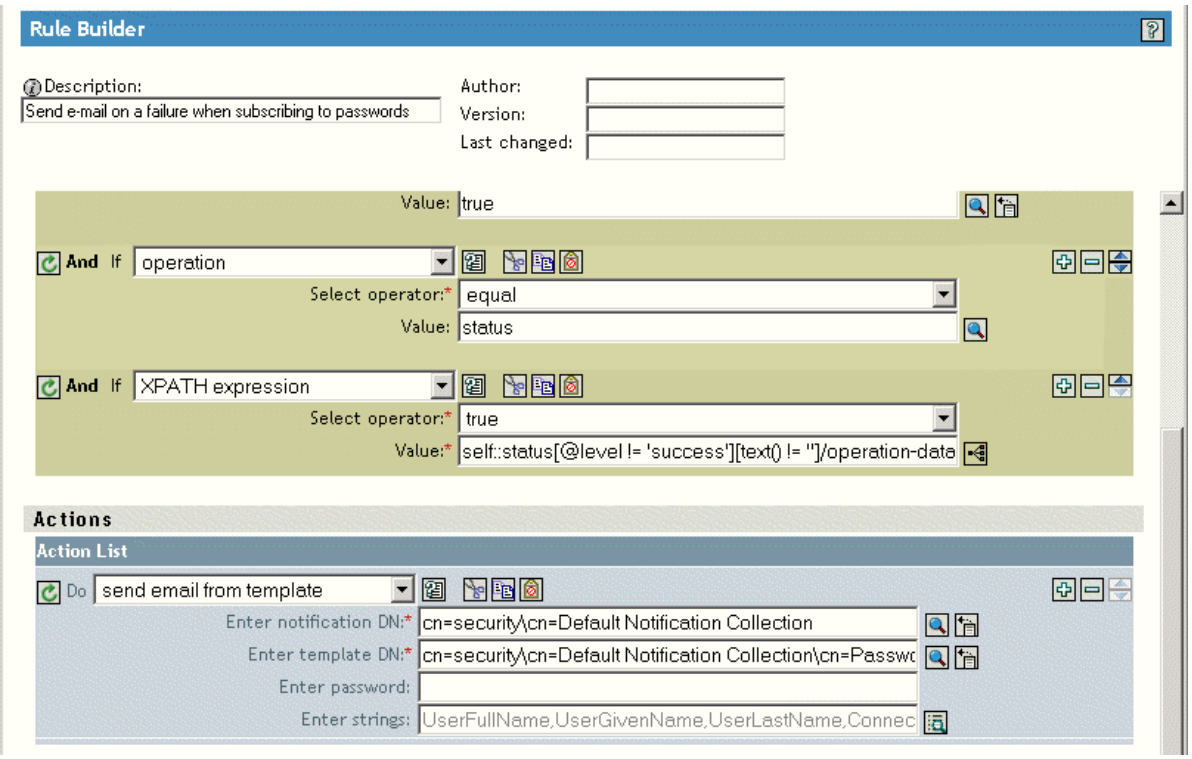
   For example, in the Password(Pub)-Sub Email Notifications policy, you see the following list of rules. Both of these rules reference one of the password synchronization e-mail templates. You need to edit both rules if you are adding tags to both templates.



If you click the first rule, the following page appears:

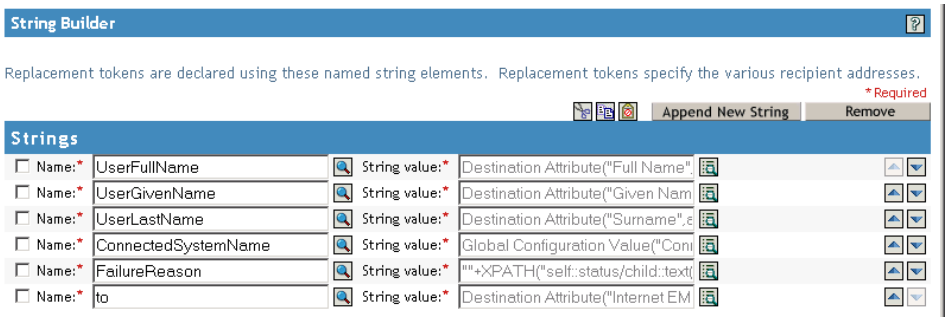


7 Scroll to the **Actions** section.



8 For the **Do Send Email from Template** rule, click the browse button for the **Enter strings** field.

This opens the string builder. For the example rule, the following figure shows the list of strings you would see. The default tags that are used in the e-mail notification templates are already defined in the password synchronization policies that are part of the Identity Manager driver configurations, like this one. You can use the default tags as an example.



9 To define a tag that you could use in an e-mail notification template, click **Append New String**, then enter a name for the tag.

Make sure that the name is exactly the same name you use in the e-mail notification template.

10 In the **String value** field, click the browse button to help you define the tag.

11 On the Argument Builder page, specify the value that should be brought in when this tag is used in an e-mail notification template.

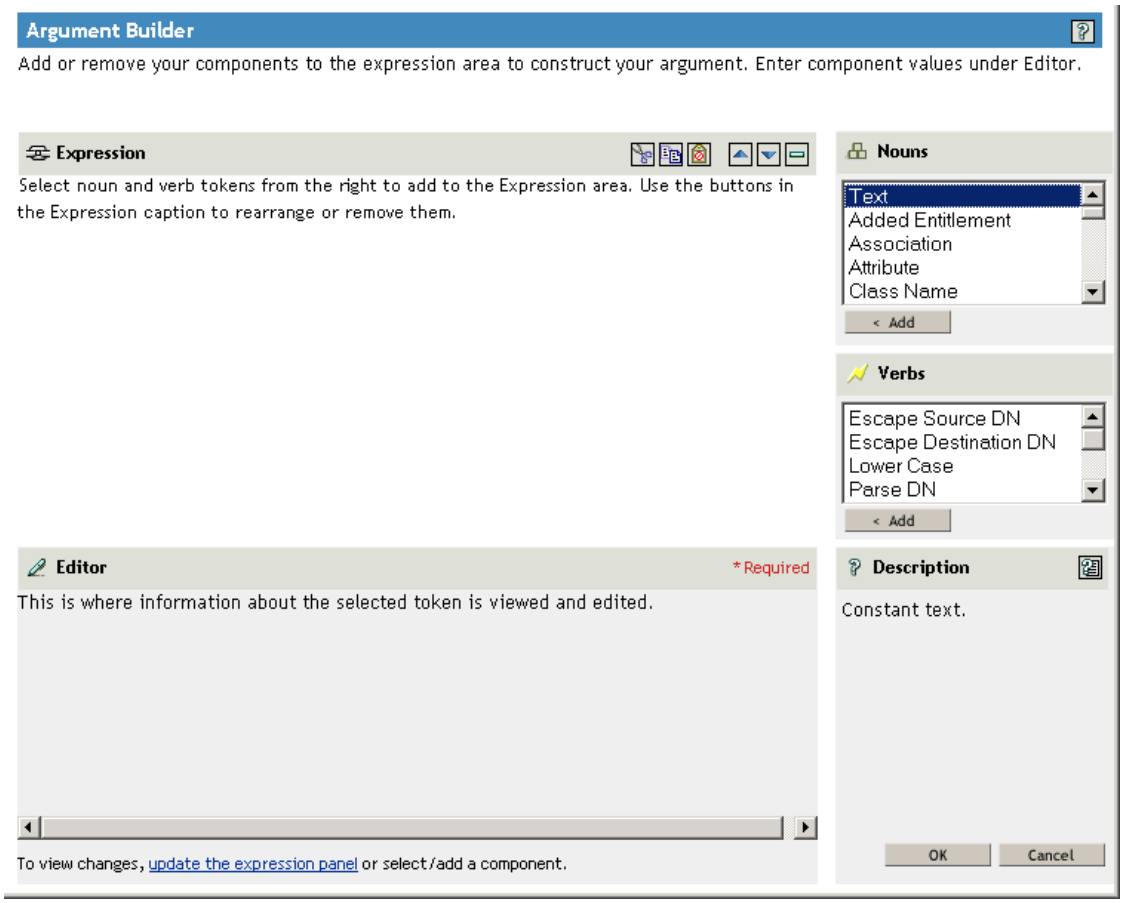
You can define the tag to be any of the following:

- Any Source or Destination attribute for the user

Unlike adding tags for the e-mail templates for Forgotten Password, simply adding a tag that has the same name as an attribute on the user object in the Identity Vault does not cause the tag to work. As with all tags used in password synchronization e-mail notification templates, you must also define the tag in the policy that is referring to the e-mail template.

- A global configuration value
- An XPATH expression

The following figure illustrates how to define the tag:



After you define the tag and click **OK**, it shows up as one of the strings in the String Builder page.

12 Make sure you click **OK** to complete all the pages, so that your changes to the policy are saved.

13 Repeat the steps to edit the rules in all the policies that refer to the e-mail notification template.

14 Add the tag you defined in the policy to the e-mail notification template, using the exact name you used in the policies.

At this point, you can use the tag name in the body of the e-mail notification template.

15 Save the changes and restart the driver.

Adding Replacement Tags to Forgotten Password E-Mail Notification Templates

Using the following guidelines, you can add tags to the e-mail notification templates for Forgotten Password:

- You can add only tags that correspond to LDAP attributes on the User object that the message is being sent to.
- The name of the tag you add must be exactly the same as the LDAP attribute name on the user object.

  To see how LDAP attributes correspond to eDirectory attribute names, refer to the Schema Mapping Policy that is provided in the Identity Manager Driver for LDAP.
- No other configuration is necessary.

By default, the Forgotten Password E-Mail Notification template uses the UserFullName variable. The full name attribute is not used by the e-mail notification template, instead it uses the login attribute. For example, if the full name attribute is Alison Blake and the login attribute is ablake, the e-mail greeting is “Dear ablake” instead of “Dear Alison Blake”.

The e-mail notification template uses the cn value of the variable found in eDirectory. For example, if cn=ablake, the e-mail notification template uses ablake. If the cn value is changed to Allison Blake, the e-mail notification template uses the full name, Allison Blake. If the FullUserName variable is used instead of FirstName variable, the e-mail notification template appears without the user's first name.

Sending E-Mail Notifications to the Administrator

The default configuration is for the e-mail notification to go only to the user. The policies that ship with Identity Manager use the e-mail address from the Identity Vault object for the user that is affected.

However, you can configure the password synchronization policies so that e-mail notifications also go to the administrator. To do this, you must modify the Identity Manager script for one of the policies.

Send a Blind Copy to the administrator by defining the token with the administrator's e-mail address.

To copy an administrator, modify the policy that generates the e-mail (such as `PublishPasswordEmails.xml`, in which the policy looks up the e-mail address to send notifications) and add an additional `<arg-string>` element with the administrator's e-mail address.

The following example illustrates the additional arg-string element:

```
<arg-string name="to">
   <token-text>Admin@company.com</token-text>
</arg-string>
```

Make sure to restart the driver after making these changes.

Localizing E-Mail Notification Templates

Keep in mind the following:

- The default templates are in English, but you can edit the text to use other languages.
- The names and the definitions of the replacement tags must remain in English, so that the arg-string token definitions in the policies match the names of the replacement tags.
- For Forgotten Password e-mail notifications only, to specify what encoding you want on your mail item, you need to add a setting in the `portalservlet.properties` file. For example:

  ```
  ForgottenPassword.MailEncoding=EUC-JP
  ```

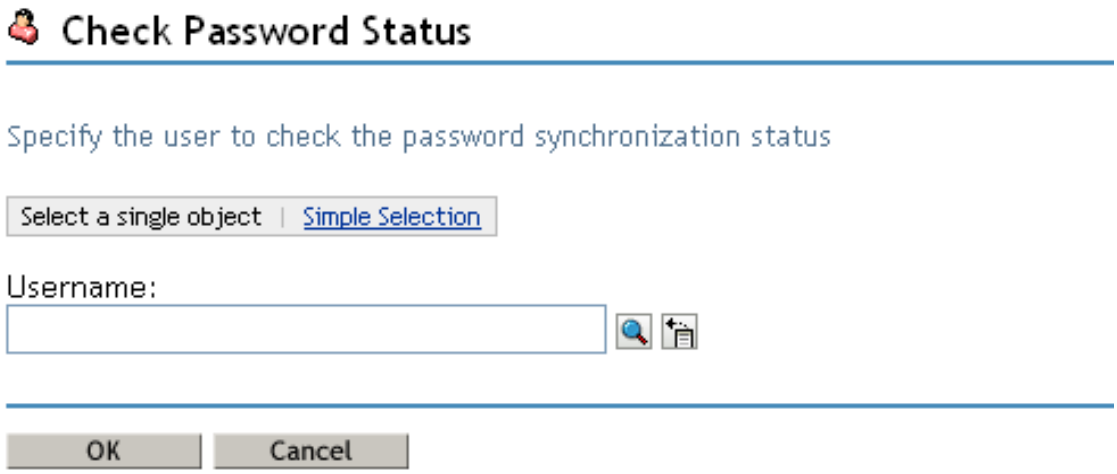
  If this setting doesn't exist, no encoding is used on the mail transformation.
- For Password Synchronization e-mail messages, an XML attribute named charset can be specified on the following elements: `<mail>`, `<message>`, and <‘>.

  For information on using these elements, see the NetIQ Identity Manager Manual Task Service Driver Implementation Guide.

6 Checking the Password Synchronization Status for a User

You can determine whether the Distribution password for a specific user is the same as the password in the connected system.

1. In iManager, click to display the Identity Manager Administration page.
2. In the **Passwords** list, > click **Check Password Status**.



