

LOCKING DOWN
IDENTITY AND
PASSWORD
MANAGEMENT
WITH THE NEW
DIRXML:
NSURE IDENTITY
MANAGER 2.0

BY LINDA KENNARD

PHOTOGRAPH BY HOLLY LINDEM



As a network administrator, you probably have experienced firsthand the difficulty of managing and synchronizing identity information across network applications, directories, and databases. In fact, if you're like Richard Reid, an IT manager for True North Communications, you consider this job "one of the worst tasks in the world." Despite this sentiment, you (like Reid) probably recognize that synchronizing identity information is less painful and far more secure than the alternative, which is to manually enter and re-enter the same information in your network's myriad systems.

I must confess that Reid shared this sentiment more than three years ago, during a Novell Connection interview for an article introducing DirXML. ("Too Many Directories? Sync 'em With DirXML," *Novell Connection*, May 2000, pp. 8-19. You can download this article from www.novell.com/connectionmagazine/2000. For more recent information about DirXML, see the October 2001 and May/June 2003 issues.)

According to Reid, DirXML—even in beta, which is what he was using at the time—helped ease his struggle to synchronize directories, which highlights this point: from the outset, Novell's objective in designing DirXML has been to make the task of synchronizing identity information as simple as good technology can possibly make it.

A GOOD THING GETS BETTER

DirXML is a cross-platform service that helps you manage identity information across select systems on your corporate network or your partners' networks. (For more information on the Novell Nsure solution, visit www.novell.com/solutions/nsure.)

DirXML helps you manage identity information in any system for which Novell provides (or you or a third-party write) a special connector. Novell provides connectors that interface with popular applications, databases and directories, including PeopleSoft, SAP HR, GroupWise, Microsoft Exchange, Lotus Notes, Oracle and Microsoft Active Directory. (For a complete list of the connectors Novell provides, visit www.novell.com/products/dirxml/drivers.)

To control when and how identity information is exchanged between these systems, you configure their respective connectors

by creating various types of rules. (You base these rules on your company's needs and on its relationship with partners and employees.) In the past, many customers have found this rule-building process intimidating, particularly customers who are unfamiliar with eXtensible Markup Language (XML) and eXtensible Stylesheet Language Transformations (XSLT), the two formats in which DirXML rules have traditionally been represented. Over the years, Novell engineers have worked to simplify this process and, in this latest release of DirXML, they have outdone themselves, frankly.

Due to be released in February 2004, the new solution powered by DirXML and now called Novell Nsure Identity Manager 2.0 includes features that exceed traditional DirXML capabilities. Novell Nsure Identity Manager 2.0 not only significantly simplifies the rule-building process, but also simplifies another management hotspot: password management.

Novell Nsure Identity Manager 2.0 (hereafter called Nsure Identity Manager) runs on eDirectory 8.7.1 and supports all of the platforms that eDirectory supports, including NetWare, Microsoft Windows NT/2000, Red Hat Linux, Solaris, AIX and HP-UX. (For specific version numbers, visit www.novell.com/products/edirectory/sysreqs.html.) Nsure Identity Manager improves upon its parent DirXML product by introducing several enhancements and new features, including logging and monitoring capabilities and the new role-based entitlement policies. (For more information, see *Role Playing* and *System Status* on pages 49 and 50, respectively.)

While Nsure Identity Manager includes several noteworthy features, these features are among the most exciting (and thus merit the attention they get in this article):

- A new graphical user interface for building the policies (previously called rules) that control the flow of information between connected systems.
- New password management features that
 - enable you to create password policies that define criteria for password creation across your connected systems;
 - help users to recover forgotten passwords or to reset expired ones;

DirXML is a cross-platform service that helps you manage identity information across select systems on your corporate network or your partners' networks.

For more information on the Novell Nsure solution, visit www.novell.com/solutions/nsure.

- synchronize passwords between eDirectory and several other connected systems.

