AUTHORIZED DOCUMENTATION

Registry Settings Reference

Novell® SecureLogin

July, 2009

www.novell.com

Legal Notices

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide contains technical notes that give an overview of the system registry settings used in Novell SecureLogin.

Audience

This guide is intended for:

- Novell Technical Support
- IT Administrators

![NOTE TO THE READERS:]

![This is document is an effort to collate the documented and undocumented registry keys avaialble through various sources such as TIDs and NTS knowledge base.

This is for INTERNAL circulation only.

Use the document in resolving customer issues. Do not circulate it to customers. This document is not available for customer consumption.

The document is not reviewed for technical accuracy and edited for language and grammar.

If you have any changes and corrections to the document, send me an e-mail at mrama@novell.com]

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Additional Documentation

For documentation on other Novell SecureLogin documentation, see the Novell Documentation Web site. (http://www.novell.com/documentation/securelogin70)

Documentation Conventions

In Novell 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.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

1 Introduction

This document describe the Novell SecureLogin entries written to the system Registry when you install Novell SecureLogin.

1.1 Windows System Registry Overview

The Windows System Registry is essentially a database that is used to store Windows Operating System settings and options. It contains essential information and settings for the operating system, system hardware and devices, application software, user preferences, and similar information.

The system registry provides a window into the operation of the operating system’s kernel, exposing runtime information such as performance counters and currently active hardware.

Whenever new software is installed, or a user makes changes to *Control Panel* settings, file associations, or system policies, these changes are reflected and stored in the system registry.

1.2 System Registry Structure

The system registry is divided into a number of logical sections or Hives normally named by their Windows Application Program Interface (API) definitions. Sections begin with HKEY, an abbreviation for Hive Key. They are normally referred to in an abbreviated, a three or four letter short name starting with the letters HK, for example, HKCU for HKEY_CURRENT_USER and HKLM for HKEY_LOCAL_MACHINE and HKU for HKEY_USERS.

The HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER nodes have similar structures and applications typically look up their settings by first searching in `HKEY_CURRENT_USER\Software\[Vendor Name]\[Application Name]\Version\Setting` name. If the setting is not found, then the application searches the same location under the `HKEY_LOCAL_MACHINE` key.

Registry key syntax is similar to Windows' path names, using a backslash to indicate the hierarchy level. For example `HKEY_LOCAL_MACHINE\Software\Protocom\SecureLogin\` refers to the sub key SecureLogin of the sub key Protocom of the sub key Software of the HKEY_LOCAL_MACHINE key.

SecureLogin SSO searches for settings in:

- `HKEY_CURRENT_USER\Software\Protocom\SecureLogin\setting\`

  or

- `HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\setting\`

When applications write settings back to the registry, the reverse approach is used. HKEY_LOCAL_MACHINE is normally written first, but if the settings cannot be written, normally the case if the current user is not an administrator, the setting is stored in the HKEY_CURRENT_USER section instead.

1.2.1 Registry Values

Registry values are not referenced via the registry syntax. Windows API functions that query and manipulate system registry values take value names separately from the HKEY path or specific handle that identifies the parent HKEY.

Each HKEY is divided into sub keys, which may contain further sub keys, and so on. Any key may contain entries with various types of values.

The values of these entries can be:

Table 1-1 *The Registry Values*

Type	Description
REG_NONE	No Type
REG_SZ	A constant string value, typically iso8859 or UTF-16, often zero-terminated.
REG_BINARY	Any arbitrary binary data
REG_DWORD	A DWORD (double word) is a unit of data twice the size of a word and half the size of a QWORD. A DWORD is normally 32 bits long.
REG_LINK	A symbolic link.
REG_MULTI_SZ	A multi-string value, which is an array of strings.
REG_RESOURCE_LIST	A resource list.
REG_FULL_RESOURCE_DESCRIPTOR	A resource descriptor.
REG_RESOURCE_REQUIREMENTS_LIST	A resource requirements list.
REG_QWORD	A QWORD (quadruple word) is a unit of data four times the size of a word and twice the size of a DWORD. A QWORD is normally 64 bits long.

1.2.2 HKEY_CLASSES_ROOT (HKCR)

HKCR stores information about registered applications, including associations from file extensions and OLE object Class IDs to the applications used to handle these items. On Windows 2000 and later, HKCR is a compilation of HKCU\Software\Classes and HKLM\Software\Classes. If a given value exists in both HKCU and HKLM sub keys, the HKCU value is used.

1.2.3 HKEY_CURRENT_USER (HKCU)

HKCU stores settings that are specific to the current user. The HKCU key is a link to the sub key of HKEY_USERS that corresponds to the current logged on user; the same information is reflected in both HKCU and HKU locations.

1.2.4 HKEY_LOCAL_MACHINE (HKLM)

HKLM stores settings that are general to all users on the computer. This key is found within the file %SystemRoot%\System32\Config\systemprofile in Microsoft Windows 2000 and later. Information about system hardware is located under the SYSTEM key.

1.2.5 HKEY_USERS (HKU)

HKU contains sub keys corresponding to the HKEY_CURRENT_USER keys for each user registered on the machine.

1.2.6 HKEY_CURRENT_CONFIG (HKCC)

The HKPD key provides runtime information and performance data provided by either the OS kernel or other programs that provide performance data. This key is not displayed in the Registry Editor, but it is visible through the registry functions in the Windows API.

1.3 Editing The Registry

The registry can be edited manually in Microsoft Windows by running regedit.exe from the command prompt.

Many “third party” registry optimization and miscellaneous "hacking" tools are available to modify the system registry. We do not recommend using the third party tools unless the administrator has a thorough understanding and high level knowledge of registry workings.

NOTE: Careless registry editing can cause irreversible damage and performing a registry back-up prior to editing is highly recommended.

- Section 1.3.1, “Using the Registry Editor,” on page 13
- Section 1.3.2, “Editing Through Command Line,” on page 14

1.3.1 Using the Registry Editor

The Registry Editor tool has a left side navigation tree that begins at "My Computer” and lists all loaded Hives. Hives can be expanded or collapsed using the + or – button.

The right side displays the three components of the sub key value, Name, Type and Data as separate columns of a table.

A Status Bar, when enabled, displays the current navigation status.

1.3.2 Editing Through Command Line

The registry can be edited and manipulated from the command line by running the Console Registry Tool (reg.exe) from the command prompt. The reg.exe utility is included as part of the Windows XP and Windows Vista operating systems. The Console Registry Tool can also be downloaded for previous operating system versions.

For help on specific reg.exe tool operations, type reg /? at the Command Prompt, then click OK.

1.4 How SecureLogin Uses the Registry

SecureLogin adds data to the Registry by creating and modifying existing keys. The data added by SecureLogin is sorted by computer-specific data or user-specific data. Through this distinction, SecureLogin supports multiple users and uniquely locates user profile data.

Novell SecureLogin:

- Creates a key
- Writes data to the key
- Closes or deletes a key
- Deletes a value from the key
- Saves specific key data
- Saves whole part of the system registry in a file

Registry Settings

2

This section provides information on the following:

2.1 MinimizeActiveFootprint

Purpose: memory management

- Minimizes memory usage by advising Windows to trim the amount of reserved memory down to just the amount the program is actually using
- For each executable, Windows reserves memory for its execution. The amount or memory Windows reserves for a program is not necessarily the amount that program requires, it is a best guess at how much it will use in the short term. This best guess is always a generous estimate.
- This setting can be used to advise Windows to:
  - Continue guessing how much memory each of our executables needs, just like it does for every other program (this is the default mode)
  - Continuously trim the amount of reserved memory down to only that which is currently being used. (This is aggressive mode)
  - Aggressive mode can be used to minimize the memory footprint of a running program.

