



## NOVELL CERTIFIED PROFESSIONAL

Sandy Stevens

# Novell Single Sign-On 2.0

## Forget Multiple Passwords

**W**ith the Internet and the myriad web servers and applications that require authentication, you must maintain numerous user identities. If you are struggling to remember which username and password you used for a particular web site or application, you know users are having the same problem.

How do you make password management easier for both you and other users? The answer is the Novell Single Sign-on 2.0 Bundle. Available since August 2000, the Novell Single Sign-on 2.0 Bundle enables single sign-on to virtually any application.

With the Novell Single Sign-on 2.0 Bundle, one username and password can give users access to web sites, Windows applications, client-server applications, custom in-house applications, UNIX hosts, and IBM mainframes. For just U.S. \$49 per user, the Novell Single Sign-on 2.0 Bundle gives users single sign-on to all of these applications and services without requiring you to retrofit applications or to write custom connectors, wrappers, or scripts.

### YOU'VE COME A LONG WAY, BABY!

Novell introduced basic single sign-on capabilities in July 1999 with Novell Single Sign-on 1.0. (For more information, see "Novell Single Sign-on: One Stop Authentication," Jan. 2000, *NetWare Connection*, pp. 40-43. You can download this article from [www.nwconnection.com/past](http://www.nwconnection.com/past).) Although the first version of Novell Single Sign-on significantly reduces password administration, it has a few drawbacks.

For example, every application that you want to integrate with Novell Single Sign-on 1.0 requires special software called a *single sign-on connector*. Novell provides single sign-on connectors for nine applications. If your company is using an application that doesn't have a single sign-on connector, you can use the Single Sign-on 1.0 software developer kit (SDK) to write a connector. Of course, you can write this single sign-on connector only if the following apply:

- You have programming resources (talent, time, and money).
- The application is an in-house application, and you have access to the source code.
- The application is not an out-sourced application (such as an extranet application) that your company is merely using.

- Users access the application while they are connected to the network.

In addition, Novell Single Sign-on 1.0 does not support web applications. To access web applications, users must continue to maintain multiple identities.

With the Novell Single Sign-on 2.0 Bundle, Novell addresses these issues by providing an off-the-shelf single sign-on solution that supports practically all of your company's applications with no coding and little setup and configuration.

### WHAT'S IN THE BUNDLE?

The Novell Single Sign-on 2.0 Bundle combines two products:

- Novell Single Sign-on 2.0 includes Novell's secret store and Novell International Cryptographic Infrastructure (NICI) technologies. These technologies enable you to use NDS as a secure central repository for all authentication credentials, which are also known as *secrets*.
- Passlogix Inc.'s v-GO for Novell Single Sign-on extends the capabilities of Novell Single Sign-on 2.0 to provide single sign-on access to applications without requiring the use of single sign-on connectors. (v-GO for Novell Single Sign-on is hereafter referred to as simply v-GO.)

Novell is also offering Novell Single Sign-on 2.0 with a limited version of v-GO for U.S. \$29 per user. This version allows single sign-on access to five web sites and to a limited number of predefined Windows applications.

### SECRET STORE AND NICI

Novell Single Sign-on 2.0 uses NICI to encrypt a user's secrets (such as passwords, X.509 certificates, tokens, and biometric information) and then saves these secrets in the secret store, an encrypted, hidden NDS attribute of the User object. When an application retrieves a secret from NDS, Novell Single Sign-on 2.0 sends the encrypted secret over the wire and then decrypts the secret at the workstation. After the user is authenticated to the application, Novell Single Sign-on 2.0 immediately removes and destroys the secret from the workstation's memory.



## NOVELL CERTIFIED PROFESSIONAL

*Novell Single Sign-On 2.0*

Novell Single Sign-on 1.0 also uses secret store and NICI to securely store and transport users' secrets. The difference between version 1.0 and 2.0 is the way that users' secrets are captured and retrieved. As mentioned earlier, Novell Single Sign-on 1.0 uses single sign-on connectors (which are still supported by version 2.0). The Novell Single Sign-on 2.0 Bundle uses v-GO.

### **SINGLE SIGN-ON TO WINDOWS APPLICATIONS**

v-GO is a client component that requires minimal user intervention. In most cases, v-GO automatically captures a user's authentication credentials for applications with little user intervention. When a user authenticates to NDS and launches an application for the first time, v-GO captures the user's authentication credentials (the secret). The secret is then encrypted and stored in the user's secret store.

Thereafter, whenever the user launches the application, v-GO detects the login dialog and requests the appropriate secret from NDS. NDS then delivers the authentication credentials, and v-GO automatic-

ally enters the username and password in the login dialog fields. The user is then authenticated to the application.

v-GO works by "hooking" into the Windows messaging system. (The Windows messaging system allows applications to open and close windows and notify other windows to do something.) By hooking into the Windows messaging system, v-GO captures authentication credentials.

