Novell SecureLogin

6.0 SP1

October 13, 2006

www.novell.com

CITRIX AND TERMINAL SERVICES GUIDE

Novell®

Legal Notices

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

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

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

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

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

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

Novell Trademarks

Third-Party Materials

Contents

About This Guide

This document contains information on the following:

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Installing SecureLogin On Citrix Server,” on page 13
- Chapter 3, “Citrix Application Deployment,” on page 15
- Chapter 4, “Configuring Citrix Load Balancing,” on page 23
- Chapter 5, “Using Connectors,” on page 27
- Chapter 6, “Using Secure Workstation with Citrix,” on page 29
- Chapter 8, “Upgrading SecureLogin,” on page 49

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.

Documentation Updates

This is the Support Pack 1 (SP1) release for Novell SecureLogin 6.0. The version for this support pack in the product is, 6.0.103.

For the most recent version of the *Terminal Services Guide*, visit the Novell Documentation Web site (http://www.novell.com/documentation/securelogin60).

Additional Documentation

This *Installation Guide* is a part of documentation set for SecureLogin 6.0 SP1. Other documents include:

- *Novell SecureLogin 6.0 SP1 Overview*
- *Novell SecureLogin 6.0.SP1 Administration Guide*
- *Novell SecureLogin 6.0 SP1 Installation Guide*
- *Novell SecureLogin 6.0 SP1 Application Definition Guide*
- *Novell SecureLogin 6.0 SP1 User Guide*
- *Novell SecureLogin 6.0 SP1 Congifuration Guide for Terminal Emulation*

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 Overview

SecureLogin provides tools to configure single sign-on access to applications in Citrix* and terminal service environments. This guide provides instructions for directory server and terminal server or Citrix server environment.

You must configure the Citrix and terminal server and user workstations prior to installing SecureLogin. This is because, the SecureLogin installation package detects Citrix or terminal server files and installs the requisite supporting files automatically. If Citrix or terminal services are deployed post SecureLogin implementation, the SecureLogin installation package must be deployed again to install the required SecureLogin components.

This section has the following information:

- Section 1.1, "Prerequisites," on page 9
- Section 1.2, "About Citrix Application Deployment," on page 9
- Section 1.3, "SecureLogin Attributes," on page 10

1.1 Prerequisites

The following are the prerequisites to installing SecureLogin on the Citrix and Terminal Services server:

- Extend the corporate directory schema. If the schema was extended in a SecureLogin version 3.5.x deployment, do not repeat the process. For more information see "Extending the eDirectory Schema".
- Administrator level access to the Citrix or Terminal Services server.
- A Java Runtime Engine version 1.4, or later, installed on server or workstations, if you want to enable Java applications for single sign-on.
- Unionist SecureLogin versions prior to version 3.5.x before the upgrade.

1.2 About Citrix Application Deployment

There are three modes of Citrix application deployment:

Deployment	Description
Full Desktop	Only the Citrix client runs on the Desktop and all other applications operate on the Citrix server.
Published Applications	A combination of applications operating on the Desktop and some accessed (published) using the Citrix server.
Citrix Desktop and Published Applications	The option to run a full Citrix Desktop or a combination of Citrix published applications published and applications executed on the workstation.

1.2.1 Corporate Directory Deployment

In corporate directory environments SecureLogin data is stored on the directory. To facilitate this, the directory schema is extended to include SecureLogin attributes. For more information on extending the directory schema for your directory, refer to the *Novell SecureLogin 6.0 SP1 Installation Guide*. If you have previously installed SecureLogin version 3.5.x the required SecureLogin attributes are already installed.

1.2.2 Full Citrix Desktop Deployment

Full Citrix Desktop Deployment requires SecureLogin schema extensions on the network directory server and client installation on the Citrix server. Users operate SecureLogin using the Citrix server remotely and their SecureLogin user data is stored on the Citrix server and the network directory.

1.2.3 Published Application Deployment

Deploying published applications requires SecureLogin schema extensions on the network directory server with client installation on the Citrix server and user workstation. SecureLogin executes from the workstation to log onto applications published on the Citrix server. SecureLogin user data is only required to be stored on the user's workstation for graphical identification and authentication library (GINA) to GINA pass through unless SecureLogin is needed for SSO to applications that are running on that workstation.

Deploying published applications requires SecureLogin on the network directory server with client installation on the Citrix server and user workstation. SecureLogin executes from the workstation to log onto applications published on the Citrix server. SecureLogin user data is stored on the directory server and the user’s workstation.

1.2.4 Citrix Desktop and Published Application Deployment

The Citrix Desktop and Published Applications requires:

- SecureLogin schema extensions on the network directory server
- Citrix server and the user workstation

SecureLogin executes from the workstation or the Citrix server, depending on the mode selected by the user. SecureLogin user data is stored on the directory server, the Citrix server and the user workstation.

1.3 SecureLogin Attributes

Extending the directory schema adds the following six SecureLogin attributes:

- Protocom-SSO-Auth-Data
- Protocom-SSO-Entries
- Protocom-SSO-SecurityPrefs
- Protocom-SSO-Profile
- Protocom-SSO-Entries-Checksum
- Protocom-SSO-Security-Prefs-Checksum

NOTE: If SecureLogin version 3.5 or 3.5.x is installed, then you do not need to extend the Directory schema since the attributes are the same. However, any new directory objects, for example organizational units, still require you to assign rights.

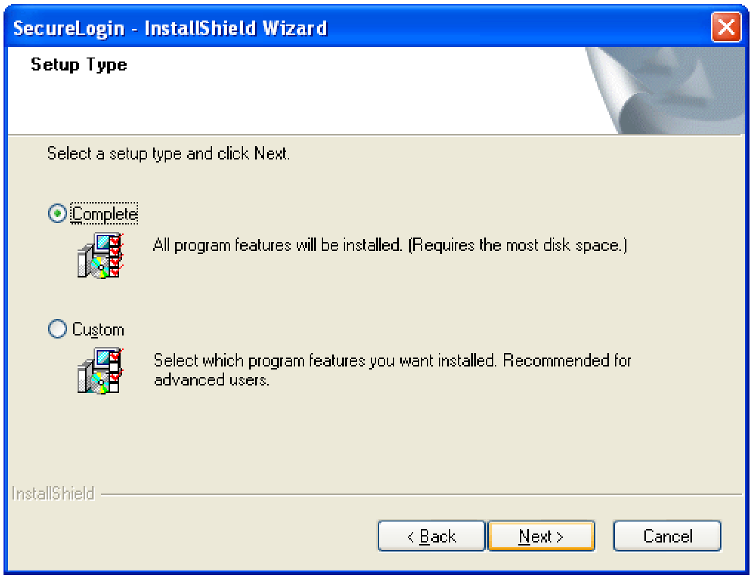
1. Log on to the server as administrator.
2. Install the SecureLogin installation CD. The main menu is displayed.
3. Click *Install* and follow the prompts for your installation type.
4. Double-click the `ndsschema.exe` file in the `Tools` folder of the CD. The SecureLogin - `Schema extension` dialog box is displayed.
5. Extend the schema.

Installing SecureLogin On Citrix Server

2

To install SecureLogin on the Citrix server:

1. Logon to the workstation as administrator.
2. Insert the SecureLogin Distribution CD. The SecureLogin main menu is displayed.
3. Select a language, then click *Next*.
4. Accept the license agreement, then click *Next*. The Setup Type dialog box is displayed.



SecureLogin - InstallShield Wizard

Setup Type

Select a setup type and click Next.