3. Browse to and select a user.

The **Check Password Status** task causes the driver to perform a Check Object Password action.

Not all drivers support password check. Those that do must contain a password-check capability in the driver's manifest. iManager does not allow password check operations to be sent to drivers that do not contain this capability in the manifest.

The Check Object Password action checks the Distribution password. If the Distribution password is not being updated, Check Object Password might report that passwords are not synchronized.

The Distribution password is not updated if either of the following occurs:

- You are using the synchronization method described in "Scenario 1: Using NDS Password to Synchronize between Two Identity Vaults" on page 43.
- You are synchronizing Universal Password (as in "Scenario 2: Using Universal Password to Synchronize Passwords" on page 46), but you have not enabled the password policy configuration option to synchronize the Universal password to the Distribution password.

NOTE: Keep in mind that for the Identity Vault, the Check Password Status action checks the NDS Password instead of the Universal password. Therefore, if the user's password policy does not specify to synchronize the NDS password with the Universal password, the passwords are always reported as being not synchronized. In fact, the Distribution password and the password on the connected system might be in sync, but Check Password Status won't be accurate unless both the NDS password and the Distribution password are synchronized with the Universal password.

Understanding DirXML-PasswordSyncStatus Attribute

When a password synchronization operation is triggered on a user, the user's `DirXML-PasswordSyncStatus` attribute gets updated with the status of the <modify-password> operation. The value looks like:

```
39DB7DED8436EE4DF38039DB7DED8436201403251414227210000000000001Code(-8032)
Operation vetoed by policy
```

- The first 32 bytes represent the GUID of the driver the user is associated with.
- The next 17 bytes represent the password sync time in yyyyMMddHHmmssSSS format
- The next 8 bytes are 00000000
- The next 4 bytes indicate any one of the following status codes:
  - 0000: ERROR
  - 0001: WARNING
  - 0002: RETRY
  - 0003: FATAL
  - 0004: SUCCESS
  - 0005: PENDING

    NOTE: The 0005 status code indicates a password change has not synchronized because the driver is not running.
- The next string is the status message, if any.

NOTE: For a Fan-Out driver, the value of the `DirXML-PasswordSyncStatus` attribute has a length of 93 bytes. Identity Manager appends the Fan-Out instance GUID after the Fan-Out driver GUID in the attribute value. For example, in a value `F45B667425626A448C7BF45B66742562CBB39C8D3DB3904F866DCBB39C8D3DB32017011810300154200000000004`, the first 32 bits represent the Fan-Out driver GUID followed by 32 bits of Fan-Out instance GUID. The remaining bytes represent the other values for the attribute.

7 Troubleshooting Password Synchronization

- See the tips in Appendix A, “Password Synchronization Scenarios,” on page 43.
- Make sure you have the Simple Password Login Method installed with NetIQ Modular Authentication Service (NMAS).
- Make sure you have a copy of the root of the tree on the servers where you need to NMAS to enforce password policies on eDirectory login methods or on passwords from connected systems being synchronized by Identity Manager.
- Make sure that the users requiring password synchronization are replicated on the same server with the driver that is synchronizing the passwords. As with other driver functions, the driver can manage only the users that are in a master or read/write replica on the same server.
- Make sure SSL is configured properly between the Web server and the Identity Vault.
- If you see an error about a password not complying when a user is initially created, but the password is set correctly in the Identity Vault, the default password in the driver policy might not conform to the password policy that applies to that user.

  The following scenario uses the Active Directory driver. However, the same issue could occur for another driver.

  Providing an Initial Password: You want the Active Directory driver to provide the initial password for a user when the driver creates a new User object in the Identity Vault to match a user in Active Directory. The sample configuration for the Active Directory driver sends the initial password as a separate operation from adding the user, and the sample configuration also includes a policy that provides a default password for a user if no password is provided by Active Directory.

  Because adding the user and setting the password are done separately, a new user always receives the default password, even if only momentarily. The default password is soon updated because the Active Directory driver sends the password immediately after adding the user. If the default password does not comply with the Identity Vault password policy for the user, an error is displayed.

  For example, if a default password created by using the user’s surname is too short to comply with the password policy, you might see a -216 error saying the password is too short. However, the situation is soon rectified if the Active Directory driver then sends an initial password that does comply

  Regardless of the driver you are using, if you want a connected system that is creating User objects to provide the initial password, consider one of the actions listed below. These measures are especially important if the initial password does not come with the Add event but instead comes in a subsequent event.

  - Change the policy on the Publisher channel that creates the default password, so that the default password conforms to the password policies that have been defined for your organization in the Identity Vault. (Select **Passwords**, then select **Password Policies**.)

    When the initial password comes from the authoritative application, it replaces the default password.

This option is preferable because we recommend that a default password policy exist in order to maintain a high level of security within the system.

- On the Publisher channel, remove the policy that creates the default password. In the sample configuration, this policy is provided in the Command Transformation policy set. Adding a user without a password is allowed in the Identity Vault. The assumption for this option is that the password for the newly created User object eventually comes through the Publisher channel, and the User object exists without a password for only a short time.

- Password policies are assigned with a tree-centric perspective. In contrast, Password Synchronization is set up per driver. Drivers are installed on a per-server basis and can manage only those users who are in a master or read/write replica.

  To get the results you expect from Password Synchronization, make sure that the containers that are in a master or read/write replica on the server running the drivers for Password Synchronization match 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.

- Helpful DSTrace commands:

  +DXML: To view Identity Manager rule processing and potential error messages.

  +DVRS: To view Identity Manager driver messages.

  +AUTH: To view NDS password modifications.

A Password Synchronization Scenarios

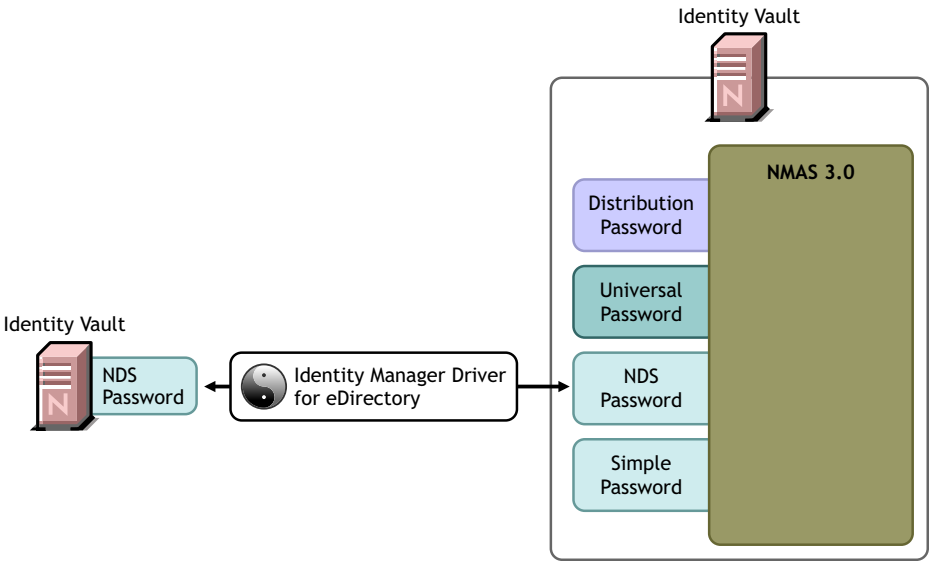
Identity Manager enables you to implement several different password synchronization scenarios. This section outlines basic scenarios that help you understand how the Identity Manager settings affect the way passwords are synchronized. You can use one or more of the scenarios to meet the needs of your environment.

- "Scenario 1: Using NDS Password to Synchronize between Two Identity Vaults" on page 43
- "Scenario 2: Using Universal Password to Synchronize Passwords" on page 46
- "Scenario 3: Synchronizing an Identity Vault and Connected Systems, with Identity Manager Updating the Distribution Password" on page 56
- "Scenario 4: Tunneling" on page 65
- "Scenario 5: Synchronizing Application Passwords to the Simple Password" on page 70

Scenario 1: Using NDS Password to Synchronize between Two Identity Vaults

You can synchronize the NDS password between two Identity Vaults by using the eDirectory driver. This scenario does not require Universal Password to be implemented, and can be used with eDirectory 8.6.x or later. Another name for this kind of password synchronization is synchronizing the public/private key pair.

Figure A-1 *Using NDS Password to Synchronize between Two Identity Vaults*



This method should be used only to synchronize passwords from Identity Vault to Identity Vault. It does not use NMAS and therefore cannot be used to synchronize passwords to connected applications.

- "Advantages and Disadvantages of Scenario 1" on page 44
- "Setting Up Scenario 1" on page 44
- "Troubleshooting Scenario 1" on page 45

Advantages and Disadvantages of Scenario 1

Table A-1 *eDirectory to eDirectory Password Synchronization Using NDS Password*

Advantages	Disadvantages
Simple configuration. Just include the correct attributes in the driver filter. If you are deploying Identity Manager and eDirectory 8.x in stages, this method can help you deploy gradually. ◆ You don't need to add the new password synchronization policies to driver configurations. ◆ Does not require Universal Password to be implemented in the Identity Vault. ◆ Can be used with connected vaults running eDirectory 8.x or later. ◆ Does not require NMAS Enforces the basic password restrictions you can set for the NDS password.	This method synchronizes passwords between Identity Vaults. Passwords cannot be synchronized to other connected systems. Does not update the Universal and Distribution passwords. Because this method does not use NMAS, you can't validate passwords against Advanced Password Rules in password policies for passwords coming from another Identity Vault. Because this method does not use NMAS, you can't reset passwords on the connected Identity Vault if the passwords don't comply with the NMAS password policy. E-mail notifications are not provided for password synchronization failures. Check Password Status operations from the iManager task are not supported. (The Distribution password is required for this feature.)

Setting Up Scenario 1

To set up this kind of password synchronization, configure the driver.

Universal Password Deployment

Not necessary.

Password Policy Configuration

None.

Password Synchronization Settings

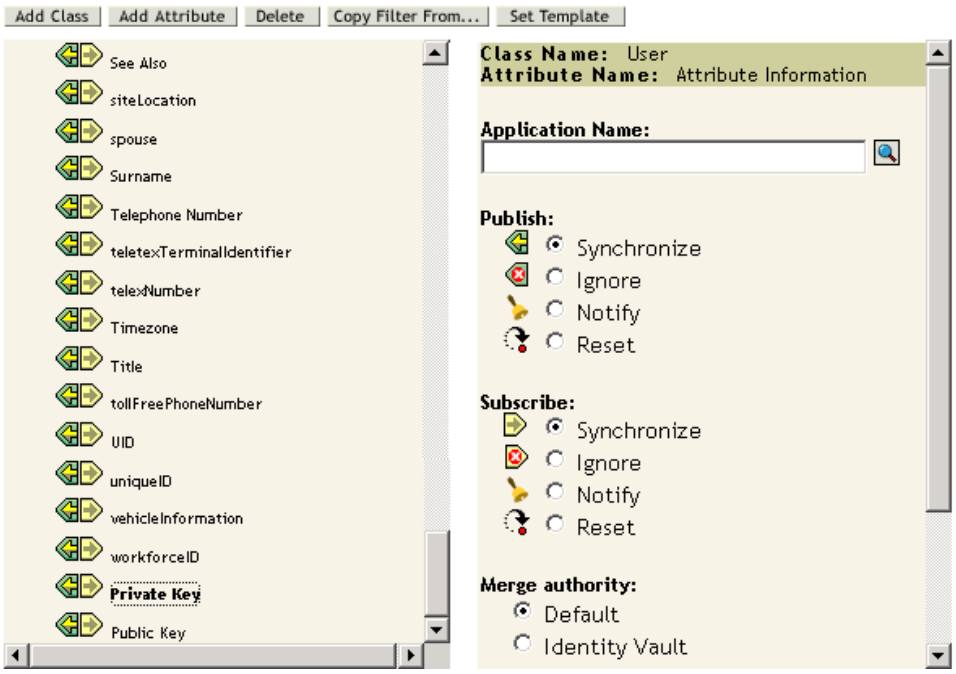
None. The settings on the Password Synchronization page for a driver have no effect on this method of synchronizing the NDS password.

Driver Configuration

Make the following changes in the eDirectory driver's filter. This must be done for both eDirectory drivers involved in the synchronization.

- Remove the nspmDistributionPassword attribute from the User class in the filter.
- Add the Public Key and Private Key attributes for all object classes (typically, the User class) for which passwords should be synchronized. The following figure shows an example.

Figure A-2 *Synchronizing the Private and Public Key Attributes*



Troubleshooting Scenario 1

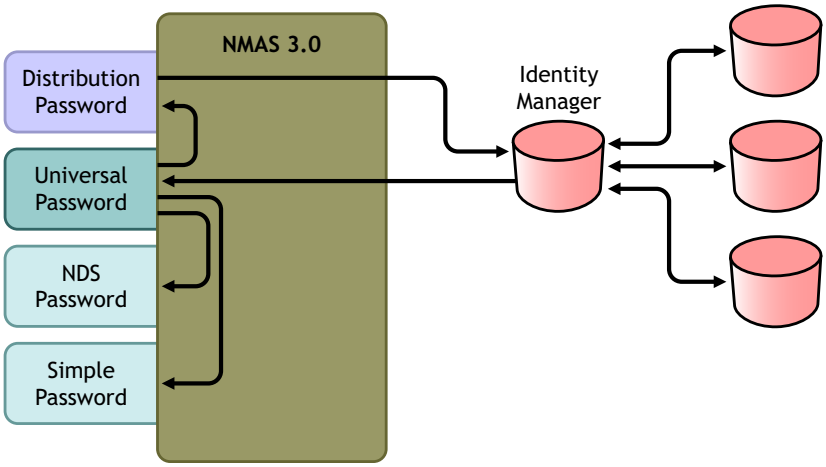
- Turn on the DSTrace option.
- Check the driver Filter to make sure the Public Key and Private Key attributes are being synchronized, not ignored.
- See also the tips in Chapter 7, "Troubleshooting Password Synchronization," on page 41.

