

Novell Nsure™ SecureLogin

3.51.1

www.novell.com

TERMINAL SERVICES GUIDE

September 7, 2004



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.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2003-2004 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

www.novell.com

Nsure SecureLogin 3.51.1 Terminal Services Guide
[September 7, 2004](#)

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.

Third-Party Trademarks

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

Contents

	About This Guide	7
1	Getting Started	9
	Supported Platforms	9
	Servers	9
	Workstations	9
	Before You Install SecureLogin	10
	Preparing the Citrix Server	10
	Preparing Workstations	10
2	Uninstalling SecureLogin	11
3	Installing SecureLogin for Citrix	13
	Installing to Network Servers and Workstations	13
	Installing SecureLogin to the Citrix Server	13
4	Enabling Citrix Applications for Single Sign-On	15
	Enabling Citrix Applications.	15
5	Using Connectors	23
	Enabling an Application with Connectors.	23
	Deleting Connectors	24
6	Using Secure Workstation with Citrix	25
	Requirements.	25
	The Server Login Method.	25
	Using PCProx with Citrix	26
	Using Secure Workstation with Citrix.	27
7	Configuring Load Evaluators	29
8	Troubleshooting	33
	GINA Credential Pass-Through.	33
	Troubleshooting a Server Installation.	34
	Protocol Files	34
	GINA Setup	34
	Troubleshooting a Workstation Installation	35
	Installing Login Extensions to the Workstation	35
	Installing Virtual Channel Drivers On the Workstation	37
	Using Debugging Log Files	38
	Log Files for Servers	38
	Log Files for Workstations	39

About This Guide

The *Terminal Services Guide* is for network administrators, system administrators, and IT Support staff. The *Guide* provides information on the following:

- ♦ Chapter 1, “Getting Started,” on page 9
- ♦ Chapter 3, “Installing SecureLogin for Citrix,” on page 13
- ♦ Chapter 5, “Using Connectors,” on page 23
- ♦ Chapter 4, “Enabling Citrix Applications for Single Sign-On,” on page 15
- ♦ Chapter 5, “Using Connectors,” on page 23
- ♦ Chapter 6, “Using Secure Workstation with Citrix,” on page 25
- ♦ Chapter 7, “Configuring Load Evaluators,” on page 29
- ♦ Chapter 8, “Troubleshooting,” on page 33

The examples provided in this guide refer to Citrix MetaFrame Feature Release 2 in a Novell® eDirectory™ environment. If your network environment is different, refer to your platform or Citrix documentation for assistance.

Additional Documentation

This *Guide* is part of a documentation set for SecureLogin 3.51.1. You can find additional information in the following:

- ♦ The Help systems in SecureLogin on the desktop as well as SecureLogin snap-ins to ConsoleOne® or Microsoft® Management Console.
- ♦ The **Nsure SecureLogin 3.51.1 Installation Guide** (installing SecureLogin, migrating secrets from earlier versions, and configuring Secure Workstation)
- ♦ The **Nsure SecureLogin 3.51.1 Administration Guide** (tools and tasks to manage SecureLogin and configure terminal emulators)
- ♦ The **Nsure SecureLogin 3.51.1 Scripting Guide** (concepts concerning scripting, scripting commands, and example scripts for applications)
- ♦ The **Nsure SecureLogin 3.51.1 Configuration Guide for Terminal Emulation** (how to configure Terminal Launcher for selected terminal emulators)
- ♦ The **Nsure SecureLogin 3.51.1 User Guide** (using SecureLogin to enable applications for single sign-on)

Documentation Updates

For the most recent version of the *Nsure SecureLogin 3.51.1 Terminal Services Guide*, see the [Novell documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

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.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with Nsure SecureLogin 3.51.1. Send e-mail to proddoc@novell.com.

1

Getting Started

Citrix servers manage distribution of and access to applications. SecureLogin provides powerful tools to configure end users' login access. Citrix requires a back end to a directory (for example, Novell eDirectory) running a network server. Therefore, SecureLogin is installed on both the network server and a Citrix server.

Supported Platforms

Servers

Operating Systems

- ♦ Windows NT* 4.0 Terminal Server Edition*
- ♦ Windows 2000/2003 Server with Terminal Services enabled

Terminal Server

Windows Terminal Server or one of the following Citrix products:

- ♦ MetaFrame 1.8 for Windows 2000
- ♦ MetaFrame 1.8 for Windows NT4.0
- ♦ MetaFrame XP

NOTE: Only the Windows 2000 Server Family operating system supports virtual channels. If you want virtual channel support on Windows NT 4.0 Terminal Server Edition, you need to install Citrix MetaFrame Server software.

Optional eDirectory environment

Novell Client™ 4.83 or later

Workstations

SecureLogin

Version 3.5.1 or later

Client

One of the following clients:

- ♦ Win32 ICA Client V.6.00.905 or later
- ♦ Terminal Server Clients that support Remote Desktop Protocol (RDP) 5.0

You need the version that is distributed with Windows 2000/2003 Advanced Server.

Optional eDirectory Environment

Novell Client 4.83 or later

Before You Install SecureLogin

Preparing the Citrix Server

Before you install SecureLogin on the Citrix server, you need to:

- ☐ Ensure that you have administrator rights and access to your network and Citrix servers.
- ☐ Ensure that the network server (in our examples, Novell® eDirectory™) is running an eDirectory tree and has SecureLogin installed.

The network server is not the same server as the Citrix server.

- ☐ Ensure that you have access to the Citrix Server Console.
- ☐ Uninstall previous versions of SecureLogin on the Citrix server.
- ☐ Install Citrix on Citrix servers.

SecureLogin detects Citrix and installs the appropriate server files. If SecureLogin doesn't detect Citrix, files for Citrix won't be installed.

