

# Novell SecureLogin 6.1 Support Pack 1 Readme

June 30, 2009

Novell®

## 1 Documentation

The following sources provide information about Novell® SecureLogin 6.1 Support Pack 1 (SP1):

- ♦ Overview: *Novell SecureLogin 6.1 SP1 Overview Guide*
- ♦ Installation: *Novell SecureLogin 6.1 SP1 Installation Guide*
- ♦ Administration: *Novell SecureLogin 6.1 SP1 Administration Guide*
- ♦ Application Definition: *Novell SecureLogin 6.1 SP1 Application Definition Guide*
- ♦ Citrix and Terminal Services: *Novell SecureLogin 6.1 SP1 Citrix and Terminal Services Guide*
- ♦ Quick Start: *NMAS Login Method and Login ID Snap-In for pcProx*
- ♦ User Manual: *Novell SecureLogin 6.1 SP1 User Guide*
- ♦ Online product documentation: [Novell Documentation Web site. \(http://www.novell.com/documentation/securelogin61/index.html\)](http://www.novell.com/documentation/securelogin61/index.html)

## 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.

## 3 Troubleshooting

During a fresh install of Novell SecureLogin 6.1 SP1, if you are prompted to upgrade, delete all references to the product key and then continue with the installation.

---

**NOTE:** Take a backup of the registry keys before deleting.

---

- 1 Click Start > Run > type regedit.
- 2 Search for 80D1DD4E-85FD-4978-B010-9C480B10DF18 in the registry keys.
- 3 Delete the references to the product key.

## 4 Integration of Desktop Automation Services

With this release of Novell SecureLogin, you can choose to install Desktop Automation Services (DAS) along with Novell SecureLogin.

Previously, DAS was released as a standalone component that you downloaded separately for use with Novell SecureLogin. With this release, you can install DAS during the installation of Novell SecureLogin 6.1 SP1. Select the Install Desktop Automation Services option on the Installation Features page when you install Novell SecureLogin 6.1 SP1.

## 5 Known Issues in 6.1 SP1

- ◆ [Section 5.1, “In a Lost Card Scenario Novell SecureLogin Repeatedly Prompts for Smart Card,” on page 2](#)
- ◆ [Section 5.2, “Deploying Novell SecureLogin in Shared Workstations,” on page 2](#)
- ◆ [Section 5.3, “Using Smart Cards to Enable Single Sign-On For Web Applications,” on page 3](#)
- ◆ [Section 5.4, “SLManager Displays History of LDAP Tree Browser,” on page 3](#)
- ◆ [Section 5.5, “The Workstation Only Option Is Selected in LDAP GINA Mode,” on page 3](#)
- ◆ [Section 5.6, “Grace Logins During Initial Authentication in GINA Mode,” on page 3](#)
- ◆ [Section 5.7, “Users Are Prompted to Specify Offline Credentials after Disconnecting from the Network,” on page 4](#)
- ◆ [Section 5.8, “Error in Installing DAS,” on page 4](#)
- ◆ [Section 5.9, “In SLManager, the Leaf Objects Are Displayed Like Container Objects,” on page 4](#)
- ◆ [Section 5.10, “On a Workstation Only Login, the User Is Prompted for a Username,” on page 4](#)
- ◆ [Section 5.11, “Ability To Search Through LDAP on SamAccountName Ported from 6.0 to 6.1,” on page 5](#)

### 5.1 In a Lost Card Scenario Novell SecureLogin Repeatedly Prompts for Smart Card

In a lost card scenario when a user tries to log in to Novell SecureLogin, the user is prompted to insert the smart card four times before displaying a message indicating SecureLogin failed to access the smart card.

The user is not prompted with the passphrase and so, cannot login. This happens because the Security preference *Lost card scenario* is set to *Require smart card* and *Enable passphrase security system* is set to *No*.

To continue with the log in, the user must either retrieve the original smart card or get a replacement card.

### 5.2 Deploying Novell SecureLogin in Shared Workstations

If Novell SecureLogin is deployed in a shared workstation where more than one user shares the local credentials, users must either use Secure Workstation or DAS to close all programs and log out of the network.

The option is mandated because,

- ♦ If a user who has logged in to Novell SecureLogin in Novell Client™ mode in Microsoft\* Windows\* Vista\* or Microsoft Windows XP or in LDAP mode (in Microsoft Windows Vista) locks the workstation and later tries to unlock using the workstation credentials, Novell SecureLogin fails to log off the directory user.

However, the directory user is still logged in and Novell SecureLogin continues to run. Because of this, the user who has logged in using workstation credentials has access to the directory credential store.

In such a scenario, avoid using the workstation lock. Instead, use secure workstation or DAS to configure the workstation to close all programs and log out of the network on an inactivity timer.

### **5.3 Using Smart Cards to Enable Single Sign-On For Web Applications**

If you have used a smart card to store the credentials when enabling single sign-on for Web applications such as Gmail\*; the next time you access the Web site with the smart card removed, you are prompted to insert the smart card. If you cancel the message, SecureLogin closes. An error might also occur in executing the application definition.

### **5.4 SLManager Displays History of LDAP Tree Browser**

SLManager displays the history of the LDAP tree browser. A maximum of 20 history entries are available. History data beyond 20 entries are overwritten to the first data entry. This is not a limitation in Novell SecureLogin. This is working as per design.

You can view the history from *Start > Run > regedit > HKCU > Software > Protocom > SLManager*.

### **5.5 The Workstation Only Option Is Selected in LDAP GINA Mode**

If the `HKLM\Software\Protocom\SecureLogin\TryRegCredinOffline` registry value is set to 1 when Novell SecureLogin is installed in LDAP GINA or Credential Provider mode, Novell SecureLogin behaves in the following ways:

- ♦ If the user logs in to the workstation by selecting the *Workstation Only* option, the user logs in to Novell SecureLogin seamlessly and the desktop is launched.
- ♦ If network connection is not available, the workstation dialog box appears. After successful authentication, users can log in after and the desktop is launched.
- ♦ If the server is not accessible, Novell SecureLogin authenticates to the workstation with the user's credentials. Users can then seamlessly log in to Novell SecureLogin.

### **5.6 Grace Logins During Initial Authentication in GINA Mode**

In the 6.1 release, at the initial login in GINA mode, if the eDirectory password had expired the user was not warned of the password expiry. Instead, the user was successfully authenticated without any notification.

The user was warned about the password expiry and the number of grace logins available only Novell SecureLogin starts after the Desktop appears. The user was then prompted to change the password.

This is now rectified and a warning is displayed at the initial login.

