Novell SecureLogin 6.0 Readme

March 14, 2006

1.0 Documentation

Because the documentation is continuously updated, documentation is not included on the product CD or download image. Instead, documentation is provided on the Novell Web site. By using this online documentation, you have the latest information, including documentation updates, for the following:

- Novell SecureLogin 6.0 Overview
- Novell SecureLogin 6.0 Administration Guide
- Novell SecureLogin 6.0 Installation Guide
- Novell SecureLogin 6.0 Application Definition Guide
- Novell SecureLogin 6.0 Guide for Terminal Emulation
- Novell SecureLogin 6.0 Terminal Services Guide
- Novell SecureLogin 6.0 User Guide

View or download documentation at:

http://www.novell.com/documentation/securelogin60/index.html

2.0 What's New

2.1 User Interface Redesign for Greater Ease in Navigation

The SecureLogin user interface has been significantly improved to provide greater ease in navigation and to provide enhancements to make managing the SecureLogin environment easy. The redesigned user interface presents a two-panel display with left and right window panes. When items are selected in the left pane, their settings and options are presented in the right pane. This is available in both the Administrative Management Utility and Personal Management Utility.

2.2 Improved Web Wizard Functionality Simplifies Enabling Web Sites

The advanced Web wizard makes it easier to single sign-on, enable Web sites, and capture virtually any Web-based login. You simply access a Web page from your browser and SecureLogin launches the Web wizard to promptly capture login details, error messages, and change password requests.

2.3 SecureLogin Administrative Management Utility Automatically Browses the Network Configuration in LDAP Environments

For administrators, there is now a powerful LDAP browser embedded in the SecureLogin management tool that automatically browses the network configuration in LDAP environments. Administrators no longer need to type the names of Organizational Units to manage them; SecureLogin automatically locates and displays the directory structure.

2.4 Mozilla Firefox Browser Support

SecureLogin now has built-in support for the Mozilla Firefox browser, enabling single sign-on to Web pages. SecureLogin supports Mozilla Firefox version 1.0.x.

2.5 Additional Predefined Applications

SecureLogin has new predefined applications, including Citrix Program Neighborhood, Citrix Web Portal, Enterprise Application Software (SAP v6.20), Heat Call Logging, Cisco VPN, and Checkpoint Firewall.

2.6 Customization of the Passphrase Security System

Typically, users set a passphrase when they first run SecureLogin. An administrative preference is now provided to disable user-defined passphrases.

2.7 User Administration Using Active Directory Group Policies

SecureLogin previously provided powerful administrative tools for managing users at the container, organizational unit, and user object level. The current version increases functionality by enabling management of users using Group Policy objects. SecureLogin now efficiently leverages the Active Directory architecture, enabling time-effective centralized user management using group policy, container, organizational unit, and user objects.

2.8 Microsoft ADAM Functionality

Organizations operating Active Directory now have an alternative to extending the corporate schema while retaining full SecureLogin functionality. This is accomplished by using a Microsoft ADAM (Active Directory Application Mode) deployment. The SecureLogin ADAM wizard facilitates easy configuration and deployment of SecureLogin in a specific ADAM instance. The ADAM deployment of SecureLogin provides full administration functionality and application management; with full access to all comprehensive management tools of SecureLogin, enabling administrators to separate the SecureLogin deployment from core Active Directory administration tasks.

2.9 Encryption and Password Protection of XML Files Used for Import/ Export of Configurations

SecureLogin provides configuration distribution functionality that enables the import and export of SecureLogin setup across containers, organizational units and user objects. In this release, this functionality is extended to the Group Policy, using an XML file. To restrict access to the contents of this XML file to the intended recipient, SecureLogin provides optional file encryption and password protection functionality.

2.10 Streamlined Standalone Installation

The deployment of SecureLogin in the Standalone mode previously required the manual creation of a user account after installation. Each time the user started and logged into their workstations, they were also required to login to SecureLogin. SecureLogin now utilizes the workstation login for user authentication. Therefore, when a user logs in once to the workstation, SecureLogin is active on the desktop.

