# Novell SecureLogin Readme 7.0 SP1 Hot Fix 2

July 20, 2010

**Novell®**

## 1 Documentation

The following sources provide information about Novell SecureLogin:

- *Getting Started*
  - *Novell SecureLogin Quick Start Guide* (http://www.novell.com/documentation/securelogin70/nsl70_quick_start/?page=/documentation/securelogin70/nsl70_quick_start/data/bimzy42.html)
  - *Novell SecureLogin Overview Guide*
- *Installation*
  - *Novell SecureLogin Installation Guide*
- *Administration*
  - *Novell SecureLogin Administration Guide*
  - *Novell SecureLogin Application Definition Wizard Administration Guide*
  - *Novell SecureLogin Citrix and Terminal Services Guide*
  - *pcProx Guide*
- *End User*
  - *Novell SecureLogin User Guide*
- *Reference*
  - *Novell SecureLogin Application Definition Guide*

## 2 Introduction

Novell SecureLogin is a single sign-on application. It consists of multiple, integrated security systems that provide authentication and single sign-on to networks and applications. It provides a single entry point to the corporate network and its user resources, increasing security while enhancing compliance with corporate security policies. It eliminates the requirement for users to remember multiple usernames and passwords and automatically enters them for users when required.

This document provides you an introduction to the new features introduced in this version of Novell SecureLogin and also lists issues related to the administration, functioning, and other aspects of Novell SecureLogin.

For detailed information on Novell SecureLogin, visit the Novell SecureLogin product Web site. (http://www.novell.com/products/securelogin/).

# 3 Prerequisites

## 3.1 Mandatory Post-Installation Step

After installing SecureLogin 7.0 and 7.0 SP1 in the eDirectory LDAP mode or NDS mode, you must at once extract the fix `FIX701100501_185`, run the `ndsschema` schema file, and extend the schema. This step is mandatory for the smooth functioning of SecureLogin.

## 3.2 Using NICI in LDAP v3 and Novell eDirectory Modes

Novell SecureLogin operates on LDAP v3 (non-eDirectory) and Novell eDirectory modes. However, for a successful installation, before installing SecureLogin on any of the platforms, install Novell International Cryptographic Infrastructure (NICI). Otherwise, an error message is displayed indicating that NICI is not installed and stops the installation process.

You must install both 32-bit and 64-bit NICI manually.

- Microsoft Windows Vista 64-bit in eDirectory, LDAP (non-eDirectory), and LDAP v3 mode
- Microsoft Windows Server 2008 (64-bit)

## 3.3 Using Client Login Extension with Novell SecureLogin

Novell Client Login Extension can help the user to recover the forgotten login password for Novell Client also. For a successful password recovery for Novell Client, install the Novell Client before installing the Client Login Extension tool.

## 3.4 Using the SLLogging Manager on Microsoft Windows Vista

The SLLogging Manager utility is provided to enable advanced logging for support purposes.

Because of Microsoft Windows Vista restrictions, the SLLogging Manager must be enhanced to run on Vista.

Right-click the SLLogging Manager application and select *Run as administrator*. Any changes made through the SLLogging Manager now change the registry correctly to create the relevant log file.

## 3.5 Installing on Microsoft Windows Vista

Before installing SecureLogin on a Windows Vista machine, ensure that the operating system is updated with latest security and service patches or with MS redistributables (32-bit or 64-bit). Otherwise, the SecureLogin installation fails and shows the error message: "`NSL Event Service failed to start`".

# 4 New Features in Hot Fix 1

## 4.1  Enhanced Wizard Support

Novell SecureLogin 7.0 introduces an enhanced administrative wizard. Enhancements are made to improve the wizard engine and provide a unified and intuitive process. The primary improvement is to provide a single wizard that manages different applications types.

Using the wizard, you can create applications definitions for Web, Windows, and Java applications. The new wizard simplifies the configurations of complex application definitions.

## 4.2  Enhancements to Scripting

This version of Novell SecureLogin provides multiple scripting enhancements to continue delivering the most flexible possible solution to accommodate complex scenarios.