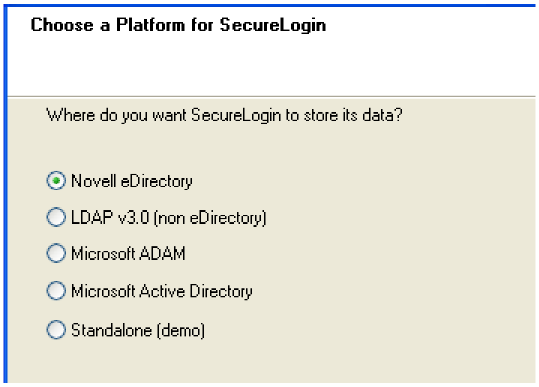
● Complete

All program features will be installed. (Requires the most disk space.)

○ Custom

Select which program features you want installed. Recommended for advanced users.

5. Select *Custom*, then click *Next*. The Choose a Platform for SecureLogin dialog box is displayed.



Choose a Platform for SecureLogin

Where do you want SecureLogin to store its data?

● Novell eDirectory

○ LDAP v3.0 (non eDirectory)

○ Microsoft ADAM

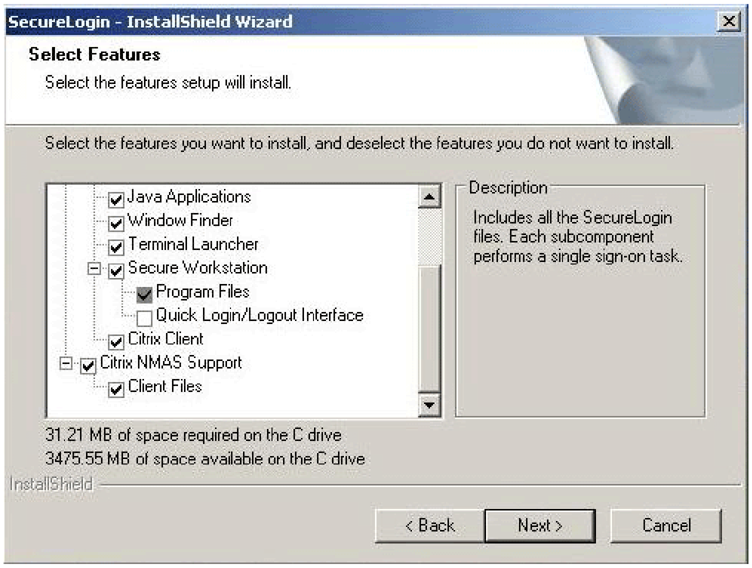
○ Microsoft Active Directory

○ Standalone (demo)

6. Select a platform, then click *Next*.
7. During the rest of the installation, select options according to the platform that you selected.

For information on installation options, see the relevant section in the *Novell SecureLogin 6.0 SP1 Installation Guide*.

8 In the Select Features dialog box, make sure that the *Citrix* check box is checked.



SecureLogin - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- ☑ Java Applications
- ☑ Window Finder
- ☑ Terminal Launcher
- ☑ Secure Workstation
  - ☑ Program Files
  - □ Quick Login/Logout Interface
- ☑ Citrix Client
- ☑ Citrix NMAS Support
  - ☑ Client Files

Description

Includes all the SecureLogin files. Each subcomponent performs a single sign-on task.

31.21 MB of space required on the C drive
3475.55 MB of space available on the C drive

9 Click *Install*.

10 By default, the *Launch Readme* option is selected. Click *Next*.

11 Click *Finish*.

12 Select when you want to restart your workstation, then click *OK*.

Citrix Application Deployment

3

This section has the following information:

- Section 3.1, "Launch an Application in a Citrix Environment," on page 15
- Section 3.2, "Publish an Application for Citrix Deployment," on page 15

3.1 Launch an Application in a Citrix Environment

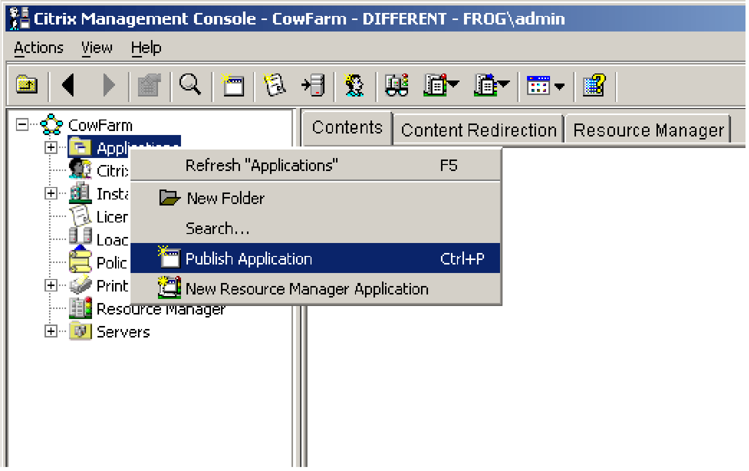
SecureLogin is unable to detect individual application screens in a Citrix environment as the Window cues are not available. You must launch SecureLogin before the application to activate the SecureLogin.

You must include the SecureLogin executable SLLauncher in the Citrix published application executable path, to achieve this. When the user starts the application, the SecureLogin runs and logs in the user then launches the application.

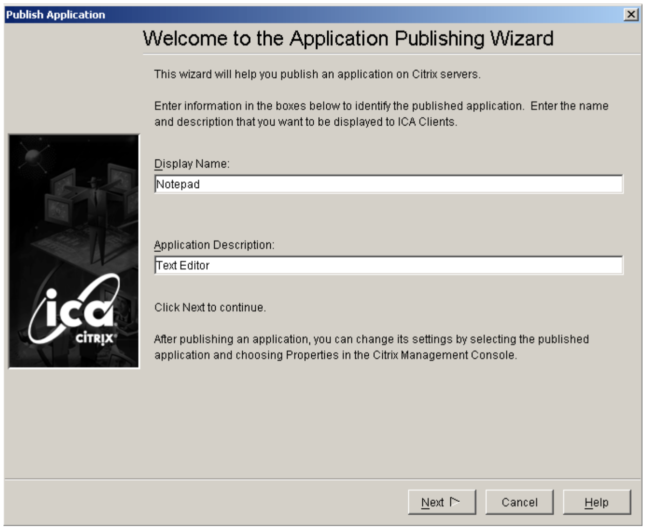
3.2 Publish an Application for Citrix Deployment

To publish an application for Citrix deployment from the Citrix Management Console and SecureLogin do the following:

1 Select Applications from the Citrix farm.



2 Right-click *Applications*, then select *Publish Application* option from the menu. The Welcome to the Application Publishing Wizard is displayed.



Publish Application

Welcome to the Application Publishing Wizard

This wizard will help you publish an application on Citrix servers.

Enter information in the boxes below to identify the published application. Enter the name and description that you want to be displayed to ICA Clients.

Display Name: Notepad

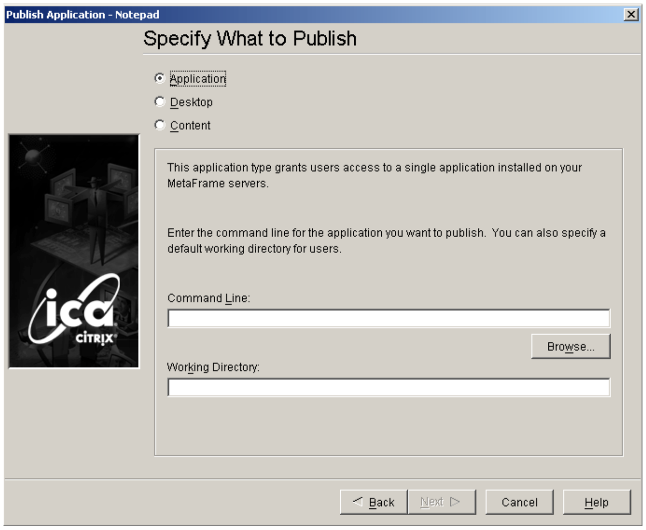
Application Description: Text Editor

Click Next to continue.

After publishing an application, you can change its settings by selecting the published application and choosing Properties in the Citrix Management Console.

