Novell Nsure™ SecureLogin

3.51

www.novell.com

TERMINAL SERVICES GUIDE

December 11, 2003

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Nsure SecureLogin 3.51 Terminal Services Guide
December 11, 2003

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.
eDirectory is a trademark of Novell, Inc. in the United States and other countries.
NDS is a registered trademark of Novell, Inc. in the United States and other countries.
NMAS is a trademark of Novell, Inc. in the United States and other countries.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.
Novell Client is a trademark of Novell, Inc. in the United States and other countries.
Novell SecretStore is a registered trademark of Novell, Inc. in the United States and other countries.
Nsure is a trademark of Novell, Inc. in the United States and other countries.
ZENworks is a registered trademark of Novell, Inc. in the United States and other countries.
ZENworks OnDemand Services is a trademark of Novell, Inc. in the United States and other countries.
DeFrame is a trademark of Novell, Inc. in the United States and other countries.

Third-Party Trademarks

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

Contents

About This Guide

This guide for network administrators provides information on the following:

Additional Documentation

For documentation on installing SecureLogin, see the Nsure SecureLogin 3.51 Installation Guide.

For documentation on managing and troubleshooting SecureLogin, see the Nsure SecureLogin 3.51 Administration Guide.

For documentation on terminal emulators, see the Nsure SecureLogin 3.51 Configuration Guide for Terminal Emulation.

For documentation on script commands and example scripts, see the Nsure SecureLogin 3.51 Scripting Guide.

Documentation Updates

For the most recent version of the *Nsure SecureLogin 3.51 Terminal Services Guide*, see Novell SecureLogin 3.51 (http://www.novell.com/documentation) at the Novell Documentation Web page.

Documentation Conventions

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

A trademark symbol (®,™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1 Overview

This section contains information about the following:

Integrating Microsoft Terminal Server and Citrix

SecureLogin can simplify authentication to numerous configurations of Microsoft* Terminal Server and Citrix* MetaFrame*. Integration of SecureLogin and the terminal server consists of the following components. Not all are necessarily required, depending on your implementation.

- The client login extension (slina.dll) applied to a workstation with the Novell® Client™, without the Novell Modular Authentication Service (NMAS™) client

  This component provides a link between the following:

  - The Novell GINA (graphical identification and authentication) or the Windows 9x login panel
  - The GINA running on the terminal server

- The NMAS client integration library (slnmas.dll) applied to a workstation with the Novell Client and NMAS client

  This component provides a link between the client login and the GINA running on the terminal server.

  NOTE: Client slina.dll and slnmas.dll also provide support for offline authentication to SecureLogin by using your NDS® or Novell eDirectory™ username and password.

- The GINA stub (sl_tscgina.dll) applied to a workstation without the Novell Client

  This component provides a link between the Microsoft GINA and the GINA running on the terminal server.

- The server login extension (slina.dll) applied to a terminal server with the Novell Client

  This component provides the server-side link to the client GINA.

- The server GINA replacement (sl_tsgina.dll) applied to a terminal server without the Novell client

  This component provides the server-side link to the client GINA stub.