## 4.3  Support for Microsoft Windows Platforms

This release supports:

- Microsoft Windows Vista SP1 (32-bit and 64-bit)
- Microsoft Windows Server 2003 SP2 (32-bit and 64-bit)
- Microsoft Windows Server 2008 SP2 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows XP

## 4.4  Support for .NET Framework

This version of Novell SecureLogin supports .NET Framework 3.5 SP1 or above. Novell SecureLogin can use only an already available .NET Framework. Novell SecureLogin does not inform about an uninstalled .NET Framework, which it cannot use anymore.

## 4.5  Novell SecureLogin Event Service

The Novell SecureLogin Event Service is a client based tool that can periodically poll the Windows Event Log, retrieve the SecureLogin events, and send them to the Audit server. From a syslog server, you can view all or specific SecureLogin event logs that are sent from every system that is configured to run this tool. As part of the SecureLogin installation, the Event Service tool also gets installed.

## 4.6  Support for Oracle Forms

Novell SecureLogin 7.0 SP1 support Web enabled Oracle form applications.

## 4.7  Support for Client Login Extension

Client Login Extension 3.7 provides password recovery support for applications that are accessed through Novell SecureLogin 7.0 SP1. The password recovery support is available for graphical authentication interfaces such as GINA and Credential Provider for LDAP clients, Novell Client, and Microsoft clients. Clients in the Windows 7 and Windows Vista operating systems support the Credential Provider model of graphical authentication interface. Clients in other operating systems support the GINA model of graphical authentication interface.

**NOTE:** Among Windows Vista (64-bit) operating systems, Client Login Extension support is available to Enterprise Editions only.

The password recovery support through Client Login Extension tool is also available for locked workstations and for workstations in which user operations are controlled by Desktop Automation Services (DAS).

**NOTE:** In the Active Directory environment, the password recovery support for Credential Provider is available for all platforms except Windows 7 and Windows Vista.

# 5  New Features in Hot Fix 2

## 5.1  Smart Card with DAS Integration

In the earlier version of Novell SecureLogin, Active Directory authentication of the workstation were used to login to SecureLogin. This version of Novell SecureLogin allows the user to login separately using the smart card credentials.

To support this feature in Desktop Automation Services, on-cardmon element has been modified. The changes in smart card and Desktop Automation Services allows switching of users using smart card in Active Directory mode.

## 5.2  Configuring pcProx card format

This version of Novell SecureLogin allows the user to configure to support different card format. If the user does not configure the card format, the default behaviour will be applied. The default behaviour is to assign all the bits as Card ID.

## 5.3  pcProx Tap and Device Removal

In the earlier version, the pcProx command element provided information to Desktop Automation Services on the action performed when configured to monitor removal of the pcProx card.

In this version, the pcProx command element provides information to Desktop Automation Services on the action to be performed when configured to monitor for tap or removal of the pcProx card.

# 6 Known Issues

## 6.1 General Issues

### 6.1.1 Novell SecureLogin Citrix Passthrough in Novell Client Credential Provider Mode

Novell SecureLogin Citrix Passthrough to Microsoft Windows 2008 in Novell Client™ Credential Provider mode is not supported.

### 6.1.2 Offline Message Is Displayed Multiple Times

If Novell SecureLogin is installed on a Citrix server in Novell Client mode, and if you select the *Workstation Only* option when restarting Windows on that Citrix server, a message indicating "`You are not logged in to a directory and SecureLogin was unable to find any cached user data`" is displayed.

This message appears twice before you are authenticated.

### 6.1.3  Unable To Delete Logins from the Manage Logins Window

In some scenarios, in the Novell SecureLogin Client Utility, users are unable to delete the logins from the *My Logins* navigation area on the left pane. When users right-click the login, both *Delete* and *Rename* options are disabled.

However, the login can be deleted from the right pane.

### 6.1.4  Unable To Instantiate Scriptbroker Module: 80070005

When a Web page could not send information to SecureLogin by using a different method, the following error message is shown:

"Unable to instantiate scriptbroker module: 80070005"

To resolve this error, uninstall SecureLogin, delete its installation directory, and also delete the registry hive: hklm/software/protocom; then, reinstall SecureLogin.

This workaround resolves this error for all Web pages, including the Web page that produced this error.