3 Specify a name for the published application in the *Display Name* field and description in the *Application Description* field.

4 Click *Next*. The Specify What to Publish dialog box is displayed.



Publish Application - Notepad

Specify What to Publish

● Application
○ Desktop
○ Content

This application type grants users access to a single application installed on your MetaFrame servers.

Enter the command line for the application you want to publish. You can also specify a default working directory for users.

Command Line:

Working Directory:

5 Click *Browse* to find the location of the application program files and select the executable.

6 Click *OK* to return to the Specify What to Publish dialog box.

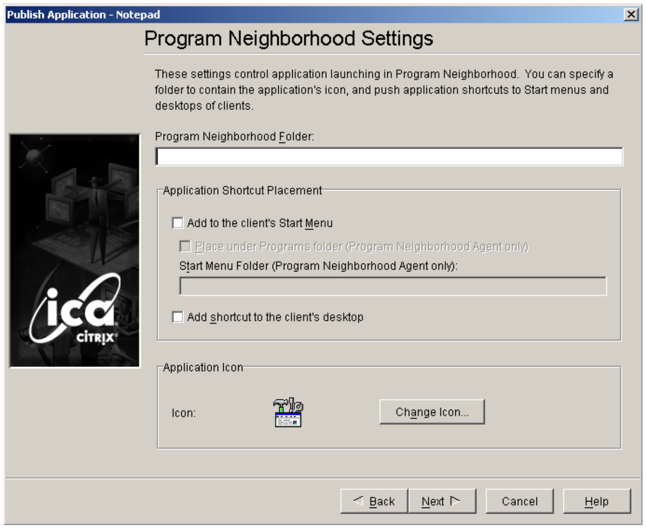
7 Specify the relevant directory path in the *Working Directory* field. The working directory is the directory path of the program executable.

The path to the `SLLauncher.exe` file of SecureLogin is specified before the published application executable. Enter a space between the SecureLogin and application executable path descriptions.

For more information on SSLauncher.exe, refer to Section 7.10.2, "Using SLLauncher Syntax," on page 44.

8 In the *Command Line* field, specify the published application executable path.

9 Click *Next*. The *Program Neighborhood Settings* dialog box is displayed.



Publish Application - Notepad

Program Neighborhood Settings

These settings control application launching in Program Neighborhood. You can specify a folder to contain the application's icon, and push application shortcuts to Start menus and desktops of clients.

Program Neighborhood Folder:

Application Shortcut Placement

□ Add to the client's Start Menu

□ Place under Programs folder (Program Neighborhood Agent only)

Start Menu Folder (Program Neighborhood Agent only):

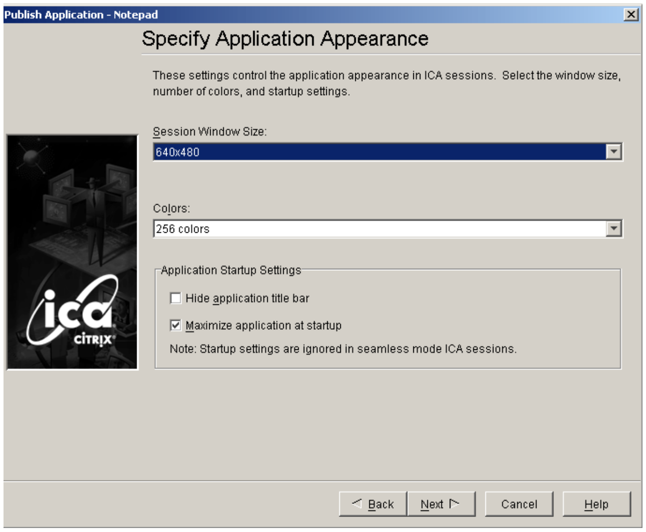
□ Add shortcut to the client's desktop

Application Icon

Icon:

10 Select the options and configure neighborhood settings as required.

11 Click *Next*. The Specify Application Appearance dialog box is displayed.



Publish Application - Notepad

Specify Application Appearance

These settings control the application appearance in ICA sessions. Select the window size, number of colors, and startup settings.

Session Window Size: 640x480

Colors: 256 colors

Application Startup Settings

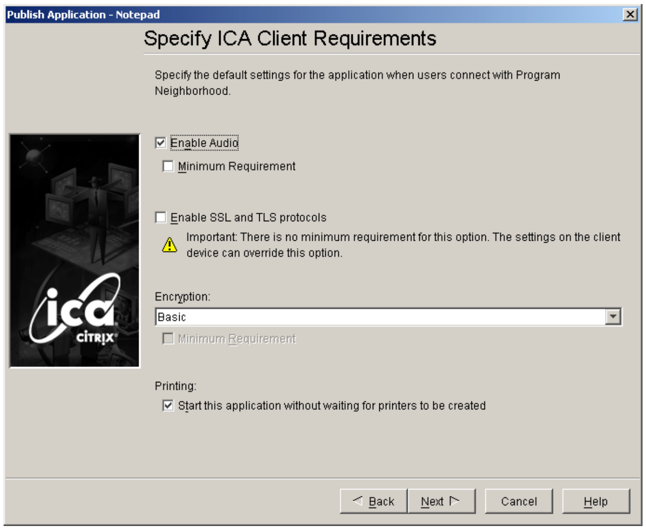
□ Hide application title bar

☑ Maximize application at startup

Note: Startup settings are ignored in seamless mode ICA sessions.

12 Select and configure application appearance options as required

13 Click *Next*. The Specify ICA Client Requirements dialog box is displayed.



Specify ICA Client Requirements

Specify the default settings for the application when users connect with Program Neighborhood.

☑ Enable Audio

□ Minimum Requirement

□ Enable SSL and TLS protocols

Important: There is no minimum requirement for this option. The settings on the client device can override this option.

Encryption: Basic

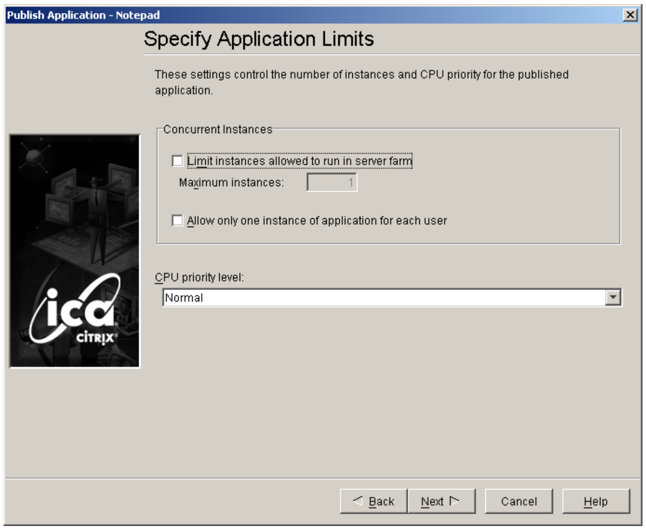
□ Minimum Requirement

Printing:

☑ Start this application without waiting for printers to be created

14 Select and configure ICA Client Requirement options as required.

15 Click *Next*. The Specify Application Limits dialog box is displayed.



Specify Application Limits

These settings control the number of instances and CPU priority for the published application.

