Schlumberger

Schlumberger Smart Card Login 4.1

Schlumberger Smart Card Login 4.1 User's Guide

Trademarks

Schlumberger, Cyberflex, and Cryptoflex are trademarks or registered trademarks of Schlumberger.

Entrust is a registered trademark of Entrust Technologies, Inc. IBM is a registered trademark of IBM Corporation. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Netscape, Netscape Communicator, and Netscape Navigator are registered trademarks or trademarks of Netscape Communications Corporation. Pentium is a registered trademark of Intel. Sun and Java are trademarks of of Sun Microsystems, Inc.

Document Edition	Date
C300470	21 November 2001

Schlumberger Austin Product Center
8311 North FM 620 Road
Austin, Texas 78726 USA

Schlumberger Smart Card Login

Contents

Schlumberger Smart Card Login

The Schlumberger Smart Card Login uses the Graphical Identification and Authentication dynamic-link library (DLL), referred to as the GINA, to enable a user to create a secure login through a personalized smart card to a PC. The Cryptographic Object Viewer and Editor (COVE), an application used to format a smart card to prepare it for the cryptographic operations required by the card's program, includes all functions necessary for GINA to provide secure logins.

COVE comes in two versions, the COVE User Tool and the COVE AdminTool, included in the Cyberflex Access Integration Kit and Software Developer's Kit:

- The COVE User Tool is intended primarily for secure login (GINA) configuration on a personalized card.

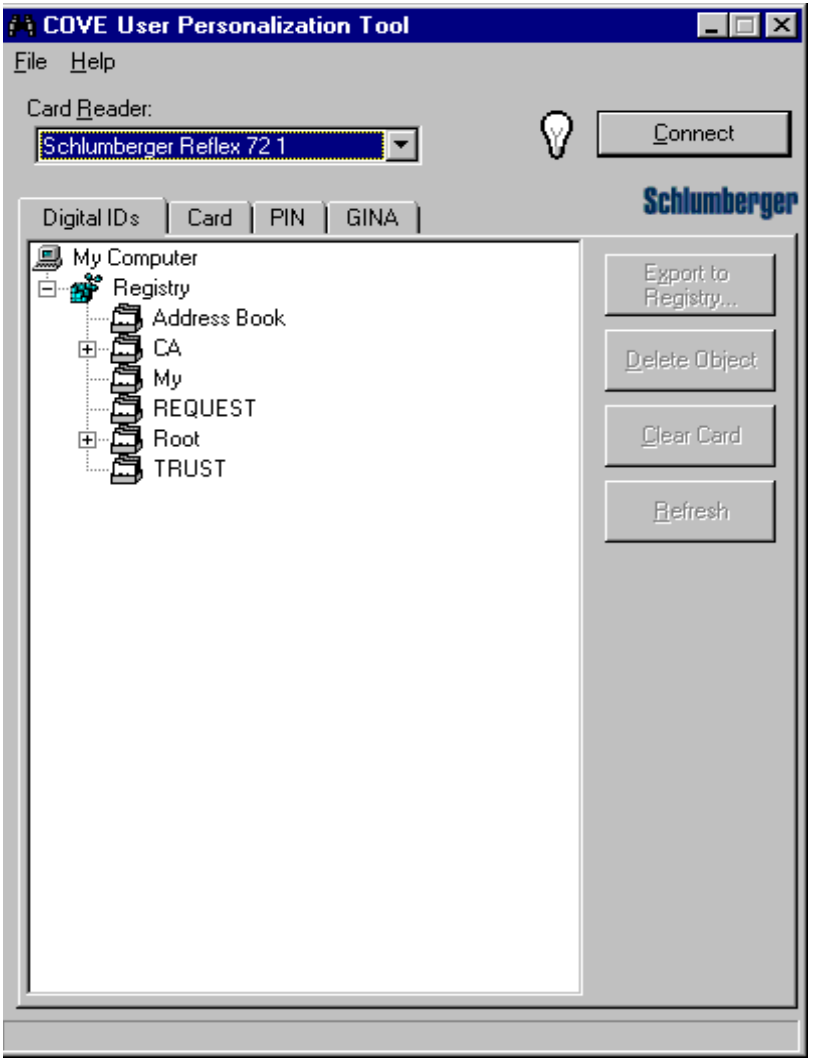
NOTE *The COVE User Tool does not have the functions to "personalize" a card for secure login configuration, so you must use a card that has already been personalized for GINA use. To install the COVE User Tool, follow the installation instructions in the Cyberflex Access Integration Kit 4.1 User's Guide.*

- The COVE Admin Tool includes both personalization functions and GINA among its many other features.