2.11 Backing Up and Restoring of Credentials and Preferences

The new local Backup and Restore functionality of SecureLogin provides users with the option to create a backup file of their SecureLogin user data, including preferences and credentials. The fast and simple Restore functionality facilitates the immediate re-creation of the SecureLogin environment if SecureLogin user data is lost or corrupted. The Backup file contains sensitive user data, including usernames and passwords. Therefore, the highest level Triple DES encryption and password access is implemented to prohibit unauthorized access.

2.12 Enhanced Startup

SecureLogin now automatically checks for any Windows 32-bit applications that have executed before it started. It then logs in the user to the application as required, or prompts the user with the option to enable the application for single sign-on, if the login dialog box is recognized. This feature is vital in environments where multiple applications are started automatically and SecureLogin is not configured to start first.

2.13 Certified Data Integrity

SecureLogin's encryption support has been expanded to include FIPS 140-2 compliant Microsoft Cryptographic API libraries for user data encryption, offering safety and security of the highest standard.

2.14 Different Users Can Unlock the Workstation in LDAP GINA Mode

The LDAP GINA for SecureLogin has been enhanced to allow different users (other than the one who locked the workstation) to unlock the workstation. The different user must be an administrator of the workstation.

2.15 NMAS 3.2 Support

The current version of SecureLogin supports NMAS 3.2 and NMAS 2.7.2 for NMAS methods.

2.16 NICI 2.6.8 Support

The current version of SecureLogin supports NICI 2.6.8

2.17 Changed Datastore Preference Behavior

The datastore preference behavior is changed to bring it in line with the SecureLogin client administration tools. When the datastore is set to version 6.0 on a container, the user should not be able to go back to earlier datastore versions. The default datastore version is 3.5

2.18 Advanced Button in the LDAP Login Dialog Box

The LDAP GINA dialog box now has an Advanced button. This button displays or hides the advanced authentication information.

2.19 Smart Card Integration

With this release, Novell SecureLogin can be integrated with existing smartcard deployments.

2.20 Novell Audit Support

SecureLogin now supports Novell Audit. Novell® Audit provides SecureLogin with a secure and efficient mechanism to report performance data and events to a central location.

2.21 Universal Password Support

Simple password is no longer required in LDAP-NMAS mode if universal password is configured on eDirectory. This requires the following configuration on eDirectory:

- Universal Password is enabled for the user you are trying to authenticate. You can enable the universal password at the container level also.
- The Universal password policy 'Allow user agent to retrieve password' is set to TRUE.

2.22 iManager Plug-ins for SSO, Secure Workstation and pcProx

SecureLogin 6.0 provides iManager plug-ins for SSO, Secure Workstation and pcProx. This requires iManager 2.5 or 2.6

3.0 Known Issues

3.1 General Issues

3.1.1 User-Defined Passphrase Questions Cannot Be Disabled

You cannot disable the user-defined passphrase question option in the SecureLogin Preferences.

3.1.2 Predefined Application Definition Might not Work for GroupWise 6.5

GroupWise 6.5, single sign-on might not work because of changes in the application definition.

If this happens, upgrade the Groupwise client to version 7.0.

3.1.3 Uninstalling SecureLogin Does Not Delete the Cache

You must manually delete the SecureLogin cache because it is not deleted during the uninstallation of SecureLogin. The **`HKEY_LOCAL_MACHINE\SOFTWARE\Protocom folder`** is also not be removed from the system registry.

3.1.4 Delete SecureLogin Configuration Option Not Working for the User Object

The Delete option in SecureLogin Configuration does not work at the user object level. After deleting the SecureLogin configuration, the user cannot log in to SecureLogin again.

3.1.5 User Not Prompted to Store iChain Basic Authentication Credentials

Launch the browser and specify the URL of iChain. After you successfully authenticate to iChain, SecureLogin does not prompt to store the credentials.

However, if you manually enable the predefined application definition for iChain, SecureLogin prompts the user to store credentials.

3.1.6 Modification to Include Smartcard Support

When SecureLogin 6.0 is installed without smart card support and the support is required later, run setup.exe in the CD again. You cannot modify the installation from Control Panel to include smart card support.