Scenario 2: Using Universal Password to Synchronize Passwords

With Identity Manager, you can synchronize a connected system password with the Universal password in the Identity Vault.

When the Universal password is updated, the NDS password, Distribution password, or Simple Password can also be updated, depending on your settings in the NMAS password policy.

Figure A-3 *Using Universal Password to Synchronize Passwords*



1. Passwords come in through Identity Manager.
2. Identity Manager goes through NMAS to directly update the Universal password.
3. NMAS synchronizes the Universal password with the Distribution password and other passwords according to the NMAS password policy settings.
4. Identity Manager retrieves the Distribution password to distribute to connected systems that are set to accept passwords.

Although multiple connected systems are shown as connecting to Identity Manager in this figure, keep in mind that you individually create the settings for each connected system driver.

The following sections provide information and instructions for this scenario:

- "Advantages and Disadvantages of Scenario 2" on page 47
- "Setting Up Scenario 2" on page 47
- "Troubleshooting Scenario 2" on page 52

Advantages and Disadvantages of Scenario 2

Table A-2 Synchronizing by Using Universal Password

Advantages	Disadvantages
Allows synchronization of passwords to and from the Identity Vault and the connected system. Allows passwords to be validated against the NMAS password policy. Allows e-mail notifications for failed password operations, such as when a password coming from a connected system does not comply with Password. Supports the Check Password Status task in iManager, if the Universal password is being synchronized with the Distribution password and if the connected system supports checking passwords. NMAS enforces the Advanced Password Rules in your password policies, if you have the rules enabled. If a password coming from a connected system does not comply, an error is generated, and an e-mail notification is sent if you have specified that option. If you don't want password policy rules enforced, you can deselect **Enable Advanced Password Rules** in the NMAS password policy.	By design, resetting passwords in the connected system is not supported with this method because the Distribution password and Universal passwords might not be the same, depending on your settings in the password policies.

Setting Up Scenario 2

Use the information in the following sections to help complete the tasks in the Password Management Checklist.

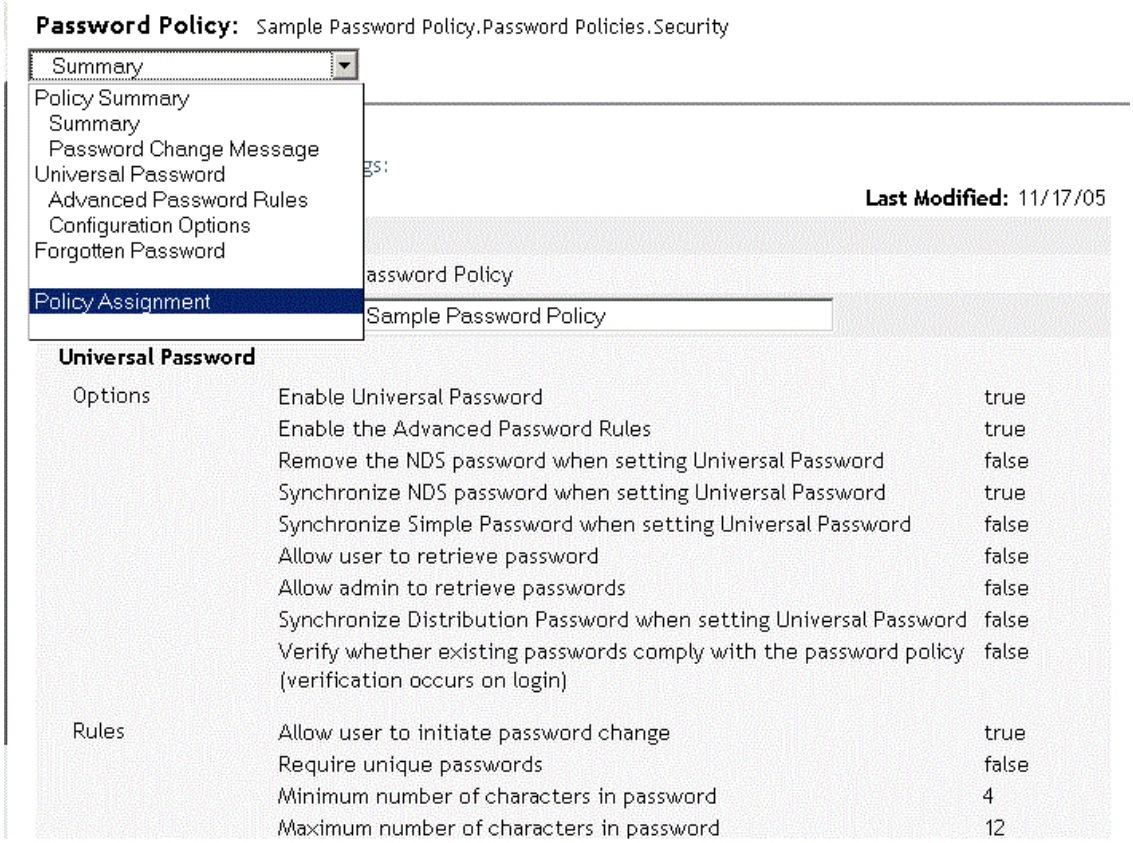
- "Password Policy Configuration" on page 47
- "Password Synchronization Settings" on page 50
- "Driver Configuration" on page 51

Password Policy Configuration

Make sure that an NMAS password policy is assigned to the parts of the Identity Vault that you want to have this kind of password synchronization.

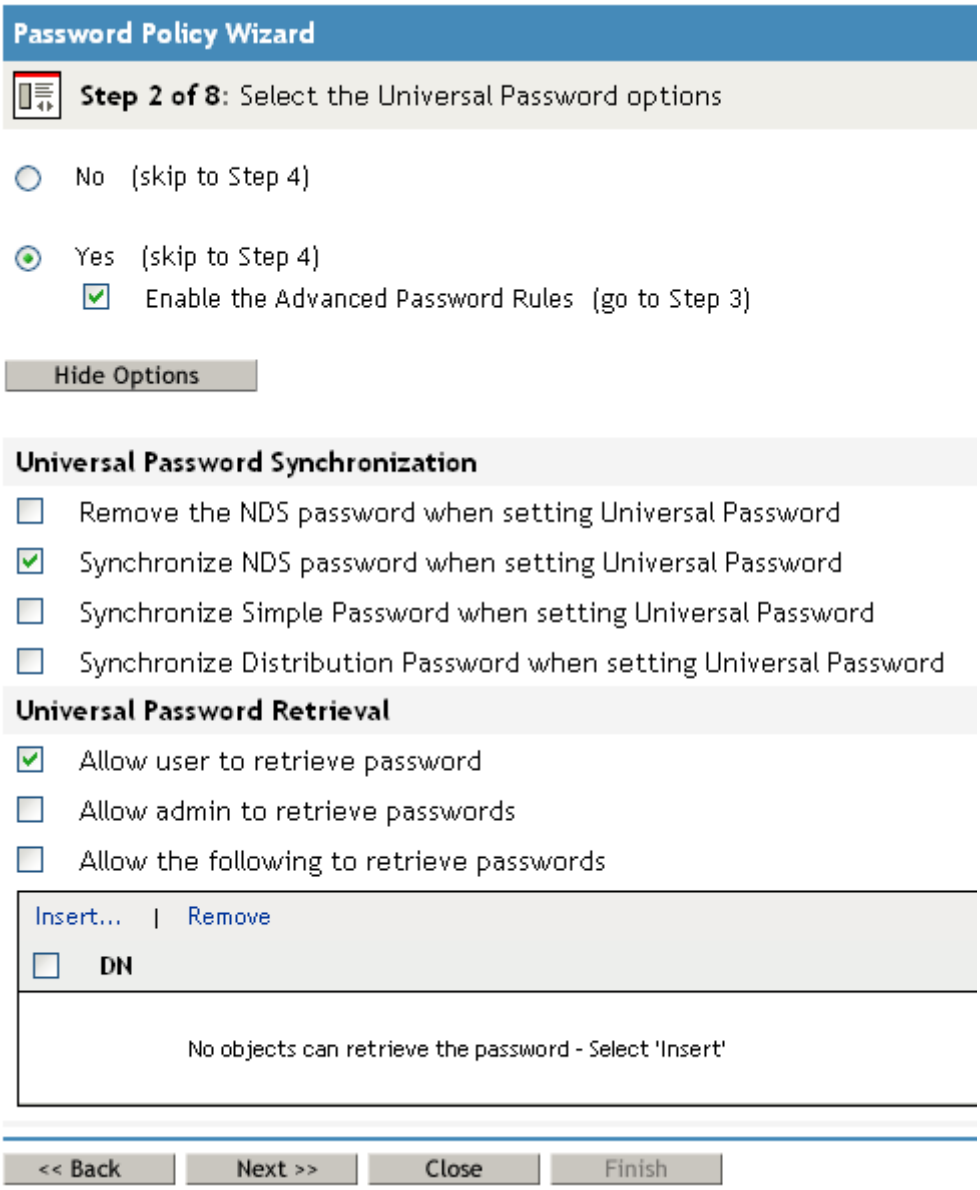
1. In iManager, select **Passwords** > **Password Policies**.
2. Select a policy, then click **Edit**.

3 Browse to and select the object where you want password synchronization to occur.



You can assign the policy to the entire tree structure (by browsing to and selecting the Login Policy object in the Security container), a partition root container, a container, or a specific user. To simplify management, we recommend that you assign password policies as high in the tree as possible.

4 In the password policy, make sure that the following are selected:



- **Enable Universal Password**
- **Synchronize NDS Password when setting Universal Password**
- **Synchronize Distribution Password when setting Universal Password**

  Because Identity Manager retrieves the Distribution password to distribute passwords to connected systems, it's important that this option be selected to allow bidirectional password synchronization.

5 Complete your password policy as desired.

NMAS enforces the Advanced Password Rules in your password policies, if you have the rules enabled. If you don't want password policy rules enforced, deselect **Enable the Advanced Password Rules**.

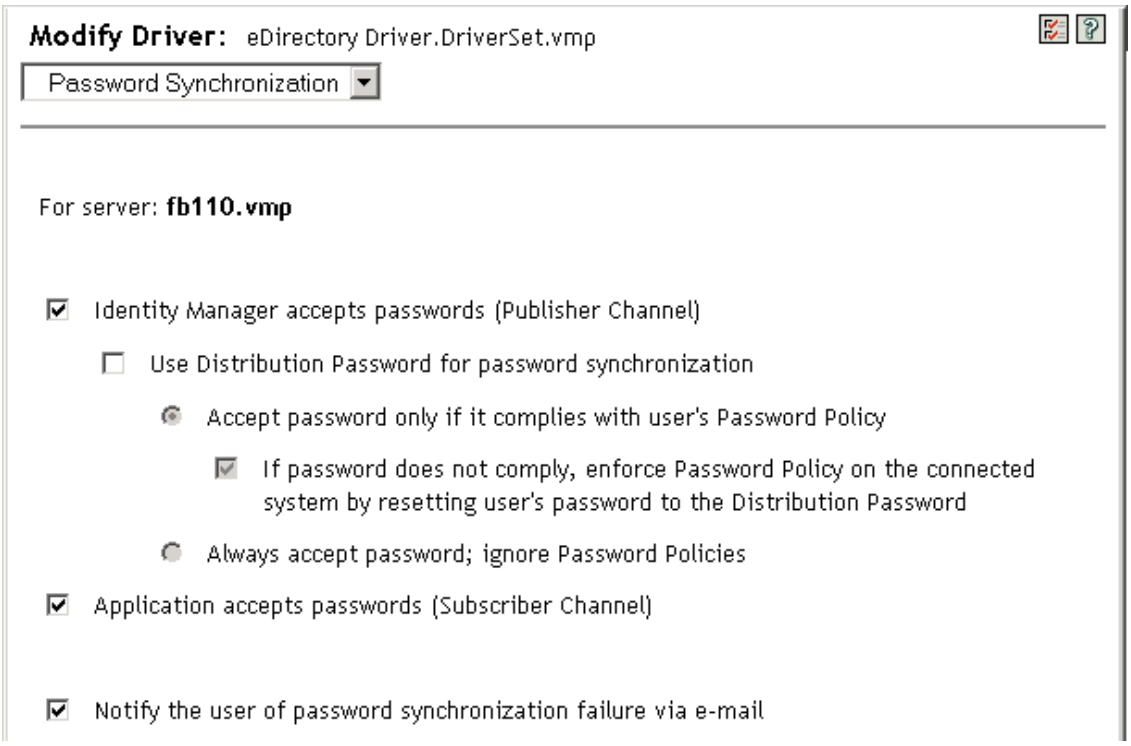
If you are using Advanced Password Rules, make sure they don't conflict with the password policies on any connected systems that are subscribing to passwords.

Password Synchronization Settings

1 In iManager, select **Passwords** > **Password Synchronization**.

2 Search for drivers for the connected systems, then select a driver.

3 Create settings for the driver for the connected system.



Make sure that the following are selected:

- **Identity Manager accepts passwords (Publisher Channel)**

  A message is displayed on the page if the driver manifest does not contain a “password-publish” capability. This is to inform users that passwords cannot be retrieved from the application and can only be published by creating a password in a the driver configuration using a policy.