NOTE *GINA is only available for Windows NT4 and Windows 2000 platforms.*

Starting the COVE User Tool

Start the COVE User Tool by selecting **Start -> Programs -> Cyberflex Access IK 4.1 -> Cove User Tool 4.1**. The Cove User Personalization Tool window appears as in the following example.



You must connect to a smart card inserted in a reader before some of the COVE functions, such as the buttons on the right of the window, are available for use. (Choose the smart card reader you want from the pull-down list if you have more than one reader installed on your system.) COVE will attempt to connect with the card when you insert it in the reader. Use the **Connect** button if necessary to establish communication with the card.

As you can see, the COVE User Tool window has four tabs: Digital IDs, Card, PIN, and GINA. You only need to use the GINA tab for setting up GINA logins, so the other tabs are briefly described for an overview of the tool first.

The Digital IDs Tab

The Digital IDs tab displays a list of all digital certificates in the host system's registry. If you have connected to a smart card, the Digital IDs tab shows whether the card has been personalized and shows any certificates stored on the card.

You can use the Digital IDs tab to examine the host system and card certificates, remove items that are not needed, and copy certificates from the card to the registry.

Contents of the Registry Tree

The digital certificates registered on the host system appear in the Registry tree, which contains these folders:

- **Address Book** — Certificates of email correspondents who have sent you email from Outlook or Outlook Express
- **CA** — Certificates of certificate authorities, used to verify correspondents' certificates
- **My** — Your personal certificates
- **REQUEST** — Certificate requests that have not been processed
- **Root** — Self-signed certificates, used as the basis for trust trees
- **TRUST** — Certificates designated as trustworthy without proof from a certificate authority

Deleting Digital ID Data from the Registry or the Card

To delete an item, follow these steps:

1. Highlight the item you want to delete in the Digital IDs tab.You can delete any of these items:
   - A certificate registration or request from the Registry tree (but not a folder)
   - A certificate from the personalization files on the card

   When you have selected an item you can delete, the Delete Object button is activated. If you select an item that you cannot delete, the Delete Object button appears dimmed.
2. Click the **Delete Object** button.

   COVE removes the object.

Clearing All Certificates and Associated Data from the Card

To clear all digital IDs and associated data that is currently on a card, follow these steps:

1. Highlight a card certificate in the Digital IDs tab display area.

   The Clear Card button is activated (no longer appears dimmed).
2. Click the **Clear Card** button.

   COVE removes all the digital IDs and associated keys from the card. The card's personalization files remain on the card, ready to receive new digital signatures and keys.

Exporting a Certificate to the Host Registry

When you download a certificate to a card, the certificate is automatically registered on the host system. If you download the certificate on one system, then use the card on another system, you must register the certificate on the new system. You cannot use the certificate until it is registered on the host system you are currently using.

You can use the Digital IDs tab in the COVE User Tool window to register certificates that were downloaded to the card on other host systems:

1. Highlight a card certificate in the Digital IDs tab display.

   The Export to Registry button is activated (no longer appears dimmed).

2. Click the **Export to Registry** button or drag-and-drop the certificate to the registry.

   COVE automatically exports the certificate data to the host system's registry.

3. Continue this process until all the certificate data is registered. (You do not register the certificates' associated keys.)

NOTE *Windows 2000 and Windows XP systems automatically export certificates in the default container when the card is inserted, but Windows 98, Me, and NT do not provide this feature. So, with Windows 2000/XP, you must explicitly export certificates stored in any container other than the default, and with Windows 98/Me/NT, you must explicitly export all certificates. If you are using PKCS #11-based PKI (Public Key Infrastructure), it is not necessary to export the certificate, but it might be necessary if you are using CryptoAPI-based PKI.*

Refreshing the Digital ID Tab Display

To refresh the display in the Digital ID tab, click the **Refresh** button.

COVE reloads the digital IDs from the host system registry, and the digital IDs from the card.

The Card Tab

The Card tab shows the card's current personalization settings and associated cryptographic contents. You can use the Card tab to view these settings. To add a label to the card or change the existing card label, enter the new value in the Card Label box and click the Apply button.

The PIN Tab

You can use the PIN tab to change the user PIN value. Enter the current PIN and then the new PIN value in the appropriate boxes on the window and then click the Change PIN button.