2.1.1 What the setting does NOT do:

- It does not start blocking DLLs
- It does not allow you to exclude SL components individually
- It does not modify the way the product runs
- It does not prevent SecureLogin (or any other application) from running, regardless of what it is set to

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin	DWORD	MinimizeActiveFootprint

Set to:	Mode	Explanation
0xFFFFFFFF / -1	Normal Default on Windows servers	Temporarily trims the working set of the SecureLogin processes to zero, forcing the process to re-load only what it needs. Routinely empties the work set for all SecureLogin processes.
0	Default on Windows workstations	Does not minimize memory usage
>0	Aggressive	Uses SetProcessWorkingSetSize in attempt to optimize the working set size for each SecureLogin process –

Note that these values are used during calls to the function: SetProcessWorkingSetSize.

For more information on SetProcessWorkingSetSize, see:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/setprocessworkingsetsize.asp (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/setprocessworkingsetsize.asp)

Refer as well to

http://www.actividentity.com/support/kbase/sso/display_article.php?kbid=402 (http://www.actividentity.com/support/kbase/sso/display_article.php?kbid=402)

2.2 Debug Logging

Purpose: creating debug files

- Creates an `SSODebug.txt` file with additional logging for debugging purposes
- Stores the text file in: `USER PROFILE/APPLICATION DATA/SECURELOGIN/LOGS`
- Used for advanced troubleshooting
- In general, you should not turn this on unless required for troubleshooting (upon support recommendation), as the debug file size can get very large and eventually will slowdown SecureLogin.
- For the same reason, after the issue is resolved, you should turn this setting off

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE \PROTOCOM\SECURELOGIN\LOGGING\	DWORD	See list below – set for each individual module, or all modules

Names	Logging produced for following Module
All	All modules
Allint	All internal modules
Broker	SLBroker module
BrokerInt	Subset of SLBroker module
IESSO	IESSO (IE plugin)
WinSSO	Windows application
Wizard	SSO Wizard
Launcher	SLLauncher (Citrix published application launcher)
LotusSSO	Lotus Notes
JavaSSO	Java applications
JavaSSOBHO	Java web applications
SLCredMan	SLCredMan (Windows login credential manager)
MadMan	Active Directory worker module
WinLib	Internal utility library
Parser	Script parser
Ldapman	LDAP directory module
TLaunch	TLaunch (terminal emulator applications)
AWS	Advanced Windows Scripting
XMLConv	XML import/export libraries
API	Connector interfaces

2.3 Debug Logging - Citrix

Purpose: creating debug files

- Creates an `SSODebug.txt` file with additional logging for debugging purposes
- Stores the text file in: `C:\WINDOWS`
- Used for advanced troubleshooting
- In general, you should not turn this on unless required for troubleshooting (upon support recommendation), as the debug file size can get very large and eventually will slowdown SecureLogin.
- For the same reason, after the issue is resolved, you should turn this setting off

Location	Type	Name
HKLM\\SOFTWARE\\Protocom\\SecureLogin\\Virtual Channel	DWORD	See list below – set for each individual module, or all modules

Table 2-1 Workstation Registry Keys

Names	Logging produced for following Module
vdslsso	Virtual channel driver (vdslssom.dll)
tsslsso	Terminal Server Virtual Channel Driver (tsslsso.dll)
slina	SSO Gina Extention for Novell Client
slnmas	SSO Novell NMAS Extension

Table 2-2 Server Registry Keys

Names	Logging produced for following Module
sl_tsgina	SSO Gina extension for workstations in AD mode
slina	SSO Gina extension for workstations with Novell Client
sl_vc	Sl_vc.dll)

Set to:	Explanation
-1	No logging – this is the default setting
0	Full/Debug – shows all messages at a higher level
1	Information messages
2	Warning messages
3	Fatal messages
4	Customer messages

2.4 PrimaryStore

Purpose: specifies the primary directory mode

- Available in Version 6.0 releases and later
- Used to specify the primary directory mode.
- The primary directory store is set by SecureLogin at install, depending on the selected install options. The registry keys set out in this section are created as part of install process, based on those selected options.
- Note that this registry key should NOT be changed manually, as the directory mode relies on files that would normally be made available at installation

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/PROTOCOM/SECURELOGIN/SECURITY	String	PrimaryStore

Value	Explanation
NDS	eDirectory (Novell client required)
Dummy	No directory – standalone mode
MAD	Microsoft Active Directory
LDAP	LDAP Directory
SecretStore	Novell eDirectory with SecretStore (relies on Novell client)
LDAPSecretStore	LDAP login to eDirectory with SecretStore (no Novell client)

2.5 Secondary Store

Purpose: specifies the secondary data store

- Available in Version 6.0 releases and later
- Used to specify whether or not there is a local cache, or whether credentials are stored on a smart card in place of a local cache.
- The secondary store is set to file by SecureLogin at install, unless smart card support is selected, in which case the secondary store will be set to smart card
- Note that even if the registry entry shows smart card for the secondary store, the file cache will still be used until the preference 'Store credentials on card' is set; that is, this setting specifies the smart card preferences are allowed to be used, the preference enforces the smart card setting
- Note that this registry key should NOT be changed manually, as the secondary store mode relies on files that would normally be made available at installation

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/PROTOCOM/SECURELOGIN/SECURITY	String	SecondaryStore

Set to:	Explanation
File	Local file cache, no smart card support
Smartcard	Option to use store on card, or PKI encryption of credentials
	NOTE: Full implementation depends on applying smart card preferences through admin console

2.6 StorageDeviceInterfaceLibraryPKCS11

Purpose: specifies the path to the PKCS11 library

- Available in Version 6.0 releases and later

- Used to specify the path to the smartcard library, which is used only when store credentials on card is selected in the preferences
- The registry key is created at install, if smart card support is selected

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/ Protocom/ SecureLogin/Security/	String	StorageDeviceInterfaceLibraryPKCS11

Set to:	Explanation
C:\windows\system32\acpkcs211.dll	Path to ActivClient

2.7 NonRepudiationKeyCSP

Purpose: specifies the name of the cryptographic service provider

- Available in Version 6.0 releases and later
- The smart card cryptographic service provider (CSP) is selected at installation, if smart card support is selected.
- Smart card PKI encryption functions require a Microsoft cryptographic service provider module

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/ Security/	String	NonRepudiationKeyCSP

Set to:	Explanation
ctivcard gold cryptographic service provider	ActivClient CSP

2.8 DisableCache

Purpose: enables or disables the local cache file

- Available in Version 6.0.100 releases and later
- Whether or not a local cache is created by default is based on the install type
- For Windows workstations, local caches are set to on by default
- For Windows servers, local caches are set to off by default
- Machine specific alternative to the preference
- Intended to be used on multi user machines such as terminal services, citrix, to avoid wasting space with cache files

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/ Protocom/SecureLogin/	DWORD	DisableCache

Set to:	Explanation
0	Enables the local cache
1	Disables the local cache

2.9 UseGPO

Purpose: specifies whether or not the client receives SecureLogin group policies

- Available in Version 5.5 releases and later
- Relevant for Active Directory installations only
- This registry key is created automatically at installation, if the AD Group policy checkbox is selected
- When the GPO option is selected at installation, the installer will copy the SLGPO.dll to local machine, which will allow SSO policy data to be retrieved from the user's group policy
- The client will receive SecureLogin GPO data when this registry key is enabled
- The client will not receive SecureLogin GPO data when this registry key is disabled.

