Novell SecureLogin

6.0 SP1

October 13, 2006

www.novell.com

CITRIX AND TERMINAL SERVICES GUIDE

Novell®

Legal Notices

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

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

Novell Trademarks

Third-Party Materials

Contents

About This Guide

This document contains information on the following:

Feedback

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

Documentation Updates

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

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

Additional Documentation

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

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

Documentation Conventions

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

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

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

Overview

1

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

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

This section has the following information:

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

1.1 Prerequisites

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

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

1.2 About Citrix Application Deployment

There are three modes of Citrix application deployment:

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

1.2.1 Corporate Directory Deployment

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

1.2.2 Full Citrix Desktop Deployment

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

1.2.3 Published Application Deployment

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

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

1.2.4 Citrix Desktop and Published Application Deployment

The Citrix Desktop and Published Applications requires:

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

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

1.3 SecureLogin Attributes

Extending the directory schema adds the following six SecureLogin attributes:

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

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

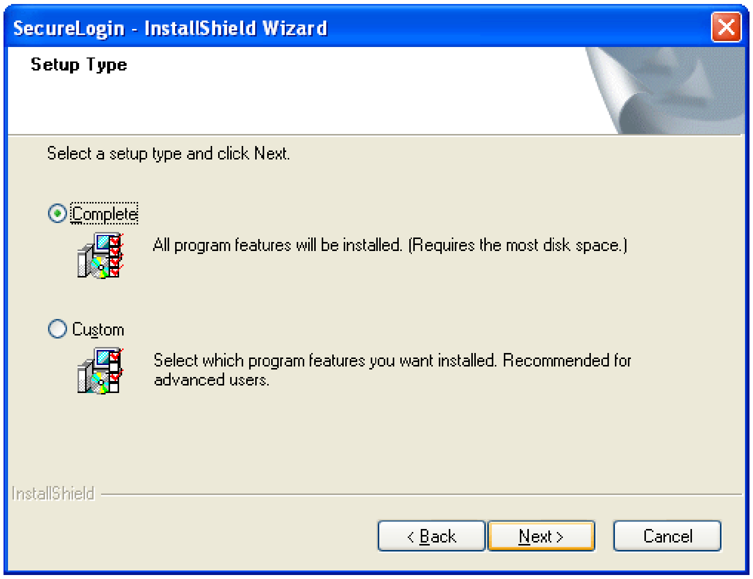
1. Log on to the server as administrator.
2. Install the SecureLogin installation CD. The main menu is displayed.
3. Click *Install* and follow the prompts for your installation type.
4. Double-click the `ndsschema.exe` file in the `Tools` folder of the CD. The SecureLogin - `Active Directory Schema` dialog box is displayed.
5. To extend the schema for a new SecureLogin installation, click *Extend Active Directory Schema*.
6. To extend the user rights for an upgrade to a newer version of SecureLogin, click *Assign User Rights*.

Installing SecureLogin On Citrix Server

2

To install SecureLogin on the Citrix server:

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



Select a setup type and click Next.