Preparing Workstations

- ☐ Install the Citrix client on workstations.

SecureLogin detects Citrix and installs the appropriate workstation files. If SecureLogin doesn't detect Citrix, files for Citrix won't be installed.

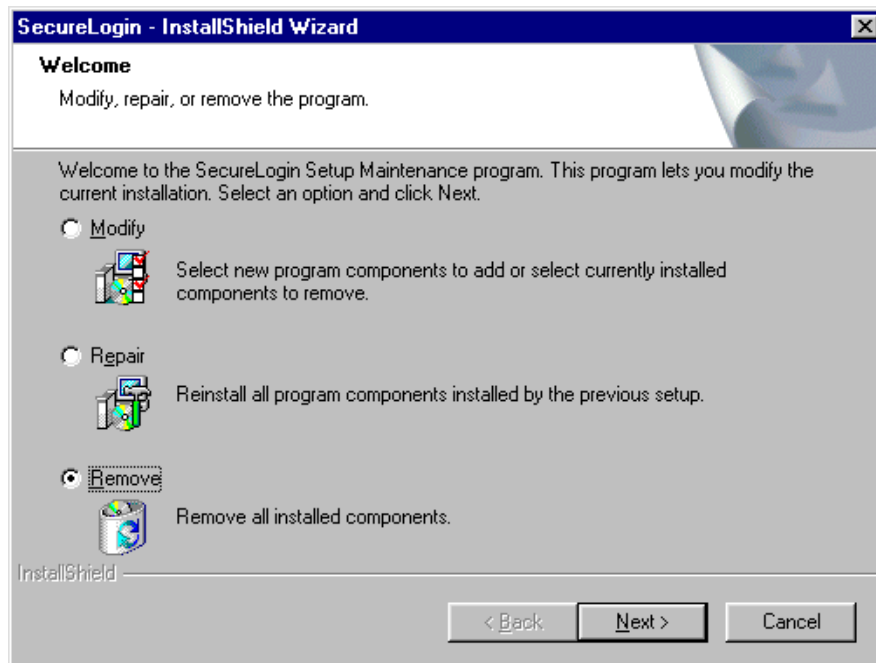
- ☐ Uninstall previous versions of SecureLogin on the workstation.

2

Uninstalling SecureLogin

To uninstall SecureLogin 3.51.1 in standalone mode:

- 1** Log in to the workstation as Administrator.
- 2** Click Start > Settings > Control Panel.
- 3** Double-click Add/Remove Programs.
- 4** Select Novell Nsure SecureLogin, then click Change/Remove.
- 5** In the SecureLogin InstallShield Wizard Welcome dialog box, select Remove, then click Next.



- 6** In the confirmation dialog box, click yes to remove all SecureLogin components, then click Finish.

3

Installing SecureLogin for Citrix

To run SecureLogin in a Citrix environment, you must install SecureLogin on the Citrix server and the network server and then enable published applications. This section provides information on the following:

- ♦ “Installing to Network Servers and Workstations” on page 13
- ♦ “Installing SecureLogin to the Citrix Server” on page 13

For information on enabling published applications, see [Chapter 4, “Enabling Citrix Applications for Single Sign-On,”](#) on page 15.

Installing to Network Servers and Workstations

You install SecureLogin on network Windows and NT servers and on Citrix servers.

To install SecureLogin on network servers and workstations, refer to the relevant section in the [Nsure SecureLogin 3.51.1 Installation Guide](#):

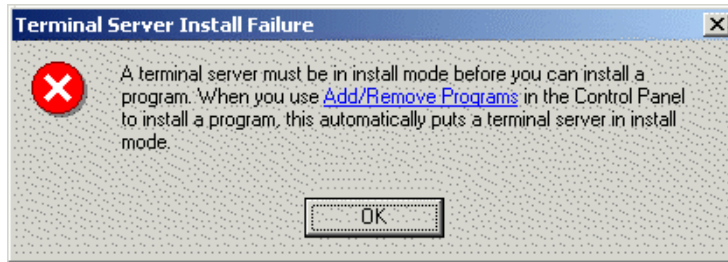
Environment	Section
Active Directory	“Installing in Active Directory Environments”
Windows NT, 2000, or 2003	“Installing in Windows NT/2000 Domains”
LDAP	“Installing in LDAP Environments”
Novell® eDirectory™	“Installing in Novell eDirectory Environments”

Installing SecureLogin to the Citrix Server

- 1 Log in to the Citrix server as Administrator.
- 2 Insert the SecureLogin CD or navigate to the unzipped download image.
- 3 Run setup.exe.

The CD automatically launches the installation program. If you are installing from a download image, run setup.exe from the \client directory.

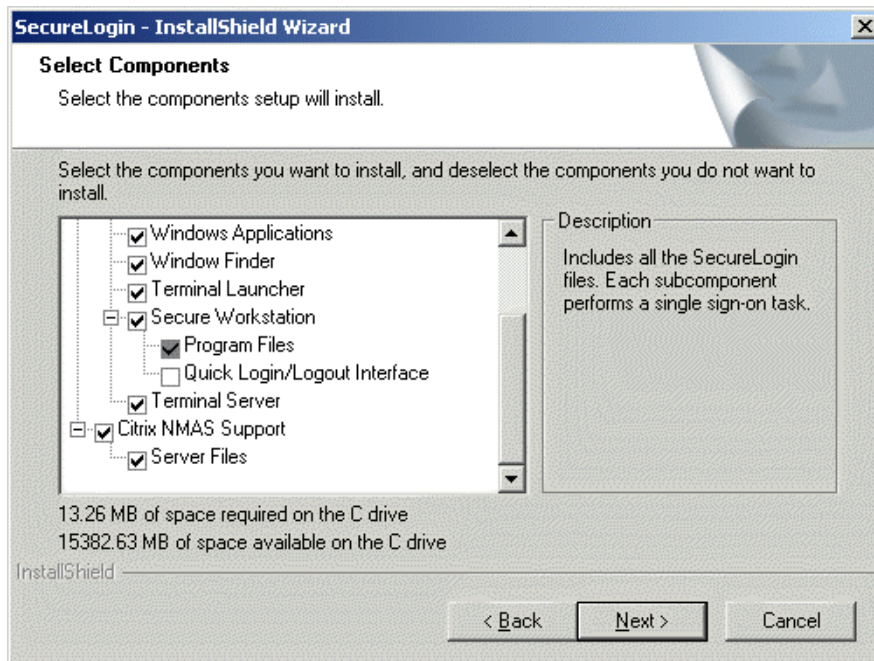
If the Terminal Server Install Failure error message displays, navigate to and run setup.exe.