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	UseGPO

Set to:	Explanation
0	Enables SecureLogin group policy updates on the client
1	Disables SecureLogin group policy updates on the client

2.10 UseUserProfileDirectory

Purpose: specifies that the local cache file will be saved in application data folder

- At install, SecureLogin allows you to choose a custom location for the cache file, or specify the user profile
- If the user profile is selected, the `USEUSERPROFILEDIRECTORY` registry key is enabled
- Once enabled, the local file cache will be stored in the application data directory of the user's Windows profile: for example `C:\DOCUMENTS AND SETTINGS\USERNAME\APPLICATION DATA\SECURELOGIN`
- This registry setting will be overwritten if the `CACHEDIRECTORY` registry key is set (specifying a custom local cache location – see Section 2.11, "CacheDirectory," on page 25)

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	UseUserProfileDirectory

Set to:	Explanation
0	Does not store the cache file in the user's application data folder: see the CacheDirectory registry setting for the cache location
1	Stores the cache file in each user's application data folder This is the recommended setting: especially if more than one user is likely to login to the machine

2.11 CacheDirectory

Purpose: specifies that the local cache file is saved in a custom location

- At install, SecureLogin allows you to choose a custom location for the cache file, or specify the user profile
- If a custom location is selected, the `CACHEDIRECTORY` registry key is enabled; and the local file cache will be stored in the named location
- Once set, this key will overwrite the UseUserProfileDirectory (page 24) registry setting

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	String	CACHEDIRECTORY

Set to:	Explanation
"CacheDirectory"="c:\path"	Stores the cache file for every user on this machine in named location

2.12 CacheExpiryDays

Purpose: specifies the number of days that the local cache will remain on the machine

- This key is NOT created by default – you must create it manually
- This key allows you to nominate the number of days that the local cache will live
- If SecureLogin has not been used for the nominated number of days, the local cache is deleted
- The counter starts again, each time the SecureLogin is run, and the local cache is refreshed

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	CacheExpiryDays

Set to:	Explanation
Number of days	Deletes the local cache after the nominated number of days, if SecureLogin has not been used and the cache updated in that time

2.13 SlowLinkOptimization

Purpose: changes how often SecureLogin saves data back up to the directory, to cater for slow network links

- This key is NOT created by default – you must create it manually
- This key provides a workaround for slow network connections, such as running SecureLogin over a dialup VPN where response times are relatively slow
- Usually, when performing credential updates such as saving a new logon, changing a password etc, SecureLogin saves the changed credential data back to the directory before proceeding with the login to the web page or application etc
- When this registry key is set, these changes will not be saved to the directory as soon as they have occurred; rather, they will be saved only to the local cache, and saved to the directory at the next cache refresh
- **WARNING:** if you have applied this setting and exit SecureLogin after changes are made but before the next refresh has occurred, the changes will not be saved to the directory until the next login on this machine. If you move to another machine during that time the changes saved to the local cache on the first machine will not be made available on the next machine

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	SlowLinkOptimization

Set to:	Explanation
1	SecureLogin will not save credential changes to the directory immediately, but will save these changes to the directory only at the next cache refresh
0	SecureLogin saves credential changes to the directory immediately

2.14 ForceHKLMandNoDPAPI

Purpose: changes the way SecureLogin creates the unique user key that encrypts SecureLogin data; used to allow Mandatory, temporary and roaming profiles to be used in MS Active Directory installs

- Available in Version 6.0.103 releases and later
- If this registry key is NOT set, the Microsoft DPAPI is used to generate a unique user key that is used to encrypt user credentials in the directory. This is the default mode
- This registry key is used when the MS DPAPI is not able to be accessed and provides an alternate method of generating the unique user key

- Deployments using standard MS profiles do not use this key
- However, if you are using roaming, mandatory or temporary profiles, the DPAPI option does not work due to limitations in the Microsoft API (the MS DPAPI does not make itself available to these types of profiles). You should create this key, to allow those profiles to be handled correctly

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	ForceHKLMandNoDPAPI

Set to:	Explanation
1	SecureLogin will not create the unique user key using the MS DPAPI Use this setting for mandatory, roaming or temporary profile deployments
0	SecureLogin creates the unique user key using the MS DPAPI This is the default, and is standard for non mandatory, roaming or temporary profile AD deployments

2.15 DlgOnSaveDirVar

Purpose: disables the SecureLogin splash screen when SecureLogin saves or loads user's data

- This key is NOT created by default, you must create it manually
- Usually, the SecureLogin splash screen displays, each time SecureLogin loads or saves data in the directory / cache file.
- From version 6.1 and onwards, an administrative preference is available to disable the splash screen at start up: "Display splash screen on start up".

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWord	DlgOnSaveDirVar

Set to:	Explanation
1	Disables SecureLogin splash screen when SecureLogin loads or saves data
0	The SecureLogin splash screen will display when SecureLogin loads or saves data (default setting)

2.16 PreferredADAMInstances

Purpose: specifies the location of the ADAM instance

- Applicable only for MS ADAM installations

- SecureLogin uses the Global Catalog to locate the ADAM instance
- This key can be used to specify a different ADAM server

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	String	PreferredADAMInstances

Set to:	Explanation
[adam-server-address]:[adam-port]	For example: 127.0.0.1:5389 Port should be the "normal" ADAM port, not the SSL port.

2.17 LDAP Settings

Purpose: Allows you to specify LDAP settings such as the Primary Host and location of the certificate file so it is made available to all users of the machine

- The keys in this section are applicable to all LDAP mode installs, including LDAP to eDirectory, LDAP to AD, LDAP to ADAM, other LDAP compliant directory installs
- It is recommended that to allow seamless login to the LDAP connection, these keys are created on the machine before a user logs into SecureLogin for the first time; the key should be created in HKLM, and the settings will be made available to all users of the machine, automatically, in HKCU
- If the keys are not present when the user logs in, the user will be prompted to select the Advanced option in the LDAP login dialog, to enter the connection details for their LDAP server

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	String	LDAP Settings

Set to:
"PrimaryHost"="IP address"
"SecondaryHost"="IP address"
"PrimaryPort"=dword:0000027c
"SecondaryPort"=dword:0000027c
"SSL Cert File"="C:\\CertLocation\\client.der"
"Context1"="cn=users,dc=abc,dc=com"
"Context2"="cn=managers,dc=abc,dc=com"

2.18 CacheLDAPCredentials

Purpose: Allows seamless LDAP login for non e-Directory installs in online mode

- Available in Version 6.0.106 release and later
- Relevant to LDAP mode installations without LDAPAuth only (ie non e-Directory LDAP modes)
- Registry key must be created manually
- This key allows seamless login into LDAP for online mode
- If the online login registry entry is set, when SSO starts up in LDAP mode, after Windows login, it presents an LDAP login dialog. The user enters their credentials into the LDAP dialog at that first login and selects OK
- SecureLogin automatically caches these credentials in the user's HKCU registry hive and for each subsequent online logon, the user will NOT be prompted to re-enter their LDAP credentials, as SSO will retrieve these from the registry
- Note that the HKLM location for the online LDAP cache setting will make this logic available to all SecureLogin users of the machine.
- However, the cached credential will be stored encrypted in HKCU for each user: in HKCU\Software\Protocom\SecureLogin\LDAPCreds. This HKCU registry key is created automatically.
- If, at first online login, the user enters incorrect LDAP credentials at the prompt, SecureLogin will prompt the user with a message that the credentials are incorrect, and will allow the user to enter the credentials again.
- If the administrator changes the user's LDAP password, when SecureLogin starts up, it will try to start SecureLogin with the cached credentials, but will fail. It will then present the user with the credentials are incorrect message and ask the user to enter their credentials again. Once the user enters the credentials, SecureLogin will ask the user for the passphrase (normal protections apply: ie non-repudiation upon admin password reset). Once the user enters the correct passphrase, SecureLogin saves the new credentials in the registry, and logs the user on. The subsequent login is seamless
- If the LDAP server is not available (eg IP address has changed, network down etc) SecureLogin will startup, try the cached credentials and fail, It will then present an error message and then re-present the online dialog prompting the user to enter their LDAP credentials (username, password, server IP)..The user can alter the server IP in this dialog. Upon successful authentication, the saved credentials will be saved to the registry
- If the user cancels the online login, and if the offline registry key is set (see registry entry in following section), SecureLogin will start automatically in offline mode
- If the offline registry key is not set, the user will be prompted with the LDAP offline dialog box

Location	Type	Name
HKLM\Software\Protocom\SecureLogin\	DWORD	CacheLDAPCredentials

Set to:	Explanation
1	Allows caching of LDAP credentials for seamless LDAP online login

Set to:	Explanation
0	Disables caching of LDAP credentials for seamless LDAP online login.