THE NEW CODE IS (ALMOST) NO CODE

Nsure Identity Manager simplifies the process of creating policies. Policies are collections of rules that define conditions and actions that govern the flow of information between connected systems in your Nsure Identity Manager environment. For example, a creation policy includes rules that dictate how and when you want new objects created.

In DirXML 1.x, you create rules in either XML or XSLT. Basically, you use XML for rules that are based on simple logic, such as many of the rules in schema-mapping, creation, matching and placement policies. You reserve XSLT for rules that require more complex logic, such as rules in input, output, event and command transformation policies. Unfortunately, the reality of this

seemingly fair equation is that you use XML for only about 20% of your rules and the more complex XSLT for the remaining 80%.

Novell engineers revamped DirXML so that Nsure Identity Manager essentially inverts these percentages. With Nsure Identity Manager, only 20% of your rules need be in XSLT and the remaining 80% of your rules are in a new, simplified version of XML called DirXML Script. What is more important, you don't have to write DirXML Script (or XML or XSLT) to create these rules. Instead, you build the rules that form your policies using a graphical user interface called Policy Builder.

In fact, for some systems, Novell provides policies that are entirely XSLT free. For example, all of the Novell-developed policies for Microsoft Active Directory were built using Policy Builder, demonstrating that configuring complex policies without writing code is possible (even probable).

Included in the Nsure Identity Manager plug-ins for Novell iManager 2.0, Policy Builder speeds the time and reduces the mental energy required to build policies. In Policy Builder, you click the connector for which you want to create a policy, after which you see a graphical representation of the subscriber and publisher channels between eDirectory and the connected system. Near these channels, you might also see icons (that look like tiny documents). (See Figure 1.) These icons represent policies that already have been written for this connector.

To create a new policy, you click one of the arrows in the publisher or subscriber channels. (See Figure 1.) This opens Rule Builder. In Rule Builder, you define and combine conditions (such as "if operation equals move") and specify the appropriate action or actions (such as "do veto").

For every variable in the condition or action that you're defining, Rule Builder provides drop-down lists that include only valid options. (See Figure 2.) For example, to open a list of valid options for the value that follows the word "if" in a condition, you click the arrow at the end of that field. As you can see in Figure 2, you do the same to view drop-down lists of options for every variable.

Policy Builder translates the rules you create into DirXML Script. Policy Builder also includes a wizard that enables you to translate into DirXML Script any rules that you already have in

In Novell Nsure Identity Manager 2.0, you build the vast majority of the rules that comprise your policies using a graphical user interface called Policy Builder.



FIGURE 1

With Nsure Identity Manager, Novell introduces its solution to password management. This solution minimizes the time and energy you and helpdesk personnel devote to managing the secrets that mark your company's first line of defense in the security battle.

old-style XML (that is, rules you wrote using previous versions of DirXML). In fact, with the exception of schema-mapping rules, you'll need to translate these old rules in order for them to work in this upgraded environment.

Of course, if you're a diehard code guy, you can view and write DirXML Script, XML and XSLT. The point here is that you don't have to because Policy Builder makes the process of building rules as simple—and code free—as possible.

This code-free theme extends to a new policy type, called role-based Entitlement policies, which you create using a wizard from the Nsure Identity Manager plug-ins for iManager. Role-based entitlement policies provide a slick new way for you to efficiently provision access to multiple systems' resources based on business needs that determine users' roles in your organization. Each role-based entitlement policy enables you to grant groups of users access rights and entitlements to memberships and accounts in

the systems that business needs determine should be associated with this policy. (For more information see *Role Playing* on p. 49.)

PASSWORD: POLICY, SERVICE AND SYNC

With Policy Builder, Novell transforms what you (like Reid) might have considered "one of the worst tasks in the world" into one of the less-troublesome tasks on your list. Of course, your identity management problems don't end with configuring the connectors that enable your systems to share identity information. Theoretically, you're still left with the hassles associated with managing passwords—at least, you would be, were it not for Nsure Identity Manager.