- 3a** Click the Add/Remove Programs hyperlink, then select Add New Programs.
- 3b** Click CD or Floppy, then click Next.
- 3c** Browse to and open setup.exe, then click Next.
- 4** In the Choose Setup Language dialog box, select your language, then click Next.
- 5** Accept the license agreement by clicking Yes, then click Next.
- 6** In the Setup Type dialog box, select Custom, then click Next.
- 7** In the Choose a Platform for SecureLogin dialog box, select your platform, then click Next.
- 8** 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 [Nsure SecureLogin 3.51.1 Installation Guide](#).

When selecting components, make sure that the Citrix check box is checked.



If the installation requires a reboot, click Next > Finish.

If the installation doesn't require a reboot, click Finish.

4

Enabling Citrix Applications for Single Sign-On

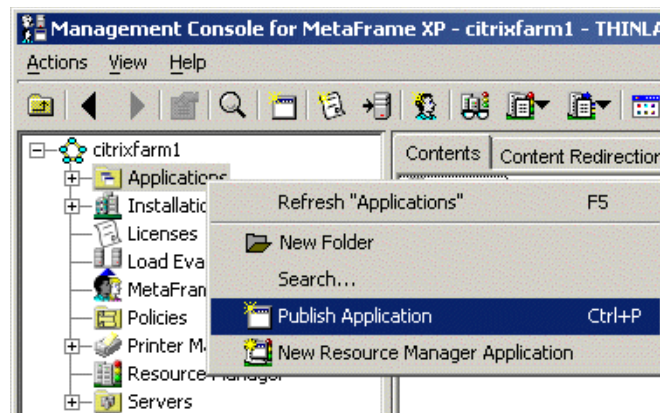
Because individual application screen cues are not available in Citrix environments, SecureLogin is unable to recognize individual applications when users access them. To enter login credentials when an application executes, SecureLogin needs to start before the application.

Also, the SecureLogin executable SLLauncher.exe must be running before the application launches. To achieve this, include SLLauncher.exe in the published application path.

Enabling Citrix Applications

To enable a Citrix published application for single sign-on by using the Citrix Management Console:

- 1 Right-click Applications from the Citrix farm, then select Publish Application.



- 2 In the Application Publishing Wizard dialog box, name and describe the published application, then click Next.

Welcome to the Application Publishing Wizard

This wizard will help you publish an application on Citrix MetaFrame XP 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:

Notepad published app

In this example, the application to be published is Notepad. The Name and Application Description edit boxes are used primarily to help you identify and administer the application.

- 3 In the Specify What to Publish dialog box, browse to and select the executable of the application program file.

For example, select `c:\winnt\system32\notepad.exe`.

Specify What to Publish

☒ Application

☐ Desktop

☐ Content

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

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

Command Line:

C:\WINNT\system32\notepad.exe

Browse...

Working Directory:

C:\WINNT\system32

- 4 Return to the Specify What to Publish dialog box by clicking OK.
- 5 Type the relevant directory path in the Working Directory field (for example, `c:\winnt\system32`).

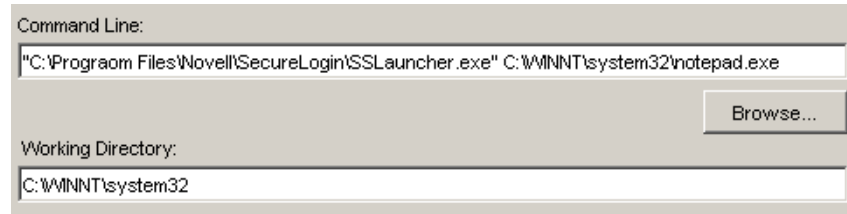
The working directory is the directory path of the program executable.

- 6 Type the path to SecureLogin's SLLauncher.exe file before the path to the published application executable, then click Next.

For example, in the Command Line edit box type

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

NOTE: Type one space between the SecureLogin path and the application executable path.