NOTE *The PIN tab is enabled only if the currently connected card contains a PIN. When a blank card is personalized, a PIN is added to the card.*

The GINA Tab

Winlogon is a component of the Microsoft Windows NT/Windows 2000 operating system that provides interactive logon support by combining the Winlogon executable program, a Graphical Identification and Authentication dynamic-link library (DLL)—referred to as the GINA—and any number of network providers.

The GINA is a replaceable DLL component that is loaded by Winlogon. The GINA implements the authentication policy of the interactive logon model, and is expected to perform all identification and authentication user interactions. In this case, GINA DLLs can implement smart-card authentication mechanisms to be used in place of the standard Windows NT/Windows 2000 user name and password authentication. Winlogon can also load zero or more network providers to perform secondary authentication.

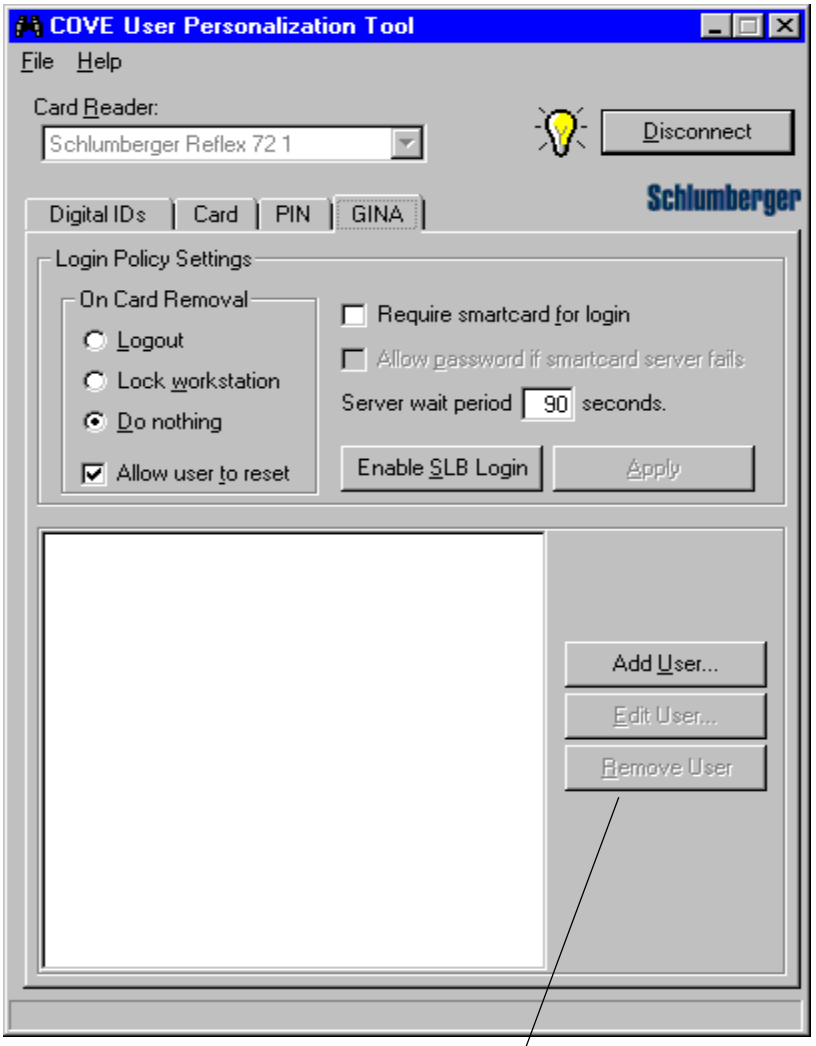
NOTE *The COVE User Tool does not include personalization functions (the COVE Admin Tool has the personalization functions). So, you must have a card that has already been personalized specifically for use with GINA before you can set up a secure login on it with the COVE User Tool.*

Setting Up Secure Logins with GINA

To set up a secure GINA login on your system for one or more users on a smart card, follow these steps:

1 Login to your system as a user with administrative privileges to be sure you have access to all of the functions on the GINA tab.

2 Click the GINA tab to display the following window as shown in the following illustration.



If the card has not been personalized for GINA, the user section does not appear on this window.