## 5.7 Users Are Prompted to Specify Offline Credentials after Disconnecting from the Network

Novell SecureLogin fails to go seamlessly into offline mode on subsequent logins where Novell SecureLogin is installed in LDAP GINA mode and is disconnected from the network, and eDirectory™ or any LDAP directory is online. Because of this, users are prompted to specify the offline credentials.

To avoid prompting for credentials and allow Novell SecureLogin to go to offline mode seamlessly, edit the registry and set the `TryRegCredInOffline` value to 1.

## 5.8 Error in Installing DAS

When you install DAS in eDirectory mode with Novell Client™, sometimes an error indicating *Error in parsing xml file during install* appears. This occurs because the server or the specified config object is invalid.

To rectify, ignore the message and proceed with the install. After the installation or restarting,

- 1 Log in as an administrator.
- 2 Set the `ConfigObject` and `ConfigTree` registries values correctly.

The `ConfigObject` is the `ArsControl` Object and the `ConfigTree` - Server or the Tree information. The registries are at `HKLM\Software\Novell\Login\ARS`

- 3 Run `ARSControl /RegServer`.

## 5.9 In SLManager, the Leaf Objects Are Displayed Like Container Objects

In SLManager, the leaf objects are displayed like the container objects. That is, you see a folder icon and a plus (+) symbol when you use SLManager to open the directory leaf objects.

If you click the plus symbol, the folder icon changes to the file icon.

## 5.10 On a Workstation Only Login, the User Is Prompted for a Username

During the Workstation Only login, if the workstation or local credentials are not the same as the eDirectory credentials, the user is prompted for credentials. Novell SecureLogin fails to seamlessly log in the user.

To allow seamless login, users must manually change the `DWORD` value of the `TryRegCredOffline` registry entry to 1.

## 5.11 Ability To Search Through LDAP on SamAccountName Ported from 6.0 to 6.1

For LDAPAuth to search on any attributes specified in SearchAttributes under the LDAPSearch key, the attribute must be publicly readable.

- 1 Create the LDAPSearch key in the registry under HKLM\Software\Novell\Login\LDAP.
- 2 Under HKLM\Software\Novell\Login\LDAP, create a SearchAttributes *REG\_MULTI\_SZ* entry.
- 3 In the entry you just created, use the value of the attribute list that you want LDAP to search, for example, cn sn samAccountname.

To enable LDAP search for sAMccountName attribute, the previous Anonymous Logon requires Read General Information and Read Public Information permissions.

## 6 New Features Introduced in 6.1

- ♦ Section 6.1, “Vista Support,” on page 5
- ♦ Section 6.2, “MSI Install Package,” on page 5
- ♦ Section 6.3, “Support for Novell Group Policy,” on page 6
- ♦ Section 6.4, “Smart Card Login,” on page 6
- ♦ Section 6.5, “Support For Smart Card Middleware,” on page 6
- ♦ Section 6.6, “Enhancement of Active Directory Group Support,” on page 7
- ♦ Section 6.7, “Improved Support for Citrix Published Applications,” on page 7
- ♦ Section 6.8, “Support for Multiple Java Runtime Engines,” on page 7
- ♦ Section 6.9, “Automatic Update of JREs at Runtime,” on page 7
- ♦ Section 6.10, “Support for Additional JRE Versions,” on page 7
- ♦ Section 6.11, “Support for MEDITECH,” on page 7
- ♦ Section 6.12, “Support for Desktop Automation Services,” on page 7
- ♦ Section 6.13, “Exporting Individual Scripts,” on page 8
- ♦ Section 6.14, “LDAP Credential Provider on Vista,” on page 8
- ♦ Section 6.15, “Support for Non-English Languages,” on page 8
- ♦ Section 6.16, “Additional Preferences,” on page 8

### 6.1 Vista Support

Novell SecureLogin 6.1 includes support for the Microsoft\* Vista\* operating system. Vista Ultimate, Vista Business, and Vista Enterprise editions are supported.

The install package supports both 32-bit and 64-bit operating systems.

### 6.2 MSI Install Package

This release of Novell SecureLogin introduces the MSI installer package for installing Novell SecureLogin.

---

**NOTE:** The MSI installer supports upgrading from the previous versions of Novell SecureLogin, which did not use an MSI installer.

---

For details, see the *Novell SecureLogin 6.1 SPI Installation Guide*.

## 6.3 Support for Novell Group Policy

This release of Novell SecureLogin introduces support for Novell eDirectory™ groups.

Novell SecureLogin preferences can now be applied at the group level, in addition to the container and user level support provided in the earlier releases.

You can specify the group from which the object inherits its Novell SecureLogin configuration through the *Configured Groups* option in the *Corporate redirection* tab of the *Advanced Settings* pane of the Administrative Management utilities.

Groups are configured at the container or the organizational unit level. Groups take precedence over containers, and users take precedence over groups and containers.

For more information, see “**Configuring Groups Within eDirectory**” in the *Novell SecureLogin 6.1 Administration Guide*.

## 6.4 Smart Card Login

This release of Novell SecureLogin introduces a change in the way the smart card preferences are handled.

If user is logging in to the workstation with a smart card, the smart card preference must be selected at installation even if the administrator sets preferences in Novell SecureLogin.

---

**NOTE:** This applies to all Microsoft Windows\* 2000, XP, and Vista workstation.

---

## 6.5 Support For Smart Card Middleware

Novell SecureLogin 6.1 supports ActivClient\*, Gemalto\* (formerly Axalto), and AET SafeSign\* smart card middleware for SecureLogin functions.

No other middleware vendors are supported.

This includes:

- ♦ Encrypting PKI credentials.
- ♦ Storing Novell SecureLogin credentials on a smart card.
- ♦ Enforcing smart card presence for Novell SecureLogin operations.

This preference is available in the Administrative Management utility under the *Security* preference as *Require Smart Card is present for SSO and administration operations*.

For more information on the *Security* preferences, see the “**The Security Preferences Properties Table**” table in the *Novell SecureLogin 6.1 Administration Guide*.

## 6.6 Enhancement of Active Directory Group Support

For Active Directory\* installations using the Microsoft Group Policy Object functionality, Novell SecureLogin now allows administrators to see the effective set of single sign-on settings that are applied through the group policies. This requires that the Microsoft Group Policy Management Console be installed on the administration workstation.

For more information, see the *Novell SecureLogin 6.1 SP1 Administration Guide*.

## 6.7 Improved Support for Citrix Published Applications

This release of Novell SecureLogin automates the published application single sign-on process for Citrix\* published applications. Citrix published applications can now be enabled for single sign-on through a Web wizard or application definition, like any other application.

