AUTHORIZED DOCUMENTATION

Citrix* and Terminal Services Guide

Novell® SecureLogin

7.0

September, 2009

www.novell.com

Legal Notices

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

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

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

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

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

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide

This document provides the following information:

Audience

This guide is intended for:

- Network Administrators
- Systems Administrators
- IT Support Staff

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 the Novell Documentation Feedback (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

For the most recent version of the *Novell SecureLogin Citrix* and Terminal Services Guide*, visit the Novell Documentation Web site. (http://www.novell.com/documentation/securelogin70/index.html)

Additional Documentation

The *Citrix and Terminal Services Guide* is part of documentation set for Novell SecureLogin 7.0. The other documents are:

- Readme: “Novell SecureLogin 7.0 Readme”
- Overview: *Novell SecureLogin Overview Guide*
- Installation: *Novell SecureLogin Installation Guide*
- Administration: *Novell SecureLogin 7.0 Administration Guide*
- Application Definition Administration: *Novell SecureLogin Application Definition Wizard Administration Guide*
- pcProx Administration: *pcProx Guide*

- Application Definition: *Novell SecureLogin Application Definition Guide*
- End User: *Novell SecureLogin User Guide*

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.

Getting Started

1

Novell® SecureLogin integrates tightly with Citrix* and terminal services, to deliver a more efficient, simple, and reliable single sign-on solution.

This document provides instructions for directory servers and terminal servers (the Citrix server environment). For example, a Microsoft Active Directory server for user provisioning and management with the applications deployed by using a Citrix server.

You must configure the Citrix and terminal server and user workstations prior to installing Novell SecureLogin. The Novell SecureLogin installation package now detects Citrix and terminal server files and installs the required supporting files automatically. In scenarios where Citrix or terminal services are deployed after your Novell SecureLogin implementation, you must redeploy the Novell SecureLogin installation package to install the required Novell SecureLogin components.

This section contains the following information:

1.1 Support on Windows Microsoft Vista

Microsoft* Windows* Vista* is recognized as a Citrix and terminal services client. The *Install Citrix and terminal services support* option is displayed when installing Novell SecureLogin.

The Microsoft Windows Vista is not supported as a Citrix or a terminal services server.

1.2 Prerequisites

The following are the prerequisites for installing Novell SecureLogin on a Citrix and terminal services server:

- Extend the relevant enterprise or corporate directory schema with the Novell SecureLogin single sign-on attributes.
- Make sure you have administrator-level access to the Citrix or Terminal Services server.
- If single sign-on is required for Java* applications, install Sun* Java Runtime Engine 1.3 or later, and Oracle* JInitiator* 1.3.1 or later on the server and workstations.
- Uninstall all versions of the Novell SecureLogin prior to version 5.5.*x* upgrade.

1.2.1 Internet Explorer Enhanced Security Configuration

This information applies to the configuration of a server in a Microsoft Windows Server 2003 operating system environment.

By default, the Microsoft Windows Server 2003 installs Internet Explorer Enhanced Security Configuration designed to decrease the exposure of enterprise servers to the potential attacks that might occur through Web content and application scripts. Because of this, some Web sites might not display or perform as expected with the installed Novell SecureLogin.

For more information on enhanced security, see the Microsoft Support Web site. (http://support.microsoft.com/kb/81514/en-us)

1.2.2 Disabling Internet Explorer Enhanced Security

If you are experiencing difficulty accessing single sign-on enabled web pages from a Windows Server 2003 server, do one of the following:

- In Internet Explorer, select *Tools > Internet Options > Advanced tab and under the Browsing heading*, select *Enable third-party web browser extensions*.

  -or-

- Use the Windows *Add/Remove Windows Components* on the Control Panel to disable Microsoft's Internet Enhanced Security Configuration.

1.3 Installation Overview

Following are the high-level tasks of the Citrix and terminal services server installation.

The documentation for installing Novell SecureLogin on a Citrix or Microsoft Terminal Services covers the default installation assuming that Novell SecureLogin is installed on both, the server and on the workstation. If you have installing only on the server and not on the workstation, see TID 7000523 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7000523&sliceId=1&docTypeID=DT_TID_1_1&dialogID=115592134&stateId=0 0 115588299) at the Novell Support Web site (http://www.novell.com/support/microsites/microsite.do).

In the default install, `Slinas.dll` is installed on the server. However, if Novell SecureLogin is not installed on the workstations, `SlinaC.dll` must be installed on the server.

1. Uninstall Novell SecureLogin versions 5.5. and earlier before upgrading to Novell SecureLogin 7.0.
2. Extend the corporate directory schema.

   IMPORTANT: If the schema was extended during the deployment of Novell SecureLogin version 3.5 or later, you do not need to repeat the process.

   Refer to the relevant directory installation and deployment guide for instructions.

3. Install Novell SecureLogin on the Citrix and terminal services server.

1.4 Overview of Citrix Application Deployment

- Section 1.4.4, “Deploying Published Applications,” on page 13
- Section 1.4.5, “Deploying Citrix Desktop and Published Applications,” on page 14

1.4.1 Application Modes

You can deploy the Citrix application in the following modes:

Deployment	Description
Deploying the Full Citrix Desktop	In this mode of deployment, only the Citrix client runs on the desktop and all other applications run on the Citrix server.
Deploying Published Applications	In this mode of deployment, a combination of applications runs on the desktop, and some are published by using the Citrix server.
Deploying Citrix Desktop and Published Applications	Use this mode of deployment to run a full Citrix desktop, or a combination of Citrix published applications and applications on the workstation.

1.4.2 Deploying in Corporate Directory Environments

In a corporate directory environments, the Novell SecureLogin data is stored on the directory. This is done by extending the directory schema to include Novell SecureLogin attributes. For information on extending the directory schema for your directory, refer to the *Novell SecureLogin Installation Guide*.

NOTE: If you have installed Novell SecureLogin 3.5.*x*, or a later version, the required SecureLogin attributes are already installed.

1.4.3 Deploying the Full Citrix Desktop

Deploying the full Citrix Desktop requires Novell SecureLogin schema extensions on the network directory server and client installation on the Citrix server.

The data of users operating the Novell SecureLogin and using the Citrix server remotely is stored on the Citrix server and the network directory.

1.4.4 Deploying Published Applications

Deploying published applications requires Novell SecureLogin schema extensions on the network directory server with the client installation on the Citrix server and the user workstation.

Novell SecureLogin executes from the workstation to log in to applications published on the Citrix server. Novell SecureLogin user data must be stored on the user’s workstation for GINA-to-GINA passthrough unless Novell SecureLogin is needed for single sign-on applications that are running on that workstation.

NOTE: The SecureLogin Application Definition Wizard cannot detect Citrix published applications. You must run the application on your workstation to create an application definition using the wizard.

1.4.5 Deploying Citrix Desktop and Published Applications

Citrix Desktop and published applications require:

- Novell SecureLogin schema extension on the network directory server.
- A Citrix server and a user workstation.

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

1.5 Novell SecureLogin Attributes

Extending the directory schema adds the following 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 Novell SecureLogin 3.5 or 3.5.*x* or later is installed, you need not extend the Directory schema because the attributes are the same.

However, any new objects, such as organizational units, still require you to assign rights.

---

1. Log in to the server as administrator.
2. Insert the Novell SecureLogin product installer package. The main menu is displayed.
3. Click *Install/Upgrade* and follow the on-screen instructions for your installation type.
4. Double-click the `ndsschema.exe` file in the `SecureLogin\Tools|Schema\NDS` folder of the installer package. The SecureLogin - Schema extension dialog box is displayed.
5. Extend the schema.

Installing Novell SecureLogin on a Citrix Server

2

After you have completed extending the schema to the required directory objects, install Novell SecureLogin single sign-on applications on the Citrix* server.

For information on extending the schema, see Extending the eDirectory Schema "Extending the eDirectory Schema" in the *Novell SecureLogin Installation Guide*.

