Novell Nsure™ SecureLogin

3.51.2

www.novell.com

TERMINAL SERVICES GUIDE

April 08, 2005

Novell®

Legal Notices

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

www.novell.com

Nsure SecureLogin 3.51.2 Terminal Services Guide
April 08, 2005

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

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.

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.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment 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

For the most recent version of the *Nsure SecureLogin 3.51.2 Terminal Services Guide*, see the Novell documentation Web site (http://www.novell.com/documentation).

Additional Documentation

This *Guide* is part of a documentation set for SecureLogin 3.51.2. 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 3.51.2 Installation Guide (installing SecureLogin, migrating secrets from earlier versions, and configuring Secure Workstation)
- The Nsure SecureLogin 3.51.2 Administration Guide (tools and tasks to manage SecureLogin and configure terminal emulators)
- The Nsure SecureLogin 3.51.2 Scripting Guide (concepts concerning scripting, scripting commands, and example scripts for applications)
- The Nsure SecureLogin 3.51.2 Configuration Guide for Terminal Emulation (how to configure Terminal Launcher for selected terminal emulators)
- The Nsure SecureLogin 3.51.2 User Guide (using SecureLogin to enable applications for single sign-on)

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.

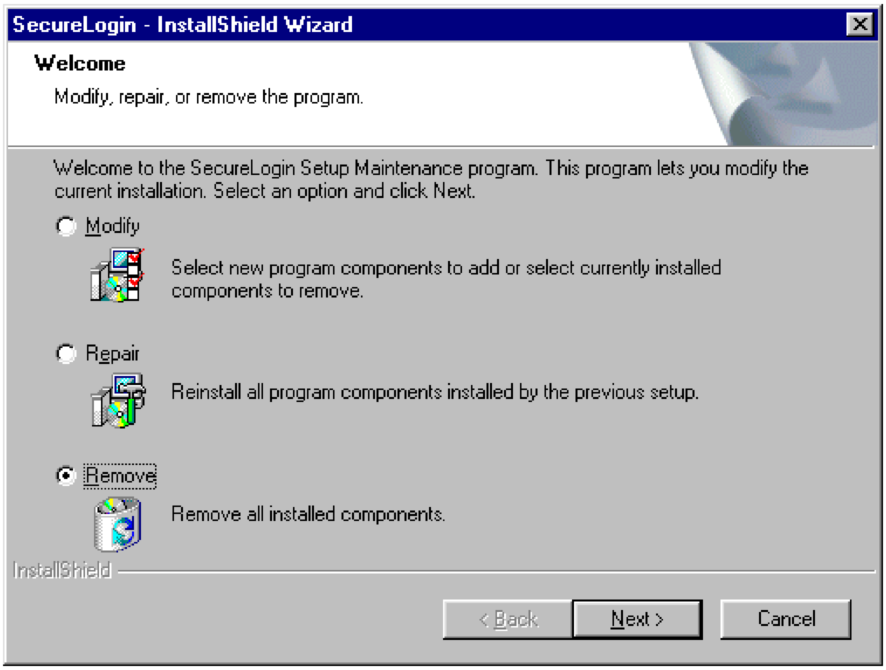
SecureLogin detects Citrix and installs the appropriate workstation files. If SecureLogin doesn't detect Citrix, files for Citrix won't be installed.

❑ Uninstall previous versions of SecureLogin on the workstation.

2 Uninstalling SecureLogin

To uninstall SecureLogin 3.51.2 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.



SecureLogin - InstallShield Wizard

Welcome

Modify, repair, or remove the program.

Welcome to the SecureLogin Setup Maintenance program. This program lets you modify the current installation. Select an option and click Next.

○ Modify

Select new program components to add or select currently installed components to remove.

○ Repair

Reinstall all program components installed by the previous setup.

● Remove

Remove all installed components.

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 3.51.2 Installation Guide:

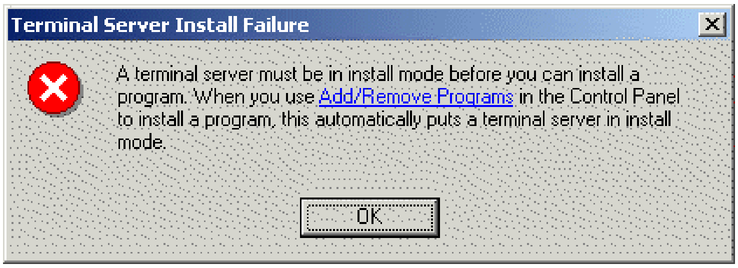
Environment	Section
Active Directory	"Installing in Active Directory Environments"
Windows NT, 2000, or 2003	"Installing in Windows NT/2000 Domains"
LDAP	"Installing in LDAP Environments"
Novell® eDirectory™	"Installing in Novell eDirectory Environments"

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.



Terminal Server Install Failure

A terminal server must be in install mode before you can install a program. When you use Add/Remove Programs in the Control Panel to install a program, this automatically puts a terminal server in install mode.

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.

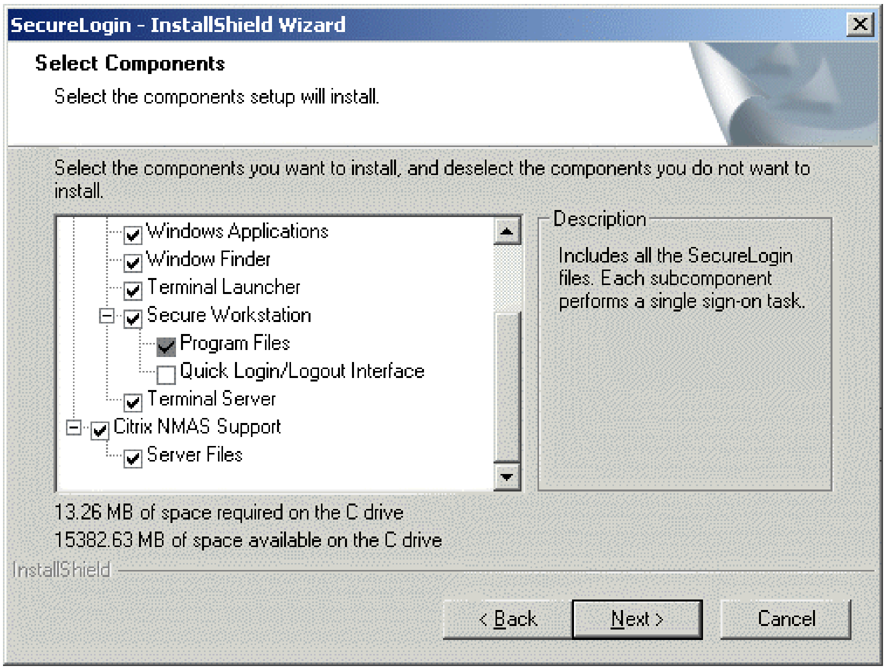
6 In the Setup Type dialog box, select Custom, then click Next.

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 3.51.2 Installation Guide.

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



SecureLogin - InstallShield Wizard

Select Components

Select the components setup will install.

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

☑ Windows Applications
☑ Window Finder
☑ Terminal Launcher
☑ Secure Workstation
☑ Program Files
☐ Quick Login/Logout Interface
☑ Terminal Server
☑ Citrix NMAS Support
☑ Server Files

Description

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

13.26 MB of space required on the C drive

15382.63 MB of space available on the C drive

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

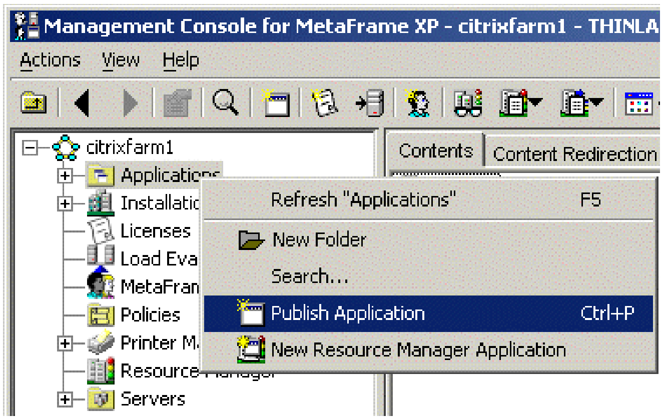
Because individual application screen cues are not available in Citrix environments, SecureLogin is unable to recognize individual applications when users access them. To enter login credentials when an application executes, SecureLogin needs to start before the application.