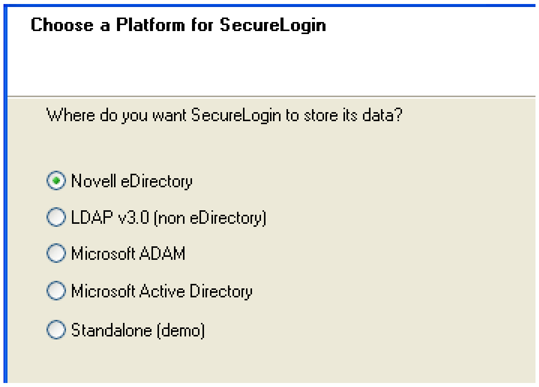
● Complete

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

○ Custom

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

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



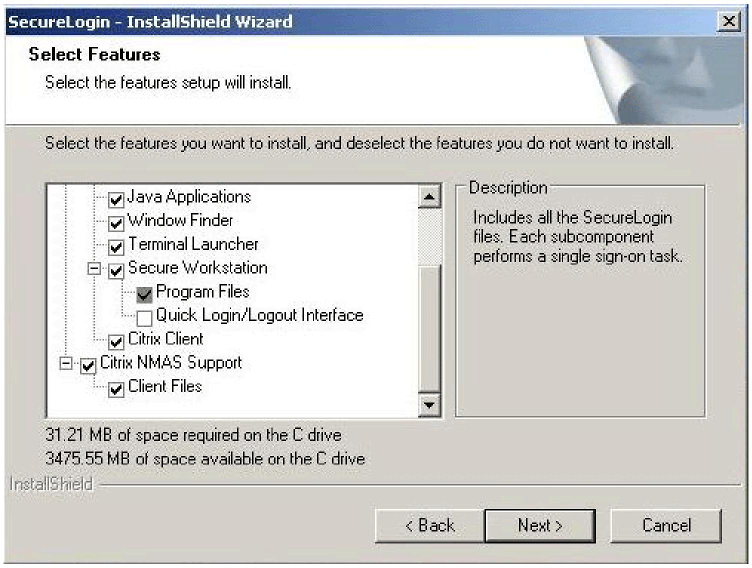
Where do you want SecureLogin to store its data?

● Novell eDirectory
○ LDAP v3.0 (non eDirectory)
○ Microsoft ADAM
○ Microsoft Active Directory
○ Standalone (demo)

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

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

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



Select Features

Select the features setup will install.

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

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

Description

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

31.21 MB of space required on the C drive

3475.55 MB of space available on the C drive

9. Click *Install*.
10. By default, the *Launch Readme* option is selected. Click *Next*.
11. Click *Finish*.
12. Select when you want to restart your workstation, then click *OK*.

Citrix Application Deployment

3

This section has the following information:

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

3.1 Launch an Application in a Citrix Environment

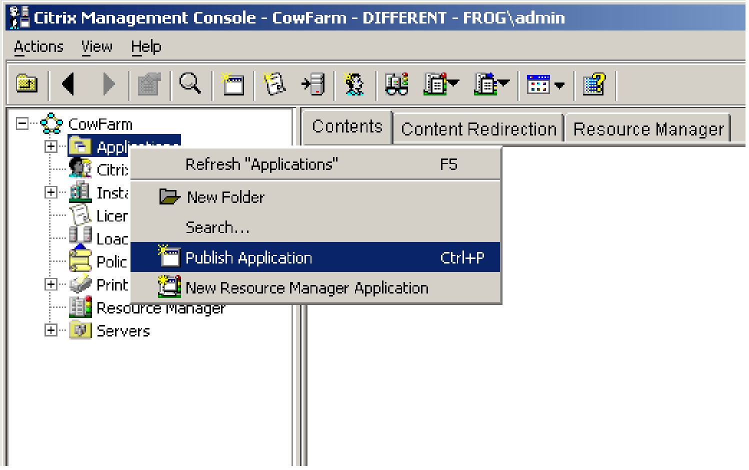
SecureLogin is unable to detect individual application screens in a Citrix environment as the Window cues are not available. You must launch SecureLogin before the application to activate the SecureLogin.

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

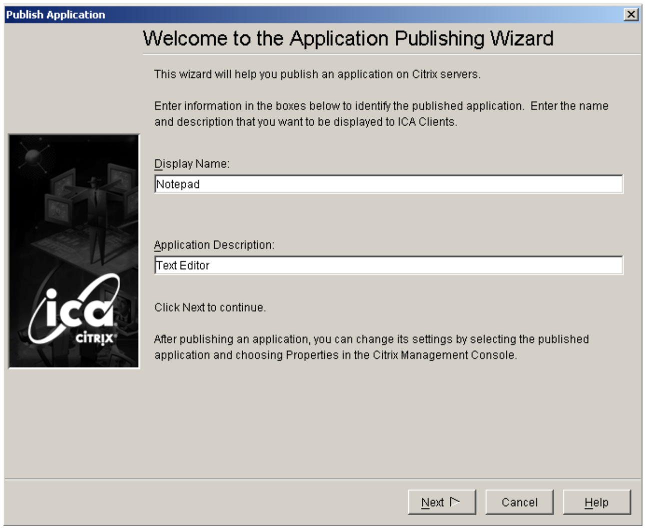
3.2 Publish an Application for Citrix Deployment