Novell SecureLogin can be installed, configured, and features added and removed by using Microsoft* Windows* installer command line options and parameters specified in the command line or specified through a bath file. For details on Novell SecureLogin installation, refer to the *Novell SecureLogin Installation Guide*.

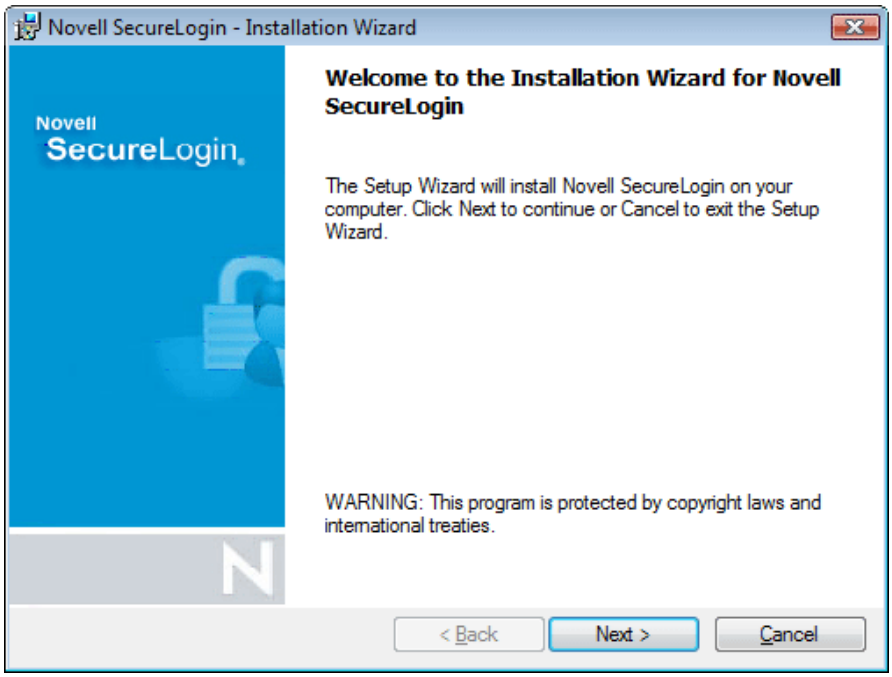
Novell SecureLogin requires Microsoft Windows installer 3.0 or later, which ships with Windows XP Service Pack 2 (SP2) and is also available as a redistributable system component for Microsoft Windows Server* 2003 (32-bit systems only). You can download this from the Microsoft Download Web site (http://www.microsoft.com/downloads/Search.aspx?displaylang=en).

NOTE: The procedures for installing on administrator workstations and user workstations are the same.

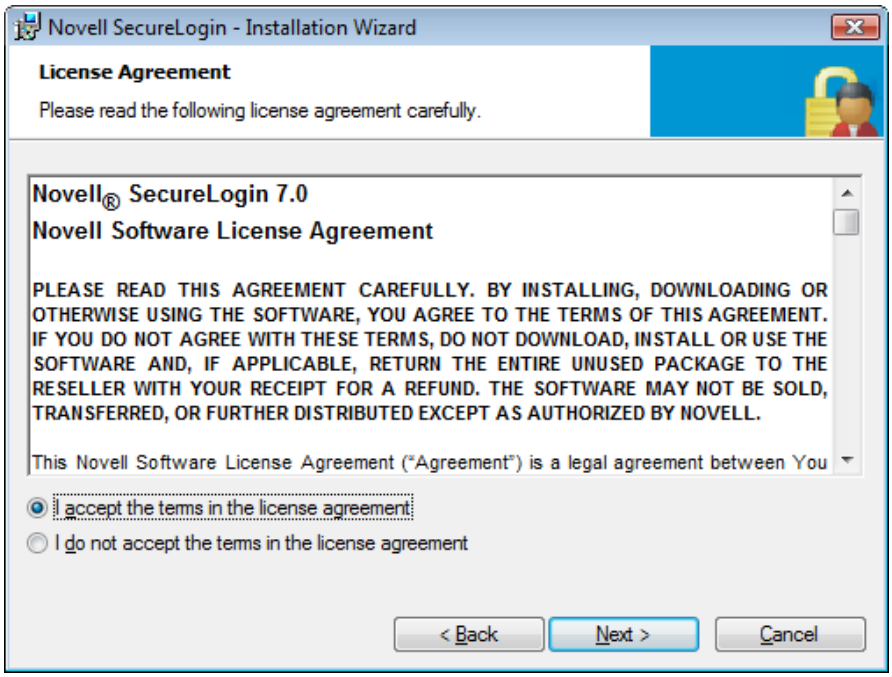
The following procedure uses the Microsoft Windows Vista 64-bit installer.

---

1. Log in to the workstation as an administrator.
2. Double-click `Novell SecureLogin.msi` located in the `SecureLogin\Client\x64` directory of the Novell SecureLogin installer package. The Welcome to the Installation Wizard for Novell SecureLogin is displayed.



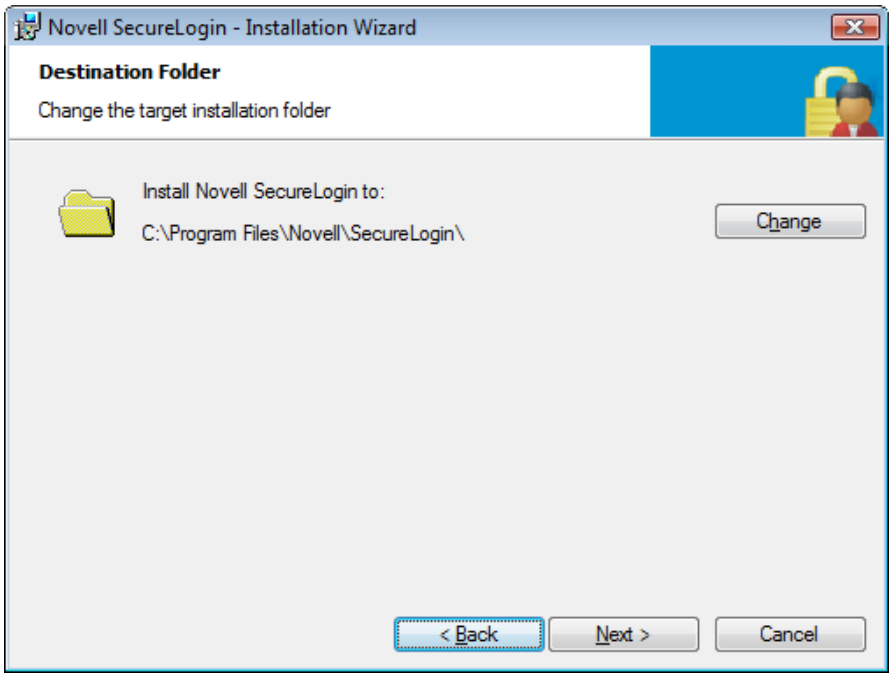
3 Click *Next*. The License Agreement page is displayed.