2.19 AlwaysClearUsername

Purpose: clear SSO credentials on sys Tray reload

- This only applies to NDS and SecretStore mode

Location	Type	Name
HKLM\Software\Protocom\SecureLogin\	DWORD	AlwaysClearUsername

Set to:	Explanation
1	SecureLogin will clear SSO credentials on sys Tray reload(slproto /reload)
0	SecureLogin will not clear SSO credentials

2.20 SeamlessStandalone

Purpose: Defines the standalone behavior

- Available in 6.0 and onwards
- Defines the standalone behavior in regards to credentials to use to start SecureLogin.
- Either SecureLogin starts using the logged in user's credentials or it is in multiple account mode and starts prompting for the users to select their account

Location	Type	Name
HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin	DWORD	SeamlessStandalone

Set to:	Explanation
1	When login credentials are used to start SSO (single user mode)
0	When multiple users mode is on.

2.21 IESSOBHO

Purpose: configure the way SecureLogin works with IE

- Relevant to the way SecureLogin process IE dialogs: it can either process through the BHO interface, as it does by default, or watch the IE process and attach to it
- Side effect: this may slow down the process

Location	Type	Name
HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin	DWORD	IESSOBHO

Set to:	Explanation
1	Default value: SecureLogin works through the BHO interface
0	Integrate to the IE process instead.

2.22 AllowAPIAccessPreference

Replaced by the preference “Provide API Access”

Location	Type	Name
HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin	DWORD	AllowAPIAccessPreference

Set to:	Explanation
0	Default value: no access is allowed
1	Access to the API is granted

2.23 SyncToHandHeldPreference

Purpose: Enables synchronization with API-enabled handheld device for an application definition

- This has been replaced by a preference setting attached to each application definition: “Synchronize with Mobile”

Location	Type	Name
HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin	DWORD	SyncToHandHeldPreference

2.24 JREInstallDir

Purpose: Record the JRE location against which one SecureLogin is installed

- When SecureLogin detects a new JRE and installs its component against it, then a registry key is created to keep track of the supported JRE
- In versions prior to 6.1 this key was referencing the only supported JRE
- In SecureLogin 6.1 and later, this key is used for backward compatibility purpose only as SecureLogin is able to install and work with several JREs.

Location	Type	Name
HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin\JavaSSO	REG_SZ	JREInstallDir

Set to:	Explanation
path	Path to the JRE directory

2.25 DisplayInitialLoadSplash

Purpose: disables the SecureLogin splash screen at startup

- Available in 6.1 and onwards
- This key is created by default and linked to the preference: “Display splash screen on start up”

Location	Type	Name
HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin	DWORD	DisplayInitialLoadSplash

Set to:	Explanation
1	Default setting: Display SecureLogin splash screen at startup
0	Disable SecureLogin splash screen at startup

2.26 StopIESSOForDownloadPage

Purpose: performance with IE when file download occurs

- This key is not created by default
- During file download, it can happen that IE hangs.
- The key is used to inform that SecureLogin whether it should execute script or not when a file download occurs

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	StopIESSOForDownloadPage

Set to:	Explanation
0	Default setting: IESSO does not check the title of foreground window and executes a script
1	IESSO checks the title of foreground window; if the title is “File Download”, then script execution is skipped

2.27 APISettingsEnabled

This key is not used any more

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	APISettingsEnabled

2.28 LDAPIsSynched

Purpose: Configure the LDAP credentials synchronization mode

- This key has been introduced in SecureLogin 6.1 Hotfix FIXC0803002
- Relevant only in LDAP mode, tested with Sun One only
- Informs if the login and LDAP credentials are synchronized.
- This key is not created by default

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	LDAPIsSynched

Set to:	Explanation
0	Or not present is the default setting. Credentials from the first login directory and the SecureLogin data store directory are not synchronized.
1	Credentials from the first login directory and the SecureLogin data store directory are synchronized.

2.29 SyncDelay

Purpose: Configure a delay before retrying to authenticate

- This key has been introduced in SecureLogin 6.1 Hotfix FIXC0803002
- Relevant only in LDAP passthrough mode, i.e. if the “LDAPIsSynched” registry setting is defined in HKLM registry hive and is also set to 1 (where 1 means that the credentials are synchronized between the first login directory and the SecureLogin data store directory)
- Configures the delay before trying to authenticate to the directory in case synchronization between the first login directory and the SecureLogin data store directory is quite long. Consequently the value associated to this key must be relevant with the delay in directories synchronization.
- This key is not created by default

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	SyncDelay

Set to:	Explanation
number	Delay time in seconds
0	Or non present, default setting, no delay.

2.30 Contextless login

Purpose: Several keys have been introduced in SecureLogin 6.1 Hotfix FIXC0803002, in order to perform LDAP lookup anonymously or using a default user account

- Relevant only in LDAP mode
- These keys are not created by default
- The encrypted string that contains the dummy account (full DN and password) is generated using LDAPCE tool.

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/LDAPSettings	DWORD	LDAPAnonymousLoginsDisallowed
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/LDAPSettings	DWORD	LDAPContextlessSearchBindcreds

Name	Set to:	Explanation
LDAPAnonymousLoginsDisallowed	0	Or not present is the default setting. Anonymous binding is performed
	1	Generic account is required to perform a LDAP lookup. Information are defined with the 2 following keys
LDAPContextlessSearchBindDN	DWORD	Encrypted string that contains the full user DN and the password

2.31 PromptIfLDAPServerDown

Purpose: Configure the offline mode behavior when LDAP server is not reached

- This key has been introduced in SecureLogin 6.1 Hotfix FIXC0806003
- Relevant in LDAP mode
- Configures the way SecureLogin goes offline when the LDAP server cannot be reached.
- This key is not created by default

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	PromptIfLDAPServerDown

Set to:	Explanation
0	or not present is the default configuration: (seamless) offline mode login will be effected if LDAP credentials are synchronized. The user will not be presented with any opportunity to alter their LDAP settings (IP address of the LDAP server etc). Any LDAP server configuration changes must be applied outside the login session (ie via altering the registry via ADM update). SecureLogin will not attempt to connect in online mode if and when an LDAP server connection is subsequently restored during the current user session
1	SecureLogin will initially assume LDAP and network settings are good, and ask the user if they want to operate offline ◆ A Yes response effects seamless offline mode login ◆ A no response presents the LDAP login dialog, where the user can change credentials or advanced LDAP connection settings.