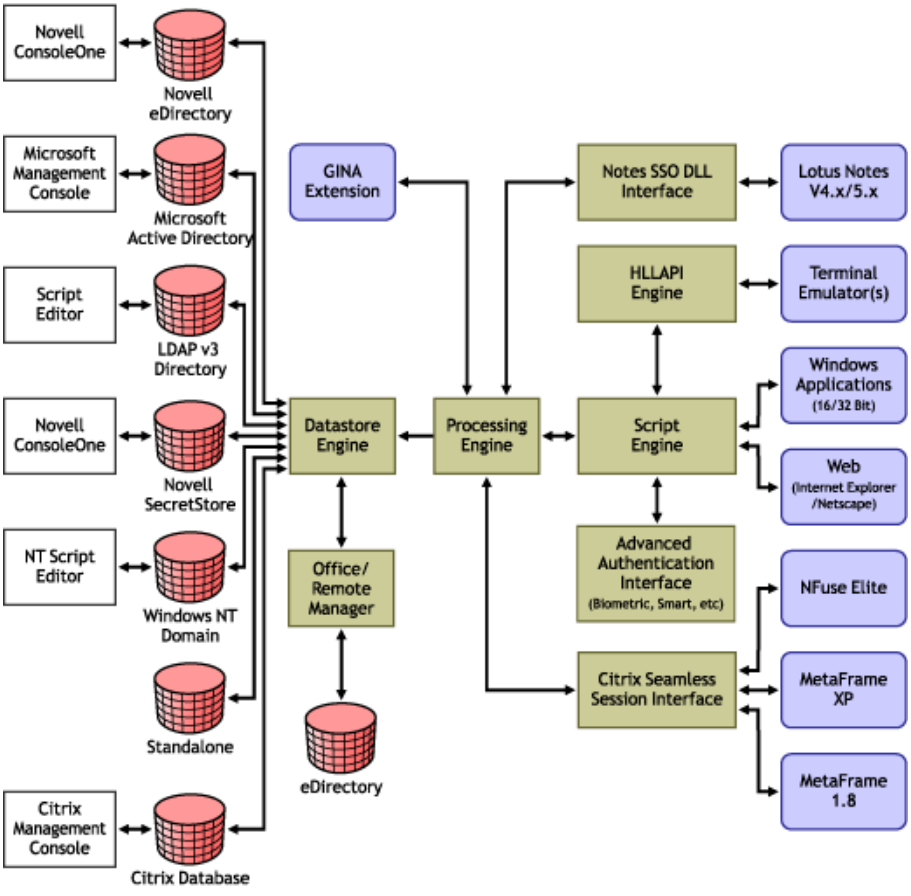
- The SecureLogin Virtual Channel Driver (vdslsson.dll or tsslsso.dll)

This component provides the conduit for secure communications between the client and server extensions

- Published Application integration (SLLauncher.exe) applied to a Citrix server

  This component provides proper initialization and termination of the SecureLogin components (slbroker.exe and proto.exe) running on the server.

The following diagram illustrates the SecureLogin architecture:



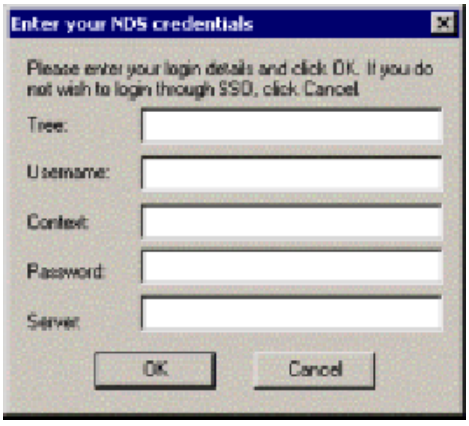
GINA Credential Pass-Through

With the SecureLogin Citrix components installed, SecureLogin provides a seamless pass-through of GINA credentials from the client to the server.

The GINA credential pass-through operates anytime that the terminal server presents a GINA login panel. If the credentials that the user used to log in to the client match the credentials of the terminal server, the credentials are automatically passed for the user.

If the credentials don't match, SecureLogin captures the error and presents a new login panel for the user to complete. SecureLogin detects which GINA is running on the Citrix server and requests the appropriate information.

For example, if SecureLogin detects that the terminal server has the Novell Client installed, SecureLogin presents the following dialog box:



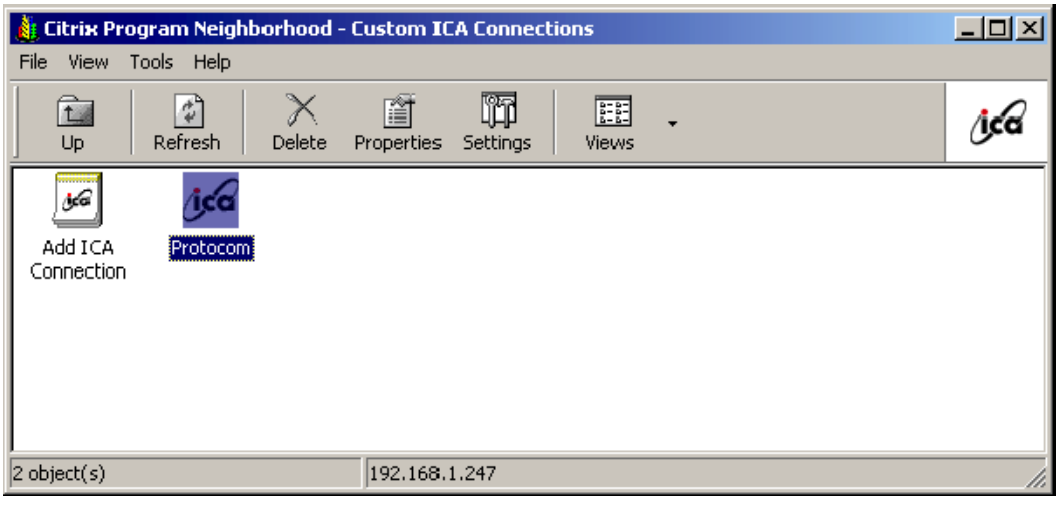
After the user completes the dialog box, SecureLogin saves the information as a hidden application (platform) within the SecureLogin datastore directory (and local cache if applicable). The next time the user accesses the terminal server, the credentials are retrieved from the hidden application and seamlessly passed to the terminal server.

Integrating Citrix Components

Citrix provides several ways to access a Citrix server or published application. How you access the server determines how SecureLogin handles the authentication to the server. Although different methods are used depending on how you access the server, SecureLogin can manage all forms of authentication.

Windows GINA Authentication

When the Citrix server requests a Windows GINA authentication, the Citrix Seamless Session Interface provides the credentials by using the hidden application (platform) method. An example of this type of authentication occurs when you connect to a Citrix server through Program Neighborhood's Custom ICA Connection interface:



Another example of this type of authentication occurs when you export a published application to an .ica file and distribute it to your workstations. This type of authentication is enabled by

installing the GINA components. The authentication isn't disabled even if SecureLogin isn't currently active.

Program Neighborhood

When a user accesses a Citrix farm using Program Neighborhood, Program Neighborhood uses wfcrun32.exe and presents a Program Neighborhood authentication dialog box:

Program Neighborhood then collects the credentials and sends them to a Citrix server in the farm.

The Citrix Seamless Session Interface doesn't handle this authentication request. However, a script can handle the wfcrun32.exe file just as it can handle any other Windows application that is requesting authentication. The SecureLogin Wizard automatically creates a script that enables single sign-on to Program Neighborhood. You should modify this script to allow for error handling, such as a bad username, domain, or password.

Using Desktop Shortcuts to Published Applications

If the Citrix Farm is configured to push out shortcuts to the user's desktops, the shortcut actually calls an executable, pn.exe (for example, C:\Program Files\Citrix\ICA Client\pn.exe). Authentication to pn.exe is handled by using a script, just like using a script for wfcrun32.exe or any other Windows application.

The SecureLogin Wizard automatically creates a script that enables single sign-on to pn.exe. Be sure to include error handling in case the user passes the wrong information into the dialog box.

Handling Password Changes

The Citrix Seamless Session Interface currently does not detect if users change their domains or NDS® or eDirectory™ passwords through a Citrix connection. If a user changes this password through a Citrix connection, the interface detects the failed seamless authentication the next time that the user connects to the Citrix server. The interface then once again prompts the user for credentials.

When the user enters the correct (new) password, the interface saves that new password in place of the previous password in the hidden application within the datastore (and the local file cache if applicable).

Virtual Channel

A virtual channel is a session-oriented and bidirectional error-free transmission connection that application layer code can use to exchange custom data packets between a terminal server and a terminal client.

SecureLogin employs this technology to allow users to single sign-on to various Published Application or Remote Desktop logins.