With Nsure Identity Manager, Novell introduces its solution to password management. This solution minimizes the time and energy you and helpdesk personnel devote to managing the secrets that mark your company's first line of defense in the security battle. The new password management features fall into three categories:

1 PASSWORD POLICY

2 PASSWORD SELF-SERVICE

3 PASSWORD SYNCHRONIZATION

Rule Builder (in Policy Builder) provides you with drop-down lists that display only valid options for the variables in the conditions and actions that define your rules.

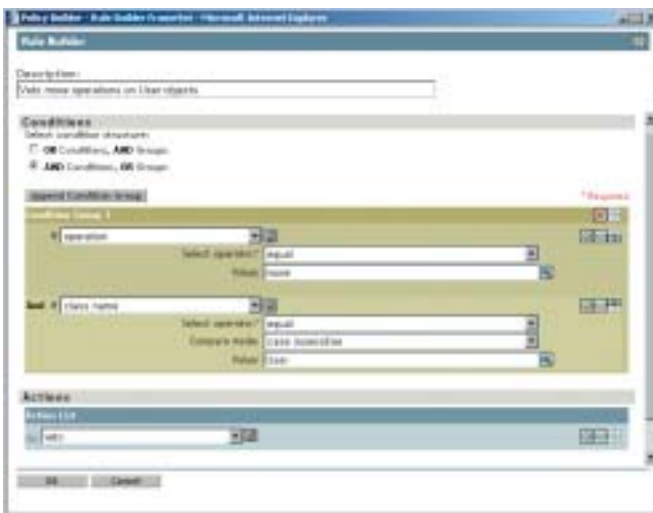


FIGURE 2

To use these features, you need to upgrade your environment to support the Universal Password, the manifestation of the new Novell password paradigm. (For more information, see *The Password Joins one Net* on p. 53.)

These new password management features should appeal to you for several reasons. One, with these features, you can enforce a consistent password policy across several heterogeneous systems and thus tighten your security belt. Two, with these features, you enable users to help themselves and, in doing so, lighten the load on your helpdesk. Three, with these features, you minimize the number of passwords that users need to remember, thereby strengthening the security of password authentication to your network. After all, with fewer passwords, users are less likely to void the password concept by writing down (and thus advertising) their secrets.

ONE (POLICY) FOR ALL (SYSTEMS)

With Nsure Identity Manager, you create a Password Policy that is a little more concrete and a lot more enforceable than a few words on a page in your security handbook.

You do so by clicking to open Manage Password Policies under the Password Management task created by the Nsure Identity Manager plug-ins for iManager 2.0. From this interface, a wizard simplifies the process of creating one or more Pass-

word Policies. You assign these policies to eDirectory root, partition, container or user objects.

In Nsure Identity Manager, a Password Policy is a collection of rules for creating and replacing user passwords. These rules specify your criteria for an acceptable password. To create rules, you select and type values for various criteria fields. (See Figure 3.) As you can see in Figure 3, the Password Policies you create can dictate

Novell iManager 2.0 plug-ins for Nsure Identity Manager 2.0 include a wizard that helps you create a Password Policy that you can enforce across multiple systems.