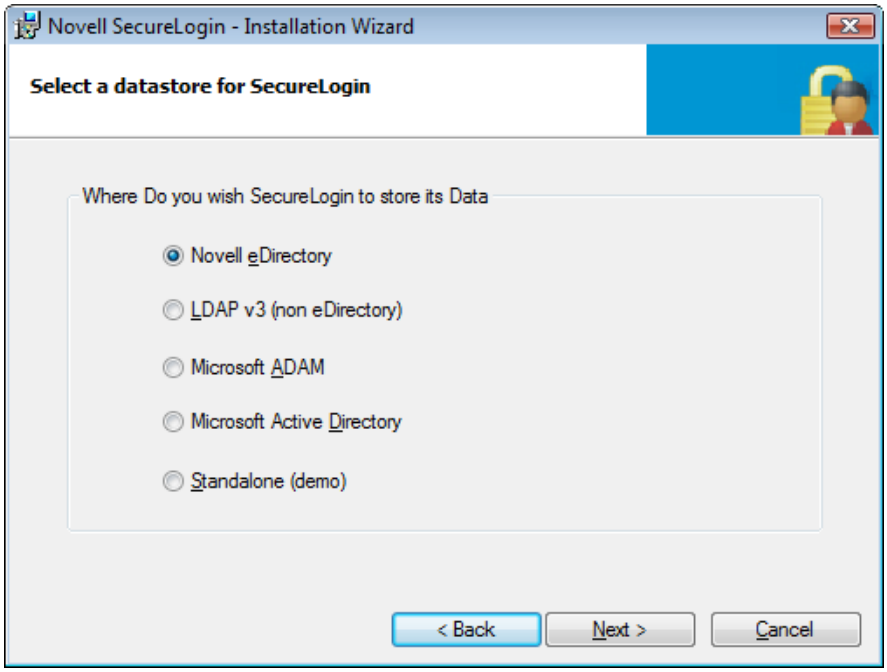
4 Accept the license agreement, then click *Next*.

The Destination Folder page is displayed. By default, the program is saved in `C:\Program Files\Novell\SecureLogin\`.You can accept the default folder or choose to change.

To change, click *Change* and navigate to your desired folder.



5 Click *Next*. Select a Datastore for SecureLogin (that is, the installation environment) page is displayed.



- If you select Novell eDirectory as the datastore, see "Installing, Configuring, and Deploying in a Novell eDirectory Environment" in the *Novell SecureLogin Installation Guide*.

- If you select Microsoft Active Directory as the datastore, see "Installing and Configuring in Active Directory Environment" in the *Novell SecureLogin Installation Guide*.e
- If you select Microsoft ADAM as the datastore, see "Configuring, Installing, and Deploying In Active Directory Application Environment" in the *Novell SecureLogin Installation Guide*..

Deploying Citrix Applications 3

This section has information on the following:

3.1 Launching an Application in a Citrix Environment

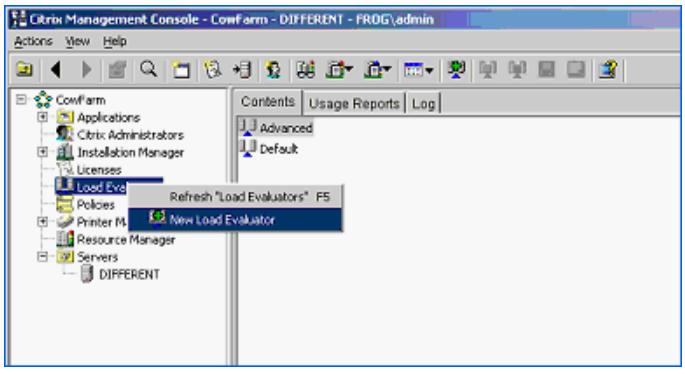
Novell SecureLogin integrates with Citrix* and terminal services and simplifies the method in which single sign-on support is provided for published applications. Novell SecureLogin can be launched without manually publishing the Citrix applications. Novell SecureLogin can be started or shut down after a user has terminated all the applications, which delivers a far more efficient, simple, and reliable single sign-on solution for any Citrix and terminal services environment.

3.2 Configuring Citrix Load Balancing

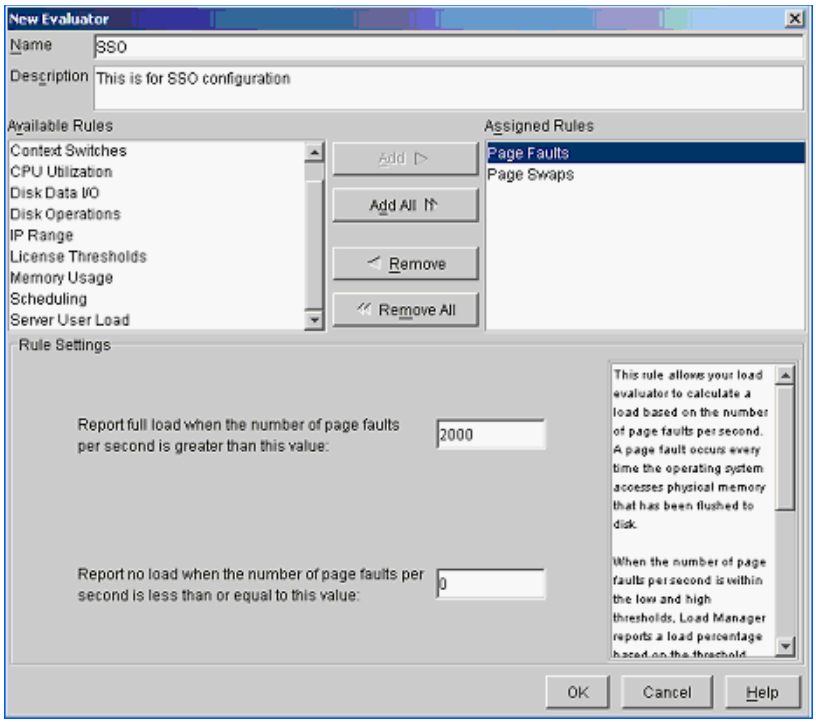
A single sign-on operation implemented for memory optimization might result in client connection dropouts. However, this does not have any adverse impact on your Citrix server, and you can resolve this by configuring Citrix Load Evaluators to increase the number of allowed page faults.

3.2.1 Creating a New Load Evaluator

1 Start the Citrix management console, then select *Load Evaluators*.



2 Right-click and select *New Load Evaluator*. The New Evaluator dialog box is displayed.



3 Specify a name for the *Load Evaluator*, and a description for the new evaluator.

4 From the *Available Rules* list, select *Page Faults* and *Page Swaps*, then click *Add*.

5 From the *Assigned Rules* lists, select *Page Faults*.

The page default settings are configured in the rule setting section, which is displayed in the bottom half of the New Evaluator dialog box.

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

7 Specify a value in the *Report full load* field when the number of page faults per second if less than or equal to this value field.

8 From the *Assigned Rules* list, select *Page Swaps* to display page swap settings in the rule settings section.

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

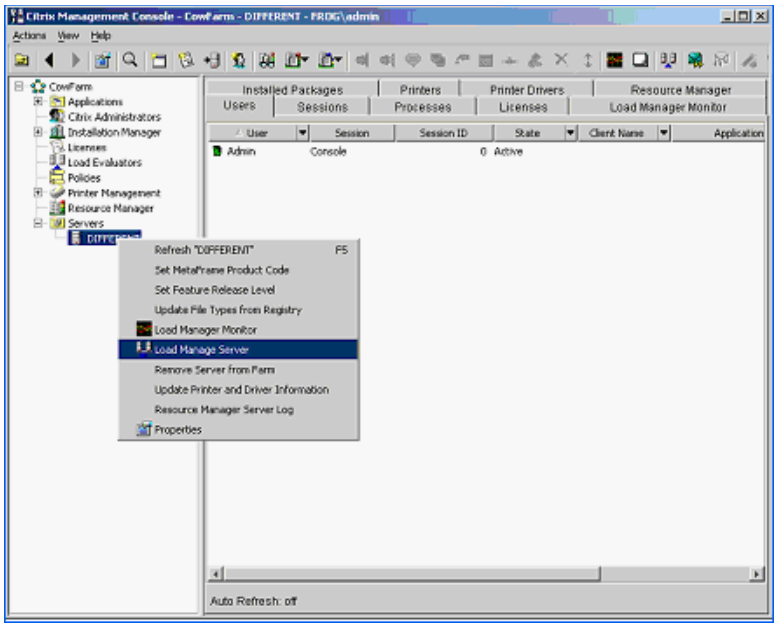
10 Specify a value in the *Report full load* field when the number of page swaps per second is less than or equal to this value field.