If the problem persists, re-register some of the SecureLogin dll files, as follows:

regsvr32 "C:\Program Files\Novell\SecureLogin\iesso.dll

regsvr32 "C:\Program Files\Novell\SecureLogin\slbroker.dll

regsvr32 "C:\Program Files\Novell\SecureLogin\slcaptain.dll

### 6.1.5  Using Unique Names

User IDs, applications, and password policies must all have unique names. Additionally, you cannot create an application named Error.

If you install SecureLogin with the SecretStore client in the eDirectory mode, you cannot add an application and name it App1 (for example) if a password policy already exists with the name App1.

### 6.1.6  Manual Entry of the Smart Card PIN required for Citrix Server Authentication

If you are using smart card authentication for the Citrix login prompt, enter the smart card PIN manually, because the PIN is not cached for the Citrix server authentication.

### 6.1.7  Novell SecureLogin Login in LDAP GINA Mode with eDirectory

Novell SecureLogin in the LDAP GINA mode with eDirectory does not work while setting a passphrase for a new user if the eDirectory user's fully distinguished name (FDN) has 128 characters or more.

### 6.1.8  Validating an Old Password

In Microsoft Windows 2003 configurations, users might be able to login to their workstation by using the old password. Because the user has logged in successfully, Novell SecureLogin loads. A Windows 2003 server attribute (the password lifetime period) allows the re-use of an old password.

To disable an old password as soon as a password change occurs, update the domain controller registry setting with the following value:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

Create new DWORD value OldPasswordAllowedPeriod

Set this value to 0.

For more information, see the Microsoft Web site. (http://support.microsoft.com/kb/906305).

### 6.1.9  Error Message on No Password Policy Is Available

If password policies already exist, ignore the incorrect error message 0 password policy that is shown when restoring user data.

## 6.2  Application Definition Wizard Issue

◆ "Credentials Fields Are Dimmed" on page 7

### 6.2.1  Credentials Fields Are Dimmed

The *Username* and *Password* fields in *Add Application > Identity Fields* are dimmed when the *Navigate to field using keystroke* option is selected. Deselecting the keystroke option does not automatically enable these fields.

This occurs because when you select the *Navigate to field by using keystrokes* option, it disables the link to the specified control. When you de select this option, the wizard cannot automatically detect the fields again. You must manually select the fields by dragging the *Choose* icon to the required text field.

## 6.3  DAS Issue

◆ "Using iManager Fails to Extend the DAS Schema" on page 7
◆ "DAS Related Data Are Not Stored in the Log File" on page 8

### 6.3.1  Using iManager Fails to Extend the DAS Schema

The DAS schema extension fails to extend correctly through iManager because of a defect in the Import Conversion Export utility of eDirectory.

Use one of the following workarounds to resolve the issue.

◆ **Using ConsoleOne:** Browse to *Tools > Schema > Add Attribute > Add Class*. Specify the attribute information.
◆ **Using the ndssch Command Line Utility:** Use the ndssch utility to extend the schema. The utility is bundled with eDirectory.

  Use the -h option and specify the IP address of the NetWare workstation where you want to extend the schema.

  **NOTE:** You can use the utility from any workstation on which eDirectory is installed.

### 6.3.2  DAS Related Data Are Not Stored in the Log File

On Windows 7 and Windows Vista, the log file for the DAS feature does not store the DAS related data when UAC is enabled. Changing the `DASLog.txt` file path from the installation location to `C:\` enables the log file to store DAS related data.

## 6.4  LDAP Issues

### 6.4.1  Control Panel Menu Is Slow to Respond

If you launch the Control Panel from the *Start* menu when LDAPAuth GINA is running on the client, the Control Panel takes more than 20 seconds to display.

### 6.4.2  ?syspassword Reflects Universal Password

When SecureLogin is installed in LDAP mode and NMAS authentication is used, ?syspassword reflects the universal password for the logged-in user.

In this mode of operation, it is mandatory to configure and set universal password for the NMAS user.

### 6.4.3  Could Not Load an Application

Using the SecureLogin wizard, you can configure a .NET application in the LDAP mode for its login credentials, change password option, change password notification, and so on.  Performance of the configured application depends upon its size (usually 64 KB maximum) and the number of associated controls (usually 10 controls maximum). If the size and number of controls occupy a huge space in the system, the application fails to load in the next login attempt. Therefore, convert such an application into an application definition and reduce its size before logging in.