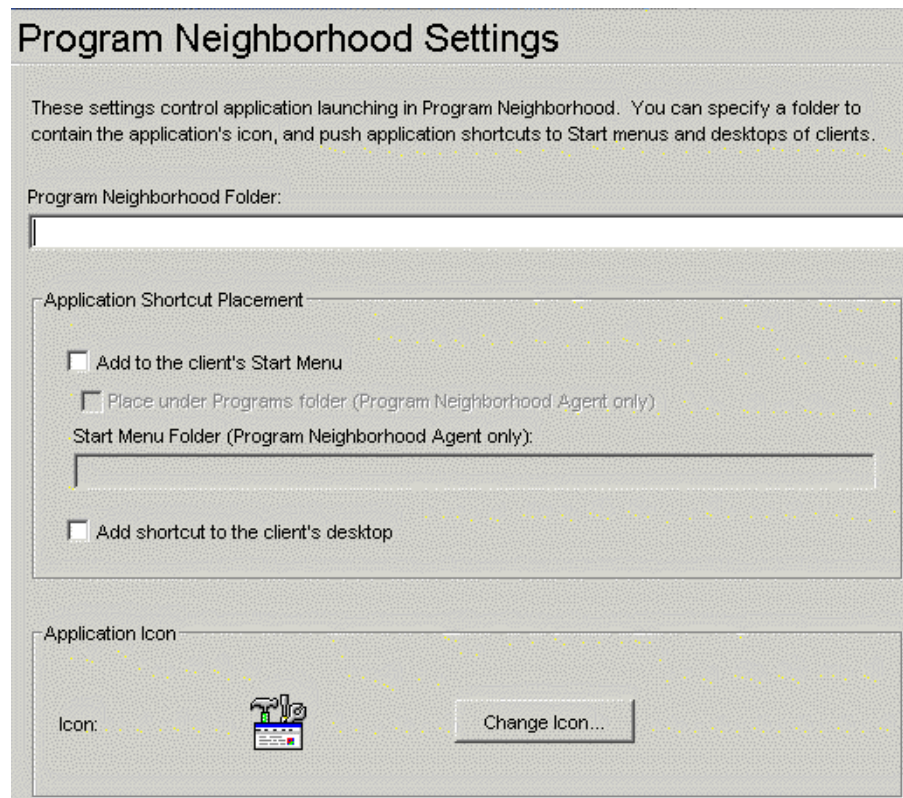


Command Line:
"C:\Program Files\Novell\SecureLogin\SSLauncher.exe" C:\WINNT\system32\notepad.exe

Working Directory:
C:\WINNT\system32

Browse...

- 7 In the Program Neighborhood Settings dialog box, select options, configure Neighborhood settings as required, then click Next.



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:
[Empty text box]

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):
[Empty text box]
- ☐ Add shortcut to the client's desktop

Application Icon

Icon: [Icon of a folder with a document] [Change Icon...]

- 8 In the Specify Application Appearance dialog box, select and configure application appearance options as required, then click Next.

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.

- 9 In the Specify ICA Client Requirements dialog box, select and configure ICA Client Requirement options as required, then click Next.


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

- 10 In the Specify Application Limits dialog box, select and configure application limits as required, then click Next.

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:

☐ Allow only one instance of application for each user

CPU priority level:

Normal

- 11** In the Specify Servers dialog box, select the relevant server from the Available servers list, click Add, then click Next.

Specify Servers

Choose the Citrix MetaFrame XP 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:

- INLDOMAIN2

Add ➤

Add All ⬆

◀ Remove

◀ Remove All

Configured Servers:

You need to specify a server to publish and deploy applications.

For this example, select INLDOMAIN2.

- 12** In the Specify Users dialog box, check Show Users.

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

Add List of Names...

Look in:

INLDOMAIN2

- Power Users
- Replicator
- Users**
- Administrator
- CTX_WEB_ADMIN

Add

Remove

☒ Show users

Configured Accounts

Users (INLDOMAIN2\Users)

- 13** Select the users (for example Users), then click Add.

The Specify File Type Associations dialog box might display, depending on the published application.

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
<input checked="" type="checkbox"/>	.wfs	ADF Installer Package
<input type="checkbox"/>	.cdf	Channel File
<input type="checkbox"/>	.ini	Configuration Settings
<input type="checkbox"/>	.JSE	JScript Script File
<input type="checkbox"/>	.JS	JScript Script File
<input type="checkbox"/>	.bat	MS-DOS Batch File
<input type="checkbox"/>	.reg	Registration Entries
<input type="checkbox"/>	.inf	Setup Information
<input type="checkbox"/>	.zap	Software Installation Settings
<input type="checkbox"/>	.log	Text Document

- 14** (Conditional) If the Specify File Type Associations dialog box displays, check boxes as required, then click Finish.

The published application now displays in the Contents tab of the Citrix Management Console.

- 15** Repeat publishing steps for all applications that will be enabled for SecureLogin single sign-on.

After all required applications have been published, test executing an application to ensure that SecureLogin for Citrix has installed successfully.

For information on enabling applications, see “[Managing SecureLogin](#)” in the [Nsure SecureLogin 3.51.1 Administration Guide](#).

5

Using Connectors

SecureLogin enables applications for single sign-on by using connectors. A connector is the program that recognizes the specific application and runs the login script. 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:

- ♦ “Enabling an Application with Connectors” on page 23
- ♦ “Deleting Connectors” on page 24

For information on building or modifying connectors, see the [Nsure SecureLogin 3.51.1 Administration Guide](#) and the [Nsure SecureLogin 3.51.1 Scripting Guide](#).

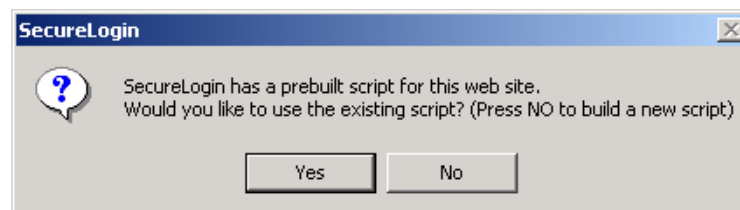
Enabling an Application with Connectors

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.



- 4 Click Yes.
- 5 In the Enter Your User ID Information dialog box, type your Yahoo username and password, then click OK.

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 automatically enters your login credentials, activates the Sign In button, and logs you in to your Yahoo account. Your Yahoo e-mail account displays and your credentials have been saved.

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.

Deleting Connectors

- 1** Double-click the SecureLogin icon located in the system tray.
- 2** Select Applications.
- 3** Select Yahoo.com, then click Delete.
- 4** At the confirmation dialog box, click Yes > OK.