## 6.8 Support for Multiple Java Runtime Engines

Novell SecureLogin now supports multiple instances of Java\* Runtime Engine (JRE\*). The installation detects and automatically enables single sign-on for multiple JREs on the client. This occurs automatically. No manual selection of Java options is required at installation.

## 6.9 Automatic Update of JREs at Runtime

After installation and on startup, Novell SecureLogin checks for new JREs on the client. All JREs are automatically enabled for single sign-on with no user prompt or intervention.

---

**NOTE:** This update process requires the user to have administrative rights on the local machine. If the user does not have administrative rights, the update process fails silently.

---

## 6.10 Support for Additional JRE Versions

This release supports Oracle\* JInitiator\* 1.3.1 and later and Sun\* JRE 1.3 and later.

## 6.11 Support for MEDITECH

Novell SecureLogin 6.1 supports MEDITECH\* 3.x and 4.x.

This feature depends on the presence of the MEDITECH `mrwscript.dll` file. This file must be installed during the installation of the MEDITECH application on the workstation.

For more information on MEDITECH support, see “[Support for the MEDITECH Predefined Application](#)” in the *Novell SecureLogin 6.1 Administration Guide*.

## 6.12 Support for Desktop Automation Services

Novell SecureLogin 6.1 supports Desktop Automation Services. Novell SecureLogin is mandatory for Desktop Automation Services to function.

Desktop Automation Services is an add-on to Novell SecureLogin that handles unique use cases associated with shared workstations or kiosks (multiple users using the same workstation during the day).

For more information, see the *Desktop Automation Services Administration Guide* at the [Novell Documentation Web site](http://www.novell.com/documentation/das20/index.html). (<http://www.novell.com/documentation/das20/index.html>)

## 6.13 Exporting Individual Scripts

With this release of Novell SecureLogin, administrators have the option to export all or selected scripts through the iManager SSO plug-in. A new dialog box prompts the administrator to select the scripts he or she wants to export.

For details, see the *Novell SecureLogin 6.1 SPI Installation Guide*.

## 6.14 LDAP Credential Provider on Vista

LDAP GINA is no longer supported on Windows Vista.

Instead, the LDAP credential provider replaces the LDAP GINA in Windows Vista.

## 6.15 Support for Non-English Languages

In this version, the approach for language support is different from the previous versions of Novell SecureLogin. In the earlier versions, the user was prompted to choose a language for the setup during the installation.

In this version of Novell SecureLogin, this option is not offered, and the installation uses English throughout.

However, you can use a command line option to install in non-English languages.

- 1 At the command line, specify the following command:

```
msiexec.exe /i "Novell SecureLogin.msi" TRANSFORMS=<lang-code>.mst
```

<lang-code> denotes a specific language.

- ♦ 1041 represents the Japanese language
- ♦ 1036 represents the French language
- ♦ 1046 represents the Brazilian language
- ♦ 1031 represents the German language
- ♦ 1034 represents the Spanish language

## 6.16 Additional Preferences

This release of Novell SecureLogin introduces some more Preference options that can be applied through any of the Administrative Management utilities: iManager, Microsoft Management Console, or SLManager.

These are administrative preferences only, not user preferences.

- ♦ Hiding the Novell SecureLogin splash screen when Novell SecureLogin is switched off.



- ◆ Removing the *Log Off User* option on the Novell SecureLogin notification area icon.
- ◆ Allowing the administrator to remove the *Close Novell SecureLogin* option from the Novell SecureLogin notification area icon.
- ◆ Disabling the *Refresh Cache* option in the Novell SecureLogin notification area icon.
- ◆ Disabling the *Work Offline* option in the Novell SecureLogin notification area icon.
- ◆ Enhancing the options for editing and deleting credentials.
- ◆ Separation of the *View* and *Change* scripts preference into two separate preferences.
- ◆ New settings in the Password Policy preference.

For detailed information of these preferences, see the *Novell SecureLogin 6.1 SPI Administration Guide*.

## 7 Known Issues in 6.1

Following are issues you might encounter in this version of Novell SecureLogin:

- ◆ [Section 7.1, “General Issues,” on page 9](#)
- ◆ [Section 7.2, “iManager Issues,” on page 18](#)
- ◆ [Section 7.3, “Java Issues,” on page 19](#)
- ◆ [Section 7.4, “LDAP Issues,” on page 20](#)
- ◆ [Section 7.5, “NMAS Issues,” on page 21](#)
- ◆ [Section 7.6, “pcProx Issues,” on page 22](#)
- ◆ [Section 7.7, “Scripting Issues,” on page 23](#)
- ◆ [Section 7.8, “SecretStore Issue,” on page 24](#)
- ◆ [Section 7.9, “Secure Workstation Issues,” on page 24](#)
- ◆ [Section 7.10, “TLaunch Issues,” on page 25](#)
- ◆ [Section 7.11, “Web-Related Issues,” on page 26](#)

### 7.1 General Issues

- ◆ [“Novell Client Login Fails After an Upgrade” on page 10](#)
- ◆ [“Installing Novell SecureLogin on a Citrix Server” on page 11](#)
- ◆ [“Single Sign-On For Microsoft Windows Vista Remote Desktop Client” on page 11](#)
- ◆ [“RDP On Microsoft Windows 2000 Domain Controller” on page 11](#)
- ◆ [“Logging In to a Citrix ICA Client with the Store on Card Option” on page 12](#)
- ◆ [“Modifying the Smart Card Support Option” on page 12](#)
- ◆ [“The Disable Passphrase Security System Option Appears During an Upgrade” on page 12](#)
- ◆ [“The Datastore Mode Display” on page 12](#)
- ◆ [“Incorrect Database Mode Version Displayed in the Novell SecureLogin About Window” on page 12](#)
- ◆ [“Availability of the Change Passphrase Option” on page 12](#)
- ◆ [“Selecting a Value for the Enable Passphrase Security System Preference” on page 13](#)