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

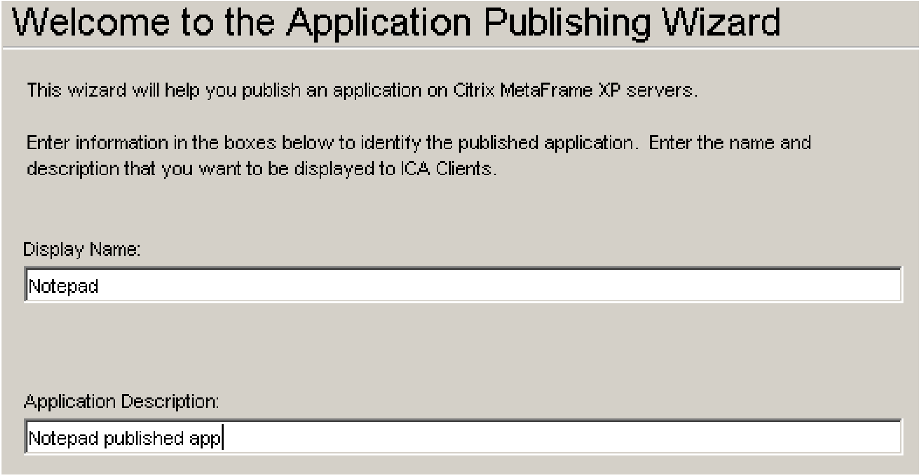
Enabling Citrix Applications

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

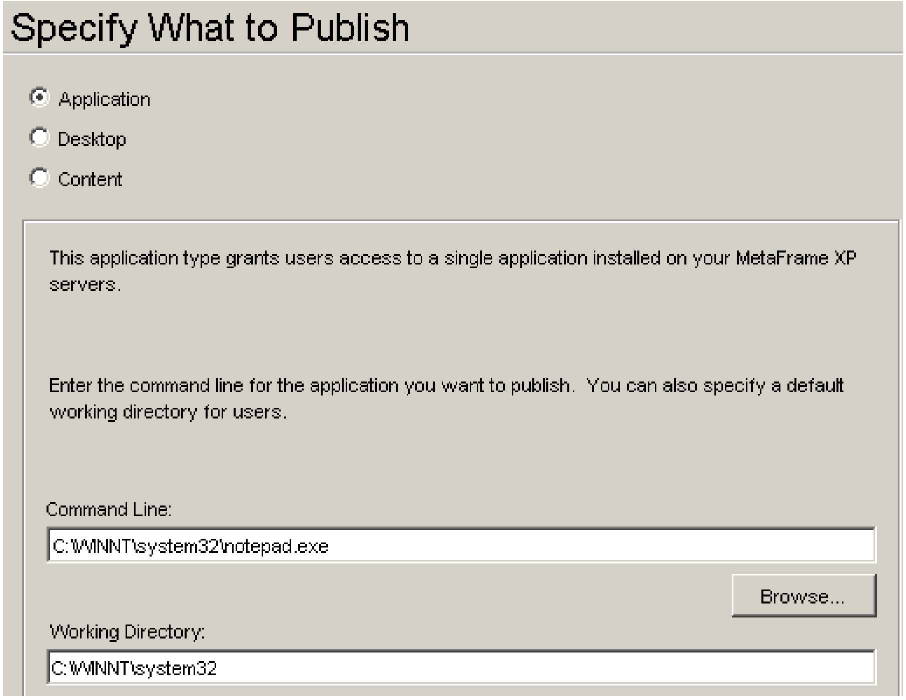
Application Description:

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

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).

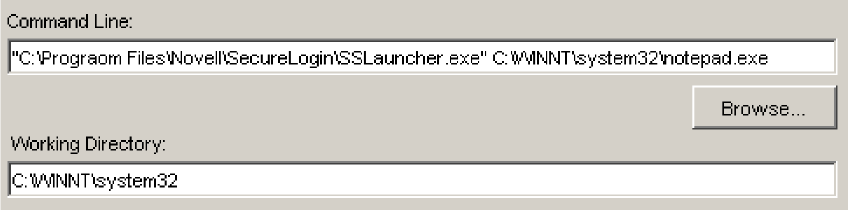
The working directory is the directory path of the program executable.

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.



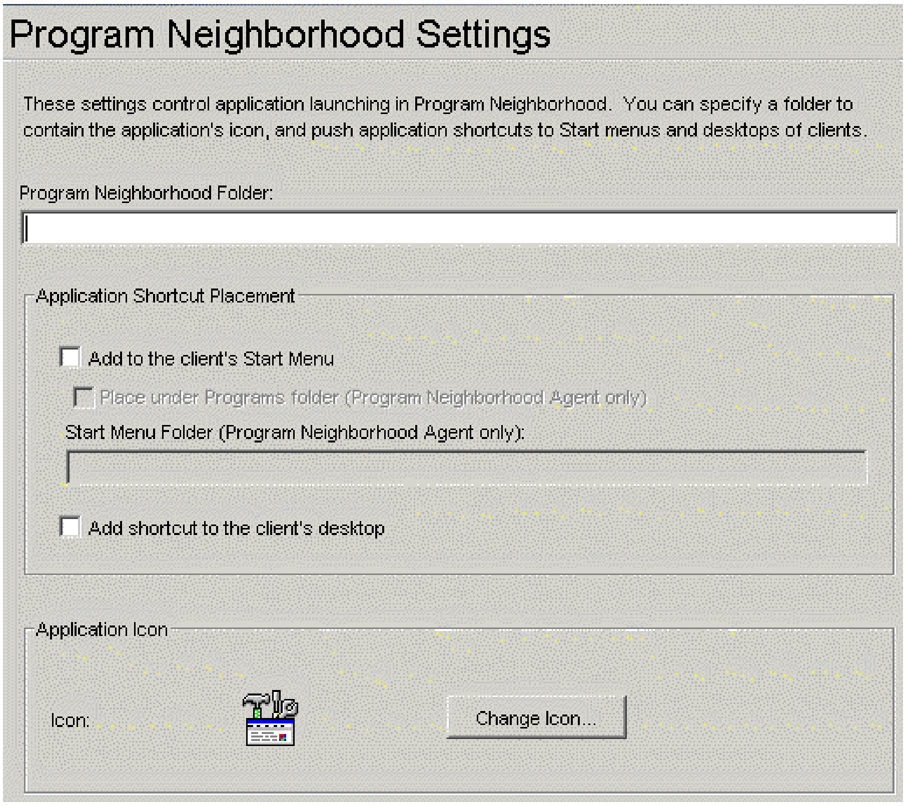
Command Line:

"C:\Prograom Files\Novell\SecureLogin\SSLauncher.exe" C:\WINNT\system32\notepad.exe

Working Directory:

C:\WINNT\system32

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:

Application Shortcut Placement

☐ Add to the client's Start Menu

☐ Place under Programs folder (Program Neighborhood Agent only)

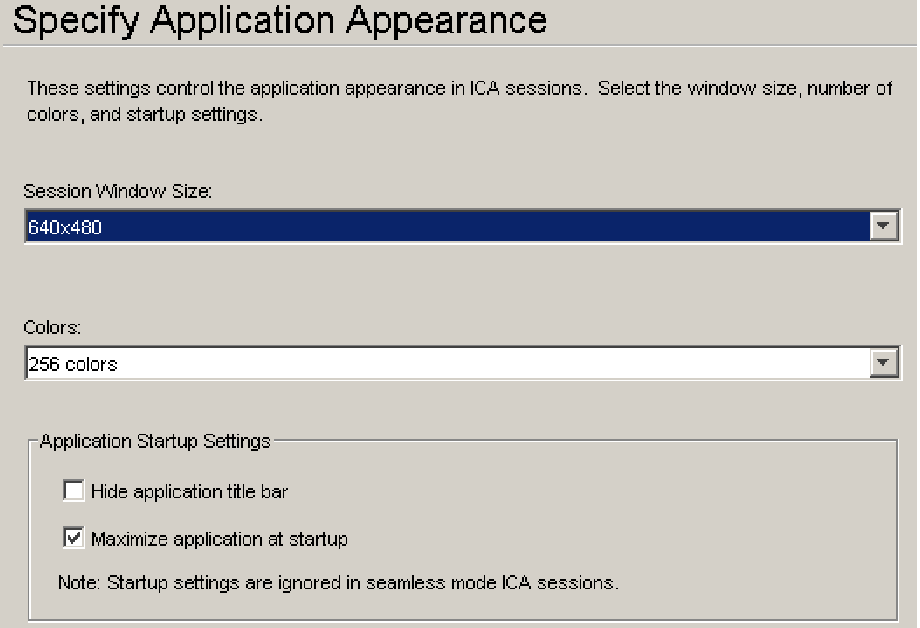
Start Menu Folder (Program Neighborhood Agent only):