Virtual Channel Components

SecureLogin Terminal Server single sign-on has three major components:

Component	Description
Client login extension	Collects users' login credentials for single sign-on
Virtual channel driver (VCD)	The heart of SecureLogin Terminal Server single sign-on. The VCD liaises between the server login extension and single sign-on to perform all terminal session single sign-on processes.
Server login extension	Requests users' login credentials from the VCD and initiates the login process. After authentication, the login extension returns credentials to the VCD to update single sign-on.

SecureLogin uses the following process:

1. A user enters a username and password, a domain (optional), an eDirectory context, and an eDirectory tree. This information is encrypted and stored in the registry.
2. SecureLogin's slbroker.exe consumes the registry information and destroys the data in the registry. Login credentials are saved under a generic and hidden platform name.
3. When the user starts the Citrix ICA client or a published application through an .ica file, the SecureLogin VCD is loaded. This driver receives the domain or preferred tree name of the server. To retrieve the username, password, domain, eDirectory context, and tree, the driver then reads the platform name from slbroker.exe.

   If the platform doesn't exist, the VCD reverts to the generic platform name.

   If the generic platform name doesn't match the requested platform (tree or domain), the VCD displays a dialog box to prompt the user to enter NDS, eDirectory, or NT credentials. The credentials that are expected depend on whether the request is coming from a server with a Novell Client or from an NT/2000 server. The collected credentials are then sent to the server for verification.

   When the user enters and accepts the credential dialog box, a hidden application is created for the next authentication request.

   If the user chooses to abort entering credentials, the server login box appears as usual.

   NOTE: SecureLogin doesn't currently handle the actual password change process. Therefore, SecureLogin does not send back the new password when it is changed on the Citrix server. However, when the password stored in slbroker.exe is invalid because of a recent password change done on the Citrix Server, the user is prompted to enter login credentials again. After the new password is verified, it is then sent back to the VCD to update slbroker.exe.
4. After a successful authentication, the server login extension always sends the user's login credentials back to the workstation. If an application does not exist, this procedure creates a

new application in slbroker.exe. If the password has recently been changed and the application already exists, this procedure updates the new password to slbroker.exe.

Auto-Detecting the Client Protocol

The server detects whether the ICA protocol is present or not. If the ICA protocol is present, the server loads it. If the client is trying to establish a session by using the RDP protocol, the server loads the RDP protocol and the session begins. After the server is installed, it automatically responds to the RDP or ICA protocol.

By default, the Auto Detection feature is on.

Windows NT* 4.0 Terminal Server Edition (RDP 4.0) does not support the virtual channel operation. If the client tries to establish a session by using the RDP protocol, Windows NT 4.0 Terminal Server Edition won't respond to the client.

2 Installing Terminal Services

This section contains information on the following:

Requirements for Terminal Services

Server Requirements

- Windows NT 4.0 Terminal Server Edition or Windows 2000 Server family with Terminal Service enabled

  NOTE: Only Windows 2000 Server family operating systems support Virtual Channel. If you want virtual channel support on Windows NT 4.0 Terminal Server Edition, you need to install an appropriate Citrix server.

- One of the following Citrix servers installed (optional):
  - MetaFrame 1.8 for Windows 2000
  - MetaFrame 1.8 for Windows NT 4, Terminal Server Edition
  - MetaFrame 2.0
  - Citrix XP
- (Optional) Novell® Client™ 4.7 or later

Workstation Requirements

- Novell Client version 4.7 or later

  If you use the Novell Client, use version 4.7 or later. The Novell Client is not required unless you are using Windows 95.

- SecureLogin version 3.0.1 or later
- One of the following:
  - Win32 ICA Client Version 6.00.905 or later
  - Terminal Server Client that supports RDP 5.0 (for example, the version that shipped with Windows 2000 Advanced Server)

Setting Up the Server

The following procedures outline the steps necessary to set up your servers to support terminal server integration. Based on your server's environment, determine which set of steps to follow.

You must match the appropriate files from the installation source to your environment. Otherwise, the extensions won't function properly. If you later install or uninstall the Novell Client, you must modify the SecureLogin modules to match.