For example, v-GO monitors the Windows desktop for known login events, such as windows that have descriptive components indicating login credentials are required. v-GO also looks for variables such as the executable name and other unique identifiers. When v-GO detects supported login dialogs, it provides the appropriate authentication information for that user.

v-GO supports a number of applications by default. If you want single sign-on to an application that is not supported by v-GO, you can use the v-GO Logon Wizard to "train" v-GO to recognize the application. Using the v-GO login wizard, you define an unrecognized application by defining the application name and type.

When you reach the login screen of the application you are defining, you drag-and-drop a v-GO wizard icon on the login name and password field. The next time you run the application, v-GO will recognize the application's login dialog box.

### **SINGLE SIGN-ON TO WEB SITES**

v-GO can also automatically log users in to web sites on the Internet, intranet, or extranet. After a user is authenticated to NDS, v-GO monitors the HTML data stream for known login events. When v-GO detects a known event, it automatically provides the appropriate username and password.

### **SINGLE SIGN-ON TO IBM MAINFRAME APPLICATIONS**

v-GO natively integrates with popular terminal-emulation programs using the HLLAPI interface. Through this integration, v-GO can monitor 3,270 sessions and automatically respond to login requests for users who are authenticated to NDS. v-GO currently supports the following terminal-emulation programs:

**Visit our advertiser  
CyberStateU.com at  
[www.CyberStateU.com](http://www.CyberStateU.com)**



**Figure 1.** The v-GO Logon Wizard enables users to easily configure Novell Single Sign-on to automatically log in to resources, such as a web site, that require a username and password.

- Attachmate Extra! 6.5
- Wall Data Rumba
- WRQ Reflections
- IBM Personal Communicator
- Hummingbird Host Explorer
- Browser-based emulators (such as IBM's Host on Demand and Host Publisher)

#### SINGLE SIGN-ON FOR ROAMING USERS

Because the Novell Single Sign-on 2.0 Bundle is based on NDS authentication, users have single sign-on to all of their applications from any desktop on the network. However, the Novell Single Sign-on 2.0 Bundle also supports an optional disconnected mode, which enables users who are not connected to the network to have single sign-on capabilities to desktop and web applications. To provide this capability, v-GO uses a local store technology to cache secrets locally when a user logs out of NDS. v-GO synchronizes changes made to the user's local store when the user reconnects to NDS.

A user's v-GO local store is an encrypted file that is stored under the Windows subdirectory. The filename is a combination of the username and AML.INI. For example, the local store filename for MATT would be MATT.AML.INI.

#### A REAL-LIFE EXAMPLE

The following example shows how easy v-GO is to use: Suppose you want to retrieve a stock portfolio and track preferred stocks using the Yahoo! Finance web site. When you access the Yahoo! Finance web site and select sign in, Yahoo! requests a username and password. At this point, v-

GO automatically launches a dialog box, indicating it did not find login information for this web site. This dialog box allows you to choose whether or not you want to create this information. When you select OK, the v-GO logon wizard automatically launches. (See Figure 1.)

Next, v-GO prompts you to identify this site. By default, v-GO uses the title of the web page (in this case: Welcome to Yahoo! Finance). v-GO also lets you enter a description to help you identify the site in your secret store.

Next, v-GO prompts you to enter a complete or partial URL. This URL helps v-GO identify the site the next time you access it. (Of course, an application does not require a URL.)

The next dialog box that appears prompts you to enter a username. If you have an existing identity (username and password) for this web site, you enter that information. If you have not logged in to this web site before, you can use v-GO to create an identity for this web site.

Next, the password dialog box appears. (See Figure 2 on p. 44.) You then enter the password for your existing identity or the password for the new identity.

As Figure 2 shows, the password dialog box has a few interesting options. For example, if you select the Generate button, v-GO generates a random password, which is a complex mixture of alphanumeric characters (such as 456y78IH8dO) that is difficult for a hacker to guess. Since Novell Single Sign-on 2.0 will always provide the login credentials for this web site, it can use a complex password and you do not have to worry about forgetting that password. All you need to remember is your NDS username and password—Novell Single Sign-on 2.0 does the rest!

The Properties button is also worth mentioning. You can use this option to view the password policy, which defines password rules such as minimum and maximum password lengths and uppercase and lowercase character support. You can

use the default password policy or configure your own in NDS.

After you enter this information, you never have to enter login credentials for this web site again. v-GO automatically supplies this information for you. If you use the disconnected feature, v-GO can automatically log you in to this web site even when you are not logged in to NDS.