☐ Add shortcut to the client's desktop

Application Icon

Icon:

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

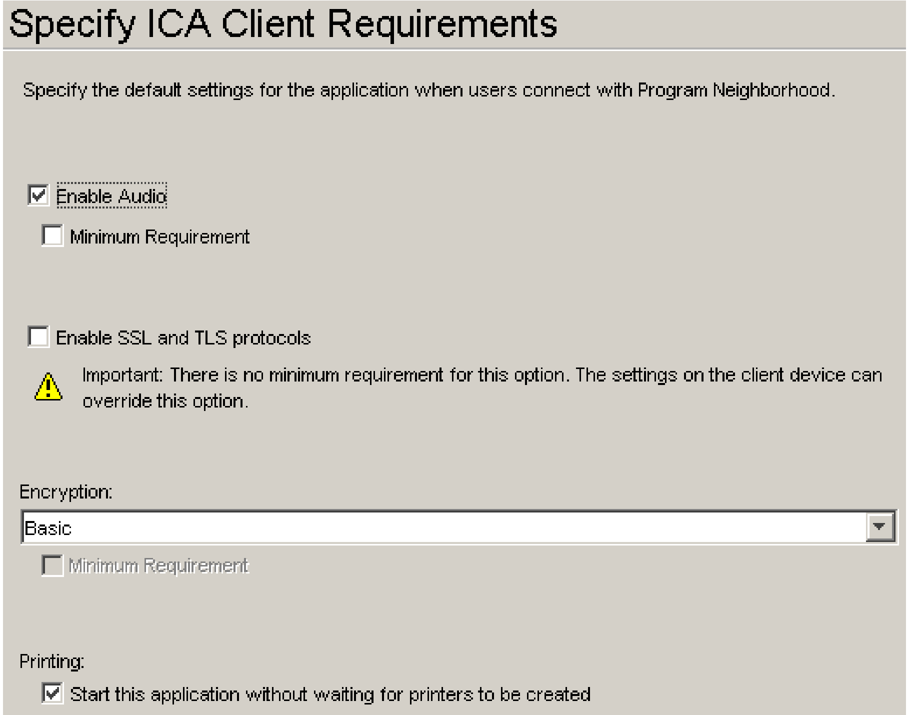
Application Startup Settings

□ 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.

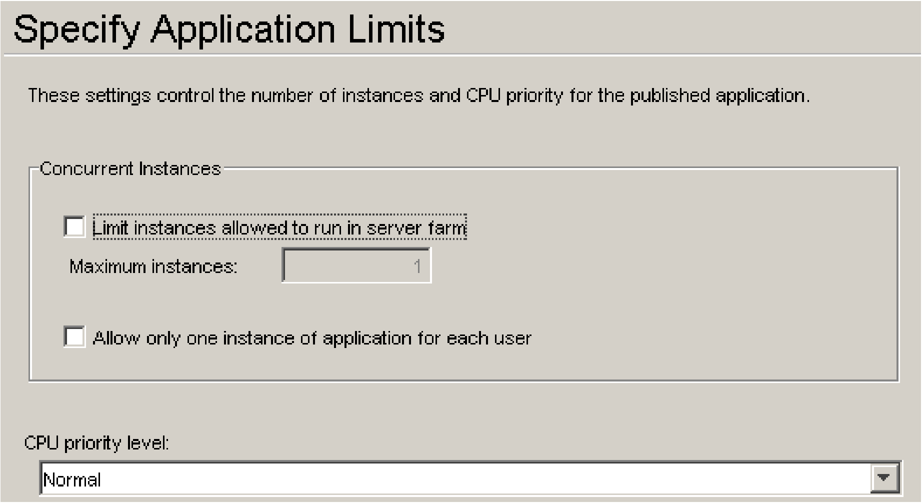
Encryption: Basic

□ 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

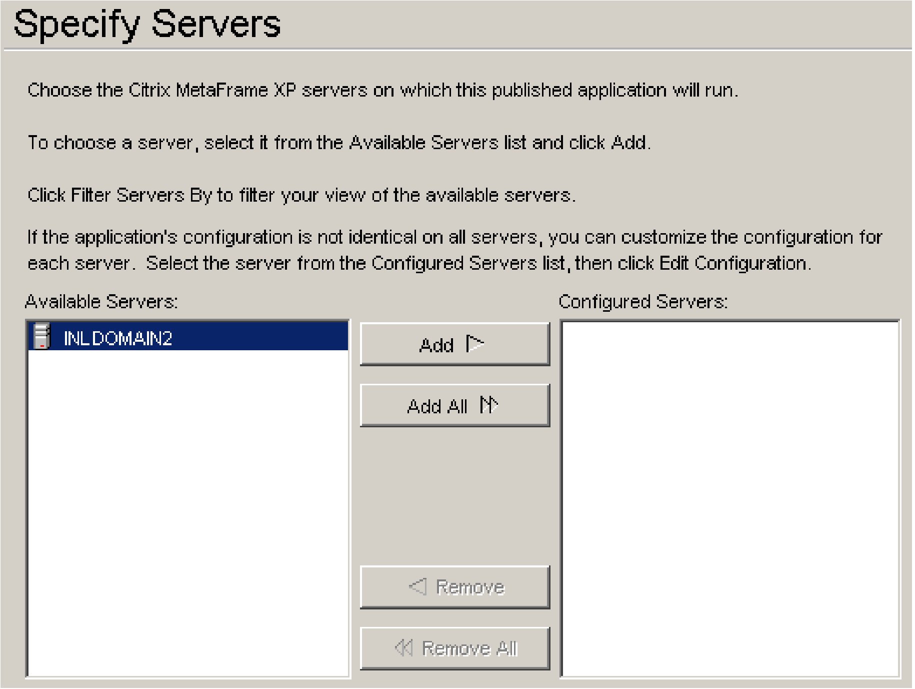
□ Limit instances allowed to run in server farm

Maximum instances: 1

□ 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.