- ◆ “User Is Unable to Re-enter the Passphrase Answer” on page 13
- ◆ “LDAP Error 49” on page 13
- ◆ “Offline Message Is Displayed Multiple Times” on page 13
- ◆ “Unable To Delete Logins From the Manage Logins Window” on page 13
- ◆ “The Installation Is Interrupted” on page 14
- ◆ “During Novell SecureLogin Upgrade, Confusing Dialog Boxes Are Displayed” on page 14
- ◆ “Novell SecureLogin Fails When a User With the Same Name and Context in Two Different eDirectory Trees Tries To Log In To The Same Windows Machine” on page 14
- ◆ “Failure to Add Users In Standalone Mode After Upgrade” on page 14
- ◆ “Playing an AVI File For a Secure Workstation Inactivity Timeout Warning on Windows Vista” on page 14
- ◆ “NSL Does Not Recognize the Novell iFolder 2.1.x Client During Workstation Login” on page 14
- ◆ “NSL Is Not Exited When Users Cancel Logging into NSL in LDAP Mode” on page 15
- ◆ “Unable To Instantiate Scriptbroker Module: 80070005” on page 15
- ◆ “Users Cannot Use the Same Smart Card to Authenticate in Both eDirectory and LDAP Modes” on page 15
- ◆ “AES Encryption Is Not Supported on Windows 2000” on page 15
- ◆ “Case Sensitive Feature for Passwords Does not Work While Unlocking the Notification Area Icon” on page 15
- ◆ “Notification Area Icon Cannot Be Unlocked Using pcProx Authentication” on page 15
- ◆ “Cache Refresh Reduces the Grace Logins in LDAP Mode” on page 16
- ◆ “The NICI Client Is Not Uninstalled” on page 16
- ◆ “Using Unique Names” on page 16
- ◆ “Logging In after Uninstalling the ZENworks for Desktops Management Agent” on page 16
- ◆ “Manual Entry of the Smart Card PIN required for Citrix Server Authentication” on page 16
- ◆ “Issues in Updating the Datastore Version In Active Directory” on page 16
- ◆ “Login Required if the Enable Passphrase Security System Is Modified” on page 17
- ◆ “Cache Expiry” on page 17
- ◆ “ViewNow Terminal Emulator” on page 17
- ◆ “Using the ?syspassword Variable in Standalone Mode” on page 17
- ◆ “Using the SLLogging Manager on Microsoft Windows Vista” on page 17
- ◆ “Executing Event Commands” on page 17
- ◆ “Selecting Objects in SLManager” on page 17
- ◆ “Validating an Old Password” on page 18
- ◆ “QuickEdit Mode in the Telnet Window” on page 18

### **7.1.1 Novell Client Login Fails After an Upgrade**

The Novell Client™ login fails after upgrading Novell SecureLogin from 6.0 to 6.1 in the Novell Client mode.

To resolve this, do the following before upgrading the Novell SecureLogin client:

- 1 Upgrade NICI
- 2 Restart the client.

---

**IMPORTANT:** Restarting is mandatory.

---

- 3 Upgrade NMASTM.
- 4 Upgrade Novell SecureLogin.
- 5 Restart the client.

If the login to the Novell Client fails because of NICI, re-install NICI, and restart the client.

### 7.1.2 Installing Novell SecureLogin on a Citrix Server

When installing Novell SecureLogin on a Citrix server, although the Citrix server goes in to the install mode, it does not install Novell SecureLogin. To install, you must revert the Citrix server to the execute mode.

- 1 Go to the DOS prompt.
- 2 Type `change user/install` at the prompt.  
This puts the Citrix server in the install mode.
- 3 Press Enter.
- 4 Install Novell SecureLogin.

---

**WARNING:** Do not restart the server after completing the installation.

---

- 5 After completing the installation, go to the DOS prompt.
- 6 Type `change user/execute` at the prompt.
- 7 Press Enter.  
This reverts the Citrix server to the execute mode.
- 8 Restart the server.

### 7.1.3 Single Sign-On For Microsoft Windows Vista Remote Desktop Client

Novell SecureLogin might not pass the correct domain name while performing a single sign-on operation for the Microsoft Windows Vista Remote Desktop client in either the Novell Client or LDAP mode.

### 7.1.4 RDP On Microsoft Windows 2000 Domain Controller

To start an RDP session on a Microsoft Windows 2000 server that is a domain controller, the user must be added in the domain controller policy to act as part of the operating system.

This is Microsoft setting.

### 7.1.5 Logging In to a Citrix ICA Client with the Store on Card Option

When logging in to a Citrix ICA client with the *Store on Card* option set to *Yes*, application credentials added by the user during the Citrix session might not be stored on the card. The credentials are stored successfully in the directory.

### 7.1.6 Modifying the Smart Card Support Option

If you selected the smart card support option during the installation of Novell SecureLogin, do not attempt to modify and remove the smart card support option through the *Modify* option of the installer, or the secondary datastore (offline cache) might not be available.

---

**NOTE:** You can control user access to smart card options through Novell SecureLogin preferences.

---

### 7.1.7 The Disable Passphrase Security System Option Appears During an Upgrade

When you are upgrading the datastore from 3.5 to 6.0 and upgrading to Novell SecureLogin 6.1, if the *Disable passphrase security system* is set to *Yes*, a message indicating "Your cache files have lost synchronization with directory authentication data. Would you like to delete your cache files and have them re-created?"

Click *Yes* to load Novell SecureLogin successfully.

### 7.1.8 The Datastore Mode Display

The information displayed in the Novell SecureLogin About window is created at login. A change applied to the user's Database mode is not updated in the user's About window display until after the next login.

### 7.1.9 Incorrect Database Mode Version Displayed in the Novell SecureLogin About Window

If you view When you access Novell SecureLogin for the first time after providing the passphrase question and answer, the Database Mode in the About window (accessed from the Novell SecureLogin notification area icon) displays the Database mode version as 3.0 3.0 Data Present PP Enabled.

On subsequent logins, the correct version is displayed.

### 7.1.10 Availability of the Change Passphrase Option

If the administrator disables the *Enable passphrase security system* option when you have already set up the passphrase system, a warning message that the administrator has disabled the passphrase security system appears. The passphrase setting change is not applied until you accept the change. If you do not accept the change, you can continue using the passphrase security system. This is the expected behavior because it prevents an administrator from disabling the passphrase protection without the user's knowledge.

However if this occurs, the *Change Passphrase* option that is available through the *Advanced* menu on the Novell SecureLogin notification area is not available until the administrator resets the passphrase setting.

### 7.1.11 Selecting a Value for the Enable Passphrase Security System Preference

If the *Disable passphrase security system* option is set to *Yes* when configuring Novell SecureLogin 3.5, then you upgrade Novell SecureLogin from 3.5.x to 6.1 and upgrade the data store from 3.5 to 6.0, the *Enable passphrase security system* value is displayed as *Yes* in Novell SecureLogin 6.1.

---

**NOTE:** The *Disable passphrase security system* preference was changed to *Enable passphrase security system* in version 6 releases and above.

---

The *Enable passphrase security system* option must be set to *Hidden*, because the *Disable passphrase security system* value was set to *No* in Novell SecureLogin 3.5.

This issue appears only in SecureLogin Manager.

### 7.1.12 User Is Unable to Re-enter the Passphrase Answer

In a Microsoft Windows Vista environment, when you log in to Novell SecureLogin in an offline mode with an incorrect password, you are prompted to provide the passphrase answer. If an incorrect passphrase answer is specified, you are prompted to retry the authentication.