## 6.5  pcProx Issues

### 6.5.1  pcProx Identification

pcProx identification fails in Novell Client on Microsoft Windows 2008 and Windows 7, on the first attempt for a new user. An error message indicating the system cannot log in to the network appears and prompts the user to verify the credentials.

So, during the first attempt, log in to Novell Client using NMAS pcProx sequence. pcProx identification happens correctly in the subsequent logins.

### 6.5.2 pcProx Unlock Operation in Citrix Session

Unlocking a Citrix* session by using the NMAS pcProx sequence does not work. That is, if a remote Citrix session is locked by using the Secure Workstation QLL GUI or by using the Windows screen saver option, the unlock operation through the NMAS pcProx sequence does not function.

## 6.6 Scripting Issue

* "Novell GroupWise 7.0 Web Login Prebuilt Script" on page 9

### 6.6.1 Novell GroupWise 7.0 Web Login Prebuilt Script

In a Windows Vista environment, the prebuilt Novell GroupWise WebAccess script is not detected although the script exists in the application area of the Novell SecureLogin client.

The user is not prompted to use the script. Novell SecureLogin fails to run the script.

To resolve this issue, add the prebuilt script to the list of application definitions.

## 6.7 SecretStore Issue

* "SecretStore on the Server" on page 9

### 6.7.1 SecretStore on the Server

If you plan to use Novell SecretStore on the client (SecretStore mode), install or upgrade to SecretStore 3.3.5 or later on the server before selecting the SecretStore option during the client install.

## 6.8 Secure Workstation Issue

* "Secure Workstation Session Management Process Is Blocked" on page 9
* "Using the NMAS Login with the Secure Workstation Sequence on a Microsoft Windows Vista Desktop" on page 10
* "Login Fails When the Secure Workstation Post-Login Method Is Added to the Login Sequence" on page 10

### 6.8.1 Secure Workstation Session Management Process Is Blocked

When an administrator logs into the workstation in which User Access Control is enabled, the Secure Workstation Session Management Process is blocked; and, an error message is shown.

On Windows 7, the workaround is to manually run the process.

On Windows Vista, directly unblock the process from the taskbar. If it is not unblocked, you cannot log in by using the NMAS secure workstation sequence; and, would see the error message: `Error 740: Secure Workstation Session Management Process is blocked. Unblock to continue.`

This error occurs only for a user with administrator privileges, and not for a user with non-administrator privileges (that is, a standard user).

For detailed information, see the Microsoft Developer Network Web site. (http://msdn.microsoft.com/en-us/library/bb325654.aspx).

### 6.8.2 Using the NMAS Login with the Secure Workstation Sequence on a Microsoft Windows Vista Desktop

On a Microsoft Windows Vista desktop, when the administrator uses the NMAS login with Secure Workstation sequence without the administrator unblocking the Secure Workstation session management process (wsaccsmp), the NMAS login fails with error code 740.

The issue exists when the NMAS login is used with the Novell Client or Novell SecureLogin-LDAP Client.

### 6.8.3 Login Fails When the Secure Workstation Post-Login Method Is Added to the Login Sequence

The Secure Workstation policy fails when set through iManager, because the Post-Login method fails for SUSE Linux Enterprise Server 10 and eDirectory 8.8 SP1.

However, users can use the Secure Workstation Policy setting through the client policy.

## 6.9 Smart Card Issues

- "Incorrect Smart Card Error Message" on page 10
- "Failure to Access Smart Card" on page 10
- "Failure to Launch SecureLogin without User Principal Name" on page 10
- "Smart card re-authentication failed when NSLADAuth is set to 1" on page 11
- "SecureLogin fails to launch when Use Smart to encrypt SSO Data is set to Key generated on smart card" on page 11
- "SecureLogin System tray icons does not get cleared during fast user switching using smart card" on page 11

### 6.9.1 Incorrect Smart Card Error Message

If a user logs in without the smart card when the *Use Smart card to encrypt SSO Data* preference is set to *PKI Credentials* and *Enable Passphrase Passphrase Security System* preference is set to *No*, he or she is not prompted for smart card.