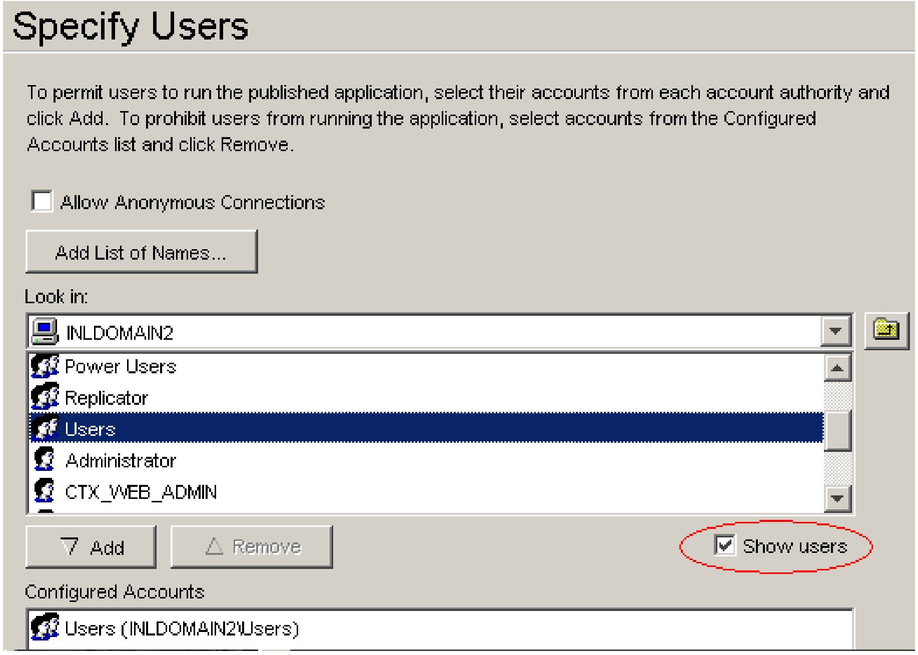
Available Servers: INLDOMAIN2

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

Look in: INLDOMAIN2

- Power Users
- Replicator
- Users
- Administrator
- CTX_WEB_ADMIN

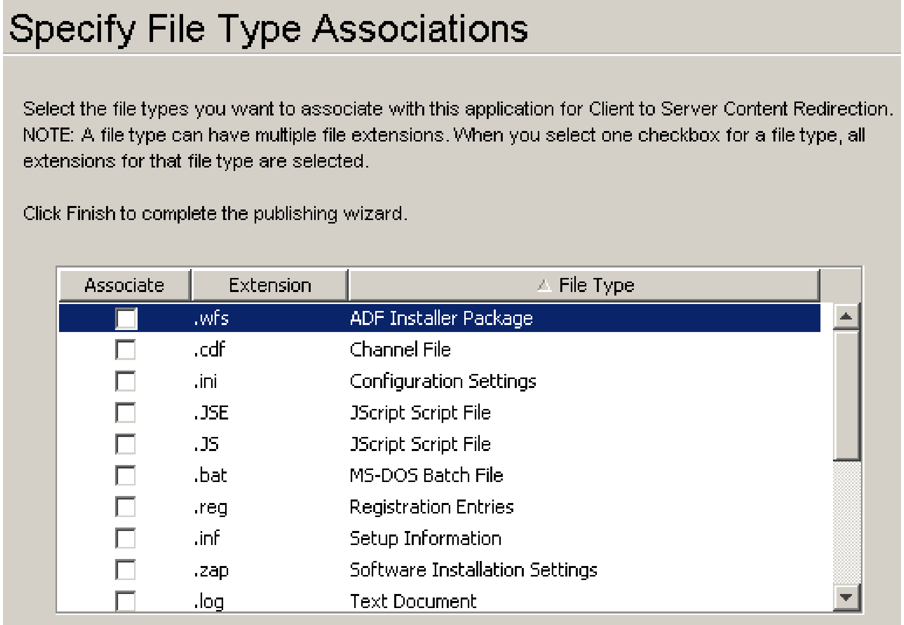
☑ Show users

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
□	.wfs	ADF Installer Package
□	.cdf	Channel File
□	.ini	Configuration Settings
□	.JSE	JScript Script File
□	.JS	JScript Script File
□	.bat	MS-DOS Batch File
□	.reg	Registration Entries
□	.inf	Setup Information
□	.zap	Software Installation Settings
□	.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 3.51.2 Administration Guide.

SLLauncher Switches

The following SLLauncher switches are options that you can use in conjunction with SLLauncher.exe:

- **/d**—Initiates a trace file saved in the SecureLogin program directory.

  Example syntax:

  "C:\Program Files\Secureogin\SSLauncher.exe" /d C:\WINNT\System32\notepad.exe

- **/w**—Delays SLLauncher from executing until a specific application has executed or an environment is present. For example, to run the executable notepad.exe with SecureLogin, you would use the following syntax:

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

  However, in order for notepad.exe to execute as required, an environment variable must be setup first. This environment is created when the batch file runtest.bat is run on the server. To specify that SLLauncher wait to execute notepad.exe until the runtest.bat has completed running, use the /w switch.

  For example:

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

- **/16**—Must be included in the Citrix publishing command when SecureLogin enables a 16-bit application. All 16-bit applications must be identified because they execute differently from 32-bit applications. For SecureLogin to single sign-on an application, the 16-bit emulator NTVDM.exe must be active.

  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 might cause memory issues if multiple 16-bit applications are SecureLogin enabled. To terminate NTVDM.exe when the 16-bit application is closed, add the switch /w NTVDM.exe to the Citrix publishing command.

  Example syntax:

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

Switches Tips

- 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.
- Switches can be used in combination. For example: "C:\Program Files\Novell\SecureLogin\SSLauncher.exe" /d /w notepad.exe C:\runtest.bat.

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 3.51.2 Administration Guide and the Nsure SecureLogin 3.51.2 Scripting Guide.

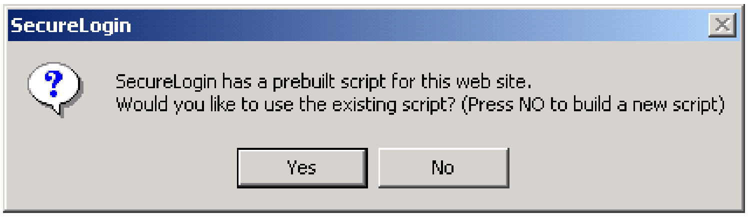
Enabling an Application with Connectors

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.



SecureLogin

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

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 3.51.2.

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

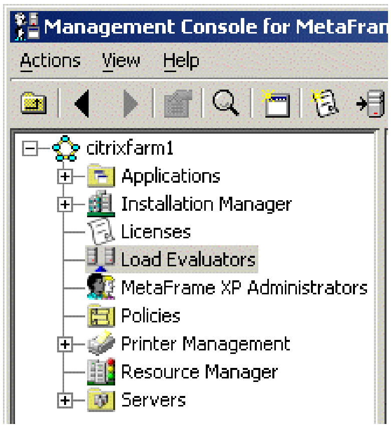
For SecureLogin to run effectively on a Citrix server, configure load evaluators for page faults and page swaps. Do this before installing SecureLogin.

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.

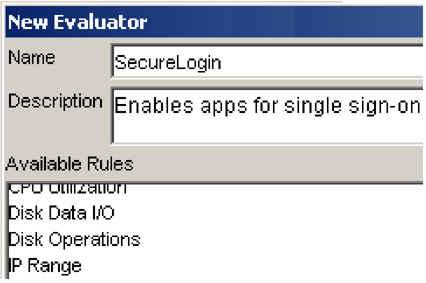
The following instructions apply to Citrix Metaframe XP Feature Release (FR).

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.

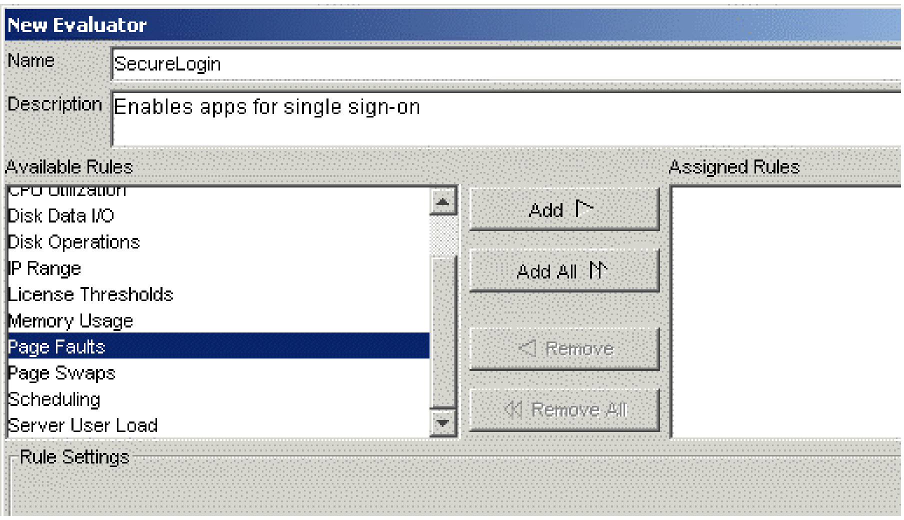


Name: SecureLogin

Description: Enables apps for single sign-on

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.