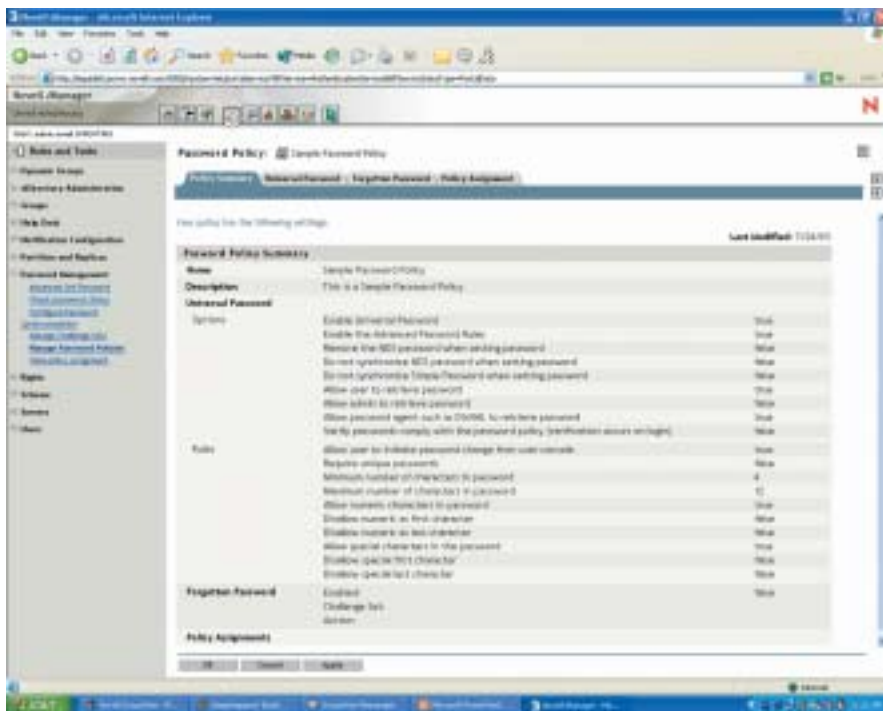


FIGURE 3

www.
omnitech.
com

Password management functions will continue to be used in help desk environments, but the end of 2003 will find most enterprise password management deployments placed within administrative capabilities, incorporated into identity management-related products such as provisioning, Web single sign-on and portals.

password syntax, length, use of special characters and whether or not you allow users to retrieve and reset their passwords.

Once you have created and assigned your Password Policy (or Policies), Nsure Identity Manager helps enforce it in a couple of ways. One way is to verify that users' passwords comply with the policy that applies to them each time they login. (You enable this feature when you create your Password Policy.) If enabled, this feature compares users' passwords to the Password Policy at login. If users' passwords comply, they are authenticated to the network as usual. If their passwords do not comply, they are informed of this fact, and you or users need to set a new password.

Nsure Identity Manager also helps enforce the policy by reminding users of the rules for password compliance when they attempt to reset their passwords from the iManager Self-Service Console. (You enable the Self-Service Console from the Manage Password Policies interface.)

LIGHTEN THE HELPDESK LOAD

As its name suggests, the Self-Service Console enables users to retrieve forgotten passwords or to reset passwords—all by themselves. The idea of empowering users with the ability to reset their own passwords or recover forgotten ones should go over very well with your helpdesk; after all, password problems account for nearly 30% of all helpdesk calls. (In case you're worried, enabling self-service does not override your ability or the ability for helpdesk personnel to reset or recover users' passwords.)

When you enable the Self-Service Console, you create a challenge set of questions using the Password Management interface made available by the iManager plug-ins. This challenge set includes required and (optionally) random questions that you and (optionally) users create. (See Figure 4.) Users answer the questions you create and create questions and answers of their own (assuming you allow them to do so) from the Manage Challenge Response page in the Self-Service Console. (If you want, you can configure Nsure Identity Manager to display this page when users log in for the first time after you have enabled a new Password Policy.)

As you can see in Figure 4, you also specify the action that you want to occur when users are presented with and correctly

answer their challenge set of questions. For example, you might choose to display a hint (which you create) or might choose to e-mail users their forgotten passwords or the hint. To simplify the process of creating the e-mail messages containing hints or forgotten passwords, Nsure Identity Manager includes five predefined and customizable notification templates for these messages.

Alternately, you might choose to enable users who correctly answer their challenge set of questions to reset their passwords directly from the console. (See Figure 5.)

PASS THE WORD!