Concurrent Instances

□ Limit instances allowed to run in server farm

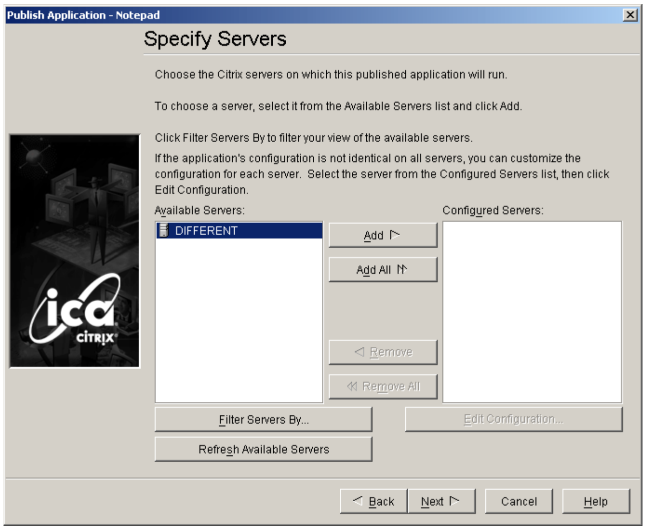
Maximum instances: 1

□ Allow only one instance of application for each user

CPU priority level: Normal

16 Select and configure application limits as required.

17 Click *Next.* The Specify Servers dialog box is displayed. You need to specify a server for application publication and deployment.



Publish Application - Notepad

Specify Servers

Choose the Citrix servers on which this published application will run.

To choose a server, select it from the Available Servers list and click Add.

Click Filter Servers By to filter your view of the available servers.

If the application's configuration is not identical on all servers, you can customize the configuration for each server. Select the server from the Configured Servers list, then click Edit Configuration.

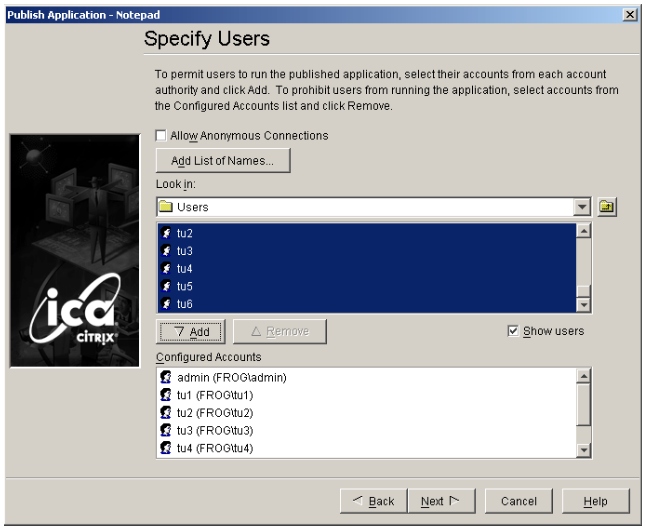
Available Servers: DIFFERENT

Configured Servers:

18 Select the relevant server from the *Available Servers* list.

19 Click *Add*.

20 Click *Next*. The Specify Users dialog box is displayed.



Publish Application - Notepad

Specify Users

To permit users to run the published application, select their accounts from each account authority and click Add. To prohibit users from running the application, select accounts from the Configured Accounts list and click Remove.

□ Allow Anonymous Connections

Look in: Users

tu2
tu3
tu4
tu5
tu6

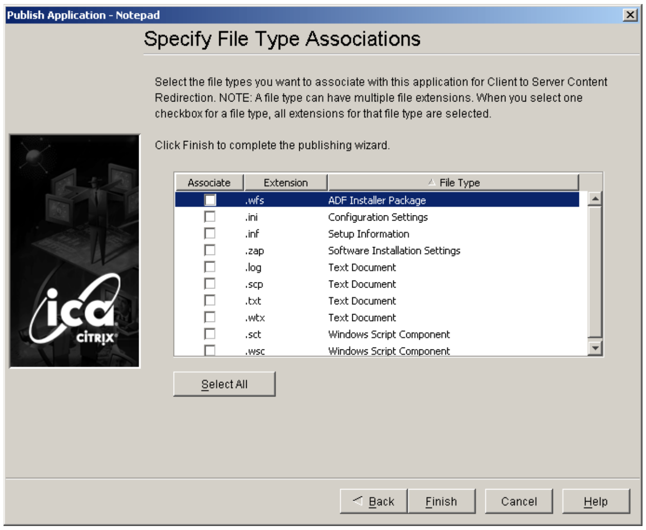
☑ Show users

Configured Accounts

admin (FROG\admin)
tu1 (FROG\tu1)
tu2 (FROG\tu2)
tu3 (FROG\tu3)
tu4 (FROG\tu4)

21 Check the *Show users* check box, then drag the pointer to select the users.

22 Click *Add*. Depending on the published application, the Specify File Type Associations dialog box may be displayed.



Publish Application - Notepad

Specify File Type Associations

Select the file types you want to associate with this application for Client to Server Content Redirection. NOTE: A file type can have multiple file extensions. When you select one checkbox for a file type, all extensions for that file type are selected.

Click Finish to complete the publishing wizard.

Associate	Extension	File Type
□	.wfs	ADF Installer Package
□	.ini	Configuration Settings
□	.inf	Setup Information
□	.zap	Software Installation Settings
□	.log	Text Document
□	.scp	Text Document
□	.txt	Text Document
□	.wtx	Text Document
□	.sct	Windows Script Component
□	.wsc	Windows Script Component

23 Check the file type check boxes as required.

24 Click *Finish*. The published application now displays in the *Contents* tab of the Citrix Management Console.

25 Repeat publishing steps for all SecureLogin enabled applications.

When all required applications have been published, test executing an application to make sure SecureLogin for Citrix is successfully installed.

3.2.1 SLLauncher Switches

You can use three switches in conjunction with the SLLauncher executable `/d`, and `/w`. Switches are not case sensitive, that is, both `/d` and `/D` are valid, however in the case of `/w`, the process name specified is case sensitive.

- `/d` is used to initiate a trace file that is saved in the SecureLogin program directory. Example syntax:

  ```
  “C:\Program Files\Novell\SecureLogin\SSLauncher.exe” /d
  C:\WINNT\System32\notepad.exe
  ```

- `/w` used to delay SLLauncher executing until a specific application has executed or environment is present.

  For example, to run the executable `notepad.exe` with SecureLogin, the syntax is:

  ```
  “C:\Program Files\Novell\SecureLogin\SSLauncher.exe”
  C:\WINNT\System32\notepad.exe
  ```

However, in order for `notepad.exe` to execute as required, you must set up an environment variable first. This environment is created when the batch file `runtest.bat` is run on the server.

Use the `/w` switch, to specify SLLauncher wait to execute until the batch file `runtest.bat` has completed running, for example:

```
"C:\Program Files\Novell\SecureLogin\SSLauncher.exe" /w
notepad.exe
```

C:\runtest.bat

Switch Combinations

You can also use switches in combination, for example:

```
"C:\Program Files\Novell\SecureLogin\SSLauncher.exe" /d /w
notepad.exe C:\runtest.bat
```

When enabling SecureLogin 16 bit application, you must include `/16` switch in the Citrix publishing command. You must identify the 16 bit applications because they execute differently to 32 bit applications. For SecureLogin to single sign-on an application, the 16 bit emulator `NTVDM.exe` must be active.

The following is an example syntax:

```
"C:\Program Files\Novell\SecureLogin\SSLauncher.exe" /16
C:\WINNT\System32\notepad.exe
```

Subsequently, each time a 16 bit application is SecureLogin signed-on, the executable `NTVDM.exe` continues to run. This may cause memory issues if multiple 16 bit applications are SecureLogin single sign-on enabled.

Add the switch `/w NTVDM.exe` to the Citrix publishing command to terminate `NTVDM.exe` when the 16 bit application is closed,

To terminate `NTVDM.exe` when the 16 bit application is closed, add the switch `/w NTVDM.exe` to the Citrix publishing command.

The following is an example syntax:

```
"C:\Program Files\Novell\SecureLogin\SSLauncher.exe" /16 /w
NTVDM.exe
```

```
C:\WINNT\System32\notepad.exe
```

NOTE: Executing 16 bit applications requires the switch /16 in the command line.

Configuring Citrix Load Balancing

4

A SecureLogin operation implemented for memory optimization may result in client connection dropouts. This has no adverse impact on your Citrix server and is resolved by configuring Citrix Load Balancers to increase the number of allowed page faults.