Your SecureLogin terminal server components must match the version of SecureLogin you are using. When you upgrade to a new version of SecureLogin, you must also upgrade the integration components.

Copying Files

Copy the following files to the Windows system directory (for example, c:\winnt\system32):

- srv\sl_vc.dll
- srv\sl_rdp.dll
- srv\sl_ica.dll
- (Conditional) srv\slaa_sso.dll

  If SecureLogin is installed on the server in LDAP mode, also copy srv\slaa_sso.dll to the Windows system directory.

Setting Up GINA

Servers with the Novell Client

1. Set up a Novell login extension.

   Copy srv\nw\slina.dll to the Windows system directory (for example, c:\winnt\system32).
2. Register the login extension.

   At the srv\nw directory, double-click Register NT LoginExt.reg.

Servers without the Novell Client

1. Replace the server GINA.

   Copy srv\ms\sl_tsgina.dll to the Windows system directory (for example c:\winnt\system32).
2. Register GINA.

   At the srv\ms directory, double-click winlogon_server.reg.
3. Reboot the server.

Configuring OnDemand

If you have set up a Microsoft* Terminal Server with Novell ZENworks® OnDemand Services™ installed, you don't need to install any new components for SecureLogin. OnDemand relies on the DeFrame™ ICA or RDP plug-ins as the client. No workstation components are necessary. When a user authenticates to the Citrix session, Novell SecureLogin launches.

If you use the SecretStore option with OnDemand Dynamic User Creation, make the following changes to the EnableUserProfileDirectory value in the HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\NICI registry key:

Value	Type	Description
EnableUserProfileDirectory	DWORD	NICI user files are created in the Application Data\Novell\NICI directory in the user's profile directory

The NICI installation program does not create EnableUserProfileDirectory. Therefore, this value is disabled.

NOTE: If the user profile directory is enabled, NICI does not set the Access Control Lists (ACLs) on this directory. NICI relies on the existing security properties (ACLs, inheritance, and ownership) of the user's profile directory.

To configure a DeFrame application object to launch Internet Explorer, with Internet Explorer using the ICA protocol:

1. In ConsoleOne®, right-click the Application object.
2. Select DeFrame, then click Application Setup.
3. Add SLLauncher.exe.

   Enclose *path\applicationname* in quotation marks (for example, "c:\Program Files\Novell\SecureLogin\SLLauncher.exe" "c:\Program Files\Internet Explorer\iexplore.exe").
4. Install the SecureLogin client at the Citrix/DeFrame server.

Setting Up Workstations

The following procedures outline the steps necessary to set up your workstations to support the Citrix integration. Based on your client workstation environment, determine which set of steps to follow.

You must match the appropriate files from the installation source to your environment. Otherwise, the extensions will not function properly. If you later install or uninstall the Novell Client or NMAS client, you must modify the SecureLogin modules to match.

Your SecureLogin terminal server components must match the version of SecureLogin you are using. When you upgrade to a new version of SecureLogin, you must also upgrade the integration components.

Your client configuration doesn't need to match your server configuration. For example, you can use a client that has the Novell Client installed and connect to a terminal server that doesn't have the Novell Client installed (or vice-versa).

Novell Client (without the NMAS Client)

1. Set up the Novell login extension.

   Copy wks\nw\slina.dll to the Windows system directory (for example, c:\winnt\system32 for Windows NT or c:\windows\system for Windows 9*x*).

   The slina.dll file is a login extension. After you copy the file, you must register it by using the registry (REG) file.

2. Register the login extension.

   If you are running Windows NT, Windows XP, or Windows 2000, double-click Register NT LoginExt.reg, found in the wks\nw directory.

   If you are running Windows 95 or Windows 98, double-click Register 98 LoginExt.reg, found in the wks\nw directory.

3. Set up Microsoft Layer for Unicode* on Windows 95/98/ME.

   If you are running Windows 9*x*/ME, copy redistributable\unicows.dll to your system directory (for example, c:\windows\system).