3.1.7 Using Smartcard with ActivClient Requires Hotfixes

If you want to use smart card to authenticate to SecureLogin and if ActivClient is installed in your system, then you must install the hotfixes.

3.1.8 User Cannot Use the Same Smartcard to Authenticate in Both eDirectory and LDAP Modes

If a user tries to log into SecureLogin in the LDAP mode using the same smartcard used to authenticate in the eDirectory mode, the authentication fails. This scenario does not work because SecureLogin smartcard implementation sees them as two different users.

3.1.9 SecureLogin Does Not Support Mobile iManager 2.6

SecureLogin throws an error if you try accessing the SecureLogin tab through the mobile iManager. This is because SecureLogin does not support Mobile iManager 2.6.

3.1.10 AES Encryption Supported Only for Windows 2003 and Windows XP Platforms

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

3.1.11 Case Sensitive Feature for Passwords Does not Work While Unlocking System Tray Icon

When installed in client32 mode, SecureLogin does not take into account the case sensitivity of passwords, while unlocking the system tray icon, if Novell Client 4.91 SP2 is used. To use this feature, update the Novell Client to version 4.91 SP3.

3.1.12 System Tray Icon Cannot Be Unlocked Using pcProx Authentication

You cannot unlock the SecureLogin system tray icon using the NMAS pcProx authentication.

Unlock the icon using the passphrase, if you have enabled the passphrase or through your directory password.

3.1.13 Credentials Deleted Through iManager Not Deleted From Local Cache

When you delete credentials through iManager, they are not deleted from the local cache. Close and re-open the SecureLogin client to re-synchronize credentials with the eDirectory.

3.1.14 SecureLogin Installation Does Not Overwrite NMAS 3.2.0

SecureLogin installation does not overwrite NMAS 3.2.0 if it is already installed on the system. In this case, manually install NMAS 3.2.1. NMAS 3.2.1 is installed automatically during the installation of SecureLogin if NMAS is not present on the system or if the version present on the system is less than NMAS 3.2.

3.1.15 Cache Refresh Reduces the Grace Logins By One

Every time the cache is refreshed, the number of grace logins allowed is reduced by one. This happens because every time cache is refreshed, SecureLogin tries to re-authenticate to the directory.

3.1.16 Choose a Destination Location Screen Goes Out of Focus

During the installation of Novell SecureLogin, if you enter an invalid location in the text box, an error message is displayed. The next time you attempt to enter a location in the text box, the Choose a Destination Location screen goes out of focus.

3.1.17 The NICI Client Is Not Uninstalled

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

- LDAP
- eDirectory with LDAP
- eDirectory with Client32™ as protocol and if NMAS or SecretStore is selected for installation.

However, if you uninstall SecureLogin, the NICI client remains because other Novell services (for example, NMAS, and NetIdentity) 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.

3.1.18 Dummy Application Definition Not Enabled

If you select Never at the add application prompt of SecureLogin, you will not be prompted to single sign-on, the next time you login to the application. But, the dummy application script that is created will not be enabled by default.

3.1.19 Logging In As Administrator after a Reboot

Make sure that the first user to log in after the install or reboot has administrative rights to the workstation.

Depending on what files were locked and the options that you select during an install, you might need to reboot the workstation. If this is the case, at the end of the install a dialog box prompts you to log in with administrative rights after the reboot. This applies to all Windows NT*-based operating systems.

3.1.20 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

3.1.21 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® for Desktops 4.01 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.

3.1.22 Integration with NetIdentity

The NetIdentity client does not work if SecureLogin is installed in LDAP non-eDirectory mode. This is because NetIdentity requires the eDirectory environment to work.

3.1.23 Issue while installing the NMAS Proximity Card Method for pcProx

During the SecureLogin installation, if you choose to install the NMAS proximity card methods for pcProx, two messages are displayed prompting to overwrite ldapsdk.dll and wsaccinst.dll files. Click No, to proceed with the installation.