The following instructions present the procedure for configuring Load Balancers, however recommendations for specific values are not provided. Due to the wide variety and complexity of system architectures it is not possible to account for all the variables that would impact on load balancing requirements.

The following procedures apply to Citrix Metaframe* XP FR2:

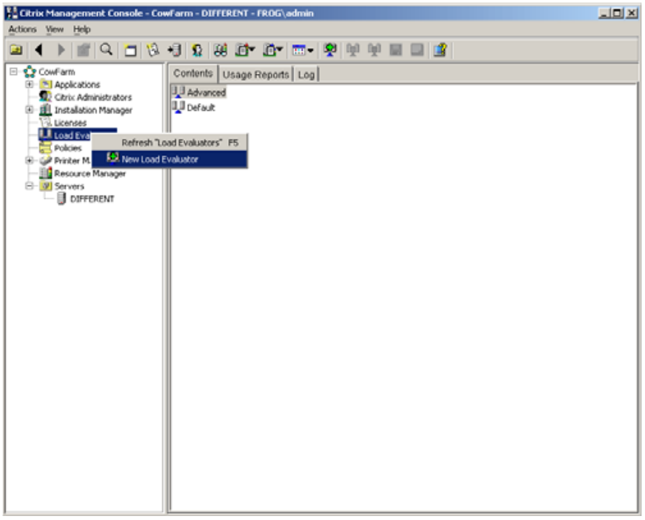
- Section 4.1, "Create a New Load Evaluator," on page 23
- Section 4.2, "Load New Evaluators to the Citrix Server," on page 25

4.1 Create a New Load Evaluator

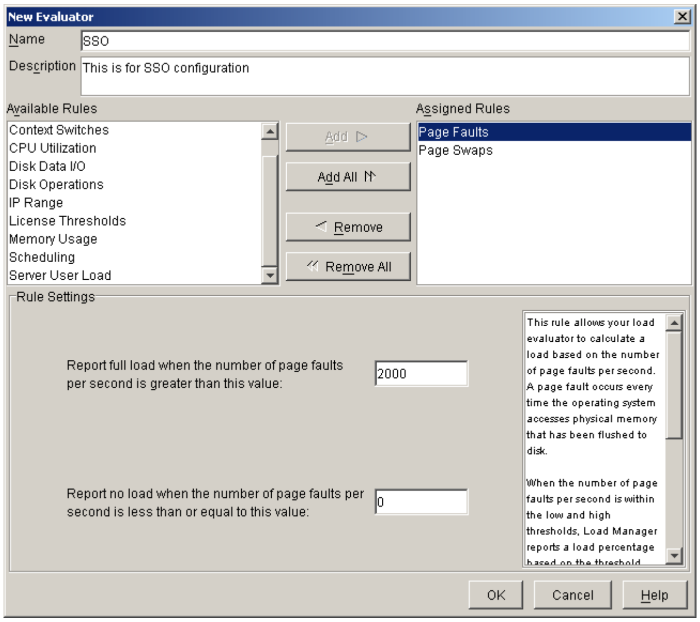
To create a new Load Evaluator:

1 Start the Citrix Management Console, then Select *Load Evaluators*.

2 Right-click to display the option menu.



3 Select *New Load Evaluato*r. The New Evaluator dialog box is displayed.



Name: SSO

Description: This is for SSO configuration

Report full load when the number of page faults per second is greater than this value: 2000

Report no load when the number of page faults per second is less than or equal to this value: 0

This rule allows your load evaluator to calculate a load based on the number of page faults per second. A page fault occurs every time the operating system accesses physical memory that has been flushed to disk.

When the number of page faults per second is within the low and high thresholds, Load Manager reports a load percentage based on the threshold

4 Specify a name for the Load Evaluator in the *Name* field.

5 Specify a description for the new evaluator in the *Description* field.

6 Select Page Faults and Page Swaps from the *Available Rules* list.

7 Click the *Add* button to add to the *Assigned Rules* list.

8 Drag to select Page Faults in the *Assigned Rules* list.

Page Fault settings are configured in the *Rule Settings* section, displayed in the bottom half of the New Evaluator dialog box.

9 Specify a value into the *Report full load when the number of page faults per second is greater than this value:* field.

10 Drag to select *Page Swaps* in the *Assigned Rules* list. Page Swap settings display in the Rule Settings section.

11 Specify a value into the *Report full load when the number of page swaps per second is greater than this value:* field.

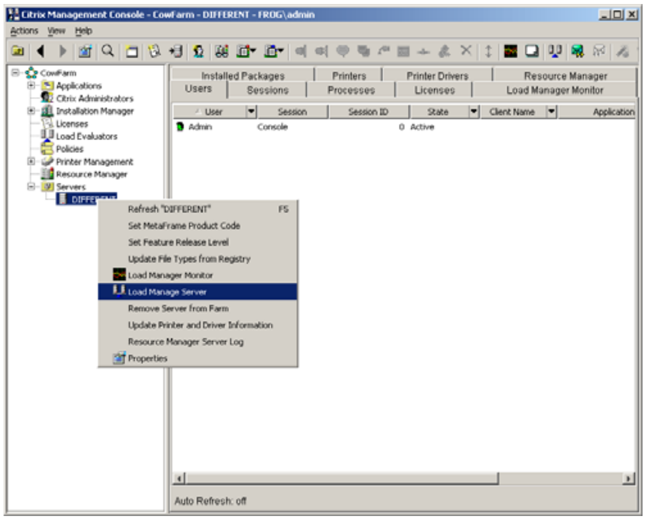
12 Specify a value into the *Report no load* when the number of page swaps per second is less than or equal to this *value:* field.

13 Click *OK*.

The required Load Evaluators are configured and loaded to the Citrix server that SecureLogin is installed.

4.2 Load New Evaluators to the Citrix Server

1. From the Citrix Management Console select the *Servers* > *Citrix servers*.



User	Session	Session ID	State	Client Name	Application
Admin	Console	0	Active		

2. Right-click on the relevant Citrix server name.
3. Select *Load Manage Server* from the options menu.The Load Manage Server – [server name] is displayed.
4. Select the configured *Load Evaluator* option from the *Available Load Evaluators* list.
5. Click *OK*.

   The new Load Evaluators are loaded to the Citrix server.

Using Connectors

5

SecureLogin enables applications for single sign-on by using connectors. A connector is the program that recognizes the specific application and runs the application definition Connectors have been created for most commonly used applications. You can build new connectors for proprietary applications or modify existing connectors.

This section provides information on the following:

- Section 5.1, "Enabling an Application with Connectors," on page 27
- Section 5.2, "Deleting Connectors," on page 28

For information on building or modifying connectors, see the *Novell SecureLogin 6.0.SP1 Administration Guide* and the *Novell SecureLogin 6.0 SP1 Application Definition Guide*.

5.1 Enabling an Application with Connectors

The SecureLogin Yahoo e-mail connector demonstrates how SecureLogin enables a standard application for single sign-on. If you do not have a Yahoo account you can use a similar application, for example Hotmail.

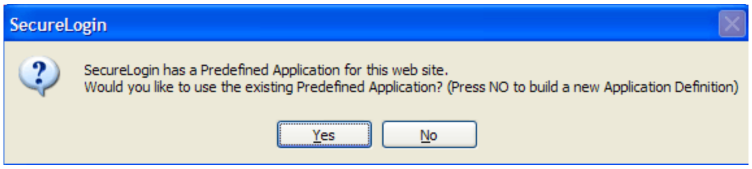
To use the Yahoo connector:

1 Start your Web browser.

2 Go to www.yahoo.com.

3 Click *Mail*.

SecureLogin detects the Yahoo login screen, executes the Yahoo connector, and displays a dialog box confirming that a password field has been detected.