However, if you again provide a wrong password, instead of seeing a prompt for the passphrase answer, you are prompted to specify the password (that is, instead of the passphrase dialog box, the password dialog box is displayed).

Close and relaunch Novell SecureLogin to be prompted for the password first, then prompted for the passphrase answer if the incorrect password is specified.

### 7.1.13 LDAP Error 49

LDAP error 49 is thrown when you click *Cancel* in the NDS<sup>®</sup> password prompt window when NMAS-NDS authentication is used with LDAP.

Click *OK* in the error window to proceed with the login.

### 7.1.14 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.

### 7.1.15 Unable To Delete Logins From the Manage Logins Window

In some scenarios, in the Personal Management 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.

### **7.1.16 The Installation Is Interrupted**

User Account Control (UAC) is a new setting on Microsoft Windows Vista. If the UAC is enabled during the installation of Novell SecureLogin, you are prompted about whether you want to continue with the installation process. If you do not respond to the prompts for a long time, a screen saver might come up (depending on the desktop setting) and interrupt the installation process, requiring you to restart the installation.

If the UAC prompts must be avoided, the administrator must disable the UAC setting within the Microsoft Windows Vista.

### **7.1.17 During Novell SecureLogin Upgrade, Confusing Dialog Boxes Are Displayed**

There are two modes in a server-based Windows operating system: Install and Execute.

While upgrading Novell SecureLogin on Microsoft Windows 2003, the administrator must be in the Install mode or must switch to the Install mode.

Even when the administrator continues to upgrade Novell SecureLogin in the Install mode, the dialog boxes might be confusing about whether to click *Finish* before or after the upgrade is complete.

Click *Finish* to proceed and complete the upgrade.

### **7.1.18 Novell SecureLogin Fails When a User With the Same Name and Context in Two Different eDirectory Trees Tries To Log In To The Same Windows Machine**

When a user with the same name and context in two different eDirectory trees tries to log in to the same Windows machine, an error message “Your Cache files have lost synchronization with your directory data. Would you like to delete your local cache files have them re-created?” appears.

When the user clicks *OK* and proceeds, user credentials of the previous user with same name are deleted and the cache file has only the credentials of the newly logged in user with same name.

### **7.1.19 Failure to Add Users In Standalone Mode After Upgrade**

When you upgrade Novell SecureLogin from 3.51 SP3 to Novell SecureLogin 6.1 in standalone mode, then decide during Novell SecureLogin upgrade that you do not want to move to seamless mode, after the upgrade the user cannot add new users to the standalone Novell SecureLogin client.

### **7.1.20 Playing an AVI File For a Secure Workstation Inactivity Timeout Warning on Windows Vista**

Playing an AVI file from a network mapped drive as part of an Inactivity timeout warning does not work on Windows Vista.

The workaround is to copy the file to a local drive and set the local path in Secure Workstation in the policy editor.

### **7.1.21 NSL Does Not Recognize the Novell iFolder 2.1.x Client During Workstation Login**

When a user logs in to a workstation, NSL does not automatically recognize the Novell iFolder<sup>®</sup> 2.1.8 login window at startup.

The workaround is to manually add the Novell iFolder prebuilt script and login again to the workstation, after which NSL identifies the iFolder 2.1.8 login window.

#### **7.1.22 NSL Is Not Exited When Users Cancel Logging into NSL in LDAP Mode**

On the Windows 2000 server, when a user cancels logging into NSL in LDAP mode, a SecureLogin message prompts the user to select whether to perform SSO or not. In this scenario, using SSO to connect to a Web application might result in crashing Internet Explorer\*.

#### **7.1.23 Unable To Instantiate Scriptbroker Module: 80070005**

Some Web pages are configured in such a way as to provide information to SecureLogin in a different manner. When working on such Web pages, user can encounter the “Unable to instantiate scriptbroker module: 80070005” error message.

In such scenarios, set the following registry key:

```
IESSO_USE_COM reg setting (Dword - value '0') under  
\HKEY_LOCAL_MACHINE\SOFTWARE\protocom\securelogin
```

This registry key changes the method of interprocess communication between SecureLogin processes, providing a workaround to the Web issue. It will work across all Web pages, not only on the Web page producing the error.

#### **7.1.24 Users Cannot Use the Same Smart Card to Authenticate in Both eDirectory and LDAP Modes**

If a user tries to log into SecureLogin in the LDAP mode, using the same smart card used to authenticate in eDirectory mode, the authentication fails. This is because SecureLogin smart card implementation sees them as two different users.

#### **7.1.25 AES Encryption Is Not Supported on Windows 2000**

The security preference to use the AES algorithm to encrypt the SSO data in the directory can only be used with Windows Vista, XP, or 2003 machines and not Windows 2000, because Windows 2000 does not support the Microsoft cryptographic libraries.

#### **7.1.26 Case Sensitive Feature for Passwords Does not Work While Unlocking the Notification Area Icon**

When installed in Client32™ mode, SecureLogin does not take into account the case sensitivity of passwords while unlocking the notification area icon, if the Novell Client™ 4.91 SP2 is used. To use this feature, update the Novell Client to version 4.91 SP3.

#### **7.1.27 Notification Area Icon Cannot Be Unlocked Using pcProx Authentication**

You cannot unlock the SecureLogin notification area icon using the NMAS pcProx authentication. Unlock the icon by using the passphrase if you have enabled one, or by using your directory password. Alternatively, you can set and use a universal password.

### 7.1.28 Cache Refresh Reduces the Grace Logins in LDAP Mode

If Novell SecureLogin is installed in LDAP mode and the LDAP user password expires, the number of grace logins is reduced by one every time the cache login is refreshed. This happens because every time the cache is refreshed, SecureLogin tries to re-authenticate to the directory.

### 7.1.29 The NICI Client Is Not Uninstalled

Novell International Cryptography Infrastructure (NICI) is installed automatically when SecureLogin is installed in any of the following modes:

- ◆ LDAP
- ◆ eDirectory with LDAP
- ◆ eDirectory with Client32 as the protocol and Novell SecretStore is selected for installation

However, if you uninstall SecureLogin, the NICI client remains because other Novell services (for example, NMAS, Novell Client, and SecretStore) might also need the NICI client.

If you plan to uninstall the NICI client, ensure that it is no longer needed before you remove it. To uninstall the NICI client, use *Add/Remove Programs*.

### 7.1.30 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.

### 7.1.31 Logging In after Uninstalling the ZENworks for Desktops Management Agent

Under the following conditions, you might not be able to log in to your workstation:

- ◆ ZENworks<sup>®</sup> for Desktops 4.0.1 Management Agent is installed.
- ◆ SecureLogin is installed
- ◆ You uninstall the ZENworks for Desktop Management Agent and then restart the workstation.