What happens when users reset their password from the iManager Self-Service Console? You can probably guess: Nsure Identity Manager updates these users' passwords across your connected systems. More specifically, Nsure Identity Manager

When you enable the Self-Service Console, you create a challenge set of questions. Nsure Identity Manager 2.0 displays all of the required questions from this set when users attempt to retrieve or reset their own passwords.

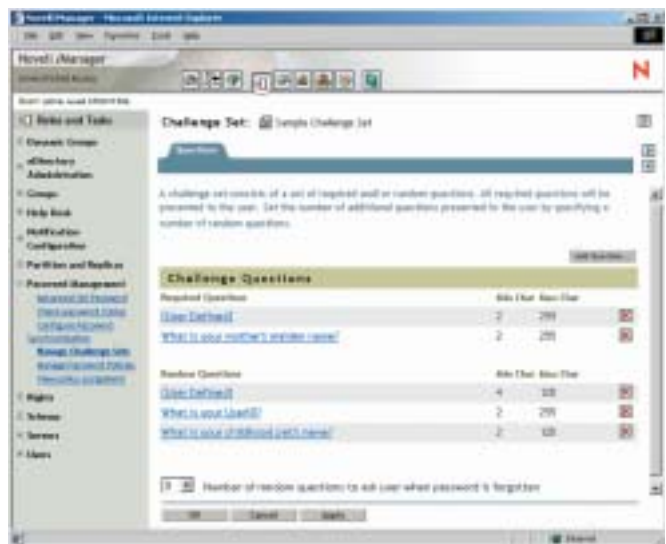


FIGURE 4

Role Playing

The Novell Nsure Identity Manager plug-ins for Novell iManager create a Role-Based Entitlements area that you use to create and manage role-based entitlement policies. Role-based entitlement policies entitle particular groups of users to memberships and accounts in various connected systems. For example, you might create a Sales Entitlement policy that entitles all users in your company's Sales department to an eDirectory group membership, a Notes user account, and a Microsoft Active Directory account.

From the Role-Based Entitlements area, you can launch a wizard that walks you through a six-step process for creating role-based entitlement policies. A quick glance at these six steps should give you an idea of just how simple it can be to provision user memberships and accounts in various connected systems.

STEP 1 *Name and describe your policy*

STEP 2 *Define the criteria for a dynamic list of members*

For each policy, you can create a membership list that changes as users' relationship to your organization changes. To do so, you create a filter that points Nsure Identity Manager to a particular portion of your tree, where it searches for and finds particular users based on a set of criteria you specify. These criteria instruct Nsure Identity Manager to search for users with similar identity information. For example, your dynamic membership list might include users with the same cost center or with particular words in their titles.

STEP 3 *Define the static list of users to always include in or exclude from this role*

STEP 4 *Select the connectors to provide entitlements on connected systems*

For each policy, you select from a drop-down list the connectors that represent the systems to which you want to grant access rights and entitlements for the users associated with this role. Connectors for the following systems support role-based entitlements:

- Novell GroupWise
- Lotus Notes
- Lightweight Directory Access Protocol (LDAP)
- MS NT Domains
- MS Active Directory
- MS Exchange

Each participating connector supports specific entitlements that you click to select. For example, the Lotus Notes connector enables you to entitle role members to a Notes User account and/or membership in a Notes User Group or Department.

STEP 5 *Select the rights members of this role have to these objects*

In this step, you click to select the list of displayed objects (servers and printers, for example) and then click the object rights (supervisor, compare and read, for example) that you want to grant to members of this role.

STEP 6 *Review the Policy summary*

This final step enables you to check out the policy you've just created to make sure you've granted the right entitlements in the right systems for the right users.

The Role-Based Entitlements feature in Nsure Identity Manager makes provisioning access rights and entitlements to memberships and accounts easier than ever for at least three reasons.