SecureLogin has a Predefined Application for this web site.
Would you like to use the existing Predefined Application? (Press NO to build a new Application Definition)

4 Click *Yes*.

5 In the Enter Your User ID Information dialog box, type your Yahoo username and password, then click *OK*. SecureLogin automatically enters your login credentials, activates the *Sign In* button, and logs you in to your Yahoo account.

If the username or password entered is incorrect, a dialog box displays, requesting that you enter the correct credentials. Enter the correct credentials, then click *OK*.

SecureLogin saves your credentials and uses it to automatically log you in to your account every time you want to access Yahoo account.

6 (Optional) Test logging in and out of Yahoo, click *Sign Out*, then click *Yes*.

6a Click *Sign Out*.

6b Click `Yes`.

SecureLogin enters your credentials to log you back in to your Yahoo e-mail account.

If the login wasn't successful, delete the SecureLogin connector by using Manage Logins. Then repeat the steps.

5.2 Deleting Connectors

1. Double-click the SecureLogin icon located in the system tray.
2. Select *Applications*.
3. Select Yahoo.com, then click *Delete*.
4. Click *OK*.

Using Secure Workstation with Citrix

6

If the installation program discovers a Citrix client, the drivers for NMAS, Secure Workstation, and pcProx are installed.

If you have never installed SecureLogin, or if SecureLogin is not currently installed, then the ICA client components will be installed by default.

This section provides information on the following:

- Section 6.1, "Requirements," on page 29
- Section 6.2, "The Server Login Method," on page 29
- Section 6.3, "Using pcProx with Citrix," on page 30
- Section 6.4, "Using Secure Workstation with Citrix," on page 31

6.1 Requirements

❑ The ICA Citrix Client must be 6.1 or later.

❑ When using NMAS with Client32 or LDAPAuth, NMAS must be 3.2 or later on the client.

❑ If you use Client32 and NMAS on a Citrix server, the NMAS on the eDirectory server must also be 3.1 or later.

6.2 The Server Login Method

The login server method uses standard NMAS authentication. It authenticates to eDirectory.

The following must be running on the Citrix server:

- Client32 or LDAPAuth
- NMAS 3.2 or later
- SecureLogin

Scenario: Problem. The user at the ICA client launches a remote session. The devices (for example, a pcProx reader, smart card, or fingerprint reader) are also at the remote client. In the past, NMAS in this environment launched a session on the Citrix server. The output was redirected to the ICA client. The programs are running on the Citrix server, but input and output occur at the ICA client. NMAS couldn't communicate with its authentication devices at the ICA client.

The user at the ICA client wants to log in with Client32 NMAS and a fingerprint reader. A Client32 login dialog box appears. Client32 and the NMAS client are running on the Citrix server. NMAS launches LCM (login client method) on the Citrix server.

The fingerprint reader is attached to the ICA client, but the LCM is being launched on the Citrix server. The LCM can't read the fingerprint reader because the network link is in the middle.The virtual channel solves this problem.

Scenario: Solution by Using Virtual Channels. Client32 calls NMAS, and NMAS calls SecureLogin before it authenticates the user. SecureLogin determines whether it is running in a remote Citrix session or in a console session. (It tries to determine whether another workstation is on the network—another workstation on the network for the session that it is attached to. The Citrix server could be serving sessions to--for example--1,000 ICA clients. One session could be running on the console.) SecureLogin determines whether it is running in a console session or one of the remote sessions.

If SecureLogin is running in a remote session, it uses the virtual channel, which runs over the Citrix protocol. SecureLogin communicates with a `.dll` file that is plugged in to the ICA client. The `.dll` file invokes NMAS. The client invokes an LCM on the ICA client, which communicates with the devices attached to the ICA client. NMAS running on the Citrix server knows that SecureLogin is handling the login.

SecureLogin redirects to the ICA client, called NMAS on that client. It is redirecting the output from NMAS across the virtual channel. Client 32 sends NetWare Core Protocols to the NMAS server like it normally would.

After redirection, Secure Workstation communicates to NMAS running on the Citrix server that the user is logged in. NMAS then provides a session.

The user is not aware that anything special or different happened. The user at the ICA client sees the login dialog box with instructions to place a thumb on the thumbprint reader. The user uses the thumbprint reader to log in.

6.3 Using pcProx with Citrix

You can configure pcProx to automatically populate the fields on a login dialog box, based on the proximity card. pcProx reads the card, does an LDAP search, figures out which user the card belongs to, puts the username in the Username field, looks up credential data (a tree name context, server name, NMAS sequence, NMAS clearance), places all the data into the login dialog box, then starts the login process.

Scenario: pcProx Reader. A doctor walks to a workstation and places his pcProx card on a reader. The doctor logs in without typing any data. The username comes from eDirectory, the other data comes from a registry on the local workstation.

Identifying the user based on the badge is a user identification process. It is separate from the authentication process that NMAS handles. The Secure Workstation plug-in plugs in to the NMAS component on the login dialog box. NMAS has its own Active X control on the login dialog box. It contains the username and password field. You sometimes don't see the password field with NMAS because the NMAS client can hide it. That control can use a .dll file, which is a user ID plug-in interface, and request a username from the device.

Thus, the identification process, the user ID plug-in, is separate from authentication. A user can identify himself with the pcProx card and then authenticate with the password. The identification process specifies to Client32 who the user is. The process could be as simple as typing a username. After the user clicks *OK*, Client32 starts the authentication process, verifying that the user is who he claims to be by making sure that the password is valid.

You can type your username or put your pcProx card on a reader and have the card get your username. After you click OK, NMAS is launched. NMAS does not know or care how you identify yourself (by putting down a pcProx card or typing your username). NMAS runs the login sequence, which might or might not include a proximity card.

Identification and authentication are separate so that you have the option to authenticate by using a proximity card but you are not required to use on.

Therefore, the pcProx method will use the virtual channel on its own.

Scenario. Client32 is running on a Citrix server. Client32 displays a login dialog box, which calls pcProx. pcProx asks who the user is. It uses the virtual channel to communicate with the ICA client. The process calls pcProx method at the ICA client. The pcProx method communicates with the reader.

At that point, the process can access the reader and request the badge number, which is returned to pcProx on the Citrix server. Using LDAP, PCProx communicates with eDirectory and gets the user ID, sends the badge number to LDAP, passes the data back to Client32. The user is identified. Then the authentication process begins.

6.4 Using Secure Workstation with Citrix

Secure Workstation uses device removal plugs. Secure Workstation renders a service on the machine. The registry has a list of `.dll` files that implement device removal plug-ins for different devices. Therefore, Secure Workstation can receive device removal events from PCProx cards, smart cards, and third-party plug-ins.

The registry can register a .dll file with Secure Workstation. The `.dll` file implements entry points to be a device removal plug-in. The `.dll` file is loaded into Secure Workstation Service's address space so that device removal events can be reported.

When a Secure Workstation service starts up, it loads those `.dll` files. As part of the Secure Workstation policy, you can configure a device removal event. At the core, the Secure Workstation policy is just events and actions. It listens for events and then, depending on the event, takes some action. For example, you can configure Secure Workstation to lock a workstation as soon as a device is removed.

In this case, when you configure the device removal event, you can specify which devices you want to listen for.

Scenario: Entry Points. A Secure Workstation post-login method delivered a policy to the workstation. Secure Workstation activates the device removal plug-in for the device specified in the policy. Secure Workstation instructs the workstation to call an entry point in the `.dll` file to start monitoring the device. Secure Workstation provides an entry point to call when the device gets removed. If the plug-in detects that the device isn't there, it informs Secure Workstation of the change. Secure Workstation then takes the action associated with the device removal event.

The problem with this scenario is that the Secure Workstation service is running on the Citrix server, but the devices are attached to the ICA client. In this case, the Secure Workstation service uses the virtual channel to communicate with a .dll file running on the ICA client. The `.dll` file calls the device removal plug-ins for the devices.

You don't install anything extra on the Citrix server. You just install SecureLogin there. All the files are copied to the server.