To solve the problem:

- 1 Start the workstation in Safe mode.
- 2 Copy the `nwgina.dll` file to the `windows\system32` directory.

### 7.1.32 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.

### 7.1.33 Issues in Updating the Datastore Version In Active Directory

In Active Directory's MMC, the current datastore version (displayed in the *Advanced Settings* page) might not update immediately when the directory database version is changed. To update, click *OK*, then exit the MMC Properties dialog box.



### 7.1.34 Login Required if the Enable Passphrase Security System Is Modified

If the *Enable passphrase security system* option is modified, you must log in again before launching SecureLogin for the settings to take effect.

### 7.1.35 Cache Expiry

Novell SecureLogin supports setting a cache expiry by using the following registry entry on the client:

```
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin
```

DWORD Value CacheExpiryDays

The value data is the number of days. Do not provide zero (0) because the cache would expire immediately on refresh. The cache expiry period is updated at each cache or directory synchronization, or each time Novell SecureLogin loads in an online mode.

---

**NOTE:** No warning is provided at cache expiry. If a cache is expired, the users cannot access Novell SecureLogin in an offline mode until they log in, and create the cache again in an online session.

---

### 7.1.36 ViewNow Terminal Emulator

Contact Novell Support for information on using a ViewNow\* terminal emulator.

### 7.1.37 Using the ?syspassword Variable in Standalone Mode

The ?syspassword variable does not work in standalone mode.

Because smart card options cannot be selected in a standalone mode installation, smart card login to standalone mode installs is not supported.

### 7.1.38 Using the SLogging Manager on Microsoft Windows Vista

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

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

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

### 7.1.39 Executing Event Commands

The Novell SecureLogin application definitions containing the event commands are not executed on existing applications that are opened before launching Novell SecureLogin. The event commands work correctly if Novell SecureLogin is launched before the application is started.

### 7.1.40 Selecting Objects in SLManager

In SLManager, select the objects from the left pane network list instead of selecting from the drop-down list.

### 7.1.41 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). (<http://support.microsoft.com/kb/906305>)

### 7.1.42 QuickEdit Mode in the Telnet Window

Some commands are not working in Telnet windows on Microsoft Windows XP, 2003, and Vista because the default configuration for Telnet has changed.

This issue does not occur on Windows 2000 because the configuration for *Quick Edit Mode* is set to *On*.

On the operating systems, the configuration for *Quick Edit Mode* is off. Because of this, the current adapter is unable to select the screen text.

As a workaround, set the following registry key:

```
HKEY_CURRENT_USER\Console\%SystemRoot%\_system32_telnet.exe
```

```
"QuickEdit"=dword:00000001
```

## 7.2 iManager Issues

- ◆ “Applications, Preferences, and Policies Added at the Group Level” on page 18
- ◆ “Web Wizard Application Support” on page 19
- ◆ “The System Is Slow to Respond” on page 19
- ◆ “Security Tab Options Not Visible in iManager after Upgrading” on page 19

### 7.2.1 Applications, Preferences, and Policies Added at the Group Level

The applications and policies added at the group level through iManager are not reflected on the client.

Every time a new group is created, you must re-assign the rights. You must manually assign read permissions for the correct functioning of the configured group.

Do the following on iManager for the applications, preferences, policies, and others added at the level to be reflected on the client:

- 1 Log in to iManager.
- 2 Select *Rights > Modify Trustees*.

- 3 Specify the object name.
- 4 Click *Add Trustee*. Browse and locate more objects.  
Selection of multiple trustees is allowed.
- 5 Select *Assigned Rights > Add Properties*. Add the following attributes:
  - ♦ Proto:SSO Entry
  - ♦ Proto:SSO Entry Checksum
  - ♦ Proto:SSO Security Prefs
  - ♦ Proto:SSO Security Prefs Checksum
- 6 Click *OK*.
- 7 Click *Done* to save the changes and exit.

### 7.2.2 Web Wizard Application Support

This release of Novell SecureLogin does not support Web wizard application management through iManager. Use SLManager instead.

### 7.2.3 The System Is Slow to Respond

If you open the iManager SSO snap-in with Internet Explorer as the browser on a client machine with SecureLogin running, the system might not respond immediately (for about 10 seconds).

### 7.2.4 Security Tab Options Not Visible in iManager after Upgrading

*Security* tab options are not visible in iManager after upgrading from SecureLogin 3.51.305, if you set the *Disable passphrase security* option to *Yes* in SecureLogin 3.51.305 by using ConsoleOne®.

In this case, change the datastore mode in iManager to 6.0 to view the security settings.

## 7.3 Java Issues

- ♦ [“Installing a New Version of Java on Windows Vista” on page 19](#)

### 7.3.1 Installing a New Version of Java on Windows Vista

If a new version of Java is installed after installing Novell SecureLogin, the next time you run Novell SecureLogin, it checks for new versions of Java to enable single sign-on.

If a new version of Java is detected, the required information must be updated in C:\Program Files\Java, and some files must also be modified in the process. However, Windows Vista does not permit you to write to the C:\Program Files\Java files unless you elevate privileges.

To resolve this:

- 1 Stop the Novell SecureLogin application.
- 2 Locate `slproto.exe` > right-click it, then select *Run As Administrator*.
- 3 Specify the administrator password.

You are now working with administrator privileges and can successfully write to the Java folder.

## 7.4 LDAP Issues

- ◆ “The Password Field in the LDAP Credential Provider Window” on page 20
- ◆ “Control Panel Menu Is Slow to Respond” on page 20
- ◆ “LDAP GINA Dialog Box Appears Continuously” on page 20
- ◆ “NSL Login in LDAP GINA Mode with eDirectory” on page 20
- ◆ “SecureLogin Using LDAP Fails to Detect Network Connection Status on VMWare” on page 20
- ◆ “?syspassword Reflects Universal Password or Simple Password” on page 20

### 7.4.1 The Password Field in the LDAP Credential Provider Window

When NMAS authentication is used with the LDAP Credential Provider on Microsoft Windows Vista, the *Password* field in the Credential Provider is redundant and is not used.

To proceed with the NMAS authentication, users must specify the LDAP username and server information, then click *Submit* without specifying any password.

### 7.4.2 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.

### 7.4.3 LDAP GINA Dialog Box Appears Continuously

If Novell SecureLogin is installed on Windows 2000 Advanced Server and if you log in to the workstation by using the *Workstation Only* option, the LDAP login dialog box appears more than once. A message appears, indicating “Your connection to the directory has been lost. SecureLogin can continue to work but changes/additions to single sign-on data may be lost. Do you wish to continue?”