11 Click *OK*.

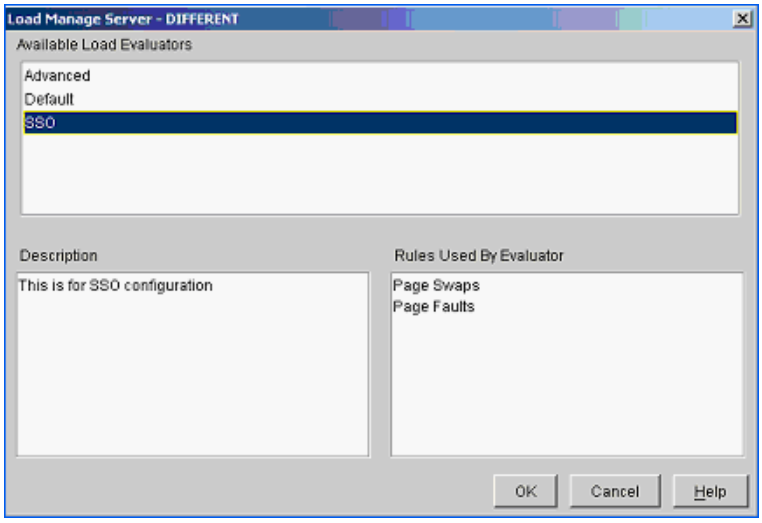
The required Load Evaluators are configured and are loaded to the Citrix server on which Novell SecureLogin is installed.

3.2.2 Loading New Load Evaluators to the Citrix Server

1 From the Citrix management console, select *Servers* > *Citrix servers*.



2 Right-click the relevant Citrix server name, then select *Load Manage Server*. The Load Manage Server - <server name> is displayed.



3 From the *Available Load Evaluators* list box, select *Configured Load Evaluators*. Click *OK*.

The new Load Evaluators are loaded to the Citrix server.

3.2.3 Deploying Existing Citrix Published Applications

If you are upgrading from a previous version of Novell SecureLogin, you do not need to change the `SLLauncher.exe` shortcuts previously created for published Citrix applications. Novell SecureLogin modifies the existing `SLLauncher.exe` automatically so that `SLLauncher.exe` is a shell that runs any command line passed to it.

The Novell SecureLogin installer now automatically detects that the installation is on a Citrix server and prompts you to verify the new Citrix components to be installed.

IMPORTANT: After installing SecureLogin, if you have both published application and published desktop open, the changes made to SecureLogin on the desktop is not reflected in the published application session until SecureLogin is restarted.

Using Connectors

4

Novell SecureLogin enables applications for single sign-on by using connectors. A connector is a program that recognizes the specific application and runs the application definition. Connectors are 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:

4.1 Enabling an Application with Connectors

The Novell 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*.

   Novell SecureLogin detects the Yahoo login screen, executes the Yahoo connector, and displays a dialog box confirming that a password field is detected.
4. Click *Yes*.
5. In the Enter Your User ID Information dialog box, specify your Yahoo username and password, then click *OK*. Novell 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*.

   Novell SecureLogin saves your credentials and uses them to automatically log you in to your account every time you want to access the Yahoo account.
6. (Optional) Test logging in and out of Yahoo. Click *Sign Out*, then click *Yes*.

   6a Click *Sign Out*.

   6b Click *Yes*.

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

   If the login is not successful, delete the Novell SecureLogin connector by using *Manage Logins*. Repeat the Step 1 through Step 5.

4.2 Deleting Connectors

1. Double-click the Novell SecureLogin  icon in the notification area.

2 Select *Applications*.

3 Select Yahoo.com, then click *Delete*.

4 Click *OK*.

Using NMAS, Secure Workstation, and pcProx with Citrix

5

The information provided in this section allows similar user experience with NMAS™, Secure Workstation, and pcProx* when these components are used in a remote Citrix* session as when they are used on a local workstation.

The Citrix virtual channels for these components allows these components to communicate with their devices in a remote session, there by giving the same end-user experience when these features are used in a Citrix session.

If the Novell SecureLogin installation program discovers a Citrix client and the users choose to Citrix support, the Citrix virtual channel drivers for Secure Workstation and pcProx are installed and configured.

This section provides information on the following:

5.1 Requirements

- The ICA Citrix Client must be 11.0 or later.
- NMAS server on eDirectory server must be 3.1 or later
- The following must be running on the Citrix client and server:
  - Client32 and LDAPAuth
  - NMAS 3.4 or later
  - Novell SecureLogin with Secure Workstation and Pcprox installed.
  - The login server method uses standard NMAS authentication. It authenticates to eDirectory.

5.2 Using NMAS with Citrix

The NMAS works in a remote Citrix session by redirecting the authentication to the remote Citrix Client (referred to as the ICA Client) so that the Login Client NMAS Methods are invoked on the same workstation on which the hardware is installed.

Example

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 cannot 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.

Solution by Using Virtual Channels: Client32 calls NMAS, and NMAS calls Novell SecureLogin before it authenticates the user. Novell 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 for the session that this workstation is attached to. The Citrix server could be serving sessions to as many as 1,000 ICA clients. One session could be running on the console.) Novell SecureLogin determines whether it is running in a console session or one of the remote sessions.

If Novell SecureLogin is running in a remote session, it uses the virtual channel, which runs over the Citrix protocol. Novell 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 Novell SecureLogin is handling the login.

Novell 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 a NetWare Core Protocol to the NMAS server as 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.

5.3 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.

Unlocking a Citrix session by using the NMAS pcProx sequence does not work. That is, if a remote Citrix session is locked by using the Secure Workstation QLL GUI or by using the Windows screen saver option, the unlock operation through the NMAS pcProx sequence does not function.

Citrix passthrough is not supported if Novell SecureLogin is installed in Novell Client mode because Novell SecureLogin does not store the card details under the ?syspassword variable with pcProx login method.

Scenario 1

pcProx Reader: A doctor walks to a workstation and places his pcProx card on a reader. The doctor logs in without specifying any data. The username comes from eDirectory, and 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 do not 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 or herself 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 one.

Therefore, the pcProx method uses the virtual channel on its own.

Scenario 2

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, and passes the data back to Client32. The user is identified. Then the authentication process begins.

5.4 Using Secure Workstation with Citrix

Secure Workstation uses device removal plug-in. 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. Basically, 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, you can specify which devices you want to listen for when you configure the device removal event.

Scenario 1

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 is removed. If the plug-in detects that the device is not 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 do not install anything extra on the Citrix server. You just install Novell SecureLogin. All the files are copied to the server.

Setting Terminal Services

6

This section contains information on the following:

6.1 Integrating Microsoft Terminal Server and Citrix

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

- The client login extension (`slinac.dll`) applied to a workstation with the Novell Client™, with or without the Novell Modular Authentication Services (NMAS™) client.
- The GINA stub (`sl_tscgina.dll`) applied to a workstation without the Novell Client.

  This component provides a link between the Microsoft GINA and the GINA running on the terminal server.
- The server login extension (`slinas.dll`) applied to a terminal server with the Novell Client.

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

  This component provides the server-side link to the client GINA stub.
- The Novell SecureLogin Virtual Channel Driver (`vdslsson.dll` or `tsslsso.dll`).

  This component provides the conduit for secure communications between the client and server extensions.
- Published Application integration (`SLLauncher.exe`) applied to a Citrix server.
  This component provides proper initialization and termination of the Novell SecureLogin components (`slbroker.exe` and `proto.exe`) running on the server.

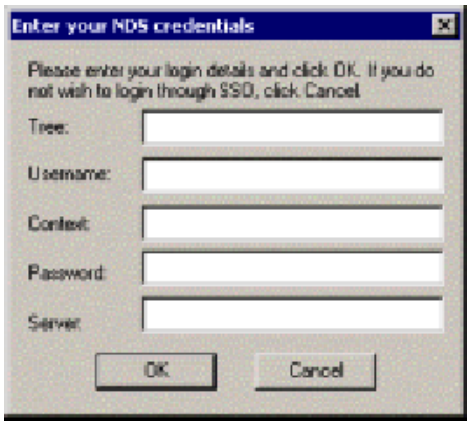
The following diagram illustrates the Novell SecureLogin architecture:

6.2 GINA Credential Pass-Through

With the Novell SecureLogin Citrix components installed, Novell SecureLogin provides a seamless pass-through of GINA credentials from the client to the server. The GINA credential pass-through operates anytime that the terminal server presents a GINA login panel. If the credentials that the user used to log in to the client match the credentials of the terminal server, the credentials are automatically passed for the user. If the credentials do no match, Novell SecureLogin captures the error and presents a new login panel for the user to complete. Novell SecureLogin detects which GINA is running on the Citrix server and requests the appropriate information.

