



SmartLock® Surf

OPERATOR GUIDE

October 2009

Table of Contents

Introduction.....	5
Server PC Requirements.....	6
Client PC Requirements.....	6
Step 1. Software Installation.....	7
Step 2. Firewall	7
Step 3. Port Listening	8
Step 4. Network Setup	11
• Wide Area Network (WAN)	11
Step 5. Server Setup	12
• Surf Server.....	12
• Pro Server	14
• Password Setup	15
• User Accounts	16
Step 6. Readers	17
• Starting the Browser	17
• Add Readers.....	18
• Edit and Delete Readers.....	21
• Reader Status	21
• Reader Commands.....	22
• Reader Communications	22
• Communication Statistics	23
• Download Controllers.....	24
• Update Date and Time.....	24
• Daylight Savings Time.....	24
• Door Unlock Schedules	26
Step 7. Cardholders	28
• Access Schedules.....	28
• Holiday Schedules	28
• User Profiles.....	29
• Add Cardholders	31
• Edit and Delete Cardholders	34
• Cardholder Searches	34
• Search Tips.....	35

Step 8. History and Audit	36
• Setup	36
• Panel Memory	37
• View History	37
• History Filters	37
Appendix	40
• File and Software Overview.....	40
• Data Backup.....	41
Index.....	42

Copyright © 2009 Cansec Systems, Ltd.
All rights reserved.

Introduction

Connect to your access control system from anywhere in the world with Cansec's browser-based SmartLock Surf software. Whether you are working from home, on the road, or just out of the office, SmartLock Surf keeps you connected - all you need is internet access!

SmartLock Surf supports 4,800 users and up to 30 doors. Surf also supports 10 concurrent client connections, so up to 10 users can connect and manage the access control system at the same time.

Using Internet Explorer, users can connect to a server computer running SmartLock Surf from virtually anywhere.



Key Features

- Browser-based
- Supports 10 simultaneous client connections
- Connect to your system over the internet
- 4,800 cardholder/user capacity
- 30 door capacity
- Real-time communications
- Programmable access profiles
- Programmable holidays
- Automatic door unlock schedules
- Extremely easy to learn and use

Server PC Requirements

- Pentium 4, 1.2 GHz processor
- Windows® 2000, Windows® XP or Windows® Vista (32-bit)
- 256 MB of memory, 20 GB hard disk space
- Network adapter (if using Canlan network communications device)
- USB port (if using CLAUSB serial communications device)
- Static IP address
- Firewall open to port 80 and 5800 to incoming traffic from specified local and remote access

Client PC Requirements

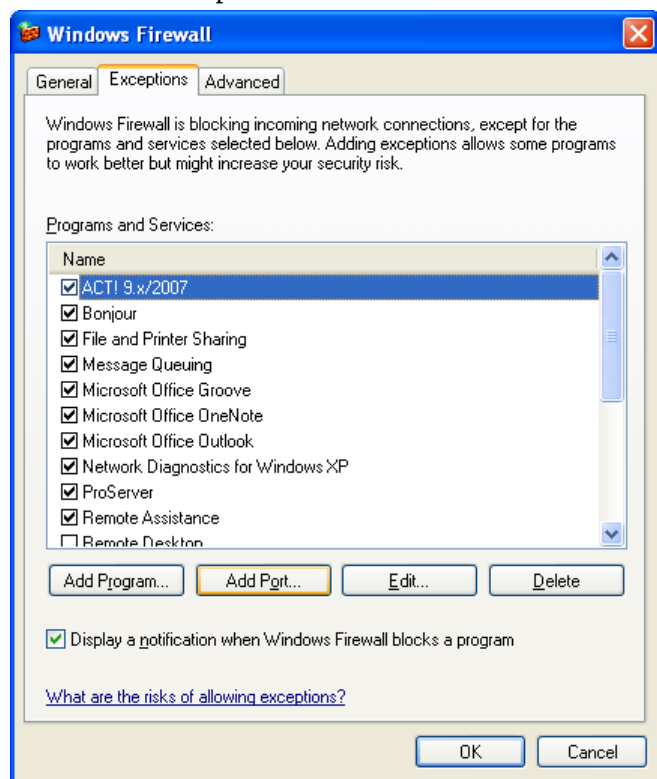
- Internet Explorer 7.0 or higher
- Internet connection

Step 1. Software Installation

1. Insert the SmartLock Surf software CD into the server PC's CD drive.
2. At the welcome screen, click **Next**.
3. Enter the software key that came with your CD.
4. Enter your company information.
5. Choose **Complete Install**.
6. Click **Install** to begin the installation.
7. Click **Finish** to complete the installation.

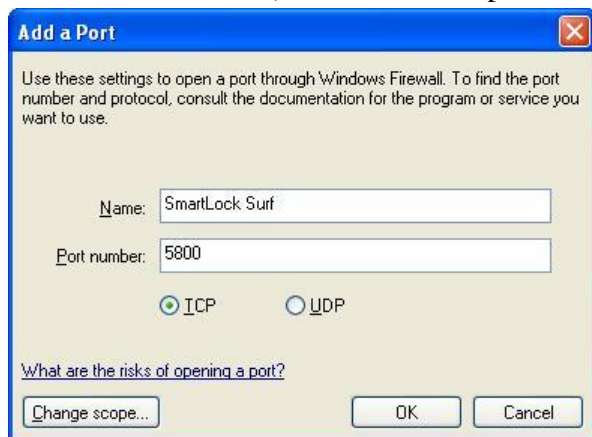
Step 2. Firewall

1. Go to **Start > Control Panel > Windows Firewall**.
2. Click the *Exceptions* tab.



3. Click **Add Port...**

4. In the **Name** field, enter a descriptive name for the port.

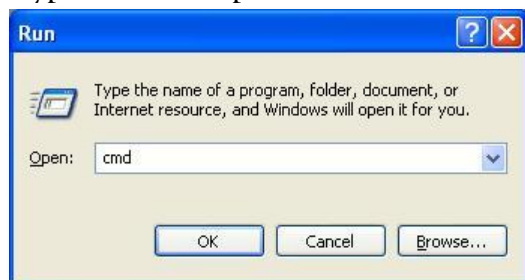


5. In the **Port Number** field, enter **5800**.
6. Click **OK** to save the port changes.
7. Repeat the above steps for **port 80**.
8. Click **OK** to close the *Windows Firewall* window.