6

Using Secure Workstation with Citrix

Functionality for PCProx, Secure Workstation, and NMAS has changed in SecureLogin 3.51.1.

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 isn't currently installed, the ICA client components will be installed by default.

This section provides information on the following:

- ♦ “Requirements” on page 25
- ♦ “The Server Login Method” on page 25
- ♦ “Using PCProx with Citrix” on page 26
- ♦ “Using Secure Workstation with Citrix” on page 27

Requirements

- ☐ The ICA Citrix client must be 6.0 or later.
- ☐ When using NMAS with Client32 or LDAPAuth, NMAS must be 2.3 or later on the client. Otherwise, NMAS won't call SecureLogin.
- ☐ If you use Client32 and NMAS on a Citrix server, the NMAS on the eDirectory server must also be 2.3 or later.

If you use LDAPAuth on the server, the NMAS version doesn't matter.

The Server Login Method

The login server method uses standard NMAS authentication. It authenticates to eDirectory. The NetWare Core Protocol (NCP) communicates with NMAS and NMAS then authenticates.

The following must be running on the Citrix server:

- ♦ Client32 or LDAPAuth
- ♦ NMAS 2.3 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 isn't aware that anything special or different happened. The user at the ICA client sees the login dialog with instructions to place a thumb on the thumbprint reader. The user uses the thumbprint reader to log in.

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 doesn't 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 aren't 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.

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.

7

Configuring Load Evaluators

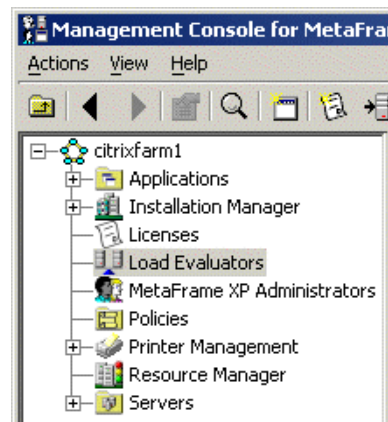
For SecureLogin to run effectively on a Citrix server, configure load evaluators for page faults and page swaps. Do this before installing SecureLogin.

If the server drops client connections when SecureLogin is running on the Citrix server, try increasing the number of page fault allowed on your load balancer template. The drops happen because SecureLogin tries to minimize memory usage.

The following instructions apply to Citrix Metaframe XP Feature Release (FR).

To create the new Load Evaluators:

- 1 Start Citrix Management Console.
- 2 Select Load Evaluators from the farm hierarchy.

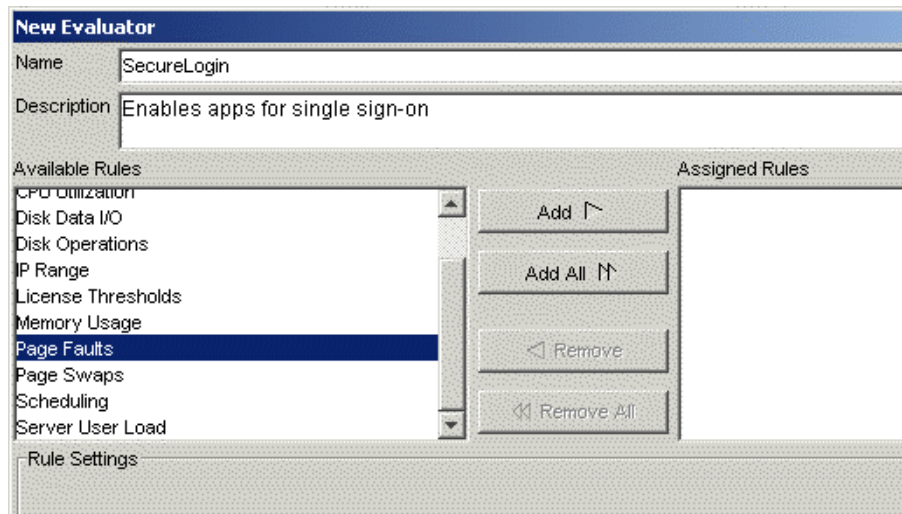


- 3 Right-click to display the option menu.
- 4 Select New Load Evaluator.
- 5 In the Name edit box, type a name for the Load Evaluator.



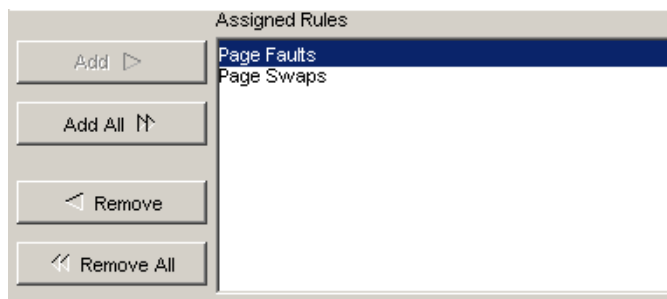
- 6 In the Description edit box, type a description for the new evaluator.

- 7** Select Page Faults from the Available Rules list, then click Add.