New Evaluator

Name: SecureLogin

Description: Enables apps for single sign-on

Available Rules

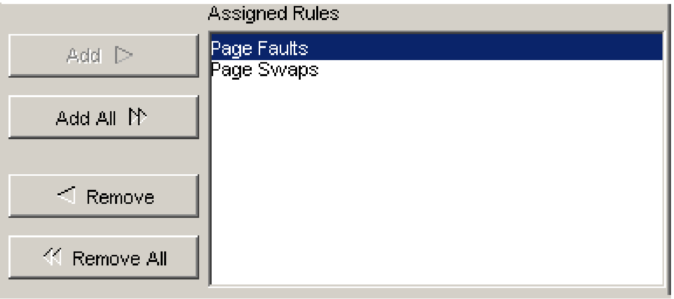
CPU Utilization
Disk Data I/O
Disk Operations
IP Range
License Thresholds
Memory Usage
Page Faults
Page Swaps
Scheduling
Server User Load

Assigned Rules

Rule Settings

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

9 Select Page Faults in the Assigned Rules list.

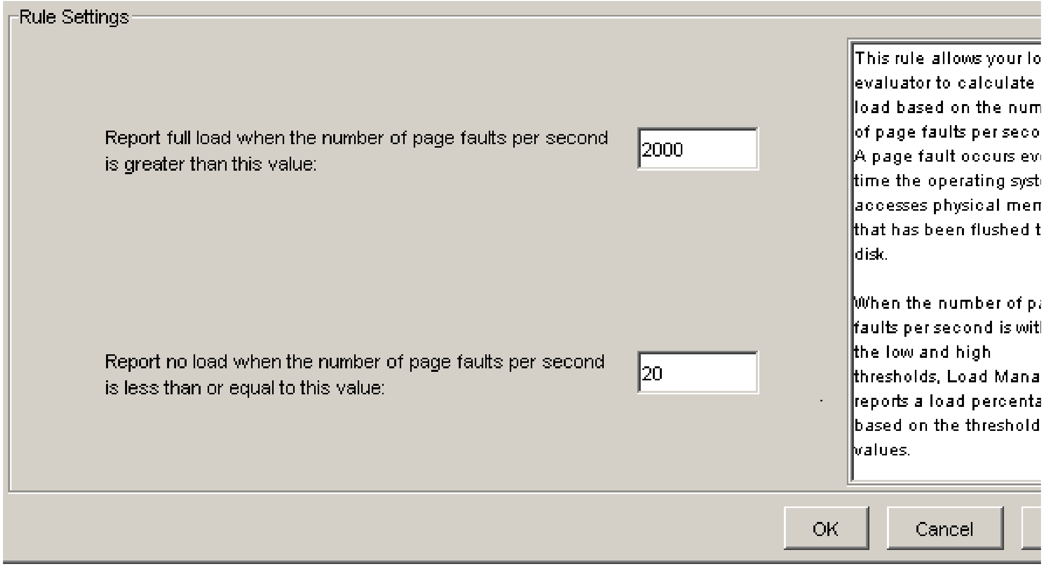


Assigned Rules

Page Faults
Page Swaps

10 In the Rule Settings edit boxes, type a value for each Page Fault setting.

Settings are configured in the Rule Settings pane.



Rule Settings

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: 20

This rule allows your lo evaluator to calculate load based on the num of page faults per seco A page fault occurs ev time the operating syst accesses physical men that has been flushed t disk.

When the number of p faults per second is wit the low and high thresholds, Load Mana reports a load percenta based on the threshold values.

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.

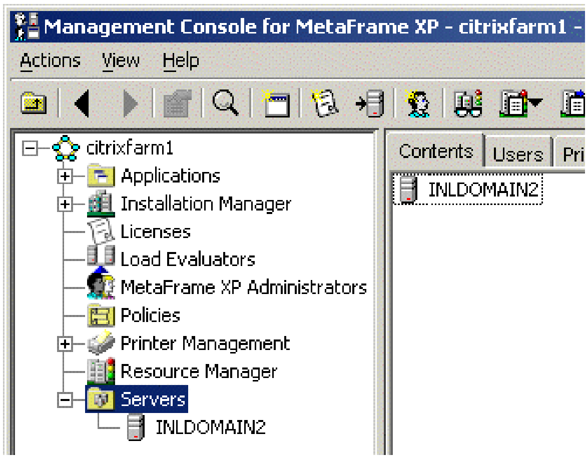
13 In the Report No Load When the Number of Page Swaps Per Second is Less Than or Equal to This Value edit box, type a value.

14 Click OK.

The required Load Evaluators have been created.

Next, they are loaded to the Citrix server that SecureLogin will be installed on.

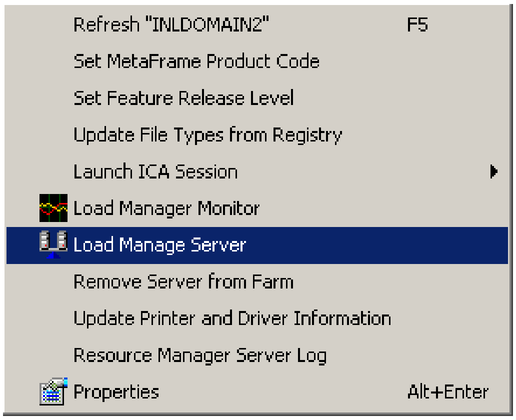
15 From the Citrix Management Console, expand the Servers option in the farm hierarchy.



Names of Citrix servers are displayed.

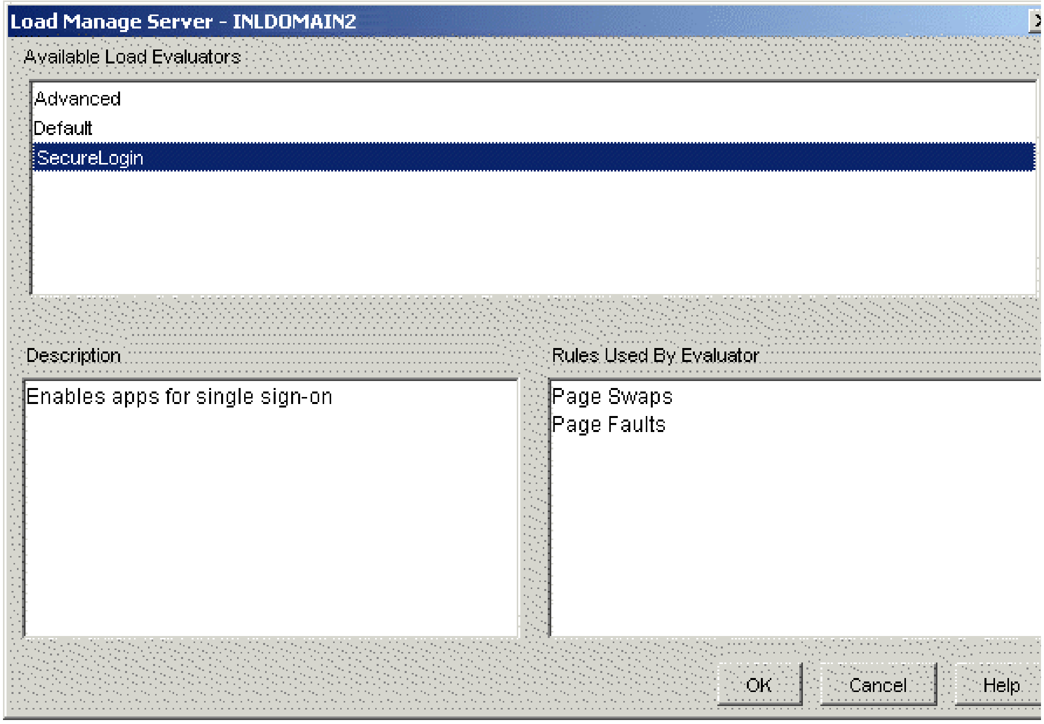
16 Right-click the relevant Citrix server name.