2.32 CustomSearchFilter

Purpose: Customize the LDAP search filter

- This key has been introduced in SecureLogin 6.1 Hotfix FIXC0803002
- Relevant only in LDAP mode
- By default, if the registry key/value is not specified, SecureLogin will now use the attributes supplied to build the search filter eg: (|(uid=*fred*)(samAccountname=*fred*))
- If the registry key is populated with a value, then SecureLogin will attempt to use that value as the search filter and will ignore the attributes listed in the LDAP login dialog.
- The CustomSearchFilter is built in the form eg: (&(objectClass=orgPerson)((orgUserAliases=%s@*)) where%s is detected and replaced with the username provided to end up as (&(objectClass=orgmPerson)((orgUserAliases=fred@*)). Any search filter can be used here and any instance of%s will be replaced with the username.
- This key is not created by default

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/LDAP Settings	REG_SZ	CustomSearchFilter

Set to:	Explanation
string	The string value can be assigned as (&(objectClass=geoPerson)(geoUserAliases=<user>@*))

2.33 SendMessageTimeoutvalue

http://www.actividentity.com/support/kbase/sso/display_article.php?kbid=982 (http://www.actividentity.com/support/kbase/sso/display_article.php?kbid=982)

2.34 WindowClassesToExclude

Purpose: Exclude application windows from being read by SecureLogin

- This key has been introduced in SecureLogin 6.1 Hotfix FIXC0804000
- Contains a list of Window classes
- This key is read at startup to exclude application windows from being read by SecureLogin
- These windows classes would include hidden windows provided by the application that are not used for SSO processes, but can slow down the SSO process as SecureLogin reads them.
- This fix was specially intended to Microsoft Outlook
- This key is not created by default.

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	REG_SZ	WindowClassesToExclude

Set to:	Explanation
string	The string holds a comma-separated list of Window classes to ignore. For Microsoft Outlook, add the following string entries to the registry: • CLIPBRDWNDCLASS, WMS ST Notif Class

2.35 PubAppReload

Purpose: Reload when Published application starts

- This key has been introduced in SecureLogin 6.1 Hotfix FIXC0808001
- This remedies an issue where SecureLogin doesn't refresh to read any new password when published application starts as a result newly started application is still using old password
- Due to the nature of how AppSetup key works in Terminal Server environment, this fix will only apply to published applications that are setup with SecureLogin prior to 6.1 using `SLLauncher.exe`
- This key is not created by default.

Location	Type	Name
HKEY_LOCAL_MACHINE/SOFTWARE/Protocom/SecureLogin/	DWORD	PubAppReload

Set to:	Explanation
0	Or non present: default configuration
1	Reload when published application starts

2.36 IgnoreADAMSCP

Purpose: Scan the ADAM SCP list or ignore and goes offline when the default SSO ADAM instance is unavailable

- Available in SecureLogin SSO 6.1 plus FIXC0810001 or above
- When the SSO configured ADAM instance is unavailable, SecureLogin reads this key to know if it needs to connect to another ADAM instance that is listed in the ADAM SCP object
- Set this key if only one ADAM instance (the default SSO registered) is configured with the SecureLogin settings

Location	Type	Name
HKLM\Software\Protocom\SecureLogin	DWORD	IgnoreADAMSCP

Set to:	Explanation
1	SecureLogin ignores the list of ADAM instances that are stored in SCP and automatically switches to offline mode.
0	Or non present: Default configuration SecureLogin scans the SCP list to find another ADAM instance to connect to

Refer to http://www.actividentity.com/support/kbase/sso/display_article.php?kbid=992 (http://www.actividentity.com/support/kbase/sso/display_article.php?kbid=992) for more information.

2.37 BannerPath

Purpose: Configuration of dialog banner image paths.

- Available in Novell SecureLogin 3.5.*x* and later.
- If BannerLeftPath, BannerRightPath, and BannerCenterPath are present, then these are applied and BannerPath is ignored
- If at least one of BannerLeftPath, BannerRightPath, or BannerCenterPath is missing, then BannerPath is considered.
- If BannerPath is missing, then the bitmaps from the SecureLogin resource dll are loaded.

NOTE: Make sure that the images (.bmps) fit in to the designated bitmap area. Otherwise, the bitmaps shrink or expand and the image do not look proportionate.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\BannerPath	REZ_SZ	BannerPath
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\BannerLeftPath	REZ_SZ	BannerLeftPath

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\BannerRightPath	REZ_SZ	BannerRightPath
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\BannerCenterPath	REZ_SZ	BannerCenterPath

2.38 server#

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- Repalce the hash (#) with a numeric value.
- From Novell SecureLogin 6.0 SP1, each server item must be a multi-string value.
- These values can be set from the installation dialogs or by an installation script.
- The port value can also be specified from the along with the server in a new line. By default, port 636 is used.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\Servers\server#	REG_MULTI_SZ	server#

2.39 EnableFieldOnLock

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- Allows the user to modify the user's distinguished name (DN) field of the LDAPAuth dialog during workstation unlock.
- The default action is to disable this field.
- If this value exists, regardless of the value contents the feature is enabled.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\EnableFieldOnLock		EnableFieldOnLock

2.40 DoNTAssoc

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- Activates an NT Workstation user ID to an LDAP DN association.

- By default, this setting is disabled.
- The value must be a DWORD set to 1.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\DoNTAssoc	DWORD	DoNTAssoc

2.41 DoClient32Assoc

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.
- Activates the use of the eDirectory user ID to an LDAP DN association.
- By default, this setting is enabled.
- To be enabled, the value must be a DWORD set to 1.
- To be disabled, the value must be a DWORD set to 0.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\DoClient32Assoc	DWORD	DoClient32Assoc

2.42 Debug Log - LDAPAuth

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.
- Activates the verbose debug logging feature of LDAPAuth.
- If the DWORD value is non-zero, the LDAPAuth outputs trace information using the OutputDebugString call. This trace information can be viewed using DebugView from sysinternals.com.
- The LDAPAuth writes the trace information to \LdapLog\nldapaut.log.

  NOTE: This key redirects the information generated by DWORD Debug to a series of logs. To generate the log files, both Debug and Debug log must be set.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\Debug	DWORD	Debug

2.43 UseDefaultUsername

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- Allows the dialog to keep the username field empty.
- The DWORD value must be set to 0.
- By default, default user's DN is always put in to the username field.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\UseDefaultUsername	DWORD	UseDefaultUsername

2.44 Custom LDAP Error Messages

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- The hash (#) is replaced with a numeric value of the LDAP error.
- The value is a string with the text of the error message.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\ErrorStrings\#		

2.45 ContextBasedSearch

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- The value is set to 1.
- To search, specify the set of contexts to search, such as Context1, Context2, and Context3 of the REG_SZ value.
- If an invalid context is specified, no explicit context validation is done. However, LDAP search returns an appropriate error.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\LDAP Search\ContextBasedSearch	DWORD	ContextBasedSearch

2.46 SearchAttributes

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- Set to a list of search attributes used in LDAP search.
- Only first give attributes are considered. They are:
  - fullName
  - givenName
  - sn
  - cn
  - uid

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\LDAP Search\SearchAttributes	REG_MULTI_SZ	SearchAttributes

2.47 UserAttributeToDisplay

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- The REG_SZ value allows the user to specify the attributes to be displayed in place of the DN in the LDAP GINA dialog.
- The valid attributes are:
  - fullName
  - givenName
  - sn
  - cn
  - uid
- The default behavior of printing to DN happens if the `UserAttributeToDisplay` is not present in the registry, if it contains invalid attribute, or if the specified attribute is not available for the user

NOTE: To make changes, the specified attribute must have public read access. Else, SecureLogin might not have adequate rights to fetch the specified attribute value.

For details, refer to TID 10096661 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10096661&sliceId=&docTypeID=DT_TID_1_1&dialogID=36598451&stateId=1%200%2036600095) at the Novell Support Web site. (http://www.novell.com/support)

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\UserAttributeToDisplay	REG_SZ	UserAttributeToDisplay

2.48 DuplicatesPrintableString

Purpose: Allows users to specify the string format for entries in the Select the user dialog.