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

1 Select Applications from the Citrix farm.


Citrix Management Console - CowFarm - DIFFERENT - FROG\admin
Actions
View
Help
CowFarm
Appl
Citri
Insta
Licer
Loac
Polic
Print
Resource Manager
Servers
Contents
Content Redirection
Resource Manager
Refresh "Applications" F5
New Folder
Search...
Publish Application Ctrl+P
New Resource Manager Application

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



Welcome to the Application Publishing Wizard

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

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

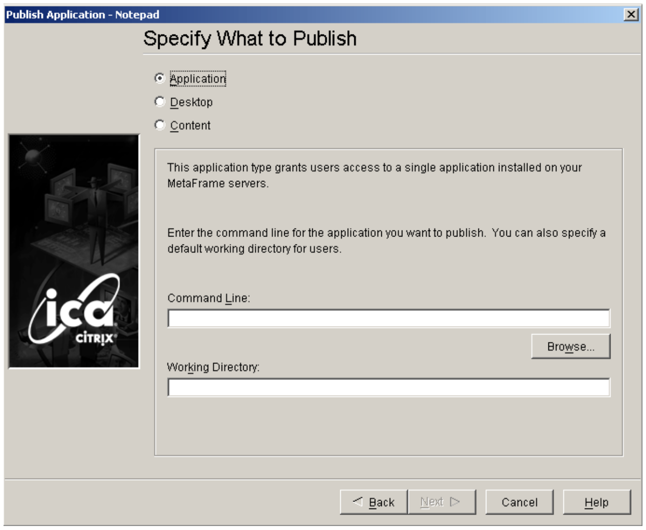
Display Name: Notepad

Application Description: Text Editor

Click Next to continue.

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

3. Specify a name for the published application in the *Display Name* field and description in the *Application Description* field.
4. Click *Next*. The Specify What to Publish dialog box is displayed.



Specify What to Publish

● Application
○ Desktop
○ Content

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

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

Command Line:

Working Directory:

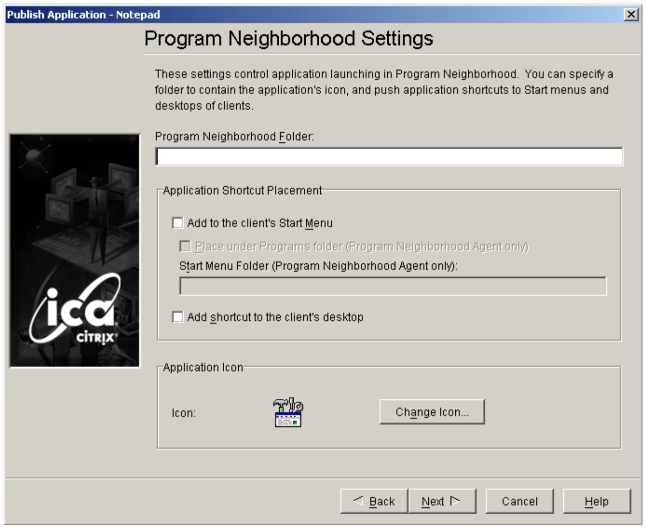
5. Click *Browse* to find the location of the application program files and select the executable.
6. Click *OK* to return to the Specify What to Publish dialog box.
7. Specify the relevant directory path in the *Working Directory* field. The working directory is the directory path of the program executable.

   The path to the `SLLauncher.exe` file of SecureLogin is specified before the published application executable. Enter a space between the SecureLogin and application executable path descriptions.
8. In the *Command Line* field, specify the published application executable path.

NOTE: Executing 16 bit applications requires the switch /16 in the command line. For more information on SLLauncher switches, see Section 3.2.1, "SLLauncher Switches," on page 20.