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

Figure 6-1 *NDS Credentials*



After the user completes the dialog box, Novell SecureLogin saves the information as a hidden application (platform) within the Novell 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.

Several components are utilized by Novell SecureLogin to perform the GINA pass-through authentication. Depending on the configuration, different modules are required. The credentials are retrieved from the hidden application and seamlessly passed to the terminal server.

6.2.1 What Happens when GINA Pass-Through is Working?

1. The users boots the workstation.
2. He or she is prompted to enter the credentials to log in.

   The Novell SecureLogin client interface module captures the login credentials, encrypts, and stores the details in the workstation registry.
3. Novell SecureLogin loads on the workstation and reads the encrypted credentials from the registry and stores the values to the `?sys` variable.
4. The user initiates the a Citrix session through the ICA Client, RDP Client, or the SLLauncher.
5. Novell SecureLogin detects the Citrix session and establishes the virtual channel.

6. When the login is required within the Citrix session, Novell SecureLogin client interface modules on the server query the virtual channel for the pass-through credentials.
7. After the credentials are obtained through the virtual channel, Novell SecureLogin passes the credentials to the configured authentication service.

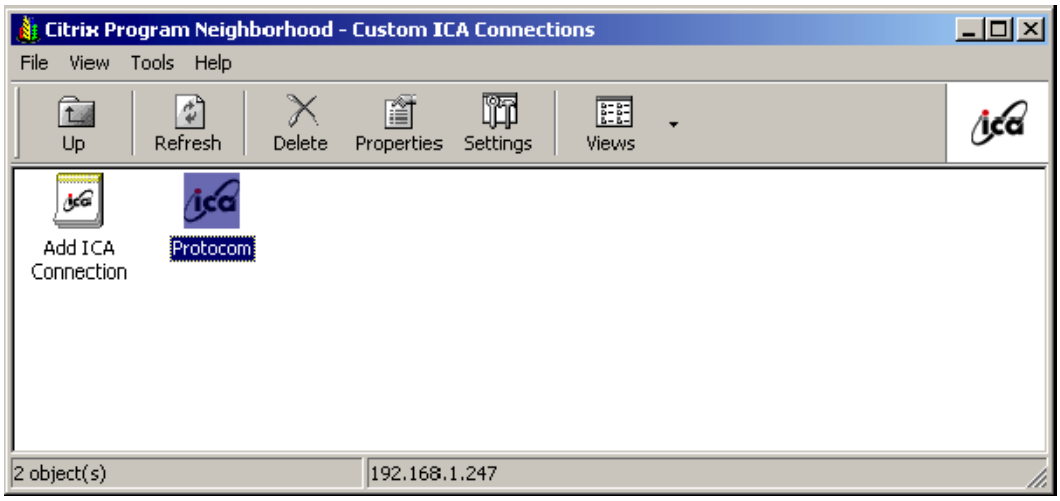
6.3 Integrating with Citrix Components

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

6.3.1 Windows GINA Authentication

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

Figure 6-2 *Custom ICA Connections*



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

6.3.2 Program Neighborhood

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

Figure 6-3 *Program Neighborhood Authentication*

Program Neighborhood then collects the credentials and sends them to a Citrix server in the farm. The Citrix Seamless Session Interface does not handle this authentication request. However, a script can handle the `wfcrun32.exe` file just as it can handle any other Windows application that is requesting authentication. The Novell SecureLogin Wizard automatically creates a script that enables single sign-on to Program Neighborhood. You should modify this script to allow for error handling, such as a bad username, domain, or password.

6.3.3 Using Desktop Shortcuts to Published Applications

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

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

6.3.4 Handling Password Changes

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

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

6.4 Virtual Channel

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

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

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

- Section 6.4.1, "Virtual Channel Components," on page 33
- Section 6.4.2, "Auto-Detecting the Client Protocol," on page 34

6.4.1 Virtual Channel Components

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

Table 6-1 *The Virtual Channel Components*

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

Novell SecureLogin uses the following processes:

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

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

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

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

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

NOTE: Novell SecureLogin does not currently handle the actual password change process. Therefore, Novell SecureLogin does not send back the new password when it is changed on the Citrix server. However, when the password stored in `slbroker.exe` is invalid because of a recent password change done on the Citrix Server, the user is prompted to enter login credentials again. After the new password is verified, it is then sent back to the VCD to update `slbroker.exe`.

---

4. After a successful authentication, the server login extension always sends the user's login credentials back to the workstation. If an application does not exist, this procedure creates a new application in `slbroker.exe`. If the password has recently been changed and the application already exists, this procedure updates the new password to `slbroker.exe`.

6.4.2 Auto-Detecting the Client Protocol

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

By default, the Auto Detection feature is on.

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

6.5 Requirements for Terminal Services

The section contains the following information:

- Section 6.5.1, “Server Requirements,” on page 34
- Section 6.5.2, “Workstation Requirements,” on page 35

6.5.1 Server Requirements

- Windows 2008 and 2003 Server Edition or the Windows 2000 Server family with Terminal Service enabled.
- One of the following Citrix servers installed (optional):
  - XenApp 5.0 or later
  - Citrix client 11.0 or later
- (Optional) Novell Client 4.9 SP5 or later

6.5.2 Workstation Requirements

- Novell Client 4.91 SP5 or later
- One of the following:
  - Win32 ICA Client Version 11.0 or later
  - Terminal Server Client that supports RDP 5.0 (for example, the version that shipped with Windows 2000 Advanced Server)

6.6 Setting Up the Server

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

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

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

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

6.6.1 Setting the GINA

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

Servers with the Novell Client

1. Set up a Novell login extension.
   Copy `srv\nw\slinas.dll` to the Windows system directory, (for example, `c:\winnt\system32`
2. Register the login extension.
   In the `srv\nw` directory, double-click `Register NTLoginExt.reg`.
3. Follow the on-screen instructions to finish the registration.

Servers without the Novell Client

1. Replace the server GINA.
   Copy `srv\ms\sl_tsgina.dll` to the Windows system directory (for example, `c:\winnt\system32`
2. Register the login extension.
   In the `srv\nw` directory, double-click `winlogon_server.orgTLoginExt.reg`.
3. Follow the on-screen instructions to finish the registration.
4. Reboot the server.

6.6.2 Configuring OnDemand

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

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

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

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

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

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

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

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

6.7 Setting Up Workstations

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

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

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

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

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

- Section 6.7.1, "Novell Client (without the NMAS Client)," on page 37
- Section 6.7.2, "Novell Client (with the NMAS Client)," on page 37
- Section 6.7.3, "Microsoft Workstation with No Novell Client Installed," on page 37

6.7.1 Novell Client (without the NMAS Client)

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

   If you are running Windows NT, Windows XP, or Windows 2000, double-click `Register NT LoginExt.reg`, in the `wks\nw` directory.
3. Follow the on-screen instructions to finish the registration.
4. Set up Microsoft Layer for Unicode* on Windows 95/98/ME.

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

6.7.2 Novell Client (with the NMAS Client)

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

   The `slnmas.dll` file is not a login extension. Instead, it is called by the NMAS client. If you are using the NMAS client and `slnmas.dll`, it is not necessary to run the registry (REG) file. You will need to install the version of NMAS client that comes with current version of Novell SecureLogin, which is `slnmas.dll` aware.
2. Set up Microsoft Layer for Unicode on Windows 95/98/ME.