3.1.24 Displaying Default Logins

If a default login does not contain data, ScptEdit (user ID tab of manage logins) does not display the default login. However, links are displayed through the main User IDs page.

3.1.25 Unable to Delete Default Logins

You cannot delete the default login from the User ID tab of Manage Logins option. To delete the default login, you must delete the associated application.

3.1.26 The 0 Setting for Cache Refresh Interval Is Invalid

In iManager, you can set the Cache Refresh Interval on a client workstation to a positive number other than 0. If you change the setting to 0 on a client workstation, the Cache Refresh Interval changes to the default setting, erasing the setting you made in iManager.

3.1.27 Old Passwords Unlock the Local Cache

When SecureLogin runs with the Novell Client, the client does not send a password change notification to SecureLogin. The old eDirectory password will still unlock the local cache.

For details, see TID 10092159 on the Novell Support Web site (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088017.htm)

3.1.28 Citrix MetaFrame Presentation Server

To enable SecureLogin for ICA connectivity on Citrix servers, create the following two registry values under the key HKLM\Software\Protocom\VirtualChannel:

AutoDetect REG_SZ 0

protocol REG_SZ ICA

3.1.29 Smartcard is Not Supported in Citrix Environment

Smartcard is not supported in Citrix environment when SecureLogin is installed with Smartcard support in the eDirectory or LDAP environment.

3.1.30 Predefined Application Definition for Citrix Program Neighborhood Does Not Work

Predefined application definition does not work for Citrix Program Neighborhood Client 9.1.5. Contact Novell Technical Support for an updated application definition.

3.1.31 Manual Entry of Smartcard PIN required for Citrix Server Authentication

If you are using Smartcard authentication for the Citrix login prompt, enter the Smartcard PIN manually as the PIN is not cached for the Citrix server authentication.

3.1.32 Configuring a Network Policy for Secure Workstation

The Secure Workstation Post-Login Method fails if you attempt to log in with it before configuring a Network Policy for Secure Workstation.

To configure a Network Policy:

1. Log in to iManager. Select Novell Secure Workstation > Select Sequence.
2. Select Activate Secure Workstation and click Configure.
3. Configure actions for various events, then click Apply.

3.1.33 System Messages on Active Directory

Some settings, such as Password Protect the System Tray Icon, require you to input a network password. If Microsoft* Active Directory has told a user to change a password during the next login, these settings fail and a system message (for example, *Password expired* or *Wrong password*) appears.

3.1.34 Updates to the Current Object Version Need to Be Saved in Active Directory

In Active Directory's MMC, the Current Object 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.

3.1.35 Quick Login/Logout Interface Fails to Launch If Installed Later

If you install the Quick Login/Logout Interface by modifying the SecureLogin install wizard (after installing SecureLogin and restarting the machine), the Quick Login/Logout Interface does not launch by itself. This happens if SecureLogin is already installed (with the Secure Workstation component) without selecting the Quick Login/Logout Interface.

To launch the Quick Login/Logout Interface, do either of the following:

- Log in to the workstation again.
- Click Start > Run, type nswqll, then click OK.

3.1.36 Relogin Required If 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.

3.2 Web-Related Issues

3.2.1 The DumpPage Command

The DumpPage command might not work on all Web-content types.

3.2.2 Adding 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 proper.

3.2.3 Mozilla Firefox Browser 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 a command line parameters for uninstalling.

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

1. Select Tools > Extensions.
2. Select the extension files that you want to delete.
3. Click Uninstall.

Restart the browser.

3.2.4 Mozilla Firefox Extension Files Must Be Manually Added

If the Mozilla Firefox browser is installed after the installation of SecureLogin 6.0, the browser extension files must be manually added at the command line as follows:

```
firefox.exe -install-global-extension
"<securelogin_dir>\slomoz.xpi
```

3.2.5 FireFox Issue During Installation

A Mozilla Firefox messagebox, indicating the import of Internet Explorer settings, is launched during the NSL 6.0 installation if Firefox is not invoked anytime before.

If this happens click Import to import the Internet Explorer setting or click Cancel to cancel the import.