---

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



Publish Application - Notepad

Program Neighborhood Settings

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

Program Neighborhood Folder:

Application Shortcut Placement

☐ Add to the client's Start Menu

☐ Place under Programs folder (Program Neighborhood Agent only)

Start Menu Folder (Program Neighborhood Agent only):

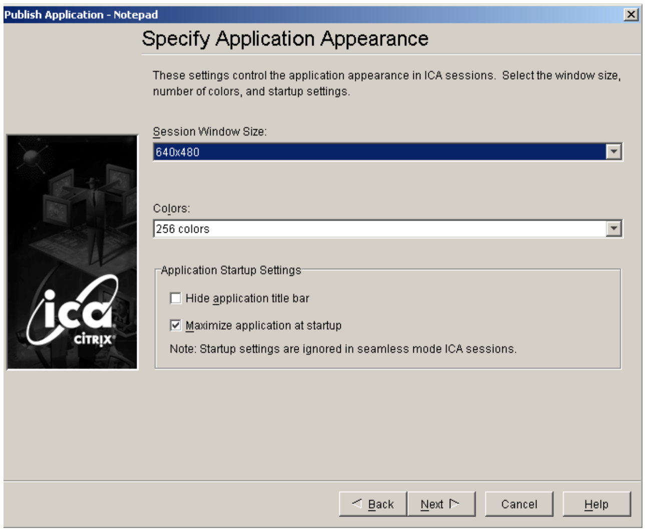
☐ Add shortcut to the client's desktop

Application Icon

Icon:

10 Select the options and configure neighborhood settings as required.

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



Publish Application - Notepad

Specify Application Appearance

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

Session Window Size: 640x480

Colors: 256 colors

Application Startup Settings

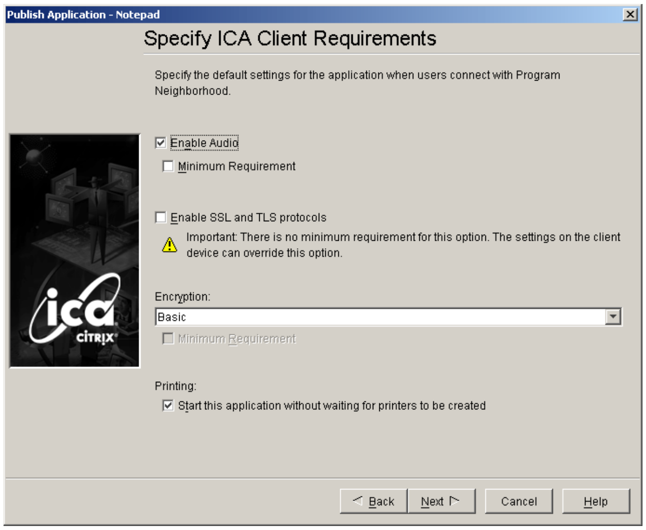
☐ Hide application title bar

☑ Maximize application at startup

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

12 Select and configure application appearance options as required

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



Publish Application - Notepad

Specify ICA Client Requirements

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

☑ Enable Audio

☐ Minimum Requirement

☐ Enable SSL and TLS protocols

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

Encryption: Basic

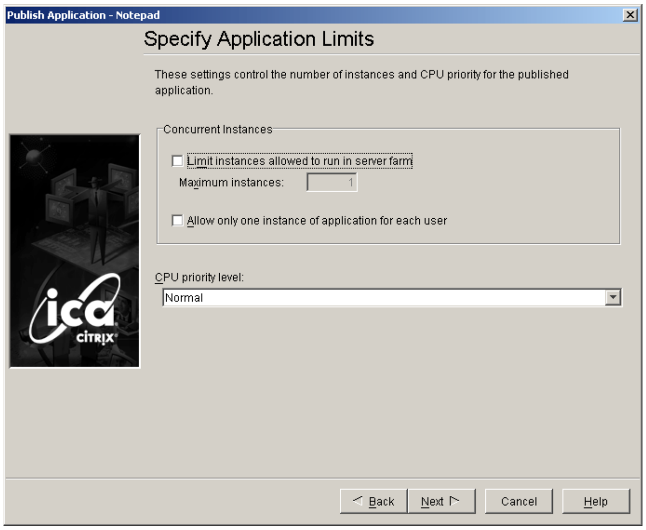
☐ Minimum Requirement

Printing:

☑ Start this application without waiting for printers to be created

14 Select and configure ICA Client Requirement options as required.

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



Publish Application - Notepad

Specify Application Limits

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

Concurrent Instances

☐ Limit instances allowed to run in server farm

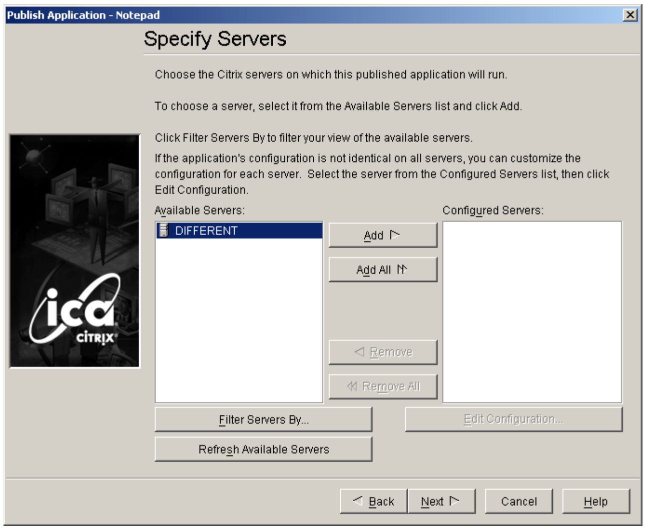
Maximum instances: 1

☐ Allow only one instance of application for each user

CPU priority level: Normal

16 Select and configure application limits as required.

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



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

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

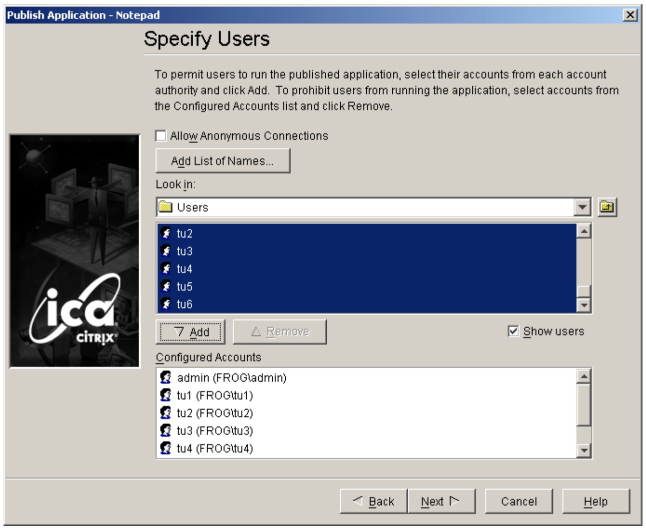
Click Filter Servers By to filter your view of the available servers.

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

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

19 Click *Add*.

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

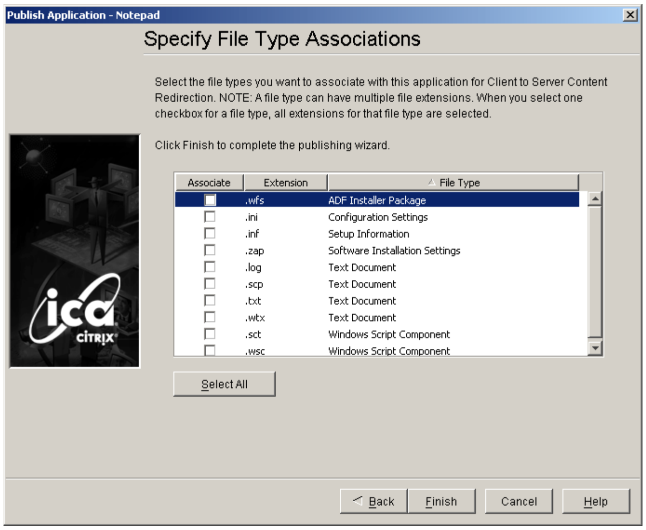


To permit users to run the published application, select their accounts from each account authority and click Add. To prohibit users from running the application, select accounts from the Configured Accounts list and click Remove.