   If you are running Windows 9x/ME, copy `unicows.dll` from the `\redistributable` directory to your system directory (for example, `c:\windows\system`).
3. Follow the on-screen instructions to finish the registration.
4. Reboot the workstation.

6.7.3 Microsoft Workstation with No Novell Client Installed

1. Replace the workstation GINA.

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

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

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

4 Reboot the workstation.

6.8 Installing the Virtual Channel Driver

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

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

6.8.1 Workstations with the Citrix Client (ICA)

1 Install the Novell SecureLogin Citrix ICA VCD.

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

2 Register the Novell SecureLogin Citrix ICA VCD.

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

- The [ICA30] section has a Virtual Driver line. Add the name of the virtual driver to the end of this line. For example, add
, SLSSO
- At the end of the [VirtualDriver] section, add a driver assignment statement. For example, for the SLSSO driver, add
SLSSO =

The extra spaces are for appropriate indentation. They are not required.

3 Create a new section, [SLSSO], as follows:
[SLSSO]
DriverNameWin32 = VDSLSSON.DLL

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

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

6.8.2 Workstations with the Terminal Server Client (RDP)

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

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

IMPORTANT: This is a per-user setting.

---

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

6.9 Installing the Terminal Server Web Client

If TSWeb Client is installed on the terminal server:

1. Locate `connect.asp` on the server. For example, go to `c:\inetpub\wwwroot\tsweb`.
2. Using Notepad, open `connect.asp`.
3. Add the following line before MsTsc.Connect():

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

   The `vcd\rdp` directory has an example `connect.asp` file that you can refer to.
4. Save and close the file.

6.10 Integrating with Citrix Published Applications

This section provides information on the following:

6.10.1 Modifying the Command Line

SLLauncher can optionally be used with any published application running on the Citrix server. This is to preserve backwards compatibility with pre-6.1 Citrix published applications that were created using the `sllauncher.exe` in the Citrix published application shortcut, and also to specify use of `sllauncher.exe` command line switches as detailed in "Using SLLauncher Syntax" on page 39.

If SLLauncher is not found within the server's path environment variable, you must include the full path to SLLauncher. For example, replace the command line of the published application as follows:

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

6.10.2 Using SLLauncher Syntax

To run `SLLauncher`, use the following command:

`SLLauncher [/wd]` *Citrix Published Application Parameters*

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

`SLLauncher` includes two command line parameters that control its behavior:

Table 6-2 *Command Line Parameters*

Parameter	Explanation

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

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

6.11 Registry Settings

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

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

6.11.1 Auto-Detecting the Client Protocol

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

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

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

6.11.2 Servers with a Novell Client

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

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\Virtual
Channel\Login\slina]

"PopulateToNT" = "1"
```

6.11.3 Localized Machine

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

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

6.11.4 Third-Party GINA

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

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


"ProtocomPassThruDLL" = "Gina DLL name"
```

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

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

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

NT\CurrentVersion\Winlogon\ProtocomPassThru]

```
"UsernameCtrlID" = "User Name field ID"

"PasswordCtrlID" = "Password Field ID"

"DomainCtrlID" = "Domain Name Ctrl ID"

"IDOK" = "OK Button ID"
```

NOTE: Define Domain Name in a combo box.

6.12 Debugging Options

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

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

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

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

6.13 Files Installed

6.13.1 Citrix Client

Citrix Client is used to capture credentials from the Workstations and send the credentials through a virtual channel when an ICA session is established, known as GINA to GINA pass through. The CitrixClient component facilitates this GINA to GINA pass through.

- The Novell SecureLogin GINA to Novell GINA pass through is different.
- The Novell SecureLogin GINA for Microsoft GINA component is only installed on Novell workstations with the ICA client installed.

The CitrixClient components install the following files:

- pcpxcitc.dll Citrix Virtual Channel Driver for NMAS pcProx.
- nmascitc.dll Citrix Virtual Channel Driver for NMAS.
- nswcitc.dll Citrix Virtual Channel Driver for Secure Workstation.
- vdslsso.dll (Novell SecureLogin Virtual Channel Driver for ICA Client) - This library file serves as a virtual channel to pass the captured credentials from the workstation to the Citrix Server GINA.
- module.ini (Configuration file in the ICA client directory) - This initialization file is modified so that the ICA client can use the Novell SecureLogin Virtual Channel driver.

6.13.2 Terminal Services Client

TerminalServicesClient is used to capture credentials from the Workstations and send the credentials through a virtual channel when a Terminal services session is established, known as GINA to GINA pass through. The TerminalServicesClient component facilitates this GINA to GINA pass through.

The TerminalServicesClient component installs the tsslsso.dll file:

6.13.3 CitrixServer

The Novell SecureLogin published application component consists of `SLLauncher.exe` used as a wrapper to launch published applications that are enabled with Novell SecureLogin.

6.13.4 Microsoft Terminal Server

This Microsoft GINA component uses the Novell SecureLogin GINA Extension (`tsgina.dll`) and a registry entry to accommodate the GINA to GINA pass through.

6.13.5 Citrix Server

This Novell GINA component uses the Novell SecureLogin GINA Extension (`tsgina.dll`) and a registry entry to accommodate the GINA to GINA pass through.

Upgrading

7

This section contains information on the following:

7.1 Issues with Upgrading

7.1.1 Changes With Encryption

Novell SecureLogin has features for single sign-on security systems. They include support for Public Key Infrastructure (PKI) encryption of single sign-on credentials and the option to use Advanced Encryption Standards (AES) for encrypting data. Both these features require changes to the Novell SecureLogin single sign-on data format to support them.

7.1.2 Issues In Reading Old Data

The Novell SecureLogin client can read data created with all the previous versions of Novell SecureLogin. However, older versions of the product cannot read data created by Novell SecureLogin 7.0. This means that in a mixed environment where some computers are running Novell SecureLogin 7.0 and some other computers are running a previous versions, issues are likely to arise when users move between these versions.

This is especially a problem in Citrix Environments, or in large enterprise deployments.

The last data format occurred in Novell SecureLogin 3.0. *x* and 3.5, and was related to the introduction of new scripting types and other features.

The impact of disruption of data upgrades like this is high. Hence, several new features are included in the version 6 data format that minimizes the disruption caused by data upgrades in the future.

7.1.3 Upgrading the Data Store

While trying to install Novell SecureLogin 7.0, it detects that Novell SecureLogin 3.5 data is in use and continues to work. In this mode, all 3.5 functionality continues to be available, but any version 7.0 functionality that relies on the new data is not available.

Significantly, this includes smart card support and AES encryption of data.

If you do not require functionality of the new version, then there is no great impetus to upgrade the data format. If, however you require the functionality of the new version, then complete the following tasks:

- Choose a section of the tree to upgrade.
- Make sure that all of the workstations used by the users in that section of the trees are upgraded to the Novell SecureLogin 7.0 client.

The next time these users log in, their data is converted to version 7 format and, the new features are available.

NOTE: When a user with Novell SecureLogin 3.5 data first loads the version 7 client, they are prompted to answer the passphrase question.

This does not happen if the passphrase system is disabled while the user was operating on a version 3.5 client.

7.1.4 Prompting for a Passphrase During an Upgrade

The new single sign-on security system stores additional passphrase information to facilitate seamless upgrades in the future. It now uses a more secure key derivation technique and allows the use of AES. The passphrase data stored in version 3.5 format does not contain the information required to support these new features, so, the users are prompted to reenter the passphrase answer.

7.1.5 About the New Protection Method

In the future, new single sign-on features might be desired. For example, the directory password and smart card might be used to protect single sign-on credentials, or a system might be available where a designated administrator can unlock a user's credentials after a password reset is done. In these cases, a new keywrapper type is needed. They keywrapper is ignored and not interpreted by the version 7 client, but the version 6 client can still access data using the old keywrappers that it does understand. This means that as long as the standard keywrappers are defined there are no upgrade issues with version 7. However, in a scenarios where the keywrappers are not defined, the existing data format upgrade process is applicable.