3.2.6 Hotmail Password Change Unsuccessful

If you do not use a predefined application definition for Hotmail, and you change the user password, SecureLogin attempts to login with the old password and log in fails.

3.2.7 Hotmail Predefined Application Throws Error After Upgrading

If you had configured the Hotmail predefined application in SecureLogin 3.51.3, the following error is displayed after upgrading from SecureLogin 3.51.3 to SecureLogin 6.0:

```
BROKER_SCR_UNMATCHED_QUOTES (-147)
```

If this happens, delete the old application definition for Hotmail and configure a new application definition.

3.3 NMAS Issues

3.3.1 The NMAS Client Is Not Uninstalled

When SecureLogin is installed, the NMAS client and, optionally, a number of NMAS login methods can be installed as well.

However, if you uninstall SecureLogin, the NMAS client remains. The NMAS client and any NMAS methods, can be uninstalled through Add/Remove Programs.

3.3.2 NMAS Client Method Must be Manually Installed

If the NMAS option is not selected during installation, the NMAS client method options in the system are not displayed.

In this case, the NMAS client method must be manually installed on the workstation.

3.3.3 Installing and Assigning a Simple Password

If users are to log in to an eDirectory server by using SecureLogin LDAP Authentication and any NMAS method, and the universal password is not configured in the edirectory, you must install the NMAS Simple Password method on both server and client. Also, all users authenticating via LDAP must have a simple password assigned to them. Otherwise, the users are prompted to log in more than once.

3.3.4 Simple Password Method Requires NMAS 2.7.2 Or Later

If you plan to use the LDAP client and any NMAS method, do the following:

- Set the simple passwords for the users
- Update the servers with the Simple Password Login Server method (LSM)

If you are currently using the Simple Password method and plan to continue using it with SecureLogin 6.0, you must install the Simple Password Login Server Method before installing SecureLogin 6.0. NMAS files are on the SecureLogin CD or in the download image.

3.3.5 ?syspassword Displays Incorrect Values If Enable Password Field Is Not Selected

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 Novell Client Login dialog box.

To select Enable Password Field:

1. Right-click the Novell Client icon on the status bar (system tray), click Novell Client Properties, then click Location Profiles.
2. In the Location Profiles window, double-click Default.
3. Select Default as the service instance and then click Properties.
4. On the Credentials tabbed page, select Enable Password Field and then click OK.

3.3.6 Silent Install Does Not Support NMAS Client

When you do a silent installation of SecureLogin, the NMAS component is not installed. If you want SecureLogin to work with the NMAS client, you must manually install the client from the SecureLogin product CD.

3.3.7 Citrix Passthrough Fails with NMAS

Citrix passthrough fails if both of the following occur together:

- SecureLogin uses Novell Client32 with NMAS mode of authentication.
- Non-NDS NMAS method is used for authentication.

For a successful passthrough,

1. Login to SecureLogin once using the NDS password.
2. Copy slnmas.dll from "SecureLogin_cd\SecureLogin\Tools\Citrix Manual Configuration\Citrix\wks\nw" to the System 32 directory of your workstation.
3. Delete slinac.dll from the System 32 directory of your workstation.
4. Reboot the workstation.

3.3.8 Citrix Passthrough Fails with NMAS 3.0

Citrix passthrough with SecureLogin fails with hardware based NMAS methods (except for pcProx) when NMAS 3.0 (that comes along with Novell Client 4.91) is installed on the Citrix server and NMAS authentication is enabled.

To resolve this issue, do either or the following on the Citrix server:

- Remove Novell Client 4.91 and install Novell Client 4.90 with NMAS 2.7
- Disable NMAS authentication from the Novell Client Configuration

3.3.9 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.

3.3.10 Using Non-Password-Based NMAS Login with 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.

3.3.11 Offline Authentication Fails in Non-Password-Based NMAS Login

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

3.4 LDAP Issues

3.4.1 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.

3.4.2 NMAS Sequence Selection Is Disabled on LDAP

If the NMAS Sequence Selection dialog box is disabled on LDAP, it means you have an earlier version of NMAS or you have not installed the simple password method on either the server or client. To use NMAS over LDAP, install NMAS 3.2 (available on the SecureLogin product CD).