To proceed, cancel all the LDAP login dialog boxes.

### 7.4.4 NSL Login in LDAP GINA Mode with eDirectory

NSL 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.

### 7.4.5 SecureLogin Using LDAP Fails to Detect Network Connection Status on VMWare

On VMWare\*, SecureLogin in LDAP mode fails to detect the network connection status. Therefore, SecureLogin never switches to the Offline Login dialog box directly and always displays the LDAP Login dialog box.

### 7.4.6 ?syspassword Reflects Universal Password or Simple 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.

## 7.5 NMAS Issues

- ◆ “Login Fails for NMAS Post Login Methods for eDirectory 8.8 SP1 or NMAS3.1.0 Server Version” on page 21
- ◆ “Users Cannot Unlock a Notification Area Icon” on page 21
- ◆ “?syspassword Displays Incorrect Values” on page 21
- ◆ “Citrix Passthrough with the NMAS pcProx Login Method” on page 22
- ◆ “Citrix Passthrough Fails with NMAS 2.7 on the Client and NMAS 3.x on the Server” on page 22
- ◆ “Using Non-Password-Based NMAS Login with the Passphrase Disabled Is Not Supported” on page 22
- ◆ “Offline Authentication Fails in Non-Password-Based NMAS Login” on page 22

### 7.5.1 Login Fails for NMAS Post Login Methods for eDirectory 8.8 SP1 or NMAS3.1.0 Server Version

If users have a login with the post-login method (Secure Workstation), users are unable to log in if the Directory is eDirectory 8.8 SP1, because the default NMAS server version installed is NMAS 3.1.0.

If users have a login with the post-login method (Secure Workstation), users are unable to log in after upgrading eDirectory to 8.8 SP1 or to NMAS 3.1.0.

To resolve this, users must upgrade to NMAS 3.1.1 or later by using the Security Service 2.0.2 available at the [Novell Download Web site](http://download.novell.com/Download?buildid=9hi7-ELIZ64). (<http://download.novell.com/Download?buildid=9hi7-ELIZ64>).

### 7.5.2 Users Cannot Unlock a Notification Area Icon

If the password field in the Novell Client is disabled and the notification area icon is password-protected, a user cannot unlock the notification area icon.

However, the user can unlock the notification area icon, if Universal Password is defined. This is the recommended mode of deployment for customers who require the password field in the NovellClient to be disabled.

### 7.5.3 ?syspassword Displays Incorrect Values

If you log in using an NMAS method, any script that accesses the ?syspassword variable displays incorrect values (instead of the password) if you have not selected *Enable Password Field* in the Novell Client Login dialog box.

To select *Enable Password Field*:

- 1 Right-click the Novell Client icon in the notification area, click *Novell Client Properties*, then click *Location Profiles*.
- 2 In the *Location Profiles* window, double-click *Default*.
- 3 Select *Default* as the service instance, then click *Properties*.
- 4 On the *Credentials* tabbed page, select *Enable Password* field, then click *OK*.

### **7.5.4 Citrix Passthrough with the NMAS pcProx Login Method**

Citrix passthrough is not supported if Novell SecureLogin is installed in Novell Client mode because Novell SecureLogin does not store the card details under the ?syspassword variable with pcProx login method.

### **7.5.5 Citrix Passthrough Fails with NMAS 2.7 on the Client and NMAS 3.x on the Server**

Citrix passthrough fails in the mixed mode scenario with NMAS 2.7 on the client and NMAS 3.x on the server.

In this case, upgrade all the clients to NMAS 3.2. Also, for non-password-based authentication, disable the NMAS virtual channel.

### **7.5.6 Using Non-Password-Based NMAS Login with the Passphrase Disabled Is Not Supported**

SecureLogin using the Novell Client does not support non-password-based NMAS logins if the passphrase options are disabled. This is not supported because SecureLogin either fails to open the local cache or opens the local cache file without any password.

### **7.5.7 Offline Authentication Fails in Non-Password-Based NMAS Login**

Offline authentication does not work if you do a non-password-based NMAS authentication with the *Passphrase Security System* disabled. This is because SecureLogin in offline mode accepts only passphrases for non-password-based NMAS authentication. This scenario occurs only if SecureLogin is installed in Novell Client mode.

## **7.6 pcProx Issues**

- ♦ [“The pcProx Unlock Operation” on page 22](#)
- ♦ [“PcProx Authentication after an Upgrade” on page 22](#)
- ♦ [“Installing the NMAS Login Server Method” on page 23](#)
- ♦ [“pcProx Might Not Work with the Latest USB Card Readers” on page 23](#)

### **7.6.1 The pcProx Unlock Operation**

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.

### **7.6.2 PcProx Authentication after an Upgrade**

If you want to use the NMAS pcProx client method, manually upgrade the pcProx client method before or after upgrading to Novell SecureLogin 6.0 or later.

Ensure that you uninstall the existing pcProx client method and install the pcProx client method that is available with Novell SecureLogin 6.0 or later.

### 7.6.3 Installing the NMAS Login Server Method

Installing the NMAS Login Server Method for pcProx by using the iManager plug-in for NMAS with iManager 2.6 fails to extend the schema definition of the User object class with the sasPcProxID attribute. This means that you are unable to associate the pcProx card ID with the User object for identification.

To resolve the issue, you must manually add the sasPcProxID attribute to the user object class by using the iManager schema plug-in.

### 7.6.4 pcProx Might Not Work with the Latest USB Card Readers

The latest USB card readers have compatibility issues with the current pcProx method. For example, pcProx does not work with USB card reader model number bse-rfid1356I-usb.

## 7.7 Scripting Issues

- ◆ [“Terminal Services and RDP Passthrough on Vista” on page 23](#)
- ◆ [“The QuickFinder Prebuilt Application Script” on page 23](#)
- ◆ [“AOL Prebuilt Application Definition” on page 23](#)
- ◆ [“Hotmail Prebuilt Application Definition” on page 23](#)
- ◆ [“Novell GroupWise 7.0 Web Login Prebuilt Script” on page 24](#)
- ◆ [“Selecting Credentials Fails When Multiple Login Credentials Are Present” on page 24](#)
- ◆ [“Single Sign-On Fails for GroupWise WebAccess” on page 24](#)

### 7.7.1 Terminal Services and RDP Passthrough on Vista

This release of Novell SecureLogin provides new prebuilt applications to handle terminal services and RDP passthrough on Vista.

### 7.7.2 The QuickFinder Prebuilt Application Script

If the QuickFinder™ script is used with Mozilla\* Firefox\*, a message indicating “Would you like to login again?” is displayed when you are already logged in to QuickFinder and try to do a search.