7.1.6 Adding the New Encryption Algorithm

If you need to use the encryption algorithm, you must upgrade tot he version supporting that algorithm. However, there is no need for customers to upgrade if a particular algorithm is working for them.

7.2 Deployment Options

This section contains information on the following:

7.2.1 Installation Options in a Citrix Environment

To install the Citrix support set:

```
X_INSTALLCITRIX="Yes"
```

Novell SecureLogin detects the type of Citrix or terminal service automatically and the following properties are set, depending on the type of the service detected.

If a Citrix client is detected: `X_ISCITRIXCLIENT="Yes"`

If a Citrix server is detected: `X_ISCITRIXSERVER="Yes"`

If a terminal client is detected: `X_ISTSCLIENT="Yes"`

If a terminal server is detected: `X_ISTSSERVER="Yes"`

Example of a Silent Command Line Citrix Installation

The following is an example of a successful and tested silent command line installation of Novell SecureLogin on a Citrix client.

```
msiexec.exe /qn /norestart /i "Novell SecureLogin.msi"
ADDLOCAL=MAD,Citrix,CitrixClient X_INSTALLCITRIX="Yes"
X_PLATFORM="CLIENT" X_ISCITRIXCLIENT="Yes"
```

7.2.2 Deploying Existing Citrix Published Applications

When upgrading from a previous version of Novell SecureLogin to Novell SecureLogin 7.0, you are not required to change any `SLLauncher.exe` shortcuts previously created for published Citrix applications.

When it is installed, the Novell SecureLogin 7.0 modifies the existing `SLLauncher.exe` automatically so it becomes a shell that runs any command line passed to it.

The Novell SecureLogin 7.0 installer now automatically detects that the installation is on a Citrix server and prompts you to verify the new Citrix components to be installed.

IMPORTANT: After the successful installation of Novell SecureLogin, if a user has a published desktop open at the same time as a published application, any changes made to the Novell SecureLogin data on the desktop are not reflected in the published application session until Novell SecureLogin is restarted.

7.2.3 Using the Installation Options

Scenario 1: A client has a Citrix environment in an Active Directory* mode. The published applications are contained in one published application set and user access to the published applications is through a Citrix Web interface. The client needs to enable single sign-on for published applications.

Install Novell SecureLogin only on the Citrix server and not on the workstations, because the client only needs to enable single sign-on for published application when access is through the Web.

The other Novell Securelogin component needed on the server is the published application component. Use `SLLauncher.exe` to enable single sign-on for published applications.

Scenario 2: A client has a Citrix environment in an Active Directory mode. Users access applications on their local workstations and also access published applications through the ICA client. Both the local application and the published applications must be enabled for single sign-on. The client also requires the users to use the same credentials to log in to both the local workstations and the Citrix server.

Install Novell SecureLogin and the Citrix components on both the local workstation and the Citrix server to allow local applications and published applications to be enabled for single sign-on. Also, enable GINA for GINA passthrough because the user has authenticated to the directory when logging in to the workstation. When an ICA connection is established, the user's credentials that are used to authenticate to the workstation are sent through a virtual channel driver (Citrix Client option) to the Citrix server GINA.

7.2.4 Deploying in Citrix Desktop Mode

Deploying the full Citrix Desktop requires Novell SecureLogin schema extensions on the network directory server and client installation on the Citrix server.

The data of users using the Novell SecureLogin and using the Citrix server remotely is stored in the Citrix directory and the network directory.

7.2.5 Deploying Existing Citrix Published Applications

If you are upgrading from a previous version of Novell SecureLogin, do not change the SLLauncher.exe shortcuts previously created for published Citrix applications. Novell SecureLogin modifies the existing SLLauncher.exe automatically so that SLLauncher.exe is a shell that runs any command line passed to it.

The Novell SecureLogin installer automatically detects that the installation is on a Citrix server and prompts you to verify the new Citrix components to be installed.

IMPORTANT: After installing SecureLogin, if you have both published application and published desktop open, the changes made to SecureLogin on the desktop is not reflected in the published application session until SecureLogin is restarted.

7.2.6 Citrix Published Applications and the Application Definition Wizard

The Application Definition Wizard included in Novell SecureLogin 7.0 or later cannot detect Citrix published applications. Run the application on your workstation to create an application definition using the wizard.

7.3 Upgrading from Earlier Versions to Novell SecureLogin 7.0

To upgrade entirely to Novell SecureLogin 7.0, you must uninstall all versions from 3.0.x to 3.5.x.

NOTE: If you are using the Mozilla* Firefox* browser, you might encounter problems when upgrading Novell SecureLogin 6.*x* with Firefox 1.0.*x* or earlier.

Install or upgrade to Novell SecureLogin by using Mozilla Firefox 1.5 or later. With this, the `SLoMoz.xpi` extension is automatically installed and configured.

If a user wants to continue using Mozilla Firefox 1.0.*x* or earlier, then the `SLoMoz.xpi` extension installed with Novell SecureLogin must be uninstalled and the `SLoMoz.xpi` extension file of the Novell SecureLogin installer package must be re-installed.

To upgrade entirely to Novell SecureLogin 7.0, you must uninstall all versions from 3.0.*x* to 3.5.*x*.

7.3.1 Restriction on Upgrades

The only restriction that Novell SecureLogin upgrade applies is for mobile users. When upgrading users who log in to multiple workstations, conflicts occur if the user accesses workstations that are upgraded and those that are not upgraded.

After the user logs in to a workstation that is upgraded, the user data is updated and they cannot subsequently use Novell SecureLogin on a workstation still running the old version.

To avoid this situation and assure a smooth transition, use a migration plan. For more information on a migration plan, see Section 7.9, “Developing a Migration Plan,” on page 52.

NOTE: When upgrading Novell SecureLogin from a previous version, make sure you have the same version running on the administrative workstation. For example, if you have Novell SecureLogin 7.0 installed on your administration workstation, you cannot administer data in the 6.0 version mode.

7.3.2 Upgrading to Novell SecureLogin 7.0 from Novell SecureLogin 3.5*x*

To upgrade from Novell SecureLogin 3.5*.x* versions:

1. On the Windows *Start* menu, click *Control Panel* > *Add/Remove Programs*.
2. Click *Novell SecureLogin on 3.5(.x)*, then click *Remove*.
3. If you are prompted to restart your workstation, click *Yes* to restart the workstation, or click *No* to restart later.

   Novell SecureLogin is now uninstalled.
4. Before installing the new version of Novell SecureLogin, log out and log in again.

7.4 Phased Upgrade

Novell SecureLogin does not currently support phased upgrades for Citrix or terminal services deployments.

Contact Novell Support for assistance on deployment issues.

7.5 Hot Desk and Mobile Users

Hot desking is the temporary physical occupation of a workstation or, work surface by a particular employee. The work surface can either be an actual desk or a terminal link. Hot desking is regularly used in large enterprises where employees are in spread across offices or geographical locations at different times, or at out of office for a long time.

An electronic kiosk houses a computer terminal that often employs custom kiosk software designed to function flawlessly while preventing users from accessing system functions.

Hot desk users do not work from a fixed workstation and their user data is stored on the directory.

For example, in a hospital environment, staff might be stationed in a different ward for each shift, and they are able to access their applications and data from any workstation.

When these users log in to Novell SecureLogin, their details are downloaded from the directory to the local workstation cache. All workstations accessed by Kiosk mode users must run the same version of Novell SecureLogin. If users log in to an upgraded workstation, they cannot access their Novell SecureLogin data on workstations running a previous version of the software.

7.6 Stopping Tree Walking

Checking for inherited values from higher level objects is referred to as “tree walking.” Each time the Novell SecureLogin user cache synchronizes with the directory, Novell SecureLogin checks for changed configuration data including preference values, password policies, preconfigured applications, and application definitions.

Novell SecureLogin data that is not manually configured at the user object level is automatically inherited from higher-level directory objects. To ensure that higher-level object settings are not inadvertently inherited by lower-level objects, you need to set the *Stop walking here* option to *Yes* before upgrading.