3.4.3 ?syspassword Reflects Simple Password

?syspassword reflects the simple password for the currently logged-in user, if universal password is not configured on edirectory. This happens when SecureLogin is installed in LDAP mode and NMAS is the authentication method.

3.4.4 Opening Local Cache in Offline Mode Requires Simple Password

If you are logged in to an eDirectory server using SecureLogin with LDAP and the NMAS mode of authentication, and universal password is not configured, you should use simple password to open the local cache in SecureLogin offline mode.

3.4.5 Simple Password Required for Unlocking SecureLogin System Tray Icon

When you do an NMAS authentication in LDAP mode, if the SecureLogin system tray icon is password protected and the universal password is not configured, you can unlock the icon only by using simple password. This is irrespective of whether you have logged in to eDirectory using as enhanced password or NDS password.

3.5 SecretStore Issue

3.5.1 SecretStore on the Server

If you plan to use 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.

3.6 pcProx Issues

3.6.1 Username Needs to Be Auto-Populated for pcProx Authentication

The SecureLogin username should be auto-populated for pcProx authentication. This can be done by selecting the Use the Card Reader to Obtain Username for Login option during installation. The

card is scanned using LoginIDs snap-in for pcProx so that the username information is also scanned along with the card ID.

3.6.2 Login Looping Problem

When logging in the LDAP mode with NMAS pcProx and Secure workstation, after the pcProx reader successfully reads the card and logs the user in, the NSL dialog appears again after several seconds and the pcProx method successfully logs the user again. This login process is repeated continually.

If this happens, upgrade NICI to 2.6.8.2, as the NICI 2.6.6 is incompatible with NMAS 3.x, while running on LDAP mode with NMAS and pcProx.

3.6.3 pcProx Might Not Work with the Latest USB Card Readers

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.

3.6.4 Logging In Using pcProx Self-Enrollment

If you selected the eDirectory, NMAS, pcProx, and Enable Self-enrollment options during installation, an internal 0xFFFFFFCE error might occur when you attempt to log in by using pcProx.

3.7 TLaunch Issue

3.7.1 Tlaunch.exe Continues to Run

While running TLaunch in the background, tlaunch.exe fails to terminate even after the full script is run or the EndScript command is executed. Tlaunch.exe continues to run even after signing in to the terminal emulator.

To resolve this issue, you can add the KillApp command to the end of tlaunch.exe script.

But, if you are running multiple copies of the terminal emulator, the KillApp command might kill all emulator sessions. To avoid this, use the keystrokes that you normally use to terminate the application. For example: Alt+F4, Alt+F+X, Ctrl+C, or Ctrl+X (depending on the terminal emulator/application that you use).

A fix for this issue is targeted for a later release.

3.8 iManager Issues

3.8.1 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 for a while (around 10 seconds).

3.8.2 Security Tab Options Not Visible in iManager after Upgrade

Security tab options are not visible in iManager after upgrading from SecureLogin 3.51.305, if the you had set the disable passphrase security option to Yes in SecureLogin 3.51.305 using Console One. In this case, change the datastore mode in iManager to 6.0 to view the security settings.

3.8.3 Error Authenticating User After Disabling Passphrase and Enabling Corporate Redirection

Set the disable passphrase security option to Yes in SecureLogin 3.51.305 using Console One and later upgrade to SecureLogin 6.0. Configure the corporate redirection from a different container using iManager. If you attempt to login now, the following error is thrown:

"SecureLogin encountered an error during authentication"

In this case, set the datastore mode in iManager to 6.0.

4.0 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)
- If you need information on LDAP Client registry settings, see TID 10093336 on the Novell Support Web site (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093336.htm).
- If you need to set -DWORD values (for example, CacheExpireDays?), contact Novell Technical Services[SM].

5.0 Support

For support, refer to the following:

- Online documentation at novell.com/documentation
- Knowledgebase, updates, or chats at support.novell.com

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

6.0 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 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.