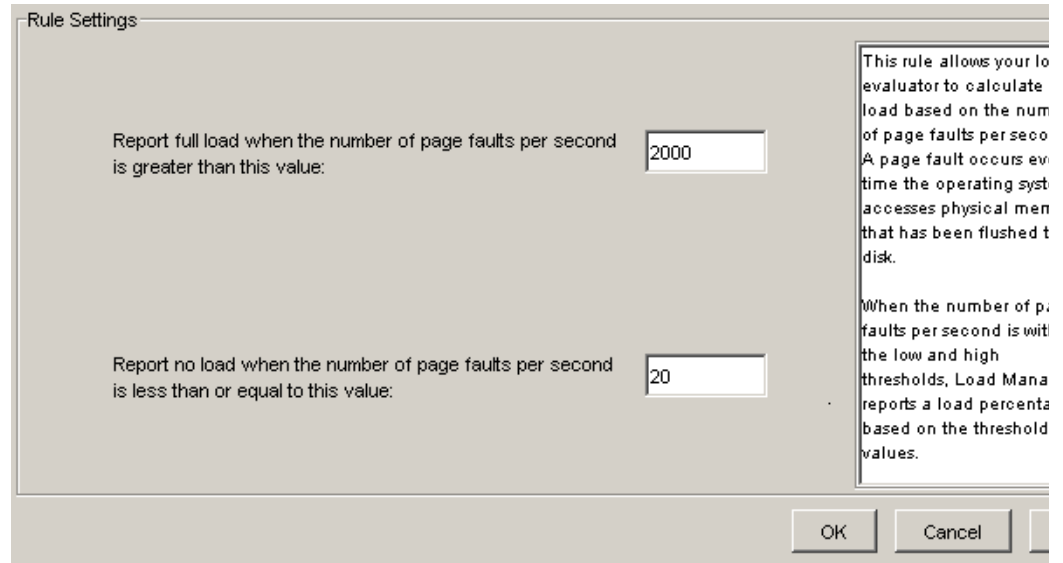


- 8** Select Page Swaps from the Available Rules list, then click Add.

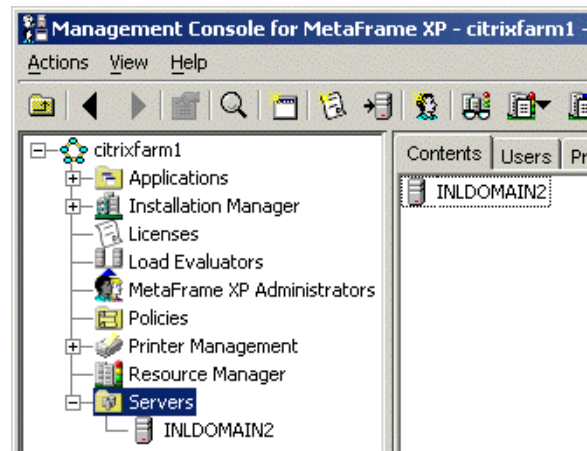
- 9** Select Page Faults in the Assigned Rules list.



- 10** In the Rule Settings edit boxes, type a value for each Page Fault setting.
Settings are configured in the Rule Settings pane.

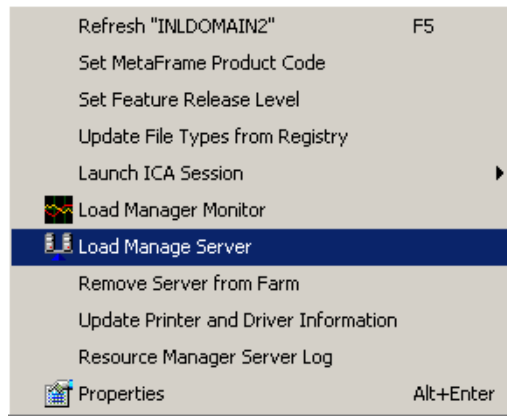


- 11** Select Page Swaps in the Assigned Rules list.
Page Swap settings display in the Rule Settings section.
- 12** In the Report Full Load When the Number of Page Swaps per Second is Greater Than This Value edit box, type a value.
- 13** In the Report No Load When the Number of Page Swaps Per Second is Less Than or Equal to This Value edit box, type a value.
- 14** Click OK.
The required Load Evaluators have been created.
Next, they are loaded to the Citrix server that SecureLogin will be installed on.
- 15** From the Citrix Management Console, expand the Servers option in the farm hierarchy.

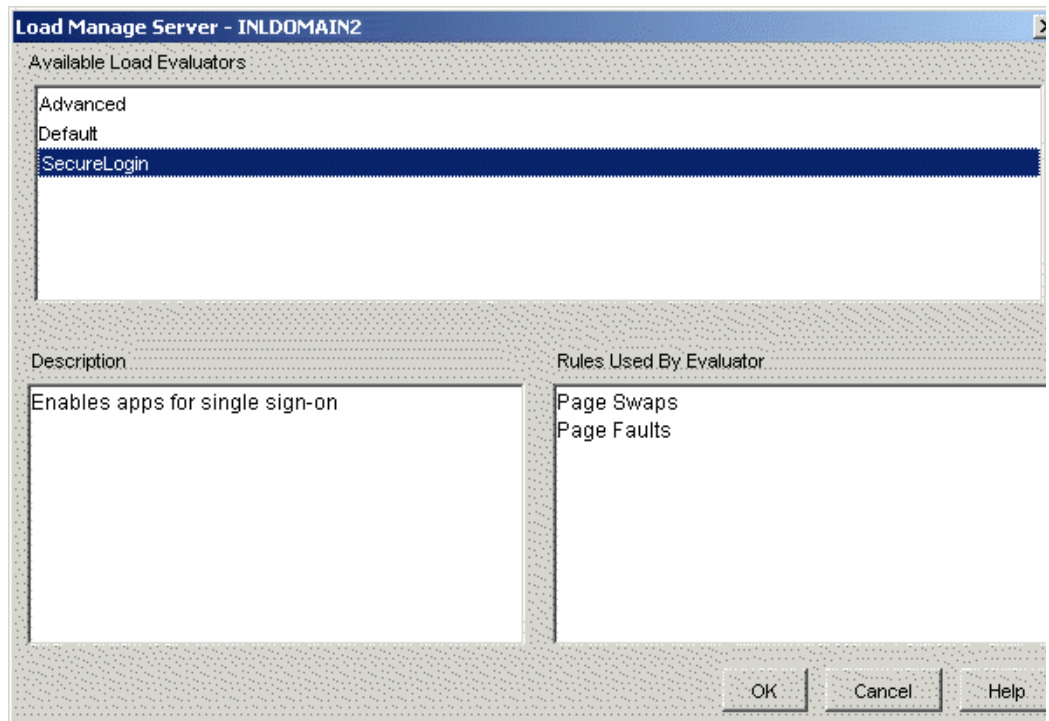


Names of Citrix servers are displayed.