#### THE SECRETSTORE MANAGER UTILITY

The Novell Single Sign-on 2.0 Bundle includes the SecretStore Manager utility (SSMANAGER.EXE), which allows users to perform basic maintenance tasks on their secret store. For example, users can unlock their secret store, delete application secrets, and perform basic troubleshooting tests on their secret store. Users can also change or set their Enhanced Protection Master Password, which is a security feature of Novell Single Sign-on 2.0.

The Enhanced Protection Master Password enables users to lock their secret against any NDS password changes. If an NDS password is changed when Enhanced Protection Master Password is enabled, the user must enter the old password (rather than the new NDS password) before access is granted to an application. This security feature prevents an unauthorized user from changing another user's NDS password multiple times in order to gain unauthorized access to an application or to the data contained in a user's secret store.

#### THE LOGON MANAGER UTILITY

The Novell Single Sign-on 2.0 Bundle also includes the Logon Manager utility, which is installed as part of the v-GO client. Users can use the Logon Manager utility to manage all of their login secrets. By clicking on the Single Sign-on icon in their Windows system tray and selecting Start Single Sign-on, users can use the Logon Manager utility to perform tasks such as the following:

- **Look Up Stored Passwords.** If a user chooses My Logons and then Reveal, Novell Single Sign-on 2.0 decrypts the passwords in the user's secret store and displays them in clear text. This feature is useful if a user needs to log in to an application from a computer that does not support Novell Single Sign-on 2.0.
- **Delete a Secret.** By choosing My Logons and selecting the desired secret, a user can delete a secret from his or her secret store. The secret is then deleted

from NDS and the user's local store. This feature is useful if a user's identity for a particular application is changed or is no longer needed.

- **Customize Single Sign-on Settings.** By selecting Settings, a user can indicate that he or she wants to be prompted to add login information for password-protected applications. After this information is added, Novell Single Sign-on 2.0 immediately opens the application or web site when the user accesses it. The user can also use this option to customize his or her personal password policy.

In addition, if users have access to ConsoleOne, they can also use ConsoleOne to manage their secrets.

#### **MANAGING THE NOVELL SINGLE SIGN-ON 2.0 BUNDLE**

Managing the Novell Single Sign-on 2.0 Bundle is easy. After you have installed the server and client components, the Novell Single Sign-on 2.0 Bundle runs as is, requiring little or no management. However, you may want to use ConsoleOne to

complete tasks such as the following:

- Managing v-GO settings in NDS
- Configuring terminal-emulation support
- Licensing and enabling v-GO to permit unlimited web logins per user and to define additional Windows applications that v-GO will recognize
- Defining v-GO recognition characteristics for undefined applications
- Defining application and password policies

#### **INSTALLATION TIPS**

Because installing the Novell Single Sign-on 2.0 Bundle is easy, this article does not provide step-by-step instructions. However, you should know the following:

- The Novell Single Sign-on 2.0 Bundle requires NetWare 5.x servers.
- If you are running NDS eDirectory on Windows NT, the Novell Single Sign-on 2.0 Bundle requires Windows NT Server 4.0 with service pack 2 or above.
- If you are running NDS eDirectory on Windows 2000, the Novell Single Sign-

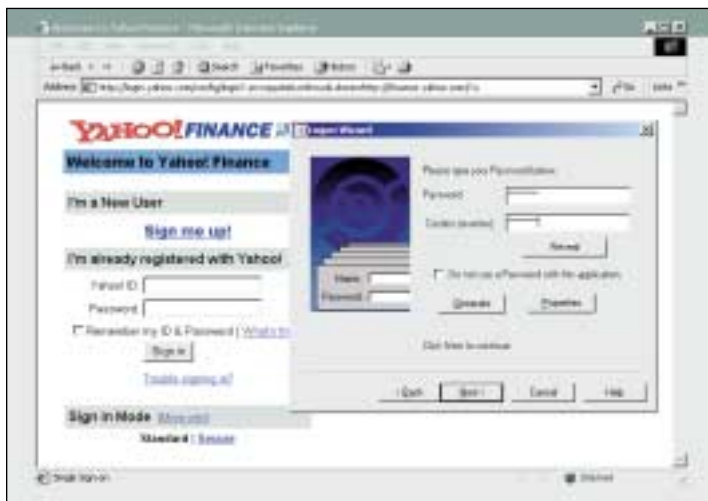
on 2.0 Bundle requires the release version of Windows 2000.

- If you are running Windows 2000 or NT 4.0, the Novell Single Sign-on 2.0 Bundle does not support a single computer being used as both an NDS server and a client.
- The Novell Single Sign-on 2.0 Bundle requires NICE 1.5.4 (which is included on the Novell Single Sign-on 2.0 Bundle CD). You must install NICE 1.5.4 on the server before you install Novell Single Sign-on.