- 1** You can write rules that instruct Nsure Identity Manager which users to grant which entitlements—without having to deal with XML or XSLT.
- 2** You need write only one policy to grant several users entitlements to several connected systems.
- 3** Users come and users go but, despite this fact of corporate life, you won't necessarily need to touch your entitlement policies. Nsure Identity Manager provisions access and entitlements based on users' roles—not their names.

www.
omnitech.
com

Nsure Identity Manager ensures that when users update their passwords from the Self-Service Console, their passwords are updated across all of the connected systems that subscribe to this information.

System Status: Checkpoints and Alerts

As is soon to be true of all Novell products, Novell Nsure Identity Manager 2.0 includes the Novell Nsure Audit Starter Pack. As you can guess by the name, the Nsure Audit Starter Pack entitles you to some but not all of the capabilities provided by the complete Nsure Audit solution. While it does not provide all of these capabilities, don't be too quick to assume that Nsure Audit Starter Pack is lacking on the feature front. In fact, it offers all of and far more than the auditing features Novell previously provided in NetWare 6.0.

Among other capabilities, Nsure Audit Starter Pack enables you to centrally log events from Nsure Identity Manager, eDirectory 8.7 and NetWare 6.5 to a flat file or MySQL database. Nsure Audit Starter Pack also provides a filter setup wizard that helps you configure the events about which you want to be notified. Nsure Audit Starter Pack can deliver real-time notifications via SMTP.

Furthermore, the Nsure Audit Starter Pack includes evaluation versions of all of the features in Nsure Audit. Among other features, the complete Nsure Audit solution enables you to log information not only to a flat file or MySQL database but also to an Oracle database. The complete product also enables real-time monitoring, real-time notification through a wide variety of methods (including SMTP, SNMP and Syslog) and report generation. Furthermore, Nsure Audit supports a wide variety of applications, including NDS 6.x and higher, eDirectory 8.5 and higher, and NetWare 5.1 and higher. (For more information, see "Police Your Policies with Novell Nsure Audit," *Novell Connection*, July/August 2003, pp. 14-24. You can view this article online at http://www.novell.com/connectionmagazine/2003/08/tech_talk_1.html.)

By including the Nsure Audit Starter Pack, Novell simplifies the task of tracking and logging what's really happening in your Nsure Identity Manager environment. This task in turn enables you to observe your identity management policies in action—and thereby determine that they're working precisely as you intended.

updates the passwords across any of your connected systems that meet these two criteria:

- Support the new password management features
- Subscribe to password information from the Nsure Identity Manager data store

Fortunately, most of the systems for which Novell provides a connector support the new password management features. Specifically, connectors for the following systems support the Nsure Identity Manager password management features:

- eDirectory
- Novell Directory Services (NDS)
- Novell GroupWise
- Microsoft Active Directory (MS AD)
- Microsoft NT Domains

When users forget their passwords or need to reset expired ones, they can do it themselves from the iManager Self-Service Console. The Change Password screen conveniently displays your Password Policy, helping to enforce your password-creation rules.

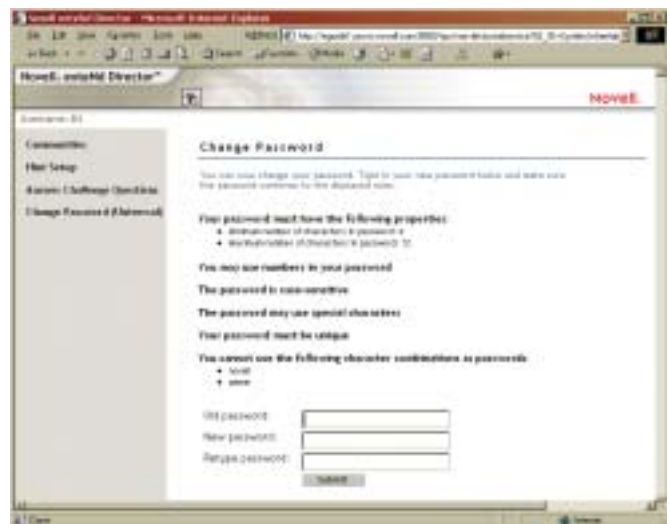


FIGURE 5

- Java Database Connectivity (JDBC)
- Lightweight Directory Access Protocol (LDAP)
- Lotus Notes
- Network Information System (NIS)
- Schools Interoperability Framework (SIF)
- SAP User Management