- **Application accepts passwords (Subscriber Channel)**

  If the connected system does not support accepting passwords, the option is dimmed.

These settings allow for bidirectional password synchronization if it is supported by the connected system.

You can adjust the settings to match your business policies for the authoritative source for passwords. For example, if a connected system should subscribe to passwords but not publish, select only **Application accepts passwords (Subscriber Channel)**.

4 Make sure that **Use Distribution Password for password synchronization** is not selected.

In this scenario, Identity Manager directly updates the Universal password. The Distribution password is still used to distribute passwords to connected systems, but is updated from the Universal password by NMAS instead of by Identity Manager.

5 (Optional) Select the following if desired:

- **Notify the user of password synchronization failure via e-mail**

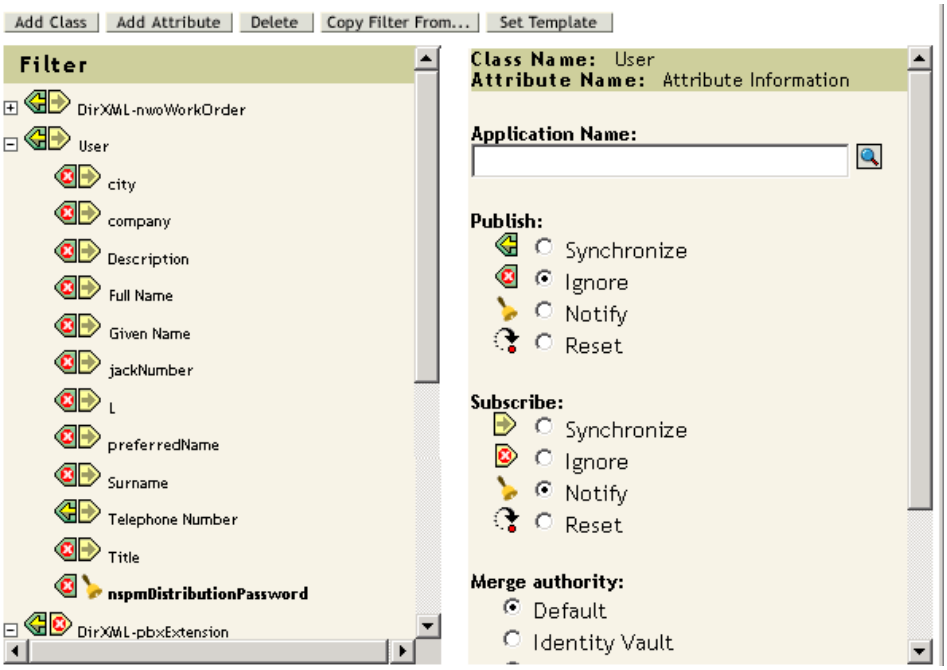
  Keep in mind that e-mail notifications require the Internet EMail Address attribute on the eDirectory User object to be populated.

  E-mail notifications are non-invasive. They do not affect the processing of the XML document that triggered the e-mail. If they fail, they are not retried unless the operation itself is retried. However, debug messages for e-mail notifications are written to the trace file.

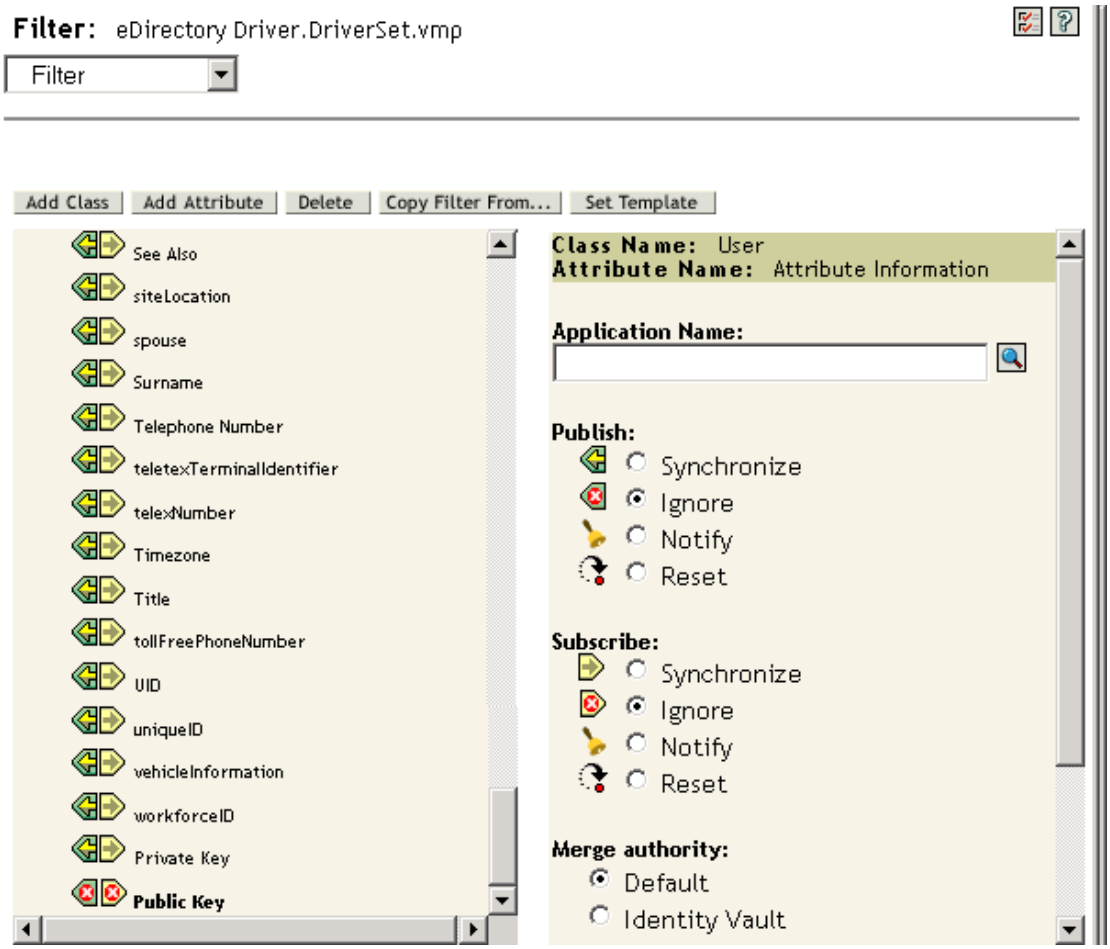
Driver Configuration

1 Set the driver filter correctly for nspmDistributionPassword attribute:

- For the Publisher channel, set the driver filter to **Ignore for the nspmDistributionPassword** attribute for all object classes.
- For the Subscriber channel, set the driver filter to **Notify for the nspmDistribution Password** attribute for all object classes that should subscribe to password changes.



2 For all objects that have **Notify** set for the nspmDistributionPassword attribute, set both the Public Key and Private Key attributes to **Ignore**.



3 To ensure password security, make sure that you control who has rights to Identity Manager objects.

Troubleshooting Scenario 2

- "Flowchart for Scenario 2" on page 52
- "Trouble Logging in to the Identity Vault" on page 53
- "Trouble Logging in to Another Connected System that Subscribes to Passwords" on page 54
- "E-Mail Not Generated on Password Failure" on page 55
- "Error When Using Check the Object Password" on page 55
- "Helpful DSTrace Commands" on page 55

Also see the tips in Chapter 7, "Troubleshooting Password Synchronization," on page 41.

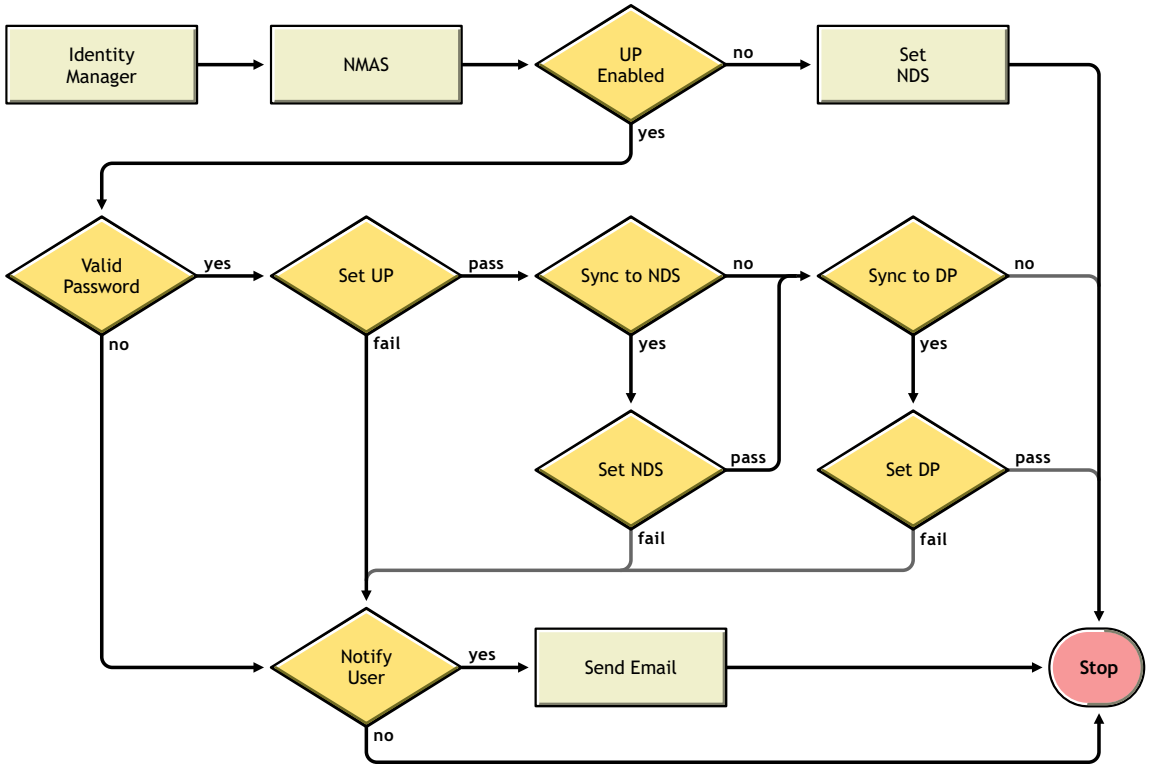
Flowchart for Scenario 2

Figure A-4 illustrates how NMAS handles the password it receives from Identity Manager. The password is synchronized to the Universal password in this scenario. NMAS decides how to handle the password based on the following:

- Whether Universal Password is enabled in the NMAS password policy.

- Whether Advanced Password Rules are enabled that incoming passwords must comply with.
- What the other settings are in the password policy for synchronizing the Universal password with the other passwords.

Figure A-4 *How NMAS Handles the Password It Receives from Identity Manager*



Trouble Logging in to the Identity Vault

- Turn on the **+AUTH**, **+DXML**, and **+DVRS** settings in DSTrace.

Figure A-5 *DSTrace Commands*

```
151.156.165.10 - PTY
TAGS: Show Event Tags      TIME: Show Event Times     ABUF: Agent Buffers
ALOC: Memory Allocation    AREQ: Agent Requests       AUMN: Audit
AUNC: Audit NCPs           AUSK: Audit Skulk          AUTH: Authentication
BASE: Base Set             BEMU: Bindery Emulator     BLNK: Backlinker
CBUF: Client Buffers       CHNG: Change Cache         COLL: Collisions
DRLK: Dist Ref Links       DXML: DirXML Events        DVRS: DirXML Drivers
FRAG: Packet Fragmenter    INIT: Initialization       INSP: Inspector
JNTR: Janitor              LMBR: Limber               LDAP: LDAP
LOCK: Locking              LOST: Lost Entries         MISC: Miscellaneous
MOVE: Move                 NCPE: NCP Engine           PART: Partition
PURG: Purger               RECM: Record Manager       RSLV: Resolve Name
SADV: Srvc Advertising     SCMA: Schema               SCMD: Schema Detail
SPKT: Server Packets       SKLK: Skulker              STRM: Streams
SYNC: Inbound Sync         THRD: Threads              TVEC: Time Vector
VCLN: Virtual Client       WANM: WAN Traffic Mgr      OBIT: Obituaries
SYDL: Sync Detail          CONN: Conn Trace           NMON: Ndsmons
OBJP: Object Producer      DNSV: Domain Name Srv      SSLI: SSL Information
PKII: PKI Information      HTTP: HTTP Stack           LSTK: LDAP Stack
NICI: NICIExt              SSTR: Secret Store         NMAS: NMAS Debugging
BLDT: Backlink Detail      DRLD: DRL Detail           SRCH: DSASearch
SRDT: Search Detail

Server: fb110
NDSTrace:
```

- Verify that the `<password>` or `<modify-password>` elements are being passed to Identity Manager. To verify that they are being passed, watch the trace screen with those options turned on.
- Verify that the password is valid according to the rules of the password policy.
- Check the NMAS password policy configuration and assignment. Try assigning the policy directly to a user to make sure the correct policy is being used.
- On the Password Synchronization page for the driver, make sure that **Identity Manager accepts passwords** is selected.
- In the password policy, make sure that **Synchronize Distribution Password when setting Universal Password** is selected.

Trouble Logging in to Another Connected System that Subscribes to Passwords

This section is for troubleshooting cases where this connected system is publishing passwords to Identity Manager, but another connected system that is subscribing to passwords does not appear to be receiving the changes from this system. Another name for this relationship is a secondary connected system, meaning that it receives passwords from the first connected system through Identity Manager.