3. Decide how you want the system to behave when the user removes the smart card from the reader, and check the appropriate radio button (you must be logged in as a user with administrative privileges to have access to these functions):
   - **Logout** means the user will be logged out but the system will remain available to other users.
   - **Lock workstation** means the user will not be logged out, but the workstation will be locked, and a user will have to unlock it to regain access.
   - **Do nothing** means the user will not be logged out and the system will remain available.
4. If you want to let the user choose another one of these options after login, check the box next to **Allow user to reset.**
5. If you want the system to be accessible *only* through a smart card GINA login, check the box to **Require smart card for login**. This prevents the alternative of password logins through Ctrl-Alt-Del. This setting will take effect when you reboot the host system.
6. To allow password logins through Ctrl-Alt-Del (if the server is unavailable, for example), check the box to **Allow password if smart card server fails**. If you do not allow this option then the user will be unable to login until the server starts successfully. This setting will take effect when you reboot the host system.
7. Specify the amount of time in seconds that you want to wait for the server to respond in the **Server wait period** field.
8. Use the **Add User** button on the lower part of the GINA tab to specify the user or users who will have GINA logins. You can return to this tab as needed to manage the user list with the other buttons: Edit User and Remove User.

   See the following sections for details about adding, editing, and removing users.
9. When you are satisfied with all the settings, click **Enable SLB Login** to activate GINA. This will take effect when you reboot the host system.

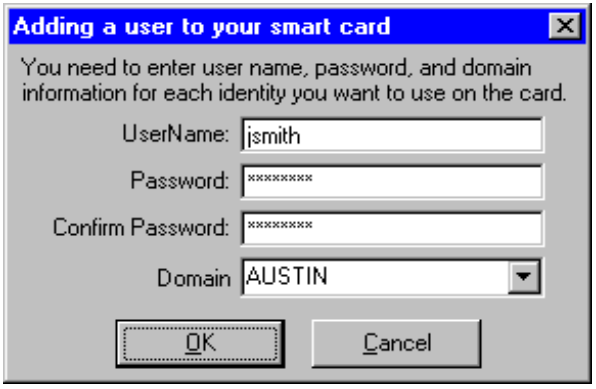
10 Click **Apply** to activate and save the GINA settings for "On Card Removal." After these settings are applied, the **Apply** button will become inactive (dimmed). These settings will take effect immediately.

Adding Users

To specify the user or users who will have GINA logins, follow these steps:

1 Click the **Add User** button on the lower part of the GINA tab. (This user part of the GINA tab only appears with a personalized card.)

This dialog box appears:



2 Enter the user name and password (twice to confirm) for each user that you want to include on the card. These entries must conform to Windows NT/2000 name and password requirements, and must match the normal login name and password for that user in the specified domain.

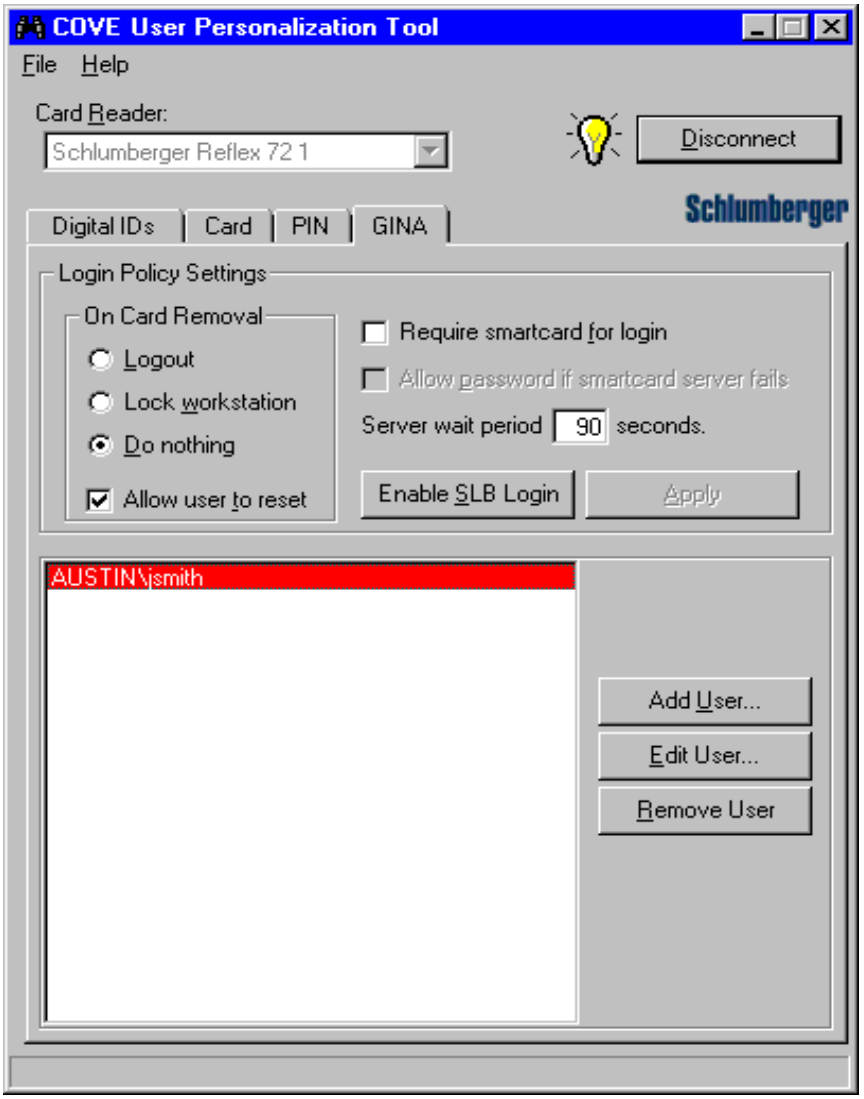
3 In the drop-down **Domain** box for each user, choose the domain for the user to log in. The list shows all the domains in the local network that are known to the host system. You can choose a domain that enables the user to log in from any system in the network, you can restrict the user to the domain on the host machine, or you can enter another domain in the editable field.