If you're well-versed in traditional DirXML lingo, you already know what "subscribing" to password information implies. Basically, every connector has a subscriber and publisher channel, and for each channel you create filters that dictate which information flows across this channel. Publisher channels enable information to flow from the extended system to the Nsure Identity Manager data store. Subscriber channels do the opposite: enable information to flow from the Nsure Identity Manager data store to the extended system.

Nsure Identity Manager ensures that when users update their passwords from the Self-Service Console, their passwords are updated across all of the connected systems that subscribe to this information.

A LEAK-PROOF SYNC

Contrary to what you might fear, users are not restricted to using only the Self-Service Console to update their passwords. In fact, you or users can reset passwords for systems that support bi-directional synchronization using any of several possible interfaces, including the following:

- Systems' native client interface (for example, Novell client or the login dialog in Windows)

- LDAP client (connected to eDirectory)
- Microsoft Management Console
- Self-Service Console
- iManager (administrative interface)
- ConsoleOne

When users or you reset passwords from one of these interfaces, Nsure Identity Manager checks the reset password against the policy. Next, Nsure Identity Manager ensures that the password information is updated across all of the systems that support bi-directional synchronization. In this release, the following systems support bi-directional synchronization:

- eDirectory
- MS AD
- MS NT Domains
- NIS

In other words, these systems essentially both subscribe to and publish password information. For example, if a user resets her password for AD from the AD interface, AD publishes this information to the Nsure Identity Manager data store, which in turn updates this information across all of the other systems that subscribe to this information. The result is that the passwords on all of these systems are always in sync.

As you might know, this capability has been available since the release of DirXML Password Synchronization 1.0. However, Nsure Identity Manager supports more clients than the previous version and more systems can now participate in this bi-directional synchronization process. These enhancements stem from the new archi-

www.begin
finite.com

With its new password management features, Nsure Identity Manager empowers the users on your corporate network by enabling them to take care of their own password problems—and possibly by reducing the number of times they experience password problems.

Let's Get Something Straight

If you've read the main text of this article, you know that Novell changed the name of its latest release of DirXML from DirXML to Novell Nsure Identity Manager 2.0. Why the change?

In the past, Novell described DirXML as a cross-platform service that shares and synchronizes data across applications, databases and directories within your intranet or between enterprises. Unfortunately, neither the name DirXML nor this description state or imply that the data being shared and synchronized is identity data. In contrast, the name Novell Nsure Identity Manager implies in an instant what this product is: a tool for managing identity data across all of your systems. It also highlights to which family of solutions this product belongs, that is, the Novell Nsure secure identity management family. (For more information about Nsure, visit www.novell.com/solutions/nsure.)

This name change also highlights one of many differences between Nsure Identity Manager and Novell exteNd, a difference that marketing rhetoric can sometimes cloud. Whereas Nsure Identity Manager enables you to better manage identity data, Novell exteNd enables you to make backend, legacy data more accessible to internal and external network users. Novell exteNd is a suite of tools for developing and deploying business applications and Web services. Using these tools, you transform resources from existing systems into open Web services, which you can then deliver through dynamic portals. (Watch for an article covering Novell exteNd in our January/February 2004 issue.)

With that said, it's obvious how the name Nsure Identity Manager now appropriately highlights the unique purpose of the product.

texture underlying this capability. (See Figure 6.) Among other differences, use of the Universal Password and new connectors for Active Directory and NT differentiate the new architecture from the old.