Instead, the user gets an incorrect message `The smartcard does not contain any certificates that match the certificate selection criteria`, is displayed.

### 6.9.2 Failure to Access Smart Card

If the PKCS#11 wrapper library file `aetpksse.dll` is missing, the error message `Access to smart card failed` is shown when the Access Manager attempts to access the smart card. To avoid this error, ensure that the `aetpksse.dll` file is available at `C:\WINDOWS\system32\`.

### 6.9.3 Failure to Launch SecureLogin without User Principal Name

Novell SecureLogin fails to launch using smart card authentication without User Principal Name, when *Use Smart card to encrypt SSO Data* is set to *No*.

This problem can be resolved if you use any of the following options:

- *Use Smart card to encrypt SSO Data* preference is set to *PKI Credentials*.
- Smart Card must be configured with User Principle Name.

### 6.9.4  Smart card re-authentication failed when NSLADAuth is set to 1

In offline mode, the smart card re-authentication fails when *NSLADAuth* is set to *1* and when the workstation is not connected to the network.

### 6.9.5  SecureLogin fails to launch when Use Smart to encrypt SSO Data is set to Key generated on smart card

When *Use smart card to encrypt SSO Data* is set to *Key generated on smart card*, SecureLogin fails to launch and a error message is displayed, `Smart Card is required for New single Sign on user.`

To resolve this problem, *Use smart card to encrypt SSO Data* must be set to default or *PKI Credentials*.

### 6.9.6  SecureLogin System tray icons does not get cleared during fast user switching using smart card

Novell SecureLogin system tray icons does not get cleared during fast user switching using smart card. By hovering the mouse over the SecureLogin system tray icons, the SecureLogin system tray icons will be cleared.

## 6.10  TLaunch Issues

- "TLaunch Shortcut Command Line /n Switch" on page 11
- "TLaunch Fails to Add New Emulators or Save the Changed Configuration of Existing Emulators" on page 11
- "Prompt to Close Windows Explorer During Upgrade" on page 12

### 6.10.1  TLaunch Shortcut Command Line /n Switch

There is a known issue with the TLaunch shortcut command line `/n` (Number) switch.

Contact Novell Support for information.

### 6.10.2  TLaunch Fails to Add New Emulators or Save the Changed Configuration of Existing Emulators

When you launch TLaunch and search for the available emulators, TLaunch fails to detect a newly created emulator.

TLaunch also fails to save the changes made to one of the existing emulators.

However, you can add and edit emulators on Microsoft Windows and Windows XP.

As a workaround, click *Start > Programs > Novell SecureLogin*, Right click *Terminal Launcher*, then select *Run as Administrator*.

### 6.10.3  Prompt to Close Windows Explorer During Upgrade

If you have installed Novell SecureLogin in LDAP mode on a Microsoft Windows Vista machine, during upgrade from version 6.1 or 6.1 SP1 to 7.0 you are prompted to close the Windows Explorer.

Click *Ignore* to proceed with the upgrade.

## 6.11  Upgrade Issues

- ◆ "Upgrading with Customized Version of Novell SecureLogin" on page 12
- ◆ "SLMANAGER.EXE is installed automatically during the upgrade" on page 12
- ◆ "Prompt for Password When Notification Area Icon is Password Protected" on page 12

### 6.11.1  Upgrading with Customized Version of Novell SecureLogin

When upgrading to 7.0 from a customized version of Novell SecureLogin (customized bitmaps, `LocalHero.dll`, and similar files), the new version replaces the customized file with the standard files.

To retain the customized setting, do one of the following:

- ◆ Replicate the customized settings on Novell SecureLogin 7.0 MSI.
- ◆ Take a backup of the customized file and apply it after upgrade.

### 6.11.2  SLMANAGER.EXE is installed automatically during  the upgrade

When upgrading from SecureLogin 6.0 to SecureLogin 7.0, `SLMANAGER.EXE` is automatically installed. There is no option available to stop the installation of `SLMANAGER.EXE` during the upgrade process.