4. Reboot the workstation.

Novell Client (with the NMAS Client)

1. Copy slnmas.dll from the wks\nw directory to the Windows system directory (for example, c:\winnt\system32 for Windows NT or c:\windows\system for Windows 9*x*).

   The slnmas.dll file is not a login extension. Instead, it is called by the NMAS client. If you are using the NMAS client and slnmas.dll, it isn't necessary to run the registry (REG) file. You will need to install the version of NMAS client that comes with NSL 3.0.1 or later, which is slnmas.dll aware.

2. Set up Microsoft Layer for Unicode on Windows 95/98/ME.

   If you are running Windows 9*x*/ME, copy unicows.dll from the \redistributable directory to your system directory (for example, c:\windows\system).

3. Reboot the workstation.

Microsoft Workstation with No Novell Client Installed

1. Replace the workstation GINA.

   Copy sl_tsc.gina.dll from the wks\ms directory to the Windows system directory (for example, c:\winnt\system32).

2. Register GINA.

   Double-click winlogon_client.reg in the wks\ms directory.

3. Reboot the workstation.

NOTE: Windows 95 does not support the GINA credential pass-through without the Novell Client installed.

Installing the Virtual Channel Driver

Install the Virtual Channel Driver (VCD) on workstations, not on servers.

Workstations with the Citrix Client (ICA)

1. Install the SecureLogin Citrix ICA VCD.

   Copy vdslssoN.dll from the vcd\ica directory to the ICA Client directory (for example, c:\program files\citrix\ica client).

2. Register the SecureLogin Citrix ICA VCD.

   Make the following changes to the module.ini file located in the directory on the client workstation where the ICA Client is installed:

   - The section [ICA 30] has a Virtual Driver line. Add the name of the virtual driver to the end of this line. For example, add

     ```
     , SLSSO
     ```

   - At the end of the [VirtualDriver] section, add a driver assignment statement. For example, for the SLSSO driver, add

     ```
     SLSSO     =
     ```

     The extra spaces are for appropriate indentation. They aren't required.

   - Create a new section, [SLSSO], as follows:

     ```
     [SLSSO]
     DriverNameWin32 = VDSLSSON.DLL
     ```

     The vcd\ica directory has an example module.ini file that you can refer to.

3. Set up Microsoft Layer for Unicode on Windows 95/98/ME.

   If you are running Windows 9*x*/ME, copy unicows.dll from the \redistributable directory to your ICA Client directory (for example, c:\program files\citrix\ica client).

Workstations with the Terminal Server Client (RDP)

1. Install the SecureLogin Terminal Server VCD by copying tsslsso.dll from the \vcd\rdp directory to the Windows system directory (for example, c:\winnt\system32).

2. Register the SecureLogin Terminal Server VCD by double-clicking VCD\RDP\Terminal Server Driver registration on Client workstation.reg.

   IMPORTANT: This is a per-user setting.

Installing the Terminal Server Web Client

If TSWeb Client is installed on the terminal server:

1. Locate connect.asp on the server.

   For example, go to c:\inetpub\wwwroot\tsweb.

2. Using Notepad, open connect.asp.

3. Add the following line before MsTsc.Connect():

   ```
   MsTsc.AdvancedSettings.PluginDlls="tsslsso.dll"
   ```

   The vcd\rdp directory has an example connect.asp file that you can refer to.

4. Save and close the file.

3 Integrating with Citrix Published Applications

This section provides information on the following:

Modifying the Command Line

SecureLogin SLLauncher starts the SecureLogin components (slbroker.exe and proto.exe) and then launches the desired published application with single sign-on support. To launch SLLauncher if you are using Citrix-published applications, you must modify the command line for each published application.

When the application is closed, SLLauncher terminates the proto.exe or slbroker.exe session. That way, these utilities don't leave the Citrix session connected.