- Available in Novell SecureLogin 3.5.*x* and later.
- String format can have any text with search attributes in%attributeName format, where attributeName can be cn, givenName, fullName, sn, or uid.

NOTE: The attribute names are case sensitive.

To make changes, the specified attribute must have public read access. Else, SecureLogin might not have adequate rights to fetch the specified attribute value.

For details, refer to TID 10096661 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10096661&sliceId=&docTypeID=DT_TID_1_1&dialogID=36598451&stateId=1%200%2036600095) at the Novell Support Web site. (http://www.novell.com/support)

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\DuplicatesPrintableString	REG_SZ	DuplicatesPrintableString

2.49 CertFilePath

Purpose: Allows users to specify a valid certificate file path for non-eDirectory servers.

- Available in Novell SecureLogin 3.5.*x* and later.
- This requires the user to create another registry entry named NonEdirLdap of REG_DOWORD type.
- CertFilePath is considered only if NonEdirLdap is present and set to 1.

Location	Type	Name
HKEY_LOCAL_MACHINE\Software\Novell\Login\LDAP\CertFilePath	REG_SZ	CertFilePath

2.50 UseCNasWindowsUserInCitrix

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

- If the REG_DWORD value set to 1, the CN can be used as the Windows username in the Citrix passthrough scenario.
- Without UseCNasWindowsUserInCitrix or if the value set to 0, LDAPAuth retains the existing functionality. It uses the previously logged in user.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\UseCNasWindowsUserInCitrix	REZ_WORD	UseCNasWindowsUserInCitrix

2.51 WSOnly

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.
- If the REZ_WORD value is set to 0, then by default, the LDAP login dialog switches to the *Workstation only* mode.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\WSOnly	REZ_WORD	WSOnly

2.52 DoNotShutdownNSL

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.
- If the REZ_WORD value is set to 1, Novell SecureLogin is not terminated when a workstation is locked with the *Workstation only* option in the LDAP GINA mode.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\DoNotShutdownNSL	REZ_WORD	DoNotShutdownNSL

2.53 LDAPAudit

Purpose:

- Available in Novell SecureLogin 6.0 and later.
- If the REG_DWORD value is set to 1, it is required to integrate LDAPAuth module with Novell Audit.
- With this registry configuration, the following events are sent to the Audit server from LDAPAuth:
  - Novell SecureLogin user login

- User password change at the time of LDAP GINA login
- Different user attempting to unlock the workstation

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\LdapAudit	REG_DWORD	LDAPAudit

2.54 HideAdvanced

Purpose:

- Available in Novell SecureLogin 6.0 and later.
- By default, the advanced authentication fields in the LDAP dialog are hidden and can be viewed by expanding the login dialog using the *Advanced* option.
- You can hide the Advanced option if the registry value is set to 1.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\HideAdvanced	REG_DWORD	HideAdvanced

2.55 NDSTree

Purpose: Allows users to specify the eDirectory tree name so that the eDirectory connection to the specified tree is used by LDAPAuth to automatically log in the SecureLogin user.

- Available in Novell SecureLogin 6.001 and later.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\NDSTree	REZ_SZ	NDSTree

2.56 DisableCancel

Purpose: Allows the user to activate or deactivate the Cancel button on the Novell SecureLogin interface.

- Available in Novell SecureLogin 6.00.005 and later.
- If the value is set to 0, the Cancel button is operational.
- If the value is set to 1, the Cancel button is disabled.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\DisableCancel	REG_DWORD	DisableCancel

2.57 TryRegCredInOffline

Purpose: Allows seamless login to offline mode using Windows user credentials

- Available in Novell SecureLogin 6.00.005 and later.
- If the value is set to 1 and the following conditions are met, Novell SecureLogin allows a seamless log in to offline mode using the Windows credentials.
  - LDAP is installed in Credential Manager, GINA, or Credential Provider mode.
  - LDAP user is associated to Windows user. This is applicable for LDAP Credential Manager mode.
  - LDAP and Windows user credentials are same.
  - Network or server is not reachable for the client workstation.
  - The Workstation only option is selected during login for GINA or Credential Provider mode.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\TryRegCredInOffline	REG_DWORD	TryRegCredInOffline

2.58 LdapDlgcaption

Purpose: Allows the user to specify a customized title for the LDAP login dialog.

- Available in Novell SecureLogin 6.1 and later.
- If this registry configuration is not present, the Novell login dialog is displayed.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\LdapDlgCaption	REZ_SZ	LdapDlgcaption

2.59 WindowsGroupstoExclude

Purpose: Allows the administrators to specify the list of Windows User Groups.

- Available in Novell SecureLogin 6.1 and later.
- The LDAP Login dialog is not be displayed in Credential Manager mode to users of the specified groups.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\WindowsGroupstoExclude	REG_MULTI_SZ	WindowsGroupstoExclude

2.60 VerifySSLCert

Purpose: Verify the certificate of the server before LDAP authentication

- Available in Novell SecureLogin 6.00.103 and later.
- If the value is set to 1, it verifies the certificate of the server before LDAP authentication.
- If the certificate does not exist for that server locally on the workstation, it prompts the user for validation and stores it after confirmation.
- If the user rejects the certificate, LDAP authentication is cancelled.

Location	Type	Name
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\LDAP\VerifySSLCert	REG_DWORD	VerifySSLCert

2.61 DefaultDN

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKEY_CURRENT_USER\Software\Novell\Login\LDAP\DefaultDN **NOTE:** The value is dynamic and is likely to change.		DefaultDN

2.62 LDAPAuthLoginSuccessful

Purpose: Indicates that the user has successfully authenticated via LDAPAuth.

- Available in Novell SecureLogin 3.5.*x* and later.
- This value is dynamic and can change without warning.

Location	Type	Name
HKEY_CURRENT_USER\Software\Novell\Login\LDAP\LDAPAuthLoginSuccessful		LDAPAuthLoginSuccessful

2.63 LDAPAuthNMASSelected

Purpose: Specifies whether the NMAS option was selected during the last authentication or not.

- Available in Novell SecureLogin 3.5*.x* and later.
- A value of 1 indicates that the NMAS option was selected.

Location	Type	Name
HKEY_CURRENT_USER\Software\Novell\Login\LDAP\LDAPAuthNMASSelected	DWORD	LDAPAuthNMASSelected

2.64 LDAPAuthNMASSequence

Purpose: Specifies the last NMAS sequence with which the user is authenticated.

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKEY_CURRENT_USER\Software\Novell\Login\LDAP\LDAPAuthNMASSequence	REG_SZ	LDAPAuthNMASSequence

2.65 PrintableName

Purpose: Specifies the printable name of the last authenticated user.

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKEY_CURRENT_USER\Software\Novell\Login\LDAP\PrintableName	REG_SZ	PrintableName

2.66 ConfigFile

Purpose: Specifies the path for the configuration file.

- Available in Novell SecureLogin 6.1*.x* and later.
- The value is set to Default if the directory mode is selected for saving the configuration file.

Location	Type	Name
HKLM\SOFTWARE\Novell\ARS	<DASINSTALLDIR>\actions.xml	ConfigFile

2.67 ConfigTree

Purpose: Mentions the server name from the configuration file is retrieved.

- Available in Novell SecureLogin 6.1.*x* and later.
- The value is applicable only if the directory is used to access the actions.xml file.
- The Default value is selected if the directory mode is selected for saving the configuration file.

Location	Type	Name
HKLM\SOFTWARE\Novell\ARS	<Tree name>	ConfigTree

2.68 ConfigObject

Purpose: Mentions the object name which contains the configuration file.

- Available in Novell SecureLogin 6.1.*x* and later.
- The value is applicable only if the directory is used to access the actions.xml file.
- The Default value is selected if the directory mode is selected for saving the configuration file.