WIN-WIN: FOR USERS, FOR YOUR COMPANY, FOR YOU

The end result of this new architecture is the same as the end result of all of the new and enhanced features in Nsure Identity Manager: the result is a win-win situation for users, your company and you.

With its new password management features, Nsure Identity Manager empowers the users on your corporate network by enabling them to take care of their own password problems—and possibly by reducing the number of times they experience password problems. By enabling you to synchronize the same password across multiple systems, Nsure Identity Manager makes it possible for you to reduce the number of passwords that users need. When users do forget their passwords, Nsure Identity Manager enables them to reset their passwords—without burdening your helpdesk. Furthermore, they'll get guidance from the iManager Self-Service Console regarding

When you or a user reset a password from one of the supported interfaces (such as Microsoft Active Directory), Nsure Identity Manager updates the information in all other systems that support bi-directional password synchronization.

BI-DIRECTIONAL PASSWORD SYNCHRONIZATION

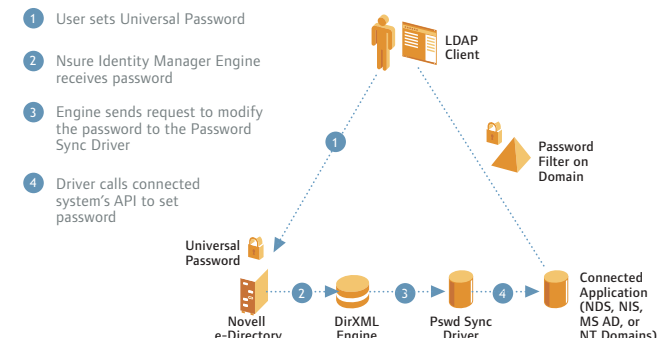


FIGURE 6

the type of password they should create.

While users probably will appreciate this freedom, they probably won't appreciate its implications, as will the powers-that-be within your company. The fact that the Self-Service Console prompts users to create passwords that conform to your policy means that users create stronger passwords. Furthermore, because you can reduce the number of passwords users require, users will be less likely to invent methods of remembering these passwords—methods that can compromise the security of these secrets.

These benefits are great for users and for your company, but what will probably interest you most about Nsure Identity Manager is the fact that it simplifies your work life. When Novell first introduced DirXML, you were probably in the habit of manually entering and re-entering identity information across scores of systems. Because you had long since accepted this inefficient process as a necessary evil in your work life, you were probably as excited as Reid about DirXML, which automated this time-consuming task. Nevertheless, you and many others found that configuring the connectors that made this automation possible was a difficult job, at best.

Nsure Identity Manager transforms this difficult job into a doable one with Policy Builder. Policy Builder enables you to configure the policies that govern your connectors without having to write a single line of code, in most cases, and you know what that means: less code means less stress, which in turn means more time. Enjoy. **N**

The Password Joins one Net

Novell envisions a networking world in which boundaries between systems and networks are inconsequential. Until recently, this vision, called one Net, had one concern: the traditional Novell password. In the proverbial nutshell, the traditional Novell password doesn't integrate well with other systems. Novell solves this problem with the Universal Password, which enables you to create and manage a single password for use across your heterogeneous systems.

With Nsure Identity Manager 2.0, you enable and configure the Universal Password from the Manage Password Policies interface in Novell iManager 2.0. Among other benefits, the Universal Password supports advanced password rules, such as extended characters and both upper and lower case characters in passwords. Universal Password also enables bi-directional synchronization of passwords between eDirectory and other connected systems. (For more information, see *A Leak-Proof Sync* on p. 51.)

Before you enable the Universal Password, you need to prepare your network for the change. For more information on how to do so, see the *NetWare 6.5 Universal Password Deployment Guide*. (You can download this guide from www.novell.com/documentation/lq/nw65/pdfdoc/universal_password/universal_password.pdf.)

www.begin
finite.com