- 16** Right-click the relevant Citrix server name.
- 17** Select Load Manage Server from the options menu.



- 18** Select the created Load Evaluator option (in this example, Novell SecureLogin), then click OK.



The new Load Evaluators have been loaded to the Citrix server.

8

Troubleshooting

This section provides information on the following:

- ♦ “GINA Credential Pass-Through” on page 33
- ♦ “Troubleshooting a Server Installation” on page 34
- ♦ “Troubleshooting a Workstation Installation” on page 35
- ♦ “Using Debugging Log Files” on page 38

GINA Credential Pass-Through

With the SecureLogin Citrix components installed, SecureLogin provides a seamless pass-through of GINA credentials (for example, username and password) 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 uses to log in to the client match the credentials of the terminal server, the credentials are automatically passed for the user.

If the stored 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 terminal 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.

Troubleshooting a Server Installation

Protocol Files

If you have problems during the installation, make sure that the following files have been copied from the \srv directory on the SecureLogin 3.51 CD or download image to the Windows System directory (c:\winnt\system32) on the server:

- ♦ sl_vc.dll
- ♦ sl_rdp.dll
- ♦ sl_ica.dll
- ♦ (Conditional) slaa_sso.dll

Slaa_sso.dll is copied if you are installing SecureLogin to the server in LDAP mode.

GINA Setup

The GINA is the login panel that is displayed when the system is first booted. To enable full single sign-on functionality, replace the standard GINA with a version that is enhanced for SecureLogin.

Server without the Novell Client Installed

- 1** Replace the server's GINA by copying srv\ms\sl_tsgina.dll to the Windows System directory (for example, c:\WinNT\System32).
- 2** Register the new GINA by double-clicking srv\ms\winlogon_server.reg.
- 3** Restart the server.

Server with the Novell Client Installed

- 1** Extend the server's GINA by copying srv\nw\slina.dll to the Windows System directory (for example, c:\WinNT\System32) on the server.

This step sets up the Novell login extensions.

- 2** Register the new GINA by double-clicking srv\nw\Register NT LoginExt.reg.
- 3** Select Yes, then click OK.
- 4** Restart the server.

Terminal Server Web Client

If TSWeb Client is installed on the Terminal Server, complete the following:

- 1** Locate the connect.asp file in the c:\inetpub\wwwroot\TSWeb directory on the server.
- 2** Using Notepad, add the following line before MsTsc.Connect():

```
MsTsc.AdvancedSettings.PluginDlls="tsPSLSSO.dll"
```
- 3** Save and close the file.

NOTE: The vcd\rdp directory contains a sample connect.asp file for reference.

Troubleshooting a Workstation Installation

Installing Login Extensions to the Workstation

To enable the login so that it can single sign-on to Terminal Services itself, you need to install the SLINA login extensions.

The procedures in the following sections set up your workstations to support the terminal services integration. The files used for the installation are specific to an environment. Therefore, match the appropriate files from the installation source to your environment. Otherwise, the extensions won't function correctly.

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

If you install or uninstall a Novell Client™ after installing the SecureLogin SSO modules, you must install the correct modules for SecureLogin SSO to work correctly. The installation steps will advise which the correct files are.

Your client configuration doesn't need to match your server configuration. For example, you can use a workstation with the Novell Client installed to connect to a server that doesn't have the client installed, and vice versa.

Workstations with the Microsoft Client

NOTE: Windows 95 does not support the GINA credential passthrough without the Novell client installed.

- 1** Using the Windows Add/Remove Programs utility, remove earlier versions of SecureLogin.
- 2** Launch the installation wizard by executing the SecureLogin Single Sign-On.msi file from the root directory of the installation CD or download image.
- 3** In the Welcome dialog box, click Next.
- 4** Read the license agreement, select I Accept the Terms in the License Agreement, then click Next.
- 5** Select Standard, then click Next.
- 6** Select Microsoft Active Directory (ADS) as the installation type from the install options list.
- 7** To launch SecureLogin each time the workstation starts, select Run at Startup, then click Next.
- 8** Click Install.

A progress meter runs during the installation.

- 9** (Conditional) Enter a passphrase.

If you selected Launch SecureLogin After Install, you are prompted to enter a passphrase. Otherwise, you are prompted to enter a passphrase the first time SecureLogin is run. For more information on the passphrase, see [“Managing Passphrases”](#) in the [Nsure SecureLogin 3.51.1 Administration Guide](#).

- 10** Replace the workstation's GINA by copying wks\ms\sl_tscgina.dll to the Windows System directory (c:\WinNT\System32).
- 11** Register the GINA by double-clicking wks\ms\winlogon_client_.reg.
- 12** Select Yes, then click OK.

- 13** Restart the workstation.

Workstations with the Novell Client (No NMAS)

- 1** Using the Windows Add/Remove Programs utility, remove earlier versions of SecureLogin.
- 2** Launch the installation wizard by executing the SecureLogin Single Sign-On.msi file from the root directory of the installation CD or download image.
- 3** In the Welcome dialog box, click Next.
- 4** Read the license agreement, select I Accept the Terms in the License Agreement, then click Next.
- 5** Click Change to select an alternative destination folder for SecureLogin, or click Next to accept the default destination folder for SecureLogin (C:\Program Files\Novell\SecureLogin).
- 6** Select eDirectory as the installation type from the install options list.
- 7** To launch SecureLogin each time the workstation starts, select Run at Startup, then click Next.
- 8** Click Install.