You can also use this option to limit directory traffic in organizations where the network is congested or geographically dispersed. Set his function at the organizational unit or container level to stop Novell SecureLogin from traversing the directory hierarchy past the specified level.

To set the *Stop walking here* option at the Users container:

1. Launch iManager, then select *Manage SecureLogin SSO* from the left pane.
2. Select *Preferences* from the drop-down list.
3. Select the *Stop walking here* option and change the value to *Yes*.
4. Click *apply*.

All user objects in the Users container inherits their Novell SecureLogin configuration from the Users container level and below.

7.7 Changing the Directory Database Version

Novell SecureLogin is backward compatible, so all workstations running previous versions continue to operate successfully after the directory is upgraded to the new version. Although the directory is upgraded, the Novell SecureLogin client on the workstation continues to function as the old version of Novell SecureLogin until you have upgraded all users to the new version and manually set the directory database version to the new version.

NOTE: The new features of Novell SecureLogin are not available to users who have not upgraded their client versions.

You can configure directory database versions at the user object, container, and organizational unit levels. We recommend that you set the database version at the container and organizational unit levels. This should help you manage the database and minimize the possibility of conflicting versions.

NOTE: To utilize the Novell SecureLogin 6.0 features such as the storage of single sign-on credentials on the user's smart card, encryption of the data store using PKI-based credentials, and the AES encryption algorithm support, the data store mode must be set to version 6.0.

To change the data store version:

1. Launch iManager, then select *Manage SecureLogin SSO* from the left pane.
2. Select *Advanced Settings* from the drop-down list.
3. From the *Select Version,* drop-down list, select the required version.

   You cannot select a version earlier than your current version
4. Click *Apply*. When the upgrade is installed on all the workstations, follow this same procedure to change the directory database version. The next time the directory server and the workstation caches are synchronized, Novell SecureLogin operates in the new version mode.

7.8 Deployment Prerequisites

Before you upgrade:

- Identify mobile and kiosk workstation users.

- Complete your migration plan. For more information on a migration plan, see Section 7.9, “Developing a Migration Plan,” on page 52
- Back up your Novell SecureLogin data by exporting to an XML file. For more information on exporting an XML file, see Exporting XML Settings in the *Novell SecureLogin Installation Guide*.
- Stop tree walking. For information on stopping tree walking, see Section 7.6, “Stopping Tree Walking,” on page 50.
- Close Novell SecureLogin. You cannot run the application during an upgrade.

7.9 Developing a Migration Plan

To ensure a smooth transition, it is recommend that you develop a migration plan. When you develop your plan, you need accurate information identifying the following:

- Version of Novell SecureLogin:
  - Set to run on the directory.
  - Installed on the administration workstation.
  - Installed on each user workstation.
- Time frame within which you must complete the full upgrade.
- Deployment method (automated or manual?)
- Total number of users.
- Which containers/organizational units each user belongs to.
- Number of kiosk mode users.
- Number of laptop users.
- Which users, if any, you need to upgrade first.
- A list of applications required to be enabled for Novell SecureLogin.

This information is the basis of the migration plan. You can develop and document migration plans in a variety of ways; the following is an example of one method.

7.9.1 Example of a Migration Plan

The Organization

Acme is an organization with a total of 30,000 users. 16,000 are allocated a fixed workstation, 3,000 are laptop users, and 11,000 access applications in Kiosk mode. The network environment is Microsoft Active Directory, and Novell SecureLogin version 3.5 is currently implemented. All users are managed from one administration workstation. ZENworks® is used for application distribution and deployment generally occurs overnight.

Sales OU users have laptops for mobile access to the network. The Central Administration OUs contain a combination of static workstations and laptop users. Manufacturing and Purchasing OU users are mobile; workstations are accessed in Kiosk mode. Users in the remaining OUs are each allocated a workstation for their sole use.

The Java functionality provided by the new version of Novell SecureLogin is eagerly awaited by users in the Sales group, so they have volunteered to test the upgrade. After the upgrade is successfully deployed to the Sales group, Novell SecureLogin is deployed in stages to the rest of Acme.

Upgrade Order

1. Directory and test user
2. Sales
3. Central Administration and Human resources
4. Account Marketing
5. Manufacturing and Purchasing
6. Administration Workstation

Week 1

Day 1: Upgrade the server directory; extend the schema, and assign rights to the organizational units. Ensure that all containers and organizational units have the following:

- Directory database version 3.5.
- *Stop tree walking* preference value is set to *Yes*.

Create a test user in the Sales OU and change the setting for the user object to directory database version value *3.5*.

Test single sign-on enabling of required application

Day 2: On successful deployment of the upgrade for the test user, manually set the directory database version to *6.0* on the Sales OU to enable full upgrade functionality.

Deploy the Novell SecureLogin upgrade on all Sales OU workstations/laptops. Assist Sales users with single sign-on enabling for Java applications.

Ensure that all laptop users have the Novell SecureLogin Cache setting enabled to ensure that the cache is stored locally.

Day 3: Monitor any upgrade issues for the upgraded Sales OU users. If all issues have been resolved successfully, install the Novell SecureLogin upgrade on all laptops and workstations associated with the Central Administration and Human Resources OUs.

Set the directory database version to 6.0 on the Central Administration and Human Resources OUs to enable full upgrade functionality.

Day 4: Install the Novell SecureLogin upgrade on workstations associated with the following OUs:

- Accounting
- Marketing

Day 5: Review and resolve any issues.

Day 6: Install the Novell SecureLogin upgrade on workstations associated with the following OUs:

- Manufacturing
- Purchasing

Review any upgrade issues encountered by Central Administration OU users. If there are no problems, change the Directory Database version to *6.0* setting for the following OUs:

- Accounting
- Marketing

Week 2

Day 7: All users now have upgraded the Novell SecureLogin application installed.

Review and resolve any issues.

Upgrade the administration workstation.

Day 8: If all issues are resolved successfully, change the directory database version to *3.5* for all remaining OUs.

Ensure that the following OUs are also enabled simultaneously to provide service for mobile and Kiosk users:

- Manufacturing
- Purchasing

The changeover is planned to occur at midnight and all users have been requested to log out prior to or at this time and wait until 12.10 am before logging back in.

Day 9: Migration is completed. Review of the migration plan commences.

Troubleshooting

8

This sections provides information to troubleshoot some of the issues encountered when using Novell SecureLogin in a Citrix environment.

SLLauncher Fails To Launch SLBroker

Source: With Novell SecureLogin 6.1 and later, SLLauncher is not needed. However, it is still available for backward compatibility.

Explanation: The requirement does not require the new `SLNRMonitorServer.exe` and `SLWTS.exe` to run for all published applications and want only SL* executibles to be active when launched by SELECTED SSO enabled published applications.

All SecureLogin components must remain dormant until a Novell SecureLogin enabled published application is launched.

Possible Cause: With Novell SecureLogin 6.1, single sign on does not occur for published applications unless `SLNRMonitorServer.exe`, `SLWTS.exe`, or SLProto are already running. If these are not available in task manager, single sign on does not occur when a published application configured with `SLLauncher.exe` is launched. The task manager shows SLLauncher as active, but does not show SLBroker

Action: The group that manages Citrix must be able to test or troubleshoot issues by logging in to the Citrix servers either with SecureLogin enabled or disabled.

To resolve:

1. On the Citrix server start regedit and go to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.
2. Double click on *AppSetup* entry and remove `sllauncher.exe`, `slwts.exe` from the value.

   All published applications that have a single sign on service are no longer available because `slbroker.exe` is not no longer started through `slwts.exe`.
3. Create a separate published application for each published application that requires single sign on service by adding `sllauncher.exe` before the name of the application.

   The behavior is now similar to the behavior prior to Novell SecureLogin 6.1.

   IMPORTANT: As with pre-6.1 releases, switches are not required to be specified after the application name.