To continue with your search, click *No* at the prompt.

---

**NOTE:** This behavior is not observed in Internet Explorer.

---

### 7.7.3 AOL Prebuilt Application Definition

This release of Novell SecureLogin does not include a predefined application definition for AOL\* Instant Messenger.

### 7.7.4 Hotmail Prebuilt Application Definition

This release of Novell SecureLogin does not include a predefined application definition for Hotmail\*.

### 7.7.5 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.

### 7.7.6 Selecting Credentials Fails When Multiple Login Credentials Are Present

The Novell SecureLogin 6.1 does not prompt the users to select the credentials when multiple logins are present. Multiple logins are not working with Yahoo\* e-mail and Novell GroupWise.

For example, when SecureLogin is running and users launch Novell GroupWise e-mail, they are prompted to save the credentials. The users save the credentials. Later, users could add more login IDs to the GroupWise application. They save these credentials and exit.

The next time they launch the GroupWise application, they are not prompted to select the credentials; instead, the credentials stored on the first occasion are stored to log in.

For applications that do not have a prebuilt script:

- 1 Click *Applications > Application Names > Definition* and verify whether the *Supply Credentials* option is selected.

If it is selected, deselect it to make multiple logins work.

### 7.7.7 Single Sign-On Fails for GroupWise WebAccess

Users must manually insert the GroupWise client script to enable single sign-on for GroupWise WebAccess.

## 7.8 SecretStore Issue

- ♦ [“SecretStore on the Server” on page 24](#)

### 7.8.1 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.

## 7.9 Secure Workstation Issues

- ♦ [“Quick Login and Logout Interface for Secure Workstation” on page 25](#)
- ♦ [“Device Removal Policy on Remote Citrix Sessions” on page 25](#)
- ♦ [“Using the NMAS Login with the Secure Workstation Sequence on a Microsoft Windows Vista Desktop” on page 25](#)
- ♦ [“Login Fails When the Secure Workstation Post-Login Method Is Added to the Login Sequence” on page 25](#)



### 7.9.1 Quick Login and Logout Interface for Secure Workstation

When Secure Workstation is upgraded from Novell SecureLogin 3.51 or 6.0 to Novell SecureLogin 6.1, the Quick Login and Logout interface is installed even if this component was not installed with Novell SecureLogin 3.51 or 6.0. This is because NSL 6.1 uses a .msi based install, and prior versions use a .exe based install. A .msi install can not detect sub-components laid down by a .exe install.

If the Quick Login and Logout interface is not wanted, it can be easily removed from the Startup programs menu. Delete the NSWQLL entry from the registry at `HLKM\Software\Microsoft\Windows\Current Version\Run`. Removing this entry will not impact the functioning of Novell SecureLogin or Secure Workstation.

### 7.9.2 Device Removal Policy on Remote Citrix Sessions

The Secure Workstation device removal policy configured for Terminal Services clients on a Citrix server fails to work on Citrix remote sessions from clients.

To resolve the issue, manually restart the Novell Secure Workstation service on the Citrix server.

### 7.9.3 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.

### 7.9.4 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.

## 7.10 TLaunch Issues

- ♦ [“TLaunch Fails to Add New Emulators or Save the Changed Configuration of Existing Emulators” on page 25](#)
- ♦ [“TLaunch Shortcut Command Line /n Switch” on page 26](#)

### 7.10.1 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*.

### 7.10.2 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.

## 7.11 Web-Related Issues

- ♦ “Accessing Web Applications from a Windows 2003 Server” on page 26
- ♦ “Novell SecureLogin Single Sign-On Prompts the Citrix MetaFrame Web Browser to Store Credentials Again” on page 26
- ♦ “Firefox and Internet Explorer” on page 26
- ♦ “Adding a Predefined Application Definition” on page 26
- ♦ “Mozilla Firefox Displays an Error After Uninstalling SecureLogin” on page 27
- ♦ “Firefox Issue During Installation” on page 27

### 7.11.1 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.

### 7.11.2 Novell SecureLogin Single Sign-On Prompts the Citrix MetaFrame Web Browser to Store Credentials Again

With Novell SecureLogin in Novell Client mode on a Windows 2000 setup, single sign-on prompts the Citrix MetaFrame\* Web browser to store again the credentials.

When users launch the Citrix Metaframe Web browser (<http://serverip/Citrix/Metaframe>) and provide the credentials, Novell SecureLogin prompts the users to save the credentials. When users log out and relaunch the browser, they are prompted to save the credentials again.

At the prompt, click *No* and proceed.

### 7.11.3 Firefox and Internet Explorer

Because Firefox and Internet Explorer have different controls, you must create the Web application definition for the two browsers separately.

### 7.11.4 Adding a Predefined Application Definition

When you use iManager to add the predefined application to a container, some Web-based applications are incorrectly identified as Win32 applications.

Check the properties of each application after the addition to validate that the configuration is correct.

### 7.11.5 Mozilla Firefox Displays an Error After Uninstalling SecureLogin

If you uninstall SecureLogin, the Mozilla Firefox browser displays an error message when it restarts. This error occurs because the Firefox extensions do not have command line parameters for uninstalling.

If this happens, uninstall the Firefox extension manually as follows:

- 1 Click *Tools > Extensions*.
- 2 Select the extension files that you want to delete.
- 3 Click *Uninstall*.
- 4 Restart the browser.

### 7.11.6 Firefox Issue During Installation

We recommend that you 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.

## 8 Registry Settings

- ♦ The Activate the Diagnostic Log File option on the Settings tabbed page starts logging by itself. For advanced debugging, see TID 10088017 on the [Novell Support Web site](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088017.htm). (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088017.htm>).
- ♦ If you need information on LDAP Client registry settings, see TID 3790292 on the [Novell Support Web site](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3790292&sliceId=SAL_Public&dialogID=49373420&stateId=0%200%2049379458). ([http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3790292&sliceId=SAL\\_Public&dialogID=49373420&stateId=0%200%2049379458](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3790292&sliceId=SAL_Public&dialogID=49373420&stateId=0%200%2049379458)).

## 9 Support

For support, refer to the following:

- ♦ Online documentation at the [Novell Documentation Web site](http://www.novell.com/documentation/securelogin61). (<http://www.novell.com/documentation/securelogin61>).
- ♦ Knowledgebase, updates, or chats at the [Novell Support Web site](http://support.novell.com). (<http://support.novell.com>)

Customers can also call Novell Support for technical support problems. The support phone number is 1-800-858-4000.

## 10 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.

# 11 Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

All third-party trademarks are the property of their respective owners.