- Turn on the **+DXML** and **+DVRS** settings in DSTrace to see Identity Manager rule processing
- Set the Identity Manager trace level for the driver to **3**.
- Make sure the Password Synchronization **Identity Manager Accepts Passwords** option is selected.

- Check the driver filter to make sure the nspmDistributionPassword attribute is set correctly, as explained in Step 1 on page 50.
- Verify that the `<password>` for an Add or `<modify-password>` element is being sent to the connected system. To verify, watch the DSTrace screen or file with the trace options turned on as noted in the first items.
- Verify that the driver configuration includes the Identity Manager script password policies in the correct location and correct order, as described in Appendix B, "Driver Configuration Policies," on page 75.
- Compare the NMAS password policy in the Identity Vault with any password policies enforced by the connected system, to make sure they are compatible.

E-Mail Not Generated on Password Failure

- Turn on the **+DXML** setting in DSTrace to see Identity Manager rule processing.
- Set the Identity Manager trace level for the driver to **3**.
- Verify that the rule to generate e-mail is selected.
- Verify that the Identity Vault object contains the correct user e-mail address in the Internet EMail Address attribute.
- In the Notification Configuration task, make sure the SMTP server and the e-mail template are configured correctly. See Chapter 5, "Configuring E-Mail Notification," on page 25.

Error When Using Check the Object Password

The Check Password Status task in iManager causes the driver to check object password action. If you have problems, review the following:

- If the Check Object Password returns -603, the Identity Vault object does not contain an nspmDistributionPassword attribute. Check the driver filter for the correct settings for the nspmDistributionPassword attributes. Also, make sure that the password policy has **Synchronize Distribution Password when Setting Universal Password** selected.
- If the Check Object Password returns `Not Synchronized`, verify that the driver configuration contains the appropriate Password Synchronization policies.
- Compare the NMAS password policy in the Identity Vault with any password policies enforced by the connected system, to make sure they are compatible.
- Check Object Password operates from the Distribution password. If the Distribution password is not being updated, Check Object Password might not report that passwords are synchronized.
- Keep in mind that for the Identity Manager driver only, Check Password Status is checking the NDS password instead of the Distribution password.

Helpful DSTrace Commands

+DXML: To view Identity Manager rule processing and potential error messages.

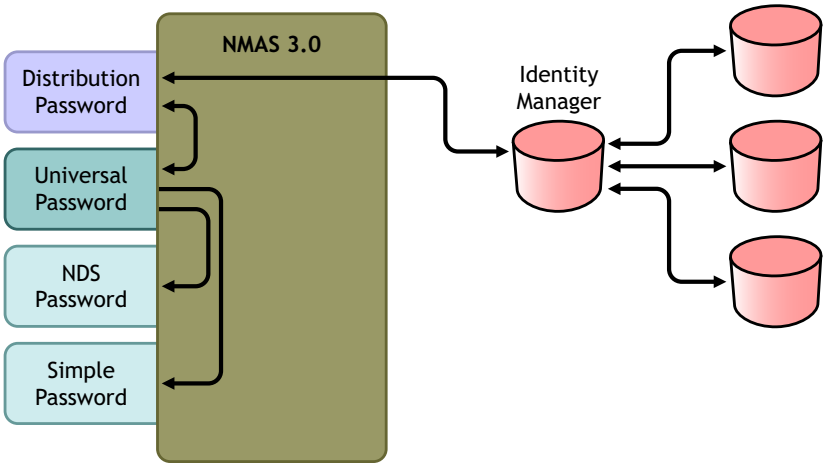
+DVRS: To view Identity Manager driver messages.

+AUTH: To view NDS password modifications.

Scenario 3: Synchronizing an Identity Vault and Connected Systems, with Identity Manager Updating the Distribution Password

In this scenario, Identity Manager directly updates the Distribution password, and allows NMAS to determine how the other Identity Vault passwords are synchronized.

Figure A-6 *Synchronizing an Identity Vault and Connected Systems by Updating the Distribution Password*



The figure in this scenario illustrates the following flow:

1. Passwords come in through Identity Manager.
2. Identity Manager goes through NMAS to directly update the Distribution password
3. Identity Manager also uses the Distribution password to distribute to connected systems that you have specified should accept passwords
4. NMAS synchronizes the Universal password with the Distribution password, and with other passwords according to the password policy settings.

Although multiple connected systems are shown as connecting to Identity Manager in Figure A-6, keep in mind that you individually create the settings for each connected system driver.

The following sections provide information and instructions for this scenario:

- "Advantages and Disadvantages of Scenario 3" on page 57
- "Setting Up Scenario 3" on page 57
- "Troubleshooting Scenario 3" on page 61

Advantages and Disadvantages of Scenario 3

Table A-3 Synchronizing an Identity Vault and Connected Systems by Updating the Distribution Password

Advantages	Disadvantages
Allows synchronization of passwords between the Identity Vault and connected systems. Lets you choose whether or not to enforce password policies for passwords coming from connected systems. You can specify that notification be sent if password synchronization fails. If you are enforcing password policies, you can choose to reset a password on the connected system to the Distribution password if the password doesn't comply.	

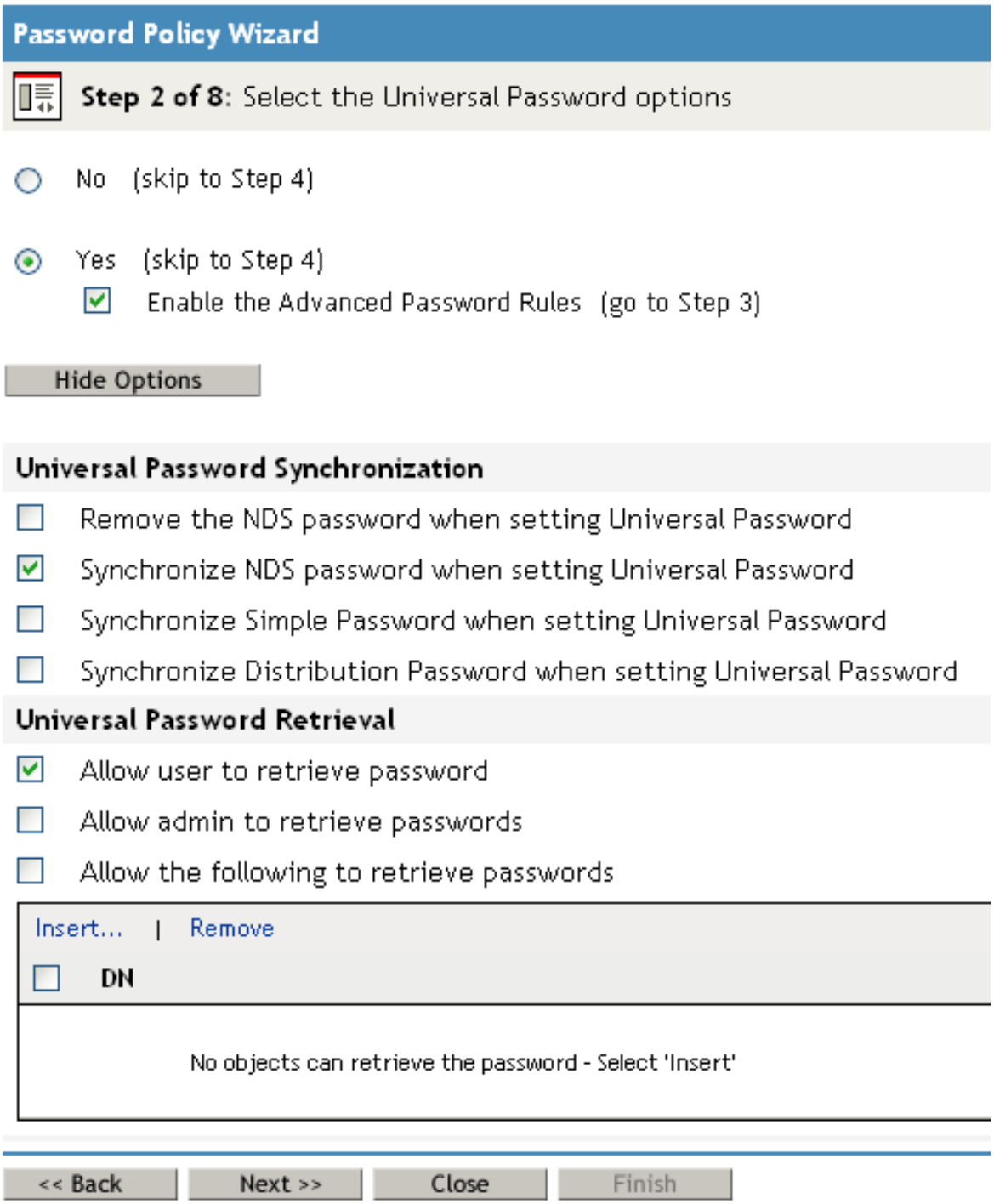
Setting Up Scenario 3

Use the information in the following sections to help complete the tasks in the Password Management Checklist.

- "Password Policy Configuration" on page 57
- "Password Synchronization Settings" on page 59
- "Driver Configuration" on page 60

Password Policy Configuration

1. In iManager, select **Passwords** > **Password Policies**.
2. Make sure a password policy is assigned to the parts of the Identity Vault tree that you want to have this kind of password synchronization. You can assign it to the entire tree structure, a partition root container, a container, or a specific user. To simplify management, we recommend that you assign password policies as high in the tree as possible.
3. In the password policy, make sure the following are selected:



- **Enable Universal Password**
- **Synchronize NDS Password when setting Universal Password**

- **Synchronize Distribution Password when setting Universal Password**

  Because Identity Manager retrieves the Distribution password to distribute passwords to connected systems, it's important that this option be selected to allow bidirectional password synchronization.

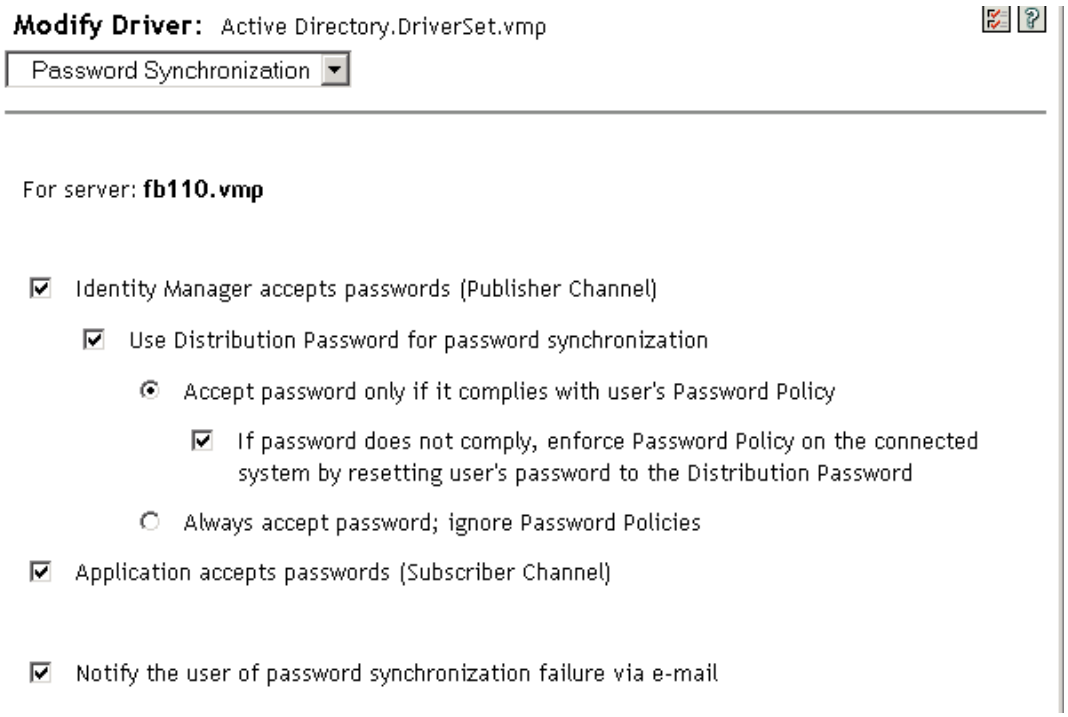
4 If you are using Advanced Password Rules, make sure that they don't conflict with the password policies on any connected systems that are subscribing to passwords.

Password Synchronization Settings

1 In iManager, select **Passwords** > **Password Synchronization**.

2 Search for drivers for the connected systems, then select a driver.

3 Create settings for the driver for the connected system.



Make sure that the following are selected:

- **Identity Manager accepts passwords (Publisher Channel)**
- **Use Distribution Password for password synchronization**

  A message is displayed on the page if the driver manifest does not contain a “password-publish” capability. This is to inform users that passwords cannot be retrieved from the application and can only be published by creating a password in the driver configuration using a policy.
- **Application accepts passwords (Subscriber Channel)**

These settings allow for bidirectional password synchronization if it is supported by the connected system.

You can adjust the settings to match your business policies for the authoritative source for passwords. For example, if a connected system should subscribe to passwords but not publish, select only **Application accepts passwords (Subscriber Channel)**.

4 Specify whether you want NMAS password policies to be enforced or ignored, using the options under **Use Distribution Password for password synchronization**.

5 (Conditional) If you have specified that you want password policies to be enforced, also specify whether you want Identity Manager to reset the connected system password if it does not comply.