17 Select Load Manage Server from the options menu.



Refresh "INLDOMAIN2" F5
Set MetaFrame Product Code
Set Feature Release Level
Update File Types from Registry
Launch ICA Session
Load Manager Monitor
Load Manage Server
Remove Server from Farm
Update Printer and Driver Information
Resource Manager Server Log
Properties Alt+Enter

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



Load Manage Server - INLDOMAIN2

Available Load Evaluators

- Advanced
- Default
- SecureLogin

Description: Enables apps for single sign-on

Rules Used By Evaluator:

- Page Swaps
- Page Faults

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

8 Troubleshooting

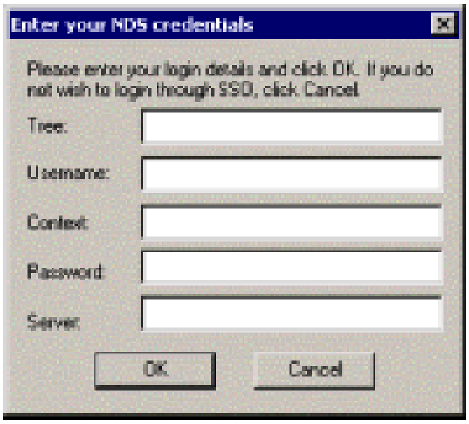
This section provides information on the following:

Troubleshooting Passthrough Authentication

GINA Credential Passthrough

With the SecureLogin Citrix components installed, SecureLogin provides a seamless passthrough 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:


Enter your 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.

Passthrough Authentication Fails

Scenario

Passthrough Authentication fails with Citrix Metaframe Presentation* Server displaying an error message.

Possible Cause

If SecureLogin is installed on a Citrix Metaframe Presentation Server 3.0, passthrough authentication might not be successful. This occurs if you set up the following configuration on the Citrix server:

- SecureLogin client is installed in eDirectory mode
- Novell Client version 4.9 or later is installed

When you attempt a Citrix client connection with the Citrix server, the error message `Unable to find Novell Login window. Press Cancel to stop finding or Retry to continue` is displayed with the window title *SLAA Citrix Server for Novell*.

If you click Retry, SecureLogin enters the user credentials in the Novell Login dialog box and passthrough continues normally. If you click Cancel, SecureLogin exits and the Novell Login dialog box prompts you to enter credentials (manually).

Solution

Ensure the following:

- The Novell Login dialog box has the title bar *Novell Login*. For details, refer to TID # 10094461 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10094461.htm).
- The Workstation captures the credentials from the initial login. For details, refer to TID # 10094565 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10094565.htm).
- SecureLogin Client runs in the same mode on both the workstation and the Citrix server.
- SecureLogin Client starts running on the workstation prior to the startup of the ICA session.
- The following registry values exist under the registry key HKLM\Software\Protocom\VirtualChannel:

Name	Type	Data
AutoDetect	REG_SZ	0
protocol	REG_SZ	ICA

- GINA on the Citrix server is Novell GINA (nwgina.dll).

When SecureLogin attempts to locate Novell GINA to provide passthrough credentials, if for some reason the server is running the Citrix GINA (ctxgina.dll), it fails to find the Novell Login window. To resolve this, change the default GINA to Novell GINA (nwgina.dll) under the registry key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

Name	Type	Data
GinaDLL	REG_SZ	*C:\windows\system32*\nwgina.dll

Changing the GINA might make certain Citrix capabilities nonfunctional. For more details, see the Citrix Website (http://support.citrix.com/kb/entry!default.jspa?categoryID=118&entryID=1987&fromSearchPage=true).

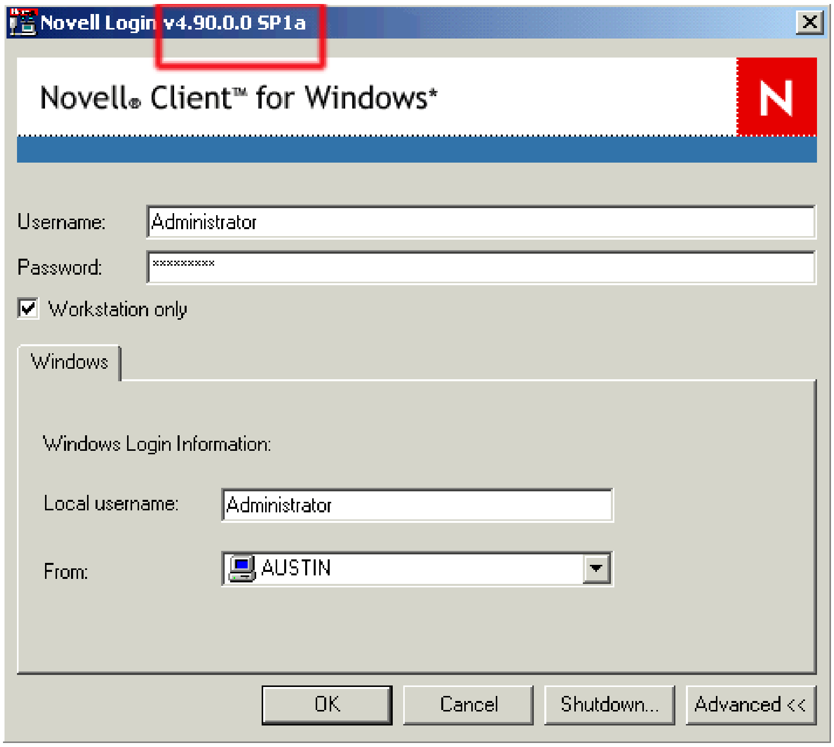
Scenario

SecureLogin enters the password, but not the username.

Possible Cause

Slina.dll failed to find the Novell client login window. Therefore, though the password is passed through, username is not, resulting in the Windows Security message `Failed to login to the Windows Workstation`.

Starting with version 4.9, Novell Client displays the version on the title bar (highlighted in the image below) of the Novell Login dialog box.



Novell Login v4.90.0.0 SP1a

Novell® Client™ for Windows*

Username: Administrator

Password: **********

☑ Workstation only

Windows Login Information:

Local username: Administrator

From: AUSTIN

Slinas.dll on the Citrix server looks for the Novell Login dialog box with the title *Novell Login*, whereas the Novell Client post-4.9 versions (as in the above case) also suffixes the version details to the title.

Solution

The title string is determined by a registry key. You can edit this in the Citrix server itself.

1. On the Windows task bar, click Start > Run.
2. Type **`regedit`** in the Open field.

   The Registry Editor is displayed.

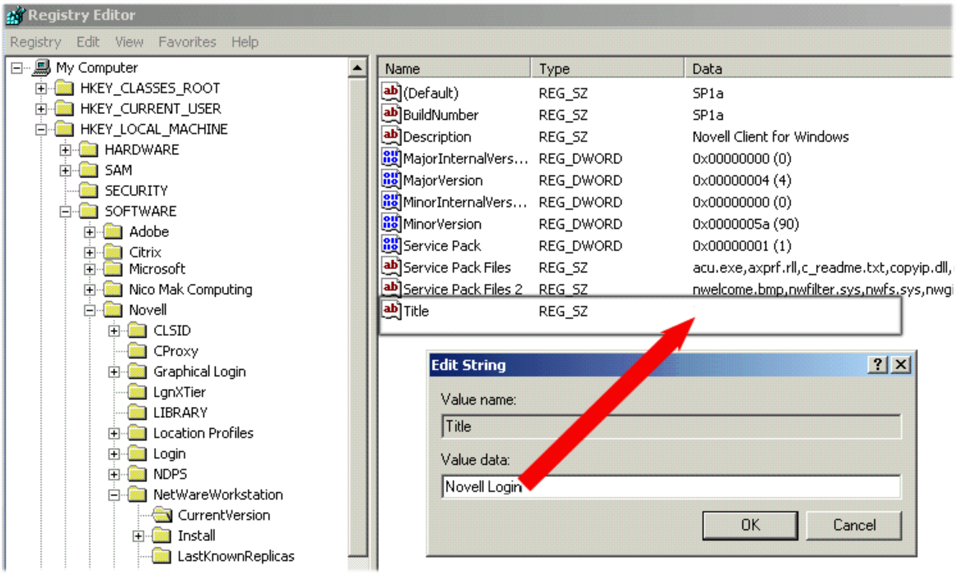
   WARNING: Any improper registry editing can damage the system functionality. Therefore, be careful when making any registry change.

3 In the left panel, click HKEY_LOCAL MACHINE > SOFTWARE > Novell > NetWareWorkstation > CurrentVersion.

4 In the right panel, click Title.

The Edit String dialog box is displayed.