Location	Type	Name
HKLM\SOFTWARE\Novell\ARS	Object pointing to actions.xml	ConfigObject

2.69 LogFilePath

Purpose: Mentions the path of the log file.

- Available in Novell SecureLogin 6.1.*x* and later.
- Takes the default path.

Location	Type	Name
HKLM\SOFTWARE\Novell\ARS	DASINSTALLDIR>DASLog.txt	LogFilePath

2.70 LogLevel

Purpose: Mentions the level for log.

- Available in Novell SecureLogin 6.1.*x* and later.
- The log level can vary from 1 to 4.
  - **0:** Log Normal
  - **1:** Log Error
  - **2:** Log Action
  - **4:** Log Verbose

Location	Type	Name
HKLM\SOFTWARE\Novell\ARS	1	LogLevel

2.71 InstallDir

Purpose: Mentions the install directory for Desktop Automation Services (DAS)

- Available in Novell SecureLogin 6.1*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\ARS	<DASINSTALLDIR>	InstallDir

2.72 Dllname

Purpose: Mentions the path for `LDAPLoginExtension.dll`

- Available in Novell SecureLogin 6.1*.x* and later.
- This is available if the install mode is LDAP or the protocol for eDirectory is LDAP.

Location	Type	Name
HKLM\SOFTWARE\Novell\Login\LDAP\Plugins\DASEvent	SystemFolder>LDAPLoginExtension.dll	Dllname

2.73 Logoff

Purpose: Specifies the event that is invoked on logging out.

- Available in Novell SecureLogin 6.1*.x* and later.
- This is available if the install mode is LDAP or the protocol for eDirectory is LDAP.

Location	Type	Name
HKLM\SOFTWARE\Novell\Login\LDAP\Plugins\DASEvent	LDAPAUTH_EventLogoff	Logoff

2.74 Logon

Purpose: Indicates the event invoked during log in.

- Available in Novell SecureLogin 6.1*.x* and later.
- This is available if the install mode is LDAP or the protocol for eDirectory is LDAP.

Location	Type	Name
HKLM\SOFTWARE\Novell\Login\LDAP\Plugins\DASEvent	LDAPAUTH_EventLogon	Logon

2.75 LoginExtDesc

Purpose: Indicates the event invoked during log in.

- Available in Novell SecureLogin 6.1.*x* and later.
- This is available only if Novell Client is installed.

Location	Type	Name
HKLMOFTWARE\Novell\Graphical Login\NWLGE\DASLoginEvent	REG_SZ	LoginExtDesc

2.76 LoginExtName

Purpose: Indicates the path for `LoginEvent.dll`

- Available in Novell SecureLogin 6.1.*x* and later.
- This is available only if Novell Client is installed.

Location	Type	Name
HKLM\SOFTWARE\Novell\Graphical Login\NWLGE\DASLoginEvent	REG_SZ	LoginExtName

2.77 LoginExtType

Purpose:

- Available in Novell SecureLogin 6.1.*x* and later.
- This is available only if Novell Client is installed.

Location	Type	Name
HKLM\SOFTWARE\Novell\Graphical Login\NWLGE\DASLoginEvent	REG_DWORD	LoginExtType

2.78 Authentication retries

Purpose: This value specifies the number of consecutive times Secure Workstation can fail before it detects the presence of AIR-ID badge and trigger a device removal event.

- Available in Novell SecureLogin 3.5.*x* and later.
- Secure Workstation pauses one second between retries.

Location	Type	Name
	To be specified by administrator	

2.79 Sequence to authenticate

Purpose: This specifies the sequence to be used when authenticating using pcProx

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
	To be specified by the administrator	

2.80 OutputDebugString

Purpose: Output trace information

- Available in Novell SecureLogin 3.5.*x* and later.
- If the value is set to yes, then pcprox will will output trace information using the OutputDebugString call. This trace information can be viewed using DebugView from sysinternals.com

Location	Type	Name
		OutputDebugString

2.81 Enable file logging

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.
- If this value is yes, then pcProx will write trace information to a set of log files for each of the pcProx component. The log files can be found at <root drive>cproxlog

Location	Type	Name

2.82 0 to 15 (Secure Workstation - Allowed Processes)

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	0
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	1
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	2
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	3
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	4
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	5
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	6
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	7
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	8
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	9
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	10
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	11
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	12

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	13
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	14
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Allowed Processes	REG_SZ	15

2.83 ConsoleLockAction

Purpose: Specifies the lock action that happens for a session connected to the local console.

- Available in Novell SecureLogin 3.5*.x* and later.
- The possible values are:
  - **0*1:** Closes all programs. This can be combined with the Logout of the Network value.
  - **0*2:** Logs out of the network (Client32 and, or the LDAP GINA). This can be combined with the Close all Programs value.
  - **0*4:** Logs out of Windows.
  - **0*8:** Locks the workstation or disconnects the terminal services session.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Policy	DWORD	ConsoleLockAction

2.84 DeviceFlags

Purpose: Specifies information about authentication devices to be monitored.

- Available in Novell SecureLogin 3.5*.x* and later.
- The possible values are:
  - **0*1:** Monitors device flags. Secure Workstation does not monitor any devices if this flag is not set.
  - **0*2:** Monitors all devices.
  - **0*4:** Uses a device list. Monitors devices specified in the Secure Workstation Policy, Devices key.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Policy	DWORD	DeviceFlags

2.85 EnableLinkedConnections

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System		EnableLinkedConnections

2.86 SecureWorkstation

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\SecureLogin		SecureWorkstation

2.87 Flags

Purpose: Contains flags specified in the local policy

- Available in Novell SecureLogin 3.5.*x* and later.
- The possible values are:
  - **0*1:** Policy active flag.
  - **0*2:** Inactivity timeout flag.
  - **0*4:** Forces logoff flag. If this flag is set, Secure Workstation passes the ESX_FORCE flag to ExitWindowsEx when logging out of Windows.
  - **0*8:** Forcefully terminate applications. If this flag is set, Secure Workstation calls TerminateProcess on applications that do not terminate within a specified time period.
  - **0*10:** Displays the inactivity warning dialog before taking the lock action due to an inactivity timeout.
  - **0*20:** Executes a post-policy command.
  - **0*40:** If a post-policy command is specified in both the local policy and the network policy, use the command from the network policy. If this flag is set, then Secure Workstation always uses the command from the local policy.
  - **0*80:** Closes all programs when the network user logs off.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy	DWORD	Flags

2.88 IdleTimeout

Purpose: Specifies the user inactivity timeout.

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Policy	DWORD	IdleTimeout

2.89 KillAppTimeout

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.
- This value is used by the Close all programs lock action.
- If the forcefully terminate applications flag is set, this is the amount of time Secure Workstation waits for applications to close before forcefully terminating them.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Policy	DWORD	KillAppTimeout

2.90 00000010

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \1.0\LCM Paths		00000010

2.91 UseClient32

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Policy	DWORD	UseClient32

Set to:	Explanation
0	Secure Workstation ignores the Client32 connections. It does not monitor the Client 32 connections and does not terminate any Client32 connections when executing the Log out of the Network lock action.

2.92 UseLDAPAuthClient

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Policy	DWORD	UseLDAPAuthClient

Set to:	Explanation
0	Secure Workstation ignores events from the LDAPAuth Client and does not clear the LDAPAuth Client credentials.

2.93 LockCommand

Purpose: This is a post-policy command.

- Available in Novell SecureLogin 3.5.*x* and later.
- The SMP executes this command using CreateProcess after a close all programs and, or the log out of the network lock action is executed.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\Secure Workstation\Policy	String	LockCommand

2.94 UseClient32

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy	DWORD	UseClient32

Set to:	Explanation
0	Secure Workstation ignores Client32 connections. In this case, it does not monitor the Client32 connection. It terminates any Client32 connections when executing the Log out of the Network lock action.