6 (Optional) Select the following if desired:

- **Notify the user of password synchronization failure via e-mail**

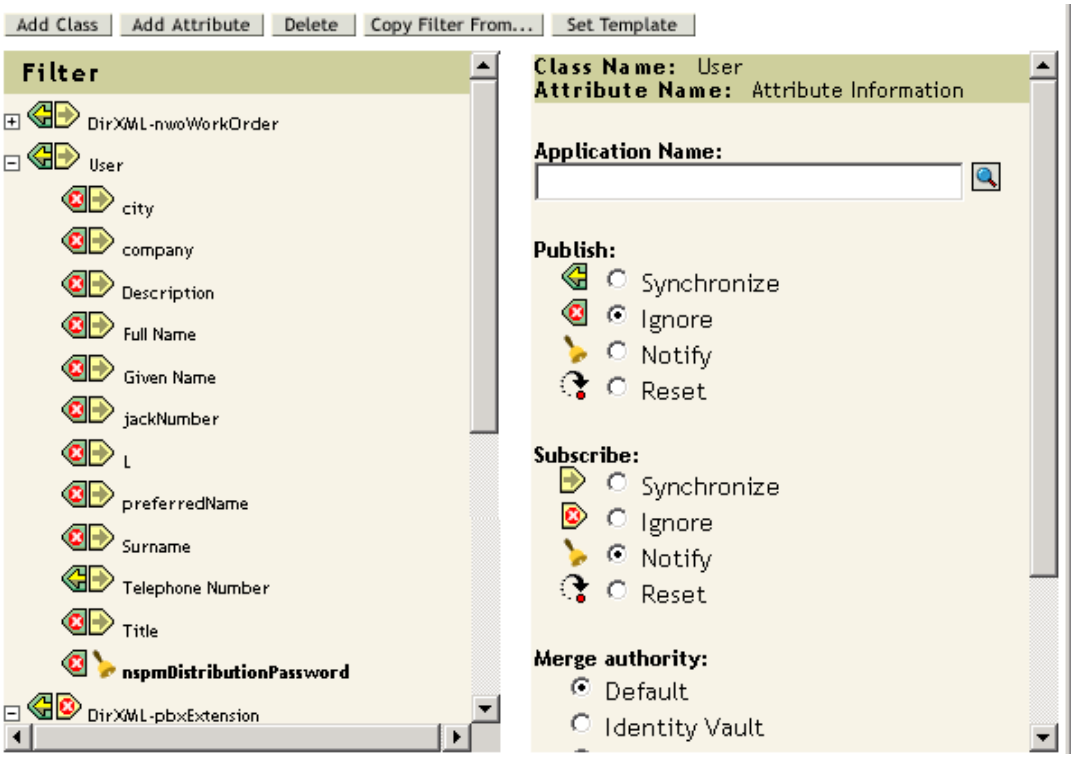
  Keep in mind that e-mail notifications require the Internet EMail Address attribute on the eDirectory user object to be populated.

  E-mail notifications are noninvasive. They do not affect the processing of the XML document that triggered the email. If they fail, they are not retried unless the operation itself is retried. However, debug messages for e-mail notifications are written to the trace file.

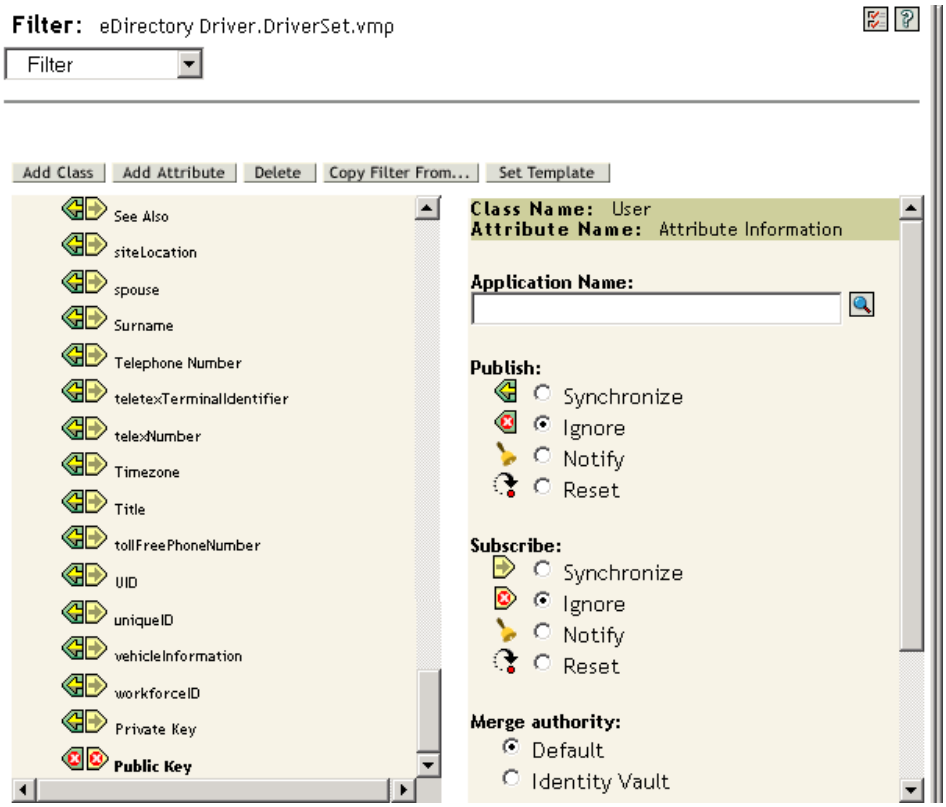
Driver Configuration

1 Set the filter correctly for nspmDistributionPassword attribute:

- For the Publisher channel, set the driver filter to **Ignore** for the nspmDistributionPassword attribute for all object classes.
- For the Subscriber channel, set the driver filter to **Notify** for the nspmDistribution Password attribute for all object classes that should subscribe to password changes.



2 For all objects that have **Notify** set for the nspmDistributionPassword attribute, set both the Public Key and Private Key attributes in the driver filter to **Ignore**.



3 To ensure password security, make sure that you control who has rights to Identity Manager objects.

Troubleshooting Scenario 3

- "Flowchart for Scenario 3" on page 62
- "Trouble Logging In to eDirectory" on page 62
- "Trouble Logging in to Another Connected System that Subscribes to Passwords" on page 69
- "E-Mail Not Generated on Password Failure" on page 55
- "Error When Using Check Password Status" on page 65
- "Helpful DSTrace Commands" on page 55

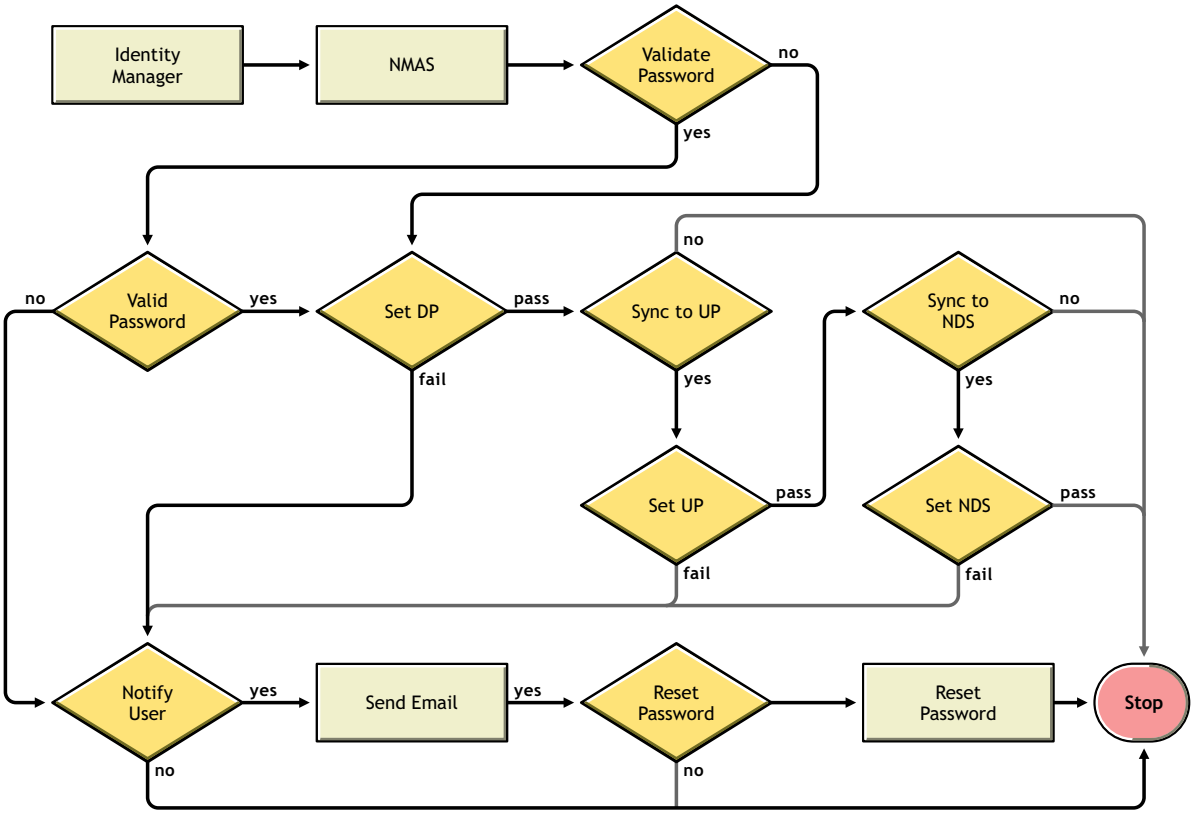
Also see the tips in Chapter 7, "Troubleshooting Password Synchronization," on page 41.

Flowchart for Scenario 3

Figure A-7 illustrates how NMAS handles the password it receives from Identity Manager. The password is synchronized to the Distribution password in this scenario, and NMAS decides the following:

- How to handle the password based on whether you have specified that incoming passwords should be validated against password policy rules (if Universal Password and Advanced Password Rules are enabled).
- What the other settings are in the password policy for synchronizing the Universal password with the other passwords.

Figure A-7 *Password from Identity Manager is Synchronized to the Distribution Password*



Trouble Logging In to eDirectory

- Turn on the **+AUTH**, **+DXML**, and **+DVRS** settings in DSTrace

Figure A-8 *DSTrace commands*

```
151.156.165.10 - PTY
TAGS: Show Event Tags      TIME: Show Event Times     ABUF: Agent Buffers
ALOC: Memory Allocation    AREQ: Agent Requests       AUMN: Audit
AUNC: Audit NCPs           AUSK: Audit Skulk          AUTH: Authentication
BASE: Base Set             BEMU: Bindery Emulator     BLNK: Backlinker
CBUF: Client Buffers       CHNG: Change Cache         COLL: Collisions
DRLK: Dist Ref Links       DXML: DirXML Events        DVRS: DirXML Drivers
FRAG: Packet Fragmenter    INIT: Initialization       INSP: Inspector
JNTR: Janitor              LMBR: Limber               LDAP: LDAP
LOCK: Locking              LOST: Lost Entries         MISC: Miscellaneous
MOVE: Move                 NCPE: NCP Engine           PART: Partition
PURG: Purger               RECM: Record Manager       RSLV: Resolve Name
SADV: Srvc Advertising     SCMA: Schema               SCMD: Schema Detail
SPKT: Server Packets       SKLK: Skulker              STRM: Streams
SYNC: Inbound Sync         THRD: Threads              TVEC: Time Vector
VCLN: Virtual Client       WANM: WAN Traffic Mgr      OBIT: Obituaries
SYDL: Sync Detail          CONN: Conn Trace           NMON: Ndsmons
OBJP: Object Producer      DNSV: Domain Name Srv      SSLI: SSL Information
PKII: PKI Information      HTTP: HTTP Stack           LSTK: LDAP Stack
NICI: NICIExt              SSTR: Secret Store         NMAS: NMAS Debugging
BLDT: Backlink Detail      DRLD: DRL Detail           SRCH: DSASearch
SRDT: Search Detail

Server: fb110
NDSTrace:
```

- Verify that the `<password>` or `<modify-password>` elements are being passed to Identity Manager. To verify, watch the DSTrace screen or file with the trace options turned on as noted in the first item.
- Verify that the password is valid according to the rules of the NMAS password policy.
- Check the NMAS password policy configuration and assignment. Try assigning the policy directly to the user to make sure the correct policy is being used.
- On the Password Synchronization page for the driver, make sure that **Identity Manager accepts passwords (Publisher Channel)** is selected.
- In the NMAS password policy, make sure that **Synchronize Distribution Password when setting Universal Password** is selected.
- In the NMAS password policy, make sure that **Synchronize NDS Password when setting Universal Password** is selected, if this is desired.
- If users are logging in through the Novell Client or ConsoleOne, check the version. Legacy Novell Clients and ConsoleOne might not be able to log in to the Identity Vault if the Universal password is not synchronized with the NDS password.

  Versions of the Novell Client and ConsoleOne that are aware of the Universal password are available. See the *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/b1j4qnr9.html).
- Some legacy utilities authenticate by using the NDS password, and also cannot log in to the Identity Vault if the Universal password is not synchronized with the NDS password. If you don't want to use the NDS password for most users, but you have administrator or help desk users who need to authenticate with legacy utilities, try using a different password policy for help desk users so you can specify different Universal password synchronization options for them.

Trouble Logging In to Another Connected System that Subscribes to Passwords

This section is for troubleshooting situations where this connected system is publishing passwords to Identity Manager, but another connected system that is subscribing to passwords does not appear to be receiving the changes from this system. Another name for this relationship is a secondary connected system, meaning that it receives passwords from the first connected system through Identity Manager.

- Turn on the **+DXML** and **+DVRS** settings in DSTrace to see Identity Manager rule processing and potential errors
- Set the Identity Manager trace level for the driver to **3**.
- Make sure that the **Identity Manager accepts passwords (Publisher Channel)** option is selected in the Password Synchronization page.
- In the password policy, make sure that **Synchronize Distribution Password when setting Universal Password** is not selected.