5 Change the value data to Novell Login.



Name	Type	Data
(Default)	REG_SZ	SP1a
BuildNumber	REG_SZ	SP1a
Description	REG_SZ	Novell Client for Windows
MajorInternalVers...	REG_DWORD	0x00000000 (0)
MajorVersion	REG_DWORD	0x00000004 (4)
MinorInternalVers...	REG_DWORD	0x00000000 (0)
MinorVersion	REG_DWORD	0x0000005a (90)
Service Pack	REG_DWORD	0x00000001 (1)
Service Pack Files	REG_SZ	acu.exe,axprf.rll,c_readme.txt,copyip.dll,
Service Pack Files 2	REG_SZ	nwelcome.bmp,nwfilter.sys,nwfs.sys,nwgi
Title	REG_SZ	

Value name: Title

Value data: Novell Login

6 Click OK.

7 If necessary, create the following registry values:

Name	Type	Data
ProductName	REG_SZ	Novell Login

IMPORTANT: If Novell Client is removed and then reinstalled or updated, the client installation program might change the title value data. Therefore, if any change is made to Novell Client on a Citrix/Terminal server, you should validate the title value data.

Verifying Slinac.dll Registration

To verify if the slinac.dll is registered properly, do the following:

- **Registry Check:** Ensure that slinac.dll is copied to Sys32 on your workstation.
- **Notepad Script:** To ensure that the SecureLogin client is able to read the workstation login credentials and store them in the ?sys variables, create a notepad.exe script to echo the values to a new notepad document.

  For details, refer to "Validation of the Workstation Components" on page 45.
- **slnmas.dll:** Ensure that slnmas.dll is not installed on your workstation. If it is installed, delete it and restart the workstation.

Manual Configuration

All the Citrix manual configuration (and related) files are available in the following path of the SecureLogin 3.51.2 CD:

SecureLogin_cd\SecureLogin\Tools\Citrix Manual Configuration\Citrix

Use these files to manually configure Citrix passthrough and to troubleshoot passthrough authentication.

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.dl
- 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\slinas.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 3.51.2 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 3.51.2 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 3.51.2 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 9*x*	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

DLL File	Log File
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

A Passthrough Authentication

Passthrough Authentication refers to the mechanism of authenticating from a Citrix client to the server without the user having to manually provide the credentials every time. The login credentials given to the client are passed through to the server.

SecureLogin provides an effective way to perform passthrough authentication.

Prerequisites

- ❑ SecureLogin must be installed in the same mode on both workstation and server.

  For example, if the workstation is configured for LDAP mode, the server also must be installed in the same mode.

- ❑ On both workstation and server, the Citrix component must be installed before SecureLogin.

  This is to ensure that SecureLogin detects the Citrix environment and installs the corresponding modules.

- ❑ The configuration and installation must be done with the Citrix server in Install mode.

  This is to ensure that all the users emon1

  receive the same configuration.

- ❑ If you are authenticating using the LDAP authentication mode, LDAPAuth should be installed in GINA mode on the Citrix server.

  Passthrough cannot happen if LDAPAuth is installed in Credential manager or Application modes on the Citrix server. On the Citrix client workstation, LDAPAuth can be installed in any mode.

- ❑ If you log in using NMAS™ method, be sure to select Enable Password Field in the Novell Client Login dialog box. Otherwise, the script that runs ?syspassword displays incorrect values (instead of the password).

  To select Enable Password Field:

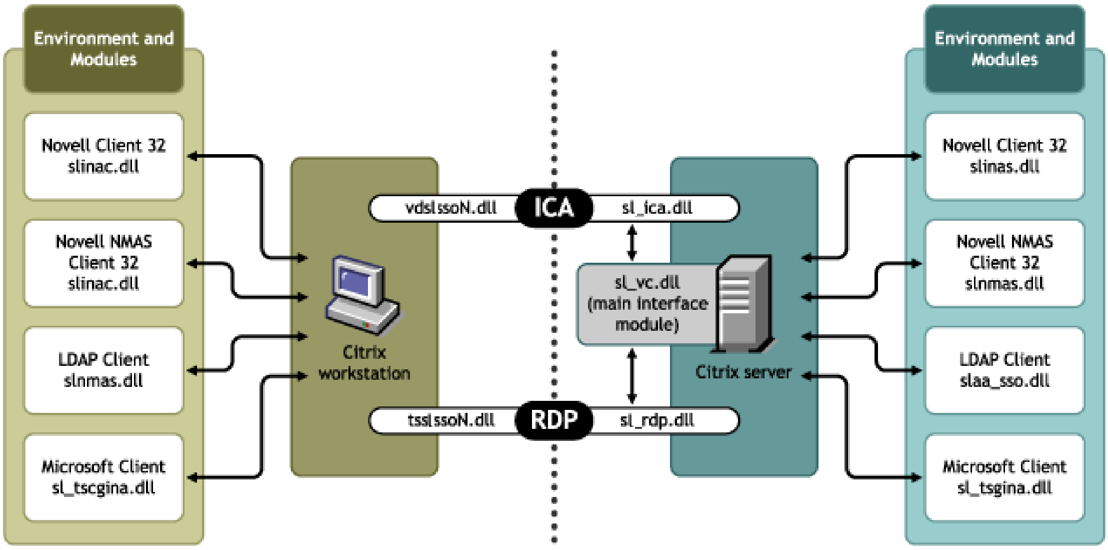
1. Right-click the Novell Client icon on the status bar (system tray), then click Novell Client Properties > Location Profiles.
2. In the Location Profiles window, double-click Default, then click Properties.
3. On the Credentials tabbed page, select Enable Password Field and then click OK.

How SecureLogin Performs Passthrough Authentication

Several components are utilized by SecureLogin to perform passthrough authentication. The modules differ depending on the passthrough configuration. The SecureLogin installation program detects the configuration and installs the correct modules to each device. For example, if the Citrix client is installed on the server and client, SecureLogin detects the corresponding components and installs them.

NOTE: Prior to NSL 3.51 SP1, this was a manual process.

The following illustration details how passthrough authentication works:



Environment and Modules
Novell Client 32 slinac.dll
Novell NMAS Client 32 slinac.dll
LDAP Client slnmas.dll
Microsoft Client sl_tscgina.dll
Citrix workstation
vdslssoN.dll
ICA
sl_ica.dll
sl_vc.dll (main interface module)
tsslssoN.dll
RDP
sl_rdp.dll
Citrix server
Environment and Modules
Novell Client 32 slinas.dll
Novell NMAS Client 32 slnmas.dll
LDAP Client slaa_sso.dll
Microsoft Client sl_tsgina.dll

Passthrough authentication features the following:

- "Workstation Components" on page 44
- "Server Components" on page 46
- "Virtual Channel" on page 47

Workstation Components

The workstation must be configured to capture the user credentials on login to the server. This might be login to a Novell network, Microsoft network, or some other LDAP-compliant network. SecureLogin uses different modules to interface with the correct GINA in each environment. This allows the capture of the username, password, or any other variable during the normal boot/login of the client.

Different information is captured depending on the configured workstation environment. For a list of the runtime variables that are captured (for example, ?syspassword or ?sysuser), refer to "Using Symbols and Variables" in the *Nsure SecureLogin 3.51.2 Scripting Guide*.

The following table shows the environments and the corresponding module used.

Table 1 **Workstation Components**

Environment	Module
Novell Client32™ (with/without NMAS)	slinac.dll
LDAP	slnmas.dll
Microsoft Client	sl_tscgina.dll

Each module captures credentials from the corresponding login dialog box and stores them in encrypted form in the registry for SecureLogin to access. When SecureLogin loads, it reads the encrypted values from the registry, deletes the registry values, and stores them in the ?sys variables as explained below:

- The username gets stored in the ?sysuser variable.
- The password gets stored in the ?syspassword variable.

NOTE: The variables can be used in scripts for all applications that utilize the same credentials.

If, for some reason, Secure Login uses the wrong module, or if the module is missing, then when SecureLogin loads, it cannot copy the values to the corresponding ?sys variable. In such a scenario, if an application script utilizes the ?sys variables, the result is an error -426. Also, if passthrough authentication is configured, no credentials are supplied to the Citrix session and a second login is required.

Proper validation should be done to ensure that the credentials are captured correctly so that SecureLogin can provide them to either application scripts or passthrough authentication.

Validation of the Workstation Components

To ensure that SecureLogin client is able to read the workstation login credentials and store them in the ?sys variables, create a notepad.exe script to echo the values to a new notepad document.