A progress meter runs during the installation.

- 9** (Conditional) Enter a passphrase.

If you selected Launch SecureLogin After Install, you are prompted to enter a passphrase. Otherwise, you are prompted to enter a passphrase the first time SecureLogin is run. For more information on the passphrase, see [“Managing Passphrases”](#) in the [Nsure SecureLogin 3.51.1 Administration Guide](#).

- 10** Set up the Novell login extensions by copying wks\nw\slgina.dll to the Windows System directory (c:\WinNT\System32) on the workstation.
- 11** Register the login extensions.

If the workstation is running Windows NT, 2000, or XP, double-click wks\nw\register nt loginext.reg.

If the workstation is running Windows 9x or ME, double-click wks\na\register 98 loginext.reg.
- 12** Set up Microsoft Layer for Unicode on Windows 9x or ME.

If the workstation is running Windows NT, 2000 or XP, skip this step.

If the workstation is running Windows 9x or ME, copy redistributable\unicows.dll to the System directory (c:\Windows\System).
- 13** Restart the workstation.

Workstations with the Novell Client (with NMAS)

- 1** Using the Windows Add/Remove Programs utility, remove earlier versions of SecureLogin.
- 2** Launch the installation wizard by executing the SecureLogin Single Sign-On.msi file from the root directory of the installation CD or download image.
- 3** In the Welcome dialog box, click Next.
- 4** Read the license agreement, select I Accept the Terms in the License Agreement, then click Next.

- 5** Click Change to select an alternative destination folder for SecureLogin, or click Next to accept the default destination folder for SecureLogin (C:\Program Files\Novell\SecureLogin).
- 6** Select eDirectory as the installation type from the install options list.
- 7** To launch SecureLogin each time the workstation starts, select Run at Startup, then click Next.
- 8** Click Install.

A progress meter runs during the installation.

- 9** (Conditional) Enter a passphrase.

If you selected Launch SecureLogin After Install, you are prompted to enter a passphrase. Otherwise, you are prompted to enter a passphrase the first time SecureLogin is run. For more information on the passphrase, see “[Managing Passphrases](#)” in the [Nsure SecureLogin 3.51.1 Administration Guide](#).

- 10** Copy wks\nw\slnmas.dll to the Windows System directory (c:\WinNT\System32) on the workstation.

NOTE: The slnmas.dll file is not a login extension. It is called by the NMAS client instead. It isn't necessary to run the Registry (.reg) file if you are using the NMAS client with slnmas.dll. However, you need to install the version of NMAS client that comes with SecureLogin v3.0.1 or later. These later versions are slnmas.dll aware.

- 11** Set up Microsoft Layer for Unicode on Windows 9x or ME.

If the workstation is running Windows NT, 2000, or XP, skip this step.

If the workstation is running Windows 9x or ME, copy redistributable\unicows.dll to the System directory (c:\Windows\System).

- 12** Restart the workstation.

Installing Virtual Channel Drivers On the Workstation

The procedures in this section outline the steps necessary to set up your workstations to support the terminal services Virtual Channel. You must match the appropriate files from the installation source to your environment. Otherwise, the extensions won't function correctly.

Install the Virtual Channel drivers on the workstation, not the server.

Workstation with Citrix Client (ICA)

To install the Virtual channel driver:

- 1** Copy vcd\ica\vdPSLSSON.dll from the SecureLogin 3.51 CD or download image to the ICA Client directory (c:\Program Files\Citrix\ICA Client).
- 2** Register the driver by making the following changes to the module.ini file located in the ICA Client directory (c:\Program Files\Citrix\ICA Client).

2a Navigate to the Virtual Driver line in the section [ICA 3.0].

2b Add the name of the Virtual Driver to the end of the Virtual Driver line.

For example, add PSLSSO.

2c At the end of the [Virtual Driver] section, add a driver assignment statement.

For the PSLSSO driver, type

```
PSLSSO      =
```

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

2d Create a new section [PSLSSO] as follows:

```
[PSLSSO]
DriverNameWin32 = VDPSLSSO.DLL
```

The vcd\ica directory contains a sample module.ini file for reference.

Workstation with Terminal Server Client (RDP)

- 1 Install the driver by copying vcd\rdp\tsPSLSSO.dll from the SecureLogin 3.51 CD or download image to the Windows System directory (c:\WinNT\System32).
- 2 Register the driver by double-clicking vcd\rdp\Terminal Server Driver registration on Client workstation.reg.

Using Debugging Log Files

SecureLogin provides several debugging log files to assist with troubleshooting functions in terminal services.

The debugging logs are turned off by default. They are enabled through registry entries.

As listed in the following table, the location of the log files will vary depending on the operating system installed:

Platform	Directory
Windows NT Windows 2000/2003	c:\winNT\system32
Windows XP	c:\windows\system32
Windows 9x	c:\windows\system

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

Log Files for Servers

The following table lists .dll files and corresponding log files found on servers:

DLL File	Log File
slina.dll	slina.log
sl_tsgina.dll	sl_tsgina.log
sl_ica.dll	sl_ica.log
sl_rdp.dll	sl_rdp.log
sl_vc.dll	Sl_vc.dll is logged to sl_vc.log

Log Files for Workstations

The following table lists .dll files and corresponding log files found on workstations:

DLL File	Log File
slina.dll	slina.log
sl_tsgina.dll	sl_tsgina.log
sl_ica.dll	sl_ica.log
sl_rdp.dll	sl_rdp.log
sl_vc.dll	Sl_vc.dll is logged to sl_vc.log