  Identity Manager uses the Distribution password to synchronize passwords to connected systems. The Universal password must be synchronized with the Distribution password for this synchronization method.
- Check the driver filter for the nspmDistributionPassword attribute.
- Verify that the `<password>` element for an Add or a `<modify-password>` element has been converted to Add and Modify attribute operations for the nspmDistributionPassword. To verify, watch the DSTrace screen or file with the options turned on as noted in the first item.
- Verify that the driver configuration includes the Identity Manager script password policies in the correct location and correct order, as described in Appendix B, “Driver Configuration Policies,” on page 75.
- Compare the password policy in the Identity Vault with any password policies enforced by the connected system, to make sure they are compatible.

E-Mail Not Generated on Password Failure

- Turn on the **+DXML** setting in DSTrace to see Identity Manager rule processing
- Set the Identity Manager trace level for the driver to **3**.
- Verify that the rule to generate e-mail is selected.
- Verify that the Identity Vault object contains the correct value in the Internet EMail Address attribute.
- In the Notification Configuration task, make sure the SMTP server and the e-mail template are configured. See Chapter 5, “Configuring E-Mail Notification,” on page 25.

E-mail notifications are non-invasive. They do not affect the processing of the XML document that triggered the e-mail. If they fail, they are not retried unless the operation itself is retried. Debug messages for e-mail notifications are written to the trace file.

Error When Using Check Password Status

The Check Password Status task in iManager causes the driver to perform a check object password action.

- Make sure the connected system supports checking passwords. See Chapter 3, "Connected System Support for Password Synchronization," on page 15.

  If the driver manifest does not indicate that the connected system supports password-check capability, this operation is not available through iManager.
- If the Check Object Password returns -603, the Identity Vault object does not contain an nspmDistributionPassword attribute. Check the driver filter, and the **Synchronize Universal to Distribution** option within the password policy.
- If the Check Object Password returns `Not Synchronized`, verify that the driver configuration contains the appropriate Identity Manager Password Synchronization policies.
- Compare the password policy in the Identity Vault with any password policies enforced by the connected system, to make sure they are compatible.
- **Check Object Password** checks the Distribution password. If the Distribution password is not being updated, **Check Object Password** might not report that passwords are synchronized
- Keep in mind that for the Identity Vault, **Check Password Status** checks the NDS password instead of the Universal password. This means that if the user's password policy does not specify to synchronize the NDS password with the Universal password, the passwords are always reported as being not synchronized. In fact, the Distribution password and the password on the connected system might be in sync, but Check Password Status won't be accurate unless both the NDS password and the Distribution password are synchronized with the Universal password.

Helpful DSTrace Commands

+DXML: To view Identity Manager rule processing and potential error message.

+DVRS: To view Identity Manager driver messages.

+AUTH: To view NDS password modifications.

Scenario 4: Tunneling

Identity Manager enables you to synchronize passwords among connected systems while keeping the Identity Vault password separate. This is referred to as "tunneling."

In this scenario, Identity Manager directly updates the Distribution password. This scenario is almost the same as "Scenario 3: Synchronizing an Identity Vault and Connected Systems, with Identity Manager Updating the Distribution Password" on page 56. The difference is that you make sure the Universal password and the Distribution password are not being synchronized. You do this either by not using NMAS password policies, or by using password policies with the option disabled for **Synchronize Distribution Password when setting Universal Password**.

Figure A-9 Tunneling, with Identity Manager Updating the Distribution Password

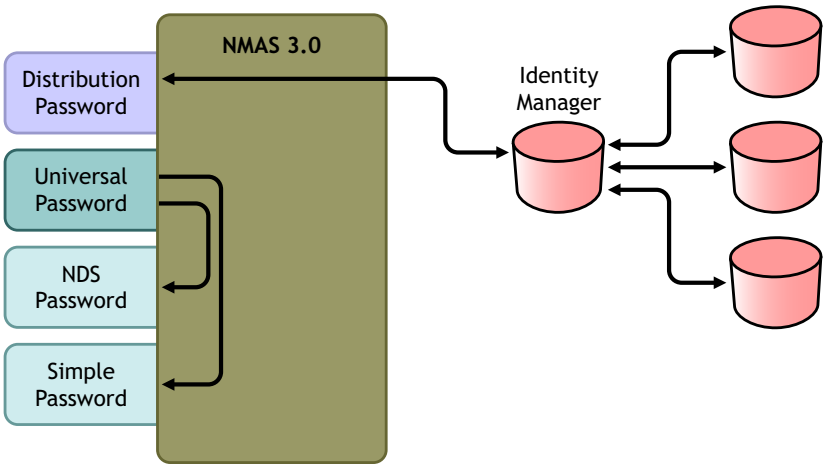


Figure A-9 illustrates the following flow:

1. Passwords come in through Identity Manager.
2. Identity Manager goes through NMAS to directly update the Distribution password.
3. Identity Manager also uses the Distribution password to distribute passwords to connected systems that you have specified should accept passwords.

The key to this scenario is that in the NMAS password policy, **Synchronize Universal Password with Distribution Password** is disabled. Because the Distribution password is not synchronized with the Universal password, Identity Manager synchronizes passwords among connected systems without affecting passwords in the Identity Vault.

Although multiple connected systems are shown as connecting to Identity Manager in this figure, keep in mind that you individually create the settings for each connected system driver.

The following sections provide information and instructions for this scenario:

- "Advantages and Disadvantages of Scenario 4" on page 67
- "Setting Up Scenario 4" on page 67
- "Troubleshooting Scenario 4" on page 69

Advantages and Disadvantages of Scenario 4

Table A-4 *Tunneling*

Advantages	Disadvantages
Allows synchronization of passwords among connected systems, while keeping the Identity Vault password separate. The password policy does not need to have Universal Password enabled, but the environment must support Universal Password. Supports the Check Password Status task in iManager, if the connected system supports it. You can specify that notification be sent if password synchronization fails. You can reset a connected system password that does not comply with password policy. If Universal Password and Advanced Password Rules are enabled, password policies are enforced if you specify that they should be enforced, and passwords on connected systems can be reset.	If Universal Password or Advanced Password Rules are not enabled, password policies are not enforced, and passwords on connected systems cannot be reset.

Setting Up Scenario 4

Use the information in the following sections to help complete the tasks in the Password Management Checklist.

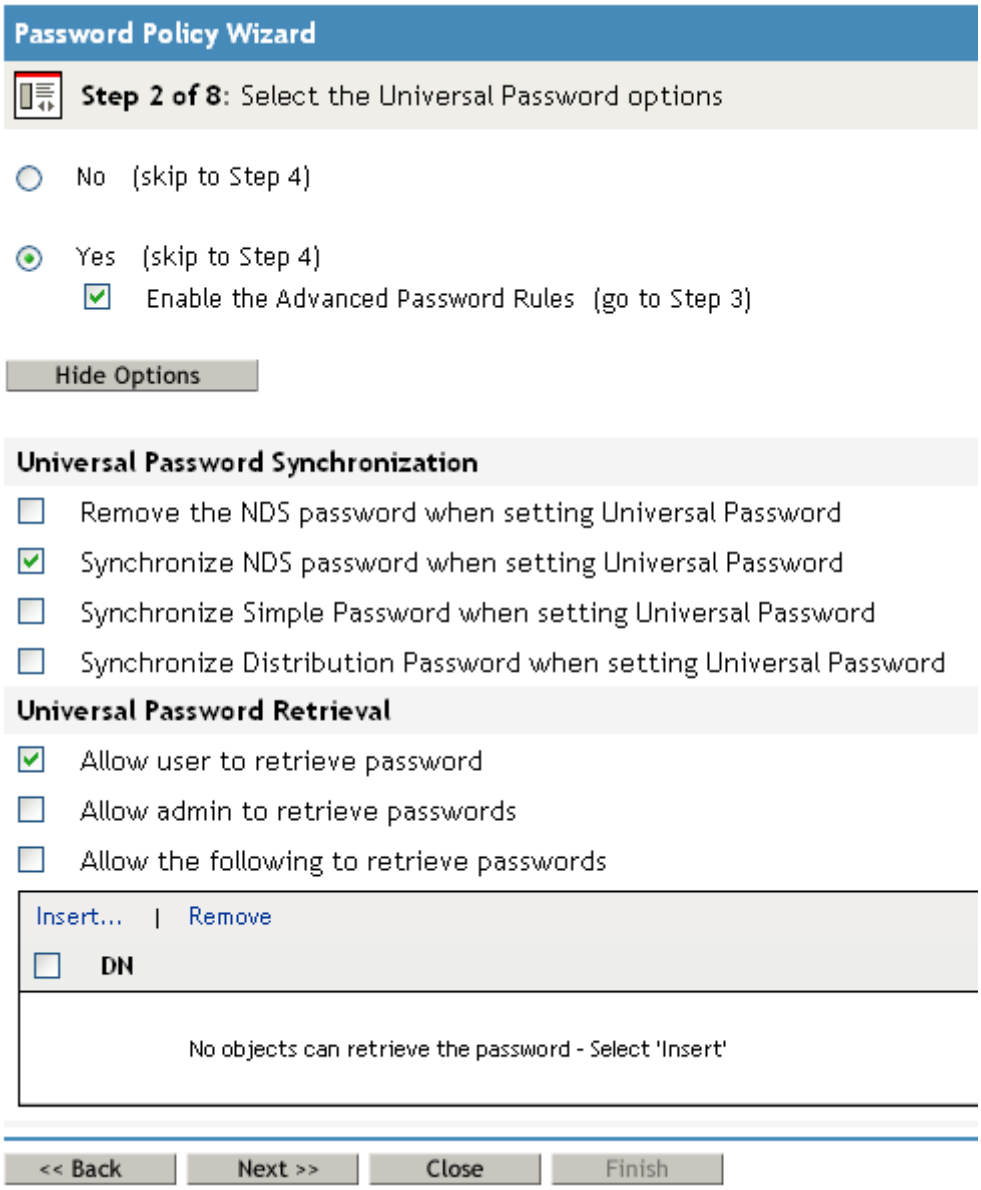
- "Password Policy Configuration" on page 67
- "Password Synchronization Settings" on page 68
- "Driver Configuration" on page 68

Password Policy Configuration

Review your password policy to confirm the following:

- Make sure that **Synchronize Distribution Password when setting Universal Password** is not selected.

  This is the key to tunneling passwords without the Identity Vault password being affected. By not synchronizing the Universal password with the Distribution password, you keep the Distribution password separate, for use only by Identity Manager for connected systems. Identity Manager acts as a conduit, distributing passwords to and from other connected systems, without affecting the Identity Vault password.



- Complete the other password policy settings as desired.

  The other password settings in the password policy are optional.

Password Synchronization Settings

Use the same settings as Password Synchronization Settings in "Scenario 3: Synchronizing an Identity Vault and Connected Systems, with Identity Manager Updating the Distribution Password" on page 56.

Driver Configuration

Use the same settings as Driver Configuration in "Scenario 3: Synchronizing an Identity Vault and Connected Systems, with Identity Manager Updating the Distribution Password" on page 56.

Troubleshooting Scenario 4

If password synchronization is set up for tunneling, the Distribution password is different than the Universal password and the NDS password.

- "Trouble Logging in to Another Connected System that Subscribes to Passwords" on page 54
- "E-Mail Not Generated on Password Failure" on page 55
- "Error When Using Check Password Status" on page 65
- "Helpful DSTrace Commands" on page 65

See also the tips in Chapter 7, "Troubleshooting Password Synchronization," on page 41.

Trouble Logging in to Another Connected System that Subscribes to Passwords

This section is for troubleshooting situations where this connected system is publishing passwords to Identity Manager, but another connected system that is subscribing to passwords does not appear to be receiving the changes from this system. Another name for this relationship is a secondary connected system, meaning that it receives passwords from the first connected system through Identity Manager.

- Turn on the **+DXML** and **+DVRS** settings in DSTrace to see Identity Manager rule processing and potential errors.
- Set the Identity Manager trace level for the driver to **3**.
- Make sure that the **Identity Manager accepts passwords (Publisher Channel)** option is selected on the Password Synchronization page.
- In the password policy, make sure that **Synchronize Distribution Password when setting Universal Password** is not selected.

  Identity Manager uses the Distribution password to synchronize passwords to connected systems. The Universal password must be synchronized with the Distribution password for this synchronization method.
- Make sure the driver filter has the correct settings for the nspmDistributionPassword attribute.
- Verify that the `<password>` element for an Add and a `<modify-password>` element have been converted to Add and Modify attribute operations for the nspmDistributionPassword. To verify, watch the DSTrace screen or file with the trace options turned on as noted in the first item.
- Verify that the driver configuration includes the Identity Manager script password policies in the correct location and correct order, as described in Appendix B, "Driver Configuration Policies," on page 75.
- Compare the password policy in the Identity Vault with any password policies enforced by the connected system, to make sure they are compatible.

E-Mails Not Generated on Password Failure

- Turn on the **+DXML** setting in DSTrace to see Identity Manager rule processing.
- Set the Identity Manager trace level for driver to **3**.

- Verify that the rule to generate e-mail is selected.
- Verify that the Identity Vault object contains the correct value in the Internet EMail Address attribute.
- In the Notification Configuration task, check the SMTP server and the e-mail template. See Chapter 5, "Configuring E-Mail Notification," on page 25.

E-mail notifications are non-invasive. They do not affect the processing of the XML document that triggered the e-mail. If they fail, they are not retried unless the operation itself is retried. Debug messages for e-mail notifications are written to the trace file.