4 Click **OK** when you have finished adding the user.

You are asked to enter your PIN number (created when your card was personalized) to show you have the authority to add this user, as in this example.

5 Enter your PIN number and click OK.

6 The added user appears in the list on the GINA tab, as shown in the example below. All user additions, deletions, and changes take place immediately.

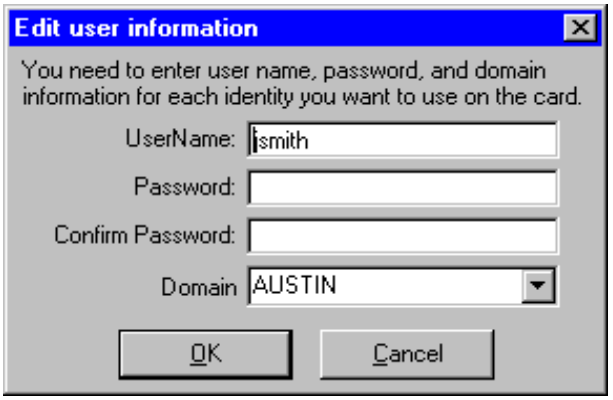


"Could not add user" Error

If you get an error message that says "Could not add user" when you click OK in the Add User dialog box, one explanation could be that you tried to add more GINA users than your card was configured to accept when it was personalized. If that is the case, the card either needs to be re-personalized to accept additional GINA users or you need to find another card for the user you wanted to add.

Editing and Removing Users

To change a user's secure login name, password or domain, go to the GINA tab, click the user you want to change and then click the **Edit User** button to display this dialog box:



Make your changes and click **OK** when done.

To remove a user, click the user name on the GINA tab and then click the **Remove User** button.

Troubleshooting

If for some reason you cannot login to your system as usual through the Schlumberger GINA, try the following "safe-mode" alternatives to gain access by modifying settings either through COVE or through your system registry.

Reboot your computer and go into "safe mode" (usually, you can press the F8 key to enter safe mode when you see the message "please select the operating system to start").

If you can start the COVE UserTool, click the GINA tab and change the settings in one of these ways:

- Check the box to "Allow password login if smartcard server fails" and then click the Apply button. The change will take effect when you reboot your system. You can then login through the standard Microsoft password login dialog as long as the smart card server is not responding.
- Click the **Disable SLB Login** button to disable the Schlumberger secure login. The change will take effect when you reboot your system. You can then login through the standard Microsoft password login dialog until you enable the secure login again.

If you cannot start COVE, you can use the Windows **regedit** command to make a change in your system's registry login setting:

1. Click **Start** → **Run...** to display the Run dialog box.
2. Type **regedit** in the Open field and click OK. The system's Registry Editor window appears.
3. Use the tree structure and folders on the left to locate the Winlogon folder following this path:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`
4. Modify the GinaDLL variable to change it from the Schlumberger secure login to the standard Microsoft login, using the following values:

Schlumberger Secure Login	Microsoft Login
GinaDLL = "slbgina.dll"	GinaDLL = "msgina.dll"

5 Save your changes and reboot your system normally. You can go back to the registry (or use COVE) and reset the login to the Schlumberger secure login when your problems have been resolved.