SLLauncher must be used with any published application running on the Citrix server. If SLLauncher isn't found within the server's path environment variable, you must include the full path to SLLauncher. For example, replace the command line of the published application as follows:

Before	After
C:\Progra~1\novell\SecureLogin\tlaunch.exe /q /auto /eWallData Rumba /pnovellMainframe	SLLauncher.exe C:\Progra~1\novell\SecureLogin\tlaunch.exe /q /auto /e"WallData Rumba" /pnovellMainframe

Using SLLauncher Syntax

To run SLLauncher, use the following syntax:

SLLauncher [Optional Parameters] *Executable to run* [optional executable's parameters]

IMPORTANT: If your executable contains a path or command line parameters that include spaces, embed the spaces in quotes. Even if your application normally accepts the parameters with spaces, SLLauncher interprets them as separate parameters, and unexpected results might occur.

SLLauncher includes two command line parameters that control its behavior:

Parameter	Explanation
/w *executable name*	Specifies another process to wait for before closing SecureLogin. Examples: ◆ SLLauncher.exe /w rumbadsp.exe C:\Progra~1\novell\SecureLogin\tlaunch.exe /q /auto /e”WallData Rumba” /p"novellMainframe" ◆ SLLauncher.exe /w mspaint.exe run_MSPaint.CMD
/d	Debug option. This option generates a debug log file (c:\sllauncher.log) and shows dialog boxes during the progress of SLLauncher. The switch must appear before the executable that you want to run. Examples: ◆ SLLauncher.exe /w rumbadsp.exe /d C:\Progra~1\novell\SecureLogin\tlaunch.exe /q /auto /e“WallData Rumba” /p"novellMainframe" ◆ SLLauncher.exe /w /d mspaint.exe run_MSPaint.CMD

A Registry Settings

This section describes optional registry settings that you can make to customize SecureLogin terminal server features.

NOTE: All registry values specified are of string type (REG_SZ).

Auto-Detecting the Client Protocol

By default, Auto Detection is enabled. To disable Auto Detection, add the following entry to the registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\Virtual Channel]
“AutoDetect” = “0”
```

To specify the protocol that the server should use, add one of the following entries in the same key:

```
“Protocol” = “RDP”
“Protocol” = “ICA”
```

If the protocol is not specified, the software checks for the presence of ICA. If the ICA protocol is present, the software loads the ICA protocol. Otherwise, the server uses the RDP protocol.

Servers with a Novell Client

To populate a user's common name to the NT Username field during a session login, set the following registry value on the server:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\Virtual
Channel\Login\slina]
“PopulateToNT” = “1”
```

Localized Machine

To support international versions of Windows, you need to add a localized login window caption to the following registry entry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
“LogonWindowCaption” = “localized caption”
```

Third-Party GINA

When using a third-party GINA (for example, Citrix GINA), enter the GINA name as follows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
“ProtocomPassThruDLL” = “Gina DLL name”
```

If the third-party GINA is using a different login window caption than Microsoft GINA does, enter it as follows in the same key:

```
"LogonWindowCaption" = "Logon window caption"
```

If the Control IDs of the third-party GINA are not the same as Microsoft GINA, enter them by creating a key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\ProtocomPassThru]

“UsernameCtrlID” = “User Name field ID”
“PasswordCtrlID” = “Password Field ID”
“DomainCtrlID” = “Domain Name Ctrl ID”
“IDOK” = “OK Button ID”
```

NOTE: Define Domain Name in a combo box.

B Debugging Options

To turn on debugging, double-click the Virtual Channel SSO Debugging Switches.reg file on the workstation or the server.

To view the log file for various components, refer to the following table:

Platform	.DLL File	Path and Log File
Server	slina.dll	c:\winnt\system32\slina.ica.log or slina.ts.log
Server	sl_tsgina.dll	c:\winnt\system32\sl_tsgina.ica.log or sl_tsgina.ts.log
Workstation	slina.dll (wks)	c:\winnt\system32\slina.log
Workstation	sl_tscgina.dll	c:\winnt\system32\sl_tscgina.log
Workstation	vdslssoN.dll	C:\program Files\Citrix\ICA Client\vdslsso.log
Workstation	tsslsso.dll	c:\winnt\system32\tsslsso.log

To turn debugging off, set “debug” = “0” for each desired component in the registry.