Error When Using Check Password Status

The Check Password Status task in iManager causes the driver to be perform a Check Object Password action.

- Make sure that the connected system supports checking passwords. See Chapter 3, "Connected System Support for Password Synchronization," on page 15.

  This operation is not available through iManager if the driver manifest does not indicate that the connected system supports password-check capability.
- If the Check Object Password action returns -603, the Identity Vault object does not contain an nspmDistributionPassword attribute. Check the Identity Manager attribute filter, and the **Synchronize Universal to Distribution** option within the password policy.
- If the Check Object Password action returns `Not Synchronized`, verify that the driver configuration contains the appropriate Identity Manager password synchronization policies.
- Compare the password policy in the Identity Vault with any password policies enforced by the connected system, to make sure they are compatible.
- The Check Object Password action checks the Distribution password. If the Distribution password is not being updated, Check Object Password might not report that passwords are synchronized

Helpful DSTrace Commands

+DXML: To view Identity Manager rule processing and potential error messages.

+DVRS: To view Identity Manager driver messages.

+AUTH: To view NDS password modifications.

+DCLN: To view NDS DCLient messages.

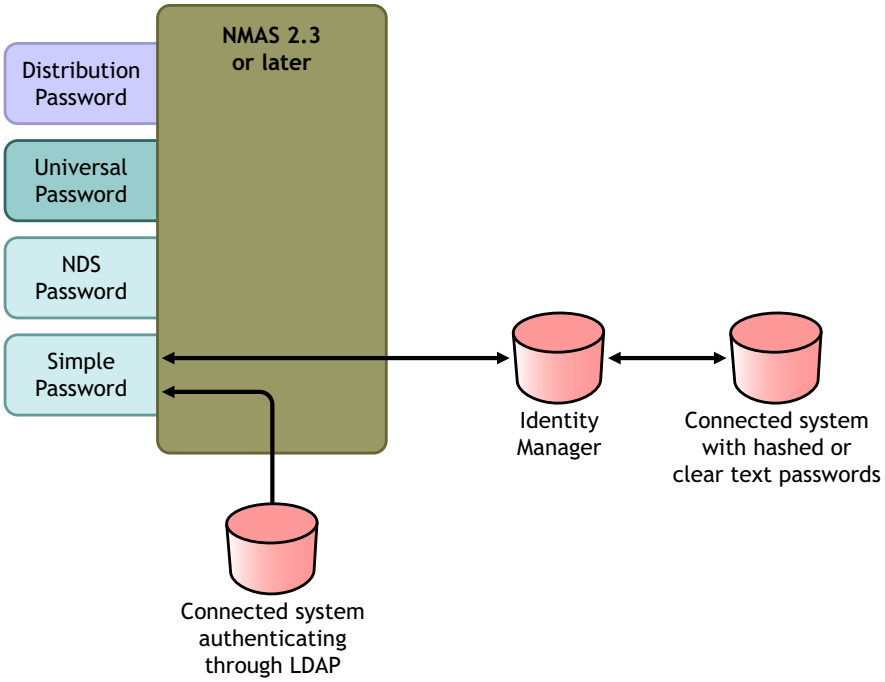
Scenario 5: Synchronizing Application Passwords to the Simple Password

This scenario is a specialized use of password synchronization features. Using Identity Manager and NMAS, you can take a password from a connected system and synchronize it directly to the Identity Vault Simple Password. If the connected system provides only hashed passwords, you can synchronize them to the Simple Password without reversing the hash. Then, other applications can

authenticate to the Identity Vault by using the same clear text or hashed password through LDAP or the Novell Client, with NMAS components configured to use the Simple Password as the login method.

NOTE: In compliance with RFC 2256, the LDAP interface of eDirectory only allows binds to occur with passwords up to 128 characters in length. Also, passwords can only be set to have up to 128 characters when set through LDAP.

Figure A-10 *Synchronizing to the NDS Password*



If the password in the connected system is in clear text, it can be published as it is from the connected system into the Identity Vault Simple Password store.

If the connected system provides only hashed passwords (MD5, SHA, SHA1,or UNIX Crypt are supported), you must publish them to the Simple Password with an indication of the kind of hash, such as {MD5}.

For another application to authenticate with the same password, you need to customize the other application to take the user's password and authenticate to the Simple Password using LDAP.

NMAS compares the password value from the application with the value in the Simple Password. If the password stored in the Simple Password is a hash value, NMAS first uses the password value from the application to create the correct type of hash value, before comparing. If the password from the application and the Simple Password are the same, NMAS authenticates the user.

In this scenario, Universal Password cannot be used.

The following sections provide information and instructions for this scenario:

- "Advantages and Disadvantages of Scenario 5" on page 72
- "Setting Up Scenario 5" on page 72

Advantages and Disadvantages of Scenario 5

Table A-5 Synchronizing to the NDS Password

Advantages	Disadvantages
◆ Lets you update the Simple Password directly. ◆ Lets you synchronize a hashed password and use it to authenticate for more than one application, without reversing the hash.	◆ This scenario does not allow the use of Universal Password. ◆ Forgotten Password and Password Self-Service features can still be used to the extent they are supported for the NDS password, but they do not work for the Simple Password. ◆ Because the Set Universal Password task is dependent on Universal Password, the administrator cannot set a user's password in the Identity Vault by using that task.

Setting Up Scenario 5

Use the information in the following sections to help complete the tasks in the Password Management Checklist.

- "Password Policy Configuration" on page 72
- "Password Synchronization Settings" on page 72
- "Driver Configuration" on page 72

Password Policy Configuration

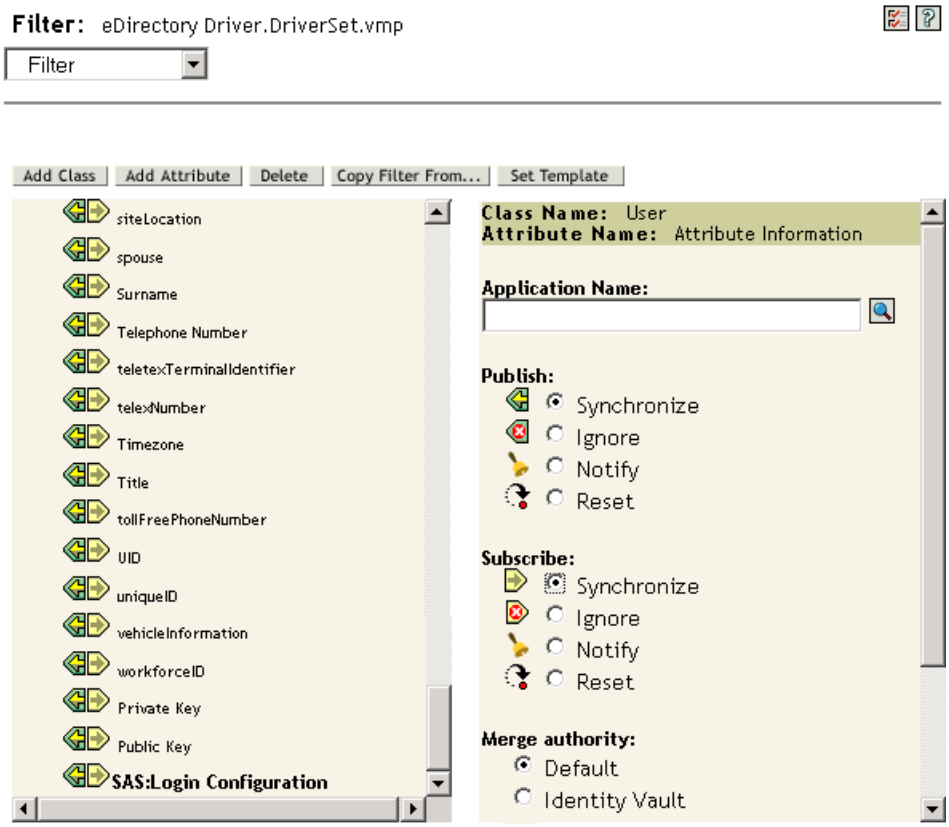
No password policy is required for users for this scenario. Universal Password cannot be used.

Password Synchronization Settings

For this scenario, you use Identity Manager Script to directly modify the SAS:Login Configuration attribute. This means that the Password Synchronization global configuration values (GCVs), which are set by using the Password Synchronization page in iManager, have no effect.

Driver Configuration

1. Make sure that the SAS:Login Configuration attribute in the filter has the setting of **Synchronize** for both Publisher and Subscriber channels.



2 Configure the driver policies to publish the password from the connected system.

3 For hashed passwords, configure the driver policies to prepend the type of hash (if it is not already provided by the application):

- {MD5}*hashed_password*

  This password is Base64 encoded.

- {SHA}*hashed_password*

  This password is Base64 encoded.

- {CRYPT}*hashed_password*

Clear text passwords and UNIX Crypt password hashes are not Base64 encoded.

4 To place the password into the Simple Password, configure the driver policies to modify the SAS:Login Configuration attribute.

The following example illustrates how to use a modify-attr element within a modify operation to change the Simple Password to an MD5 hashed password:

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
        <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
    </add-value>
</modify-attr>
```

For clear text passwords, follow this example.

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
        <value>clearpwd</value>
    </add-value>
</modify-attr>
```

For add operations, the add-attr element would contain one of the following:

```
<add-attr attr-name="SAS:Login Configuration>
    <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
</add-attr>
```

or

```
<add-attr attr-name="SAS:Login Configuration>
    <value>clearpwd</value>
</add-attr>
```

B Driver Configuration Policies

Identity Manager policies on the Publisher and Subscriber channels for each driver govern the password flow. These policies are included in the driver configurations in Identity Manager.

- "Policies Required in the Publisher Command Transformation Set" on page 75
- "Policies Required in the Publisher Input Transformation Policy Set" on page 77
- "Policies Required in the Subscriber Command Transformation Policy Set" on page 77
- "Policies Required in the Subscriber Output Transformation Policy Set" on page 78

Policies Required in the Publisher Command Transformation Set

The policies listed in the Password Synchronization Policy Name column must be present in the order listed. Also, they must be the last policies in the Publisher Command Transformation policy set.

Table B-1 Policies Required in the Publisher Command Transformation Set

Location in the Driver Configuration	Password Synchronization Policy Name	What the Policy Does
Publisher Command Transformation	Password(Pub)-Default Password Policy	Adds a default password to an Add object if the Add object does not already contain a password. This policy and the Password(Sub)-Default Password Policy are the only policies that you can modify or remove. For password synchronization functionality to work properly, the other policies should be used without changes.
	Password(Pub)-Check Password GCV	Checks the GCV to determine whether you have specified that Identity Manager accepts passwords from this connected system. If not, it strips out all password elements. The name of the GCV is enable-password-publish, and the display name is **Identity Manager accepts passwords from application**.
	Password(Pub)-Publish Distribution Password	Transforms the `<password>` element to the form that allows it to update the Universal password. This policy references the following GCVs: ◆ publish-password-to-dp ◆ enforce-password-policy
	Password(Pub)-Publish NDS Password	Allows the `<password>` element to go through if you have specified that the NDS password should be updated. If not, it strips out the `<password>` element. This policy references the GCV named publish-password-to-nds.
	Password(Pub)-Add Password Payload	Puts in payload data that is passed around in the engine for purposes of e-mail notification.

Policies Required in the Publisher Input Transformation Policy Set

We recommend that the Password(Pub)-Sub Email Notifications policy be listed last if there are multiple policies in the Input Transformation.

Table B-2 *Policies Required in the Publisher Input Transformation Policy Set*

Location in the Driver Configuration	Password Synchronization Policy Name	What the Policy Does
Publisher Input Transformation	Password(Pub)-Sub Email Notifications	If the password payload information comes through, and the status shows a problem, it sends e-mail to the user. It uses the e-mail address indicated in the Internet EMail Address attribute in eDirectory. This policy references the GCV named notify-user-on-password-dist-failure to determine whether to send notification e-mails.

Policies Required in the Subscriber Command Transformation Policy Set

The policies listed in the Password Synchronization Policy Name column must be present in the order listed. Also, they must be the last policies in the Subscriber Command Transformation policy set.

Table B-3 Policies Required in the Subscriber Command Transformation Policy Set

Location in the Driver Configuration	Password Synchronization Policy Name	What the Policy Does
Subscriber Command Transformation	Password(Sub)-Transform Distribution Password	Transforms the Universal password to a `<password>` element.
	Password(Sub)-Default Password Policy	Adds a default password to an Add object if the Add object does not already contain a password. This policy and the Password(Pub)-Default Password Policy are the only policies that you can modify or remove. For password synchronization functionality to work properly, the other policies should be used without changes,.
	Password(Sub)-Check Password GCV	Checks the GCV to determine whether you have specified that the connected system accepts passwords. If not, it strips out all password elements. The name of the GCV is enable-password-subscribe, and the display name is **Application accepts passwords from Identity Manager data store**.
	Password(Sub)-Add Password Payload	Puts in password payload data that is passed around in the engine for purposes of e-mail notification.

Policies Required in the Subscriber Output Transformation Policy Set

We recommend that the Password(Sub)-Pub Email Notifications policy be listed last if there are multiple policies in the Output Transformation.

Table B-4 Policies Required in the Subscriber Output Transformation Policy Set

Location in the Driver Configuration	Password Synchronization Policy Name	What the Policy Does
Subscriber Output Transformation	Password(Sub)-Pub Email Notifications	If the password payload information comes through, and the status shows a problem, it sendsan e-mail to the user. This policy references the GCV named notify-user-on-password-dist-failure to determine whether to send notification e-mail.