You use the NWCONFIG utility to install Novell Single Sign-on 2.0 on NetWare servers. You can also use this utility to install the secret store service NLM (SSS.NLM) and to extend the NDS schema to support new Single Sign-on objects. This process also initializes and/or validates the Security Domain Infrastructure (SDI)—the security infrastructure used by Novell Single Sign-on.

If you are installing Novell Single Sign-on 2.0 on a Windows 2000 or NT server that is running NDS eDirectory or NDS

Visit our advertiser  
AdRem at  
[www.adremsoft.com](http://www.adremsoft.com)



**Figure 2.** The v-GO logon wizard saves usernames and passwords in an encrypted secret store.

Corporate Edition, you use an installation wizard (SETUP.EXE) to install the secret store service files. This installation wizard also extends the NDS schema and sets up the SDI.

On the client side, the auto-run program on the Novell Single Sign-on 2.0 CD displays a menu that helps you install the following client components:

- The NCI client
- The Novell Single Sign-on 2.0 client
- The v-GO client
- The ConsoleOne utility
- The ConsoleOne snap-in module for Novell Single Sign-on

You must install all of these components on the workstation from which you want to manage the Novell Single Sign-on 2.0 Bundle. Users' workstations require the NCI client, the Novell Single Sign-on 2.0 client, and the v-GO Client.

### Distributing Single Sign-On Using ZENworks for Desktops

One of the most difficult parts of deploying new technology is installing the necessary software on users' desktops. To minimize the effort required to install the Single Sign-on client software, Novell has included ZENworks for Desktops software with the Novell Single Sign-on Bundle. You can use ZENworks to distribute the client software to users' desktops.

On the Novell Single Sign-on 2.0 Bundle CD, you will find a ZENWORKS subdirectory, which contains the files you need to create an Application object template (AOT) for Novell Single Sign-

on 2.0. Using this Application object and a ZENworks policy, you can mass distribute the Novell Single Sign-on client components to the desired workstations when users log in to the network.

### NDS SCHEMA EXTENSIONS

When you install the Novell Single Sign-on 2.0 Bundle, the schema of the

NDS tree is extended to support the following new objects.

#### nsoSingleSignon Objects

The nsoSingleSignon object is a container object that must be created first to hold the other Novell Single Sign-on objects. This object has a v-GO property page that allows you to set up administrative overrides for Single Sign-on User objects that reside within the container object. You can then control v-GO's behavior from an administrative level.

For example, you can use this object to define whether v-GO will support disconnected operations or to define how v-GO behaves when it detects login events. You also use this object to control whether or not users can reveal their passwords and to import predefined applications supported by v-GO.

#### nsoApplication Objects

You can use nsoApplication objects to control three types of applications:

- **Windows Override.** These applications are predefined by v-GO. To create Application objects for applications that are predefined by v-GO, you select the Import v-GO application option of the nsoSingleSignon object.
- **Windows.** You use these Application objects to define Windows applications. You can use these objects to customize v-GO to recognize applications that are not supported by default. If v-GO recognizes an application, users do not need to use the Logon Wizard.
- **Terminal Emulator.** You can use these

objects to set recognition characteristics that allow v-GO to recognize main-frame applications.

After you have created nsoApplication objects, you can then apply application and password policies to each Application object as needed.

#### nsoPasswordExcludeList and nsoPasswordPolicy Objects

The nsoPasswordExcludeList and nsoPasswordPolicy objects allow you to create password policies to govern application password requirements tailored to your company's needs. The nsoPasswordExcludeList object lets you determine passwords that are not allowed as secrets.

The nsoPasswordPolicy object lets you globally define the password policy for all User objects in the nsoSingleSignon container object. Single Sign-on policies affect all of the User objects that reside in the container object that holds the nsoSingleSignon object and below (unless another policy is encountered). You can place an nsoSingleSignon object anywhere in the NDS tree (except at the [Root]). However, you should place the nsoSingleSignon object at or below the context of the users you want to manage. In addition, any options set at the container level override password options set at the user level.

**Note.** By default, NDS does not determine password by case or mixed alphanumeric. By setting a password policy in Novell Single Sign-on 2.0, you can ensure that users are creating passwords in NDS that conform to the password requirements of external systems. With password policies, you can institute a minimum level of password security for your company.

### CONCLUSION

With NDS, users can enter one username and password and access all of the network resources they are authorized to use. NDS Corporate Edition extends this single sign-on across multiple platforms including Windows NT, Solaris, Linux, and OS/390. With the Novell Single Sign-on 2.0 Bundle, users now have the convenience of single sign-on to web sites, applications, UNIX hosts, and IBM mainframes.

*Sandy Stevens is a freelance writer based in San Diego, California. Stevens is co-author of Novell's Guide to Integrating NetWare 5 and NT, Novell's Guide to NetWare Printing, and Novell's Guide to BorderManager.* ●