2.95 UseLDAPAuthClient

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy	DWORD	UseLDAPAuthClient

Set to:	Explanation
0	Secure Workstation ignores the events form the LDAPAuth Client. It does not clear the LDAPAuth Client credentials.

2.96 NetLogoutConsoleLockAction

Purpose: Specifies the lock action that occurs for a session connected to the local console.

- Available in Novell SecureLogin 3.5*.x* and later.
- The possible values are:
  - **0*1:** Closes all the programs. This can be combined with the Logout of the Network value.
  - **0*2:** Logs out of the network (Client32 or the LDAP GINA). This can be combined with the Close all Programs value.
  - **0*4:** Logs out of Windows.
  - **0*8:** Locks the workstation or disconnects the terminal services session.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy	DWORD	NetLogoutConsoleLockAction

2.97 NetLogoutTerminalLockAction

Purpose: Specifies the lock actions that occurs for remote sessions.

- Available in Novell SecureLogin 3.5.*x* and later.
- The possible values are:
  - **0*1:** Closes all the programs. This can be combined with the Logout of the Network value.
  - **0*2:** Logs out of the network (Client32 or the LDAP GINA). This can be combined with the Close all Programs value.
  - **0*4:** Logs out of Windows.
  - **0*8:** Locks the workstation or disconnects the terminal services session.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy	DWORD	NetLogoutTerminalLockAction

2.98 DllName

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wsacclcm		DllName

2.99 Impersonate

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wsacclcm		Impersonate

2.100 Lock

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wsacclcm		Lock

2.101 Logoff (Secure Workstation)

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wsacclcm		Logoff

2.102 StartShell

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wsacclcm		StartShell

2.103 Unlock

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wsacclcm		Unlock

2.104 QLLGUI

Purpose: Contains settings for customizing the Quick Login/Logout Interface dialog.

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation	String	QLLGUI

Name	Value Type	Explanation
Bitmap	String	This value contains the path and name of a bitmap to be displayed on the dialog box. If this setting does not exist, a default bitmap will be displayed.
ShowBitmap	DWORD	If this value is zero, then a bitmap will not be shown at the top of the dialog. This will reduce the size of the dialog.
AlwaysOnTop	DWORD	If this value is non-zero, the dialog will register itself as an ?always on top? window, causing it to appear above most other windows on the system. If this setting does not exist, the dialog will have the always on top window style.
Transparent	DWORD	If this value is non-zero, the dialog will make itself transparent when it does not have the focus. If this setting does not exist, the dialog will never make itself transparent.
XCoord	DWORD	This is the X screen coordinate of the upper-left corner of the dialog. The default setting is the top-left corner of the screen.

Name	Value Type	Explanation
YCoord	DWORD	This is the Y screen coordinate of the upper-left corner of the dialog. The default setting is the top-left corner of the screen.
ShowLockButton	DWORD	If this setting is one, the ?Lock Workstation? button will not be displayed, and the ?Lock Workstation? option will not show up on the tray icon popup menu.
ShowLogoutButton	DWORD	If this setting is one, the ?Logout? button will not be displayed, and the ?Logout? option will not show up on the tray icon popup menu.
UseTrayIcon	DWORD	If this setting is zero, no tray icon will be used. If it is one, a tray icon will be used, but the dialog will not be displayed unless the user double-clicks the tray icon. If this setting is two, the dialog will display automatically each time the user ID changes. The default will be two.
ShowCloseButton	DWORD	This setting controls the ?X? button in the top right corner of the dialog. If this setting is zero, the X button will not be available to the user, and the user will be unable to close the dialog. The default setting is one.
ShowMinimizeButton	DWORD	This setting controls the minimize button in the top right corner of the dialog. If this setting is zero, the minimioze button will not be available to the user. The default setting is one.
ShowTitleBar	DWORD	This setting can be used to hide the title bar. The default setting is one.
WindowTitle	DWORD	This setting can be used to customize the window title shown in the title bar.
ShowUserID	DWORD	If this setting is non-zero, the dialog will display the current user ID. The default is one.
ShowFullDN	DWORD	If this setting is non-zero, the user?s FDN will be displayed instead of just his common name. The default setting is zero.

Name	Value Type	Explanation
ShowFullName	DWORD	If this setting is non-zero, the dialog will attempt to lookup the user?s full name and display it on the dialog if it is available. The default is one.
ShowInactivityTimeout	DWORD	If this setting is non-zero, the dialog will show the number of seconds remaining before an inactivity timeout. The default is zero.
ShowWhenLocked	DWORD	If this setting is non-zero, the dialog will display itself next to the GINA when the workstation is locked. The default is one.
ShowDialog	DWORD	If this setting is one, the dialog will not be displayed. The dialog window will be hidden, and the user will only see the tray icon, if it has been enabled. The default behavior is to show the dialog.
ShowExitOnMenu	DWORD	If this setting is zero, then the ?Exit? option will not be displayed on the tray icon popup menu. This will prevent users from shutting down the Quick Login/ Logout Interface.
TextColorB TextColorG TextColorR	DWORD	These three settings can be used to change the color of the text on the dialog. The default text color is black. These settings are only used when the dialog is transparent. Keep in mind that certain text colors may be hard to read against the background.

2.105 LockCommand

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\		

2.106 include

Purpose:

- Available in Novell SecureLogin 3.5*.x* and later.

Location	Type	Name
HKLM\	REG_DWORD	

2.107 0 to 10 (Secure Workstation - Process List)

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	0
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	1
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	2
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	3
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	4
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	5
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	6
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	7
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	8
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	9
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy\Process List	REG_SZ	10

2.108 SW

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		SW

2.109 TerminalLockAction

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy		TerminalLockAction

2.110 WarnCountdown

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Policy		WarnCountdown

2.111 Version (SecretStore)

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\Single Sign-on	REG_DWORD	Version

2.112 EventMessageFile

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		EventMessageFile

2.113 CategoryMessageFile

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		CategoryMessageFile

2.114 CategoryCount

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		CategoryCount

2.115 TypesSupported

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		TypesSupported

2.116 EventMessageFile

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		EventMessageFile

2.117 CategoryMessageFile

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		CategoryMessageFile

2.118 CategoryCount

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		CategoryCount

2.119 TypesSupported

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\\SYSTEM\CurrentControlSet\Services\EventLog\Application\SecureWorkstation		TypesSupported

2.120 Numeric values (pcProx)

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\pcProx\ID\LDAPServers		0
HKLM\SOFTWARE\Novell\NMAS\1.0\ID		1
HKLM\SOFTWARE\Novell\NMAS\1.0\ID		2
HKLM\SOFTWARE\Novell\NMAS\1.0\LCM Paths		19

2.121 Plus Sign (pcProx)

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Registered Methods\pcProx		+
HKLM\SOFTWARE\Novell\NMAS\1.0\ID		+
HKLM\SOFTWARE\Novell\NMAS\MethodData\pcProx\ID		+
HKLM\SOFTWARE\Novell\NMAS\MethodData\pcProx\ID\LDAPServers		+

2.122 MethodID

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Registered Methods\pcProx		MethodID

2.123 RemovalDLL

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\Secure Workstation\Registered Methods\pcProx		RemovalDLL

2.124 Retries

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\pcProx		retries

2.125 Tree

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\pcProx\ID		Tree

2.126 Server

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS\MethodData\pcProx\ID		Server

2.127 Sequence

Purpose:

- Available in Novell SecureLogin 3.5.*x* and later.

Location	Type	Name
HKLM\SOFTWARE\Novell\NMAS \MethodData\pcProx\ID		Sequence