1. Right-click the SecureLogin icon on the status bar (system tray), then click Manage Logins > Applications > New.
2. In the Create a New Application dialog box, select New Application.
3. In the Name edit box, type **`notepad.exe`**.
4. Leave the default (Windows) as the Type, then click Create.
5. Click Script, then copy and paste the following script:

```
## BeginSection: "Test Notepad Script to display sys variable"

Dialog

   Class "Notepad"

   Title "Untitled - Notepad"

EndDialog

Type \N

Type ?SYSUSER

Type \N

Type ?SYSPASSWORD

Type \N

## EndSection:
```

6. To save the script and close all SecureLogin windows, click OK twice.
7. On the Windows task bar, click Start > Run.
8. Type **`notepad.exe`** in the Open field.
9. Launch notepad.exe and validate that the login credentials are written to the application.

If you receive a -426 error or if the wrong values are written to the document, it means proper modules are either not loaded or configured correctly.

Some Workstation Tips

- After registration of components, reboot the system.
- If SecureLogin captures only the username whereas the ?syspassword value is blank, make sure that you are not in the Workstation Only mode.

  The Novell client does not pass a password if you are logged into the Workstation Only mode. Also, in this mode, you cannot execute a login again and expect the ?sys variables to update. This process occurs only during the initial login process.
- When the SecureLogin client acquires credentials on the workstation, it not only populates the ?sys variables but also stores the credential set within the SecureLogin data.

  If, for some reason, while SecureLogin is working, a configuration change prevents the credentials from passing, SecureLogin might still appear to work and passthrough authentication might succeed as well until the user changes the network password. But then, instead of new password, the stored credentials are used for passthrough authentication.
- To ensure that correct username and password combination are captured from the initial workstation login, do a validation using a notepad script. For details, refer to "Validation of the Workstation Components" on page 45.
- Other tests can be performed to further troubleshoot this issue:
  - Create a new user and login
  - Expire the password and try an initial login again

  NOTE: Make sure that you reboot the system and log in as a new user.

When prompted to change your password, click Yes and then change the user password. If the credentials get updated, this part of passthrough authentication is working properly.

IMPORTANT: SecureLogin supports password expiration through the Novell Client login. The option to change the Novell Client password after the completion of the boot-up process is not supported. If you change the directory password anytime after SecureLogin client loads, you must log out from the workstation and log in again for SecureLogin to pick up the new password.

Server Components

Depending on the environment, SecureLogin utilizes the server module (corresponding to the client module) to perform passthrough authentication. The environment and the module details are given in the table below.

Table 2 Server Component Environments

Environment	Module
Novell Client32 (without NMAS)	slinas.dll
Novell Client32 (with NMAS)	slnmas.dll
LDAP	slaa_sso.dll
Microsoft Client	sl_tsgina.dll

On the workstation, the concern is capturing credentials from the users' initial login, while on the server side, the focus is on taking those captured credentials and passing them through to the configured GINA.

Virtual Channel

In addition to the components on the workstation and server, SecureLogin requires a method of communicating the captured information between the workstation environment and the actual Citrix session. SecureLogin performs this using a virtual channel. The server modules rely on the virtual channel to get the credentials from SecureLogin.

A virtual channel is a session-oriented, bidirectional, error-free transmission connection that can be used by Application Layer code for exchanging custom data packets between a Terminal Server and a Terminal Client.

Virtual Channel Components

There are three major Virtual Channel components in the Terminal Server:

- **Client Login Extension:** Collects user login credentials from the login GINA.
- **Virtual Channel Driver (VCD):** The heart of SecureLogin Terminal Server single sign-on; it liaises between server login extensions and SecureLogin single sign-on to perform all Terminal session single sign-on procedures.
- **Server Login Extension:** Requests user login credentials from the VCD and initiates the login. After authentication, the login extension sends credentials back to the VCD to update the SecureLogin single sign-on data store.

Types of Virtual Channels

SecureLogin uses two types of virtual channels in the Citrix environment named ICA and RDP. Two modules installed on the workstation and server allow the SecureLogin client to communicate with the specific virtual channel.

The following table provides the details:

Table 3 Details of Virtual Channel

Virtual Channel	Session	Client Interface Module	Server Interface Module
ICA	Citrix ICA session	vdslssoN.dll	sl_ica.dll
RDP	Terminal server session	tsslsso.dll	sl_rdp.dll

On the server, there is yet another module, named sl_vc.dll. This is the main interface module on the server and provides the interface to the VCDs. It determines which of the two different virtual channels to query for the passthrough credentials.

Published Applications

An additional component is used while you launch remote applications outside of an ICA/RDP desktop session. This is typically referred to as a published application.

Here, the user clicks a shortcut to launch a remote server application without opening a full desktop session. The module SLLauncher.exe is used to interface between SecureLogin and the remote application server. SLLauncher is used to start the required SecureLogin components on the server for an application to single sign-on.

For information on SLLauncher and its configuration, refer to the "SLLauncher Switches" on page 21.

NOTE: SLLauncher is not used in the actual passthrough authentication. SecureLogin uses slinas.dll, slnmas.dll, slaa_sso.dll, or the sltsgina.dll to set up the virtual channel.

Passthrough Process

1. The user enters the username, password and, optionally, his/her Domain, NDS® context, and NDS tree. This information is encrypted and stored in the registry.
2. SSO SLBroker reads the registry data, then destroys it. The login credentials are saved under a generic and hidden application platform in the SecureLogin SSO data store.
3. When the user starts the Citrix ICA client or published application through an ICA file, the VCD is loaded. This driver retrieves the domain or preferred tree name of the server and then reads the platform name from SLBroker in order to retrieve the username, password, and other optional login information.
   - If the application platform does not exist, the VCD reverts to the generic platform name.
   - If the application platform name does not match the requested platform (Domain or Tree), the VCD displays a dialog box to prompt the user to enter his/her NT or NDS credentials, whichever is appropriate. The collected credentials are then sent to the server for verification.
   - When the user enters and accepts the credential dialog box, a hidden application platform is created for the next authentication request.
   - If the user chooses to abort entering his/her credentials, then the server login box is prompted as per normal.
4. The server login extensions always send a user's login credentials back to the workstation after a successful authentication. This creates a new application platform in SLBroker, if it does not already exist, or updates the new password to SLBroker if there is a recent password change and the platform already exists.

Auto-Detection of the Client Protocol

The server detects whether the ICA protocol is present or not. If the ICA protocol is present, the server loads the ICA protocol. If the client is trying to establish a session using the RDP protocol, the server loads the RDP protocol and the session begins. By default, the server automatically responds to either the RDP or ICA protocol.

The auto-detection feature is on by default. Because Windows NT 4.0 Terminal Server Edition (RDP 4.0) does not support the Virtual Channel operation, it does not respond to the client trying to establish a session using the RDP protocol.

Disabling Auto-Detection

You can do this by making the registry changes detailed below.

WARNING: Editing the Registry can cause irreparable damage to the system. If you are not sure of the process for adding these registry values, seek assistance from someone suitably experienced.

1 On the Windows task bar, click Start > Run.

2 Type `regedit` in the Open field.

The Registry Editor is displayed.

3 In the left panel, select HKEY_LOCAL MACHINE > SOFTWARE > Protocom > SecureLogin > VirtualChannel.

4 In the right panel, click Title.

The Edit String dialog box is displayed.

NOTE: All Registry values specified are of string type [REG_SZ]

5 Add the following entry:

"AutoDetect" = "0"

TIP: Make the following entry in the same key if needed during troubleshooting, to bypass the auto-detection feature and specify the protocol the server should use.

"Protocol" = "RDP" or "ICA"

User Scenario: What Happens When Susan Initiates a Citrix Session

1. Susan logs in to the workstation. At the prompt, she specifies the login credentials.

   The appropriate SecureLogin client interface module captures these credentials, encrypts, and stores them in the registry of the workstation.

2. SecureLogin loads the workstation, reads the encrypted credentials from the registry, then stores the values to the ?sys variables.

3. Susan initiates a Citrix session via the ICA client, RDP client, or SLlauncher.

4. SecureLogin detects the Citrix session and establishes the virtual channel.

5. When login is necessary within the Citrix session, the SecureLogin client interface modules on the server query the virtual channel for the passthrough credentials.

6. When the virtual channel provides the credentials, SecureLogin passes them through to the configured authentication service.