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

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

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



Specify File Type Associations

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

Click Finish to complete the publishing wizard.

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

23 Check the file type check boxes as required.

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

25 Repeat publishing steps for all SecureLogin enabled applications.

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

3.2.1 SLLauncher Switches

You can use three switches in conjunction with the SLLauncher executable `/d`, `/16` and `/w`. Switches are not case sensitive, that is, both `/d` and `/D` are valid, however in the case of `/w`, the process name specified is case sensitive.

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

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

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

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

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

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

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

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

C:\runtest.bat

Switch Combinations

You can also use switches in combination, for example:

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

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

The following is an example syntax:

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

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

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

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

The following is an example syntax:

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

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

Configuring Citrix Load Balancing

4

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

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

The following procedures apply to Citrix Metaframe XP FR2:

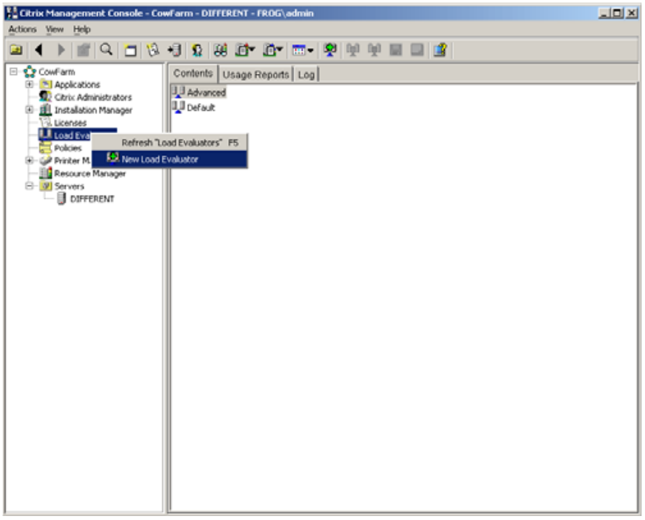
- Section 4.1, "Create a New Load Evaluator," on page 23
- Section 4.2, "Load New Evaluators to the Citrix Server," on page 25

4.1 Create a New Load Evaluator

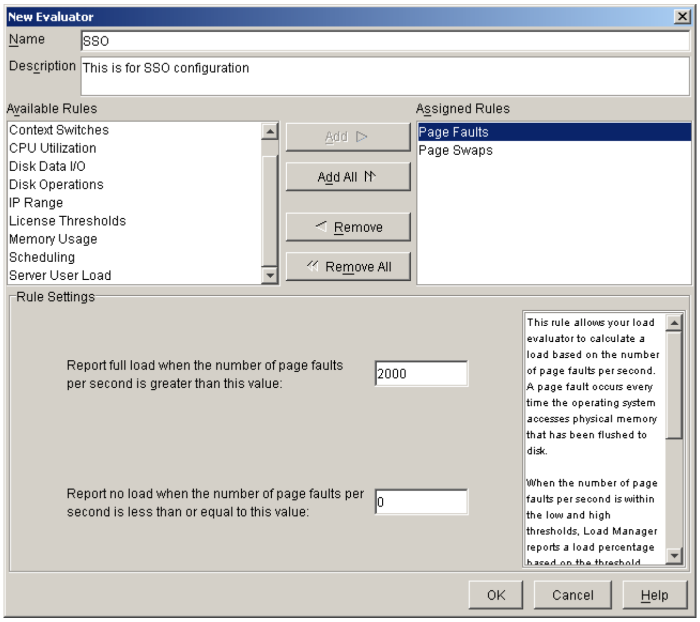
To create a new Load Evaluator:

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

2 Right-click to display the option menu.



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



Name: SSO

Description: This is for SSO configuration

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

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

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

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

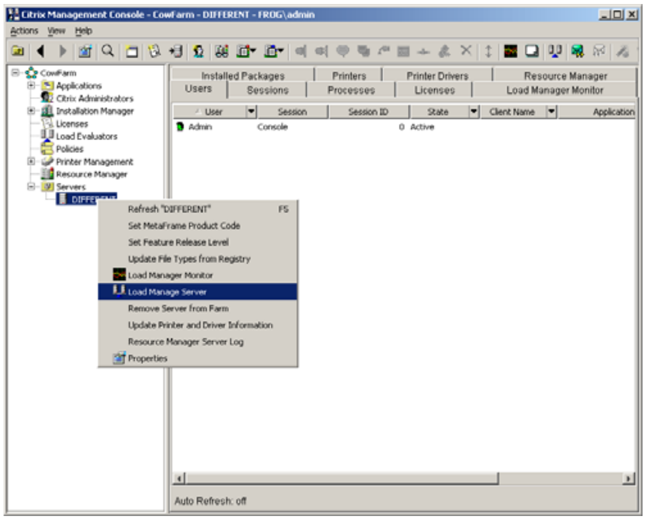
4. Specify a name for the Load Evaluator in the *Name* field.
5. Specify a description for the new evaluator in the *Description* field.
6. Select Page Faults and Page Swaps from the *Available Rules* list.
7. Click the *Add* button to add to the *Assigned Rules* list.
8. Drag to select Page Faults in the *Assigned Rules* list.

   Page Fault settings are configured in the *Rule Settings* section, displayed in the bottom half of the New Evaluator dialog box.
9. Specify a value into the *Report full load when the number of page faults per second is greater than this value:* field.
10. Drag to select *Page Swaps* in the *Assigned Rules* list. Page Swap settings display in the Rule Settings section.
11. Specify a value into the *Report full load when the number of page swaps per second is greater than this value:* field.
12. Specify a value into the *Report no load* when the number of page swaps per second is less than or equal to this *value:* field.
13. Click *OK*.

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

4.2 Load New Evaluators to the Citrix Server

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



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

2 Right-click on the relevant Citrix server name.

3 Select *Load Manage Server* from the options menu.The Load Manage Server – [server name] is displayed.

4 Select the configured *Load Evaluator* option from the *Available Load Evaluators* list.

5 Click *OK*.

The new Load Evaluators are loaded to the Citrix server.

Using Connectors

5

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

This section provides information on the following:

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

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

5.1 Enabling an Application with Connectors

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

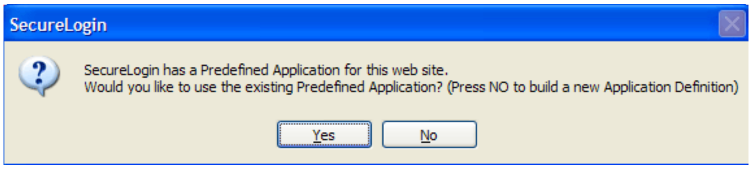
To use the Yahoo connector:

1 Start your Web browser.

2 Go to www.yahoo.com.

3 Click *Mail*.

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



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

4 Click *Yes*.

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

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

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

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

6a Click *Sign Out*.

6b Click `Yes`.

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

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

5.2 Deleting Connectors

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

Using Secure Workstation with Citrix

6

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

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

This section provides information on the following:

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

6.1 Requirements

☐ The ICA Citrix Client must be 6.0 or later.

☐ When using NMAS with Client32 or LDAPAuth, NMAS must be 3.2 or later on the client. Otherwise, NMAS will not call SecureLogin.

☐ If you use Client32 and NMAS on a Citrix server, the NMAS on the eDirectory server must also be 3.2 or later.

If you use LDAPAuth on the server, the NMAS version does not matter.

6.2 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 3.2 or later
- SecureLogin

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

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

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

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

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

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

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

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

6.3 Using pcProx with Citrix

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

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

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

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

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

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

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

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

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

6.4 Using Secure Workstation with Citrix

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

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

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

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

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

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

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

Upgrading SecureLogin

7

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

7.1 Uninstalling Version 3.0.x

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

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

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

7.2 Phased Upgrades

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