Setting Up Terminal Services

7

This section contains the following information:

7.1 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 (`slinac.dll`) applied to a workstation with the Novell® Client™, with or without the Novell Modular Authentication Service (NMAS™) client.
- 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 (`slinas.dll`) applied to a terminal server with the Novell Client.

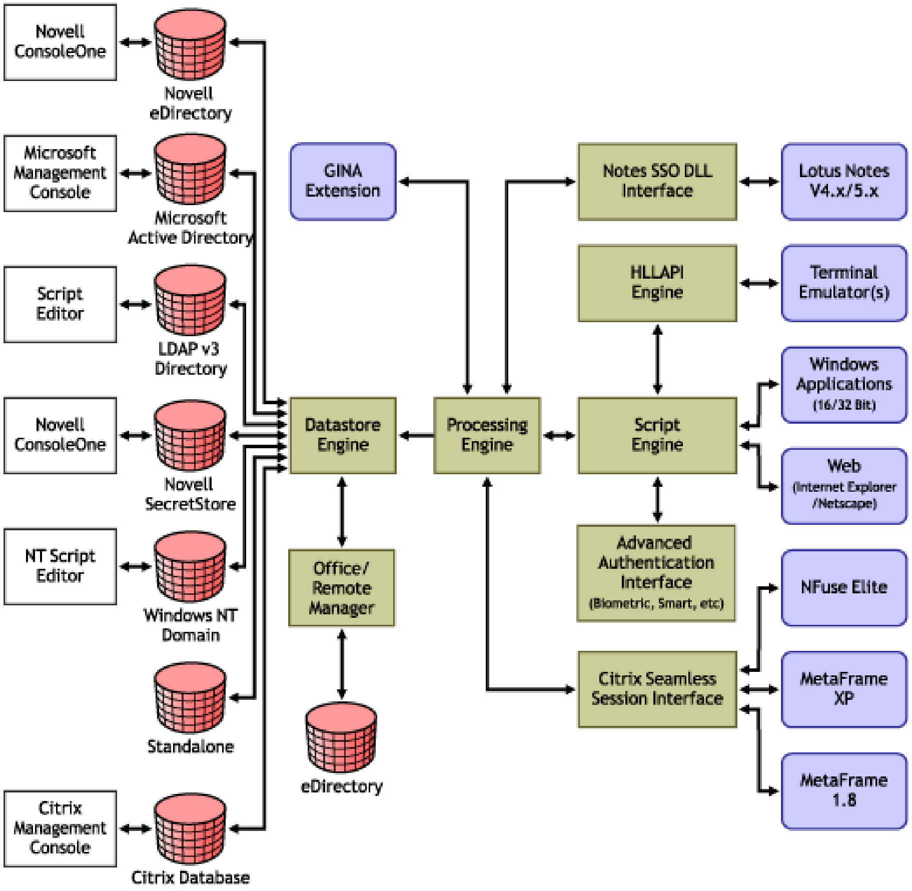
  The component provides the server-side link to the client GINA.
- The server GINA replacement (`sl_tsgina.dll`) applied to a terminal server without the Novell client.

  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:

Figure 7-1 *SecureLogin architecture*

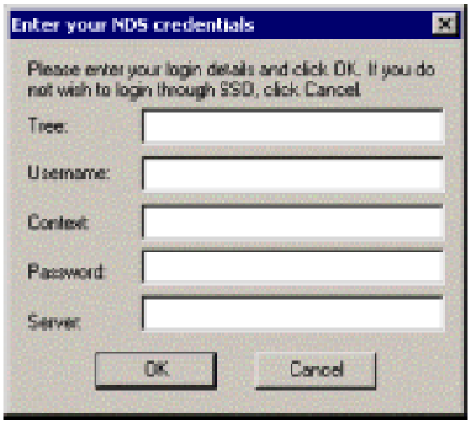


7.2 GINA Credential Pass-Through

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 do no 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:

Figure 7-2 *NDS Credentials*



Please enter your login details and click OK. If you do not wish to login through SSO, click Cancel.

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.

7.3 Integrating Citrix Components

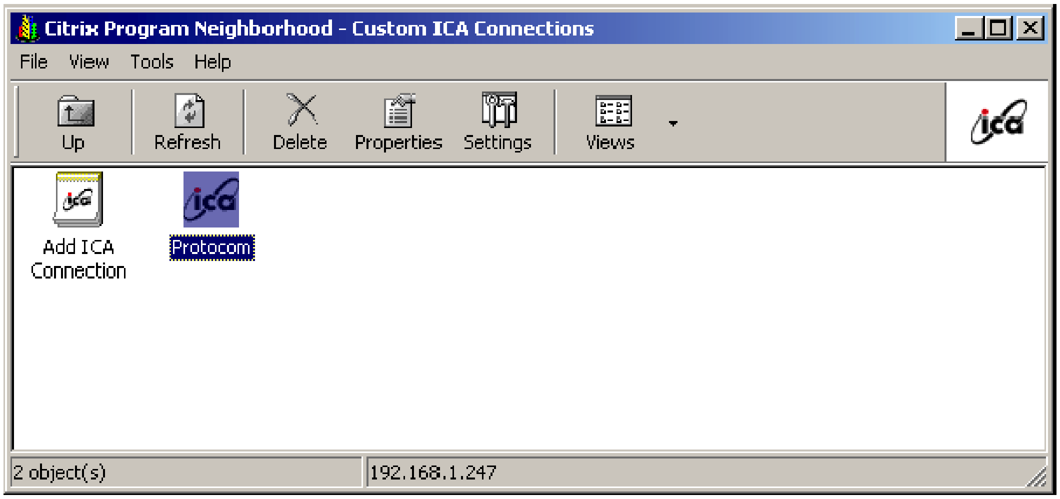
Citrix provides several ways to access a Citrix server or published application. How you access the server determines how SecureLogin handles the authentication to the server. Although different methods are used depending on how you access the server, SecureLogin can manage all forms of authentication.

- Section 7.3.1, "Windows GINA Authentication," on page 35
- Section 7.3.2, "Program Neighborhood," on page 36
- Section 7.3.3, "Using Desktop Shortcuts to Published Applications," on page 37
- Section 7.3.4, "Handling Password Changes," on page 37

7.3.1 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:

Figure 7-3 *Custom ICA Connections*

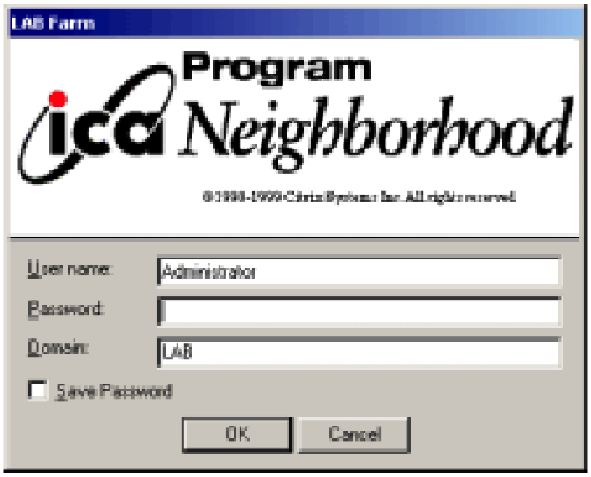


Another example of this type of authentication occurs when you export a published application to an `.ica` file and distribute it to your workstations. This type of authentication is enabled by installing the GINA components. The authentication is not disabled even if SecureLogin is not currently active.

7.3.2 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:

Figure 7-4 *Program Neighborhood Authentication*



User name: Administrator

Password:

Domain: LAB

□ Save Password

Program Neighborhood then collects the credentials and sends them to a Citrix server in the farm. The Citrix Seamless Session Interface does not 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.

7.3.3 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 enters the wrong information into the dialog box.

7.3.4 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 one of this passwords 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).