To workaround this issue, create a `.bat` file with the following lines to manually delete `SLMANAGER.EXE`:

```
@echo off
del "C:\Documents and Settings\All Users\Start Menu\Programs\Novell
SecureLogin\SecureLogin Manager.lnk"
del "C:\Program Files\Novell\SecureLogin\slmanager.exe"
```

### 6.11.3  Prompt for Password When Notification Area Icon is Password Protected

During upgrade from Novell SecureLogin 6.1 to 7.0, if the Password protect the system tray icon preference is enabled users are prompted to provide the network password.

To workaround the issue:

**1** Stop Novell SecureLogin manually before starting to upgrade.

or

Run `slproto/forceshutdown` from the commandline to shutdown Novell SecureLogin

**NOTE:** If you stop SecureLogin manually, you are prompted to specify the password.

If you use the slprotoc/forceshutdown command, you are not prompted to specify t he password.

**2** Start the upgrade.

**3** Specify the correct credentials.

## 6.12 Web-Related Issues

- ◆ "Accessing Web Applications from a Windows 2003 Server" on page 13
- ◆ "Firefox Issue During Installation" on page 13
- ◆ "Not Prompted for Credentials" on page 13
- ◆ "Java Applet Is Not Loading" on page 13

### 6.12.1 Accessing Web Applications from a Windows 2003 Server

Web applications directly accessed through Internet Explorer on a Microsoft Windows 2003 server might not work correctly until the *Windows Enhanced Security* option is disabled on the server. Alternatively, you can go to *Internet Options > Advanced* and enable the third-party Web browser extensions.

This however, does not impact clients connected to a Microsoft Windows 2003 server.

### 6.12.2 Firefox Issue During Installation

Start Mozilla Firefox at least once before installing Novell SecureLogin. Otherwise, a message prompting you to import Internet Explorer settings, is displayed during the Novell SecureLogin installation.

If this happens, click *Import* to import the Internet Explorer setting or click *Cancel* to cancel the import. The Novell SecureLogin installation proceeds.

### 6.12.3 Not Prompted for Credentials

When a DHTML enabled Web application is started, SecureLogin fails to prompt for entering the credentials. The error occurs when SecureLogin fails to run the predefined application definition to enable single sign-on for the site. Close the browser session and relaunch the Web application as a workaround to resolve this issue.

### 6.12.4 Java Applet Is Not Loading

Performance issues occur while loading Java applet of some applications. The workaround to resolve this issue is to comment out the `JavaSSOHook` property from the `accessibility.properties` and `awt.properties` files.

## 6.13 Oracle Form Issues

### 6.13.1 Support for Oracle Forms

Novell SecureLogin 7.0 SP1 supports Web enabled Oracle form applications. Therefore, Oracle JInitiator and JRE should be available in the system where Novell SecureLogin 7.0 SP1 will be used. If any of them is not present in the machine where Novell SecureLogin is already running, add the missing Java components in the machine, and then run the repair option available with the SecureLogin installer; the repair option of the installer adds the new Java component to be used for Oracle form applications.

### 6.13.2  Authentication Fields Shown on Two Windows

Clicking the *Show Me* button shows authentication fields in an application being defined in the Application Definition Wizard. When defining an Oracle form that is run from a browser, the identified fields might get shown not only on the Oracle form, but also on the browser. You may ignore this behavior.

### 6.13.3  Naming an Oracle Form Application

The Java component assigns a name taken from the title field of the innermost container to an Oracle form application. If the innermost container is not assigned with a title when the forms are created, the wizard cannot assign a name to the Oracle form application.

### 6.13.4  Application Definition Consumes Time to Open

Loading of Oracle components requires some time before an application definition for Oracle form is started. Therefore, the Wizard consumes some time when starting the application definition for Oracle form.

## 6.14  The Client Login Extension Issues

- "Specified Text is Not Displayed" on page 14
- "Forgotten Password Link Is Not Working" on page 14

### 6.14.1  Specified Text is Not Displayed

Using Client Login Extension tool, you can specify the text to be shown when a user clicks the *Did you forget your Password ?* link. The text specified for the Novell Client is not shown when the link is clicked.

### 6.14.2  Forgotten Password Link Is Not Working

Using the Forgotten Password link to recover the password forgotten for a locked workstation does not work on Microsoft Credential Provider for Novell Client.

# 7  Documentation Conventions

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

A trademark symbol ($^{®}$,™, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark.

# 8  Legal Notices

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