7.4 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.

For more information on Virtual Channel, see document 3149664 on the Novell Support Web site. (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3149664&sliceId=SAL_Public&dialogID=21162948&stateId=0%200%2021170573)

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

- Section 7.4.1, "Virtual Channel Components," on page 37
- Section 7.4.2, "Auto-Detecting the Client Protocol," on page 38

7.4.1 Virtual Channel Components

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

Component	Description
Client login extension	Collects users' login credentials for single sign-on.

Component	Description
Virtual Channel Driver (VCD)	The center of SecureLogin Terminal Server single sign-on. The VCD is the liaison 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 the single sign-on.

SecureLogin uses the following processes:

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 a `.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 does not exist, the VCD reverts to the generic platform name.

   If the generic platform name does not 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 cancel entering credentials, the server login box appears as usual.

   NOTE: SecureLogin does not 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.

7.4.2 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.

7.5 Requirements for Terminal Services

The section contains the following information:

- Section 7.5.1, "Server Requirements," on page 39
- Section 7.5.2, "Workstation Requirements," on page 39

7.5.1 Server Requirements

- Windows 2000 and 2003 Server Edition or the Windows 2000 Server family with Terminal Service enabled.

  NOTE: Only the 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):
  - Presentation Server 4.0
  - Citrix client 9.2
- (Optional) Novell Client 4.91 or later

7.5.2 Workstation Requirements

- Novell Client version 4.91 or later
- SecureLogin version 6.0 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)

7.6 Setting Up the Server

In Novell SecureLogin 6.0 and later, the server setup to support terminal server integration is automated. You are not required to carry out any manual set up.

In the process, the following files are copied to the Windows system directory, such as `c:\winnt\system32`:

- `srv\sl_vc.dll`
- `srv\sl_rdp.dll`
- `srv\sl_ica.dll`

- `srv\slaa_sso.dll`

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

7.6.1 Setting the GINA

If you are using Novell SecureLogin 6.0 or later, the installation automatically installs the necessary binaries and configures the server. In such case, you can avoid the following steps.

Servers with the Novell Client

1. Set up a Novell login extension.
   Copy `srv\nw\slinas.dll` to the Windows system directory, (for example, `c:\winnt\system32`
2. Register the login extension.

   In the `srv\nw` directory, double-click `Register NTLoginExt.reg`.
3. Follow the on-screen instructions to finish the registration.

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 the login extension.
   In the `srv\nw` directory, double-click `winlogon_server.orgTLoginExt.reg`.
3. Follow the on-screen instructions to finish the registration.
4. Reboot the server.

7.6.2 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 directory is enabled, NICI does not set the Access Control Lists (ACL) 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.

7.7 Setting Up Workstations

NOTE: If you are using Novell SecureLogin 6.0 or later, the installation automatically installs the necessary binaries and configures the workstation. If this is the case, you can skip the steps in this section.

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 do 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).

- Section 7.7.1, "Novell Client (without the NMAS Client)," on page 41
- Section 7.7.2, "Novell Client (with the NMAS Client)," on page 42
- Section 7.7.3, "Microsoft Workstation with No Novell Client Installed," on page 42

7.7.1 Novell Client (without the NMAS Client)

1. Set up the Novell login extension by copying `srv\nw\slina.dll` to the Windows system directory (for example, `c:\winnt\system32`).
2. Register the login extension.

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

3 Follow the on-screen instructions to finish the registration.

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

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

5 Reboot the workstation.

7.7.2 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 9x).

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 9x/ME, copy `unicows.dll` from the `\redistributable` directory to your system directory (for example, `c:\windows\system`).

3 Follow the on-screen instructions to finish the registration.

4 Reboot the workstation.

7.7.3 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 Follow the on-screen instructions to finish the registration.

4 Reboot the workstation.

7.8 Installing the Virtual Channel Driver

If you are using Novell SecureLogin 6.0 or later, the installation automatically installs the necessary binaries and configures the workstation. If this is the case, you can skip the following steps:

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

- Section 7.8.1, "Workstations with the Citrix Client (ICA)," on page 42
- Section 7.8.2, "Workstations with the Terminal Server Client (RDP)," on page 43

7.8.1 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 [ICA30] section 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 are not required.

3. 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.

4. Set up Microsoft Layer for Unicode on Windows 95/98/ME.If you are running Windows 9x/ ME, copy `unicows.dll` from the `\redistributable` directory to your ICA Client directory (for example, `c:\program files\citrix\ica client`).

7.8.2 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 in `Client workstation.reg`.

   IMPORTANT: This is a per-user setting.

3. Follow the on-screen instructions to finish the registration.

7.9 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.

7.10 Integrating with Citrix Published Applications

This section provides information on the following:

- Section 7.10.1, "Modifying the Command Line," on page 44
- Section 7.10.2, "Using SLLauncher Syntax," on page 44

7.10.1 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*

7.10.2 Using SLLauncher Syntax

To run `SLLauncher`, use the following command:

`SLLauncher`*Optional_ParameterExecutable_to_run optional_executable's_ parameters*

IMPORTANT: If your executable contains a path or command line parameters that include spaces, enclose 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:

***Table 7-1** Command Line Parameters*

Parameter	Explanation

/w executable name	Specifies another process to wait for before closing SecureLogin.
	Example,
	`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`
	`/p"novellMainframe"`
	`C:\Progra~1\novell\SecureLogin\tlaunch.exe /q /auto /e“WallData Rumba”`
	`SLLauncher.exe /w /d mspaint.exe run_MSPaint.CMD`

7.11 Registry Settings

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

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

- Section 7.11.1, “Auto-Detecting the Client Protocol,” on page 45
- Section 7.11.2, “Servers with a Novell Client,” on page 46
- Section 7.11.3, “Localized Machine,” on page 46
- Section 7.11.4, “Third-Party GINA,” on page 46

7.11.1 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”
```

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.

7.11.2 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"
```

7.11.3 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"
```

7.11.4 Third-Party GINA

When using a third-party GINA (for example, the 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:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
"LogonWindowCaption" = "Logon window caption"
```

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.

7.12 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:

Location	.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.

Upgrading SecureLogin

8

All versions of SecureLogin Single Sign-On, prior to versions 3.5.1.x, must be uninstalled before upgrading to version 6.0 SP1. For more information on upgrading SecureLogin from earlier versions see, “Upgrading from Earlier Versions” in the *Novell SecureLogin 6.0 SP1 Installation Guide*.

8.1 Uninstalling Version 3.0.x

To uninstall previous versions prior to version 3.5.x of SecureLogin:

1. Select *Start* > *Settings* > *Control Panel* > *Add/Remove programs*.
2. Select SecureLogin 3.0[.x], then click *Remove*.
3. A SecureLogin message box may display requesting system restart, click *Yes* if it is convenient to restart the workstation now, or *No* button to restart later.

   SecureLogin is now uninstalled.
4. Before installing the new version of SecureLogin, Logoff and logon again.

8.2 Phased Upgrades

SecureLogin currently does not support phased upgrades for Citrix or Terminal Services deployments.

Documentation Updates

A

This section lists updates to the Novell SecureLogin 6.0 Citrix and Terminal Services Guide that have been made since the initial release of Novell SecureLogin 6.0.

The information helps you to keep current on documentation updates and, in some cases, software updates (such as a Support Pack release).

The information is grouped according to the date when the Novell SecureLogin 6.0 Citrix and Terminal ServicesGuide was republished. Within each dated section, the updates are listed by the names of the main table of contents sections.

The Novell SecureLogin 6.0 Citrix and Terminal Services Guide has been updated on the following dates:

- Section A.1, "December 12, 2006," on page 51

A.1 December 12, 2006

Location	Description
Chapter 7, "Setting Up Terminal Services," on page 33	This is a new addition to the Citrix and Terminal Services Guide. This chapter gives detailed information on setting up MS terminal services.