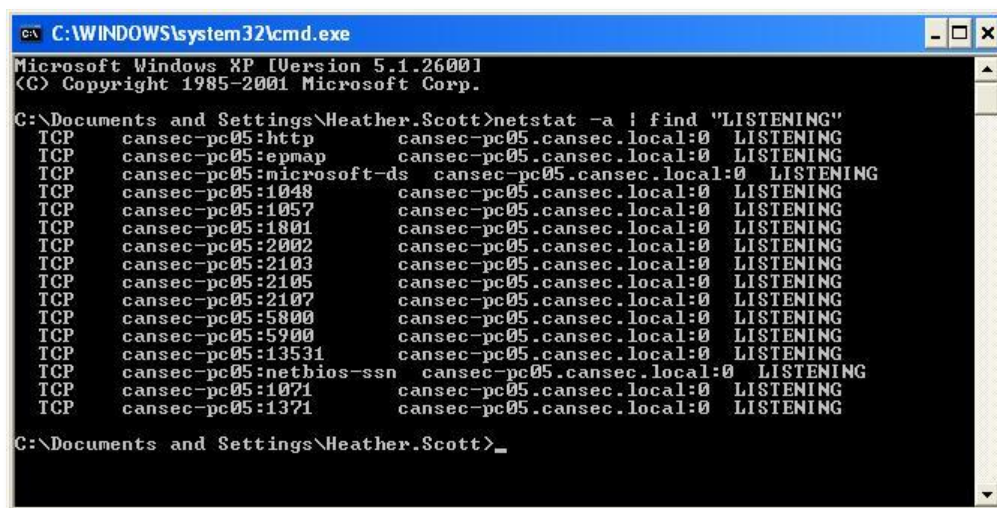
Step 3. Port Listening

Port 5800 is used by SmartLock Surf. If other applications are listening on, or connected to port 5800, they must be closed. SmartLock Surf will not function if port 5800 is not free.

1. Close *Pro Server* and *Surf Server* if running.
2. Go to **Start > Run**.
3. Type **cmd** and press **OK**.



4. At the command prompt, type: **netstat -a | find "LISTENING"**.
5. Press **Enter**.
6. A list of port numbers will be shown. If port 5800 appears on the list, an application is listening on port 5800. SmartLock Surf will not function until this application is closed.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Heather.Scott>netstat -a | find "LISTENING"
TCP    cansec-pc05:http           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:epmap          cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:microsoft-ds   cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:1048           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:1057           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:1801           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:2002           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:2103           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:2105           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:2107           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:5800           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:5900           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:13531          cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:netbios-ssn    cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:1071           cansec-pc05.cansec.local:0 LISTENING
TCP    cansec-pc05:1371           cansec-pc05.cansec.local:0 LISTENING

C:\Documents and Settings\Heather.Scott>
```

NOTE: If you know which application is listening on port 5800, you can close it using Windows® Task Manager:

1. Press **CTRL+ALT+DEL**.
2. Click on the *Processes* tab.
3. Select the appropriate process and click **End Process**.

7. If you do not know which application is listening on port 5800, download a free port scanner application such as Nmap.

EXAMPLE: Using Nmap

1. Download and install Nmap.
2. Go to **Start > Run**.
3. Type **cmd** and press **OK**.
4. At the command prompt, type: **cd "C:\Program Files\Nmap"**
5. Press **Enter**.
6. Type **nmap.exe** and press **Enter**.
7. Type **nmap -sT -PN -p5800 [Server PC IP Address]**
8. Press **Enter**.
9. Nmap will list any applications (services) listening on port 5800 as shown below.

```
C:\Program Files\Nmap>nmap -sT -PN -p5800 10.0.0.62
Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-06-23 10:57 Eastern Daylight Time
Interesting ports on 10.0.0.62:
PORT      STATE SERVICE
5800/tcp  open  vnc-http
```

10. Use task manager to end the application or adjust the application's connection settings to prevent it from using port 5800.

Step 4. Network Setup

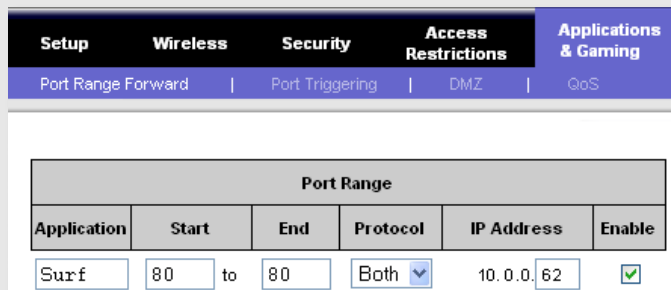
WIDE AREA NETWORK (WAN)

To allow remote computers on a WAN to connect to the Server PC running SmartLock Surf, you must configure the router to reroute any incoming traffic on port 80 to the Server PC.

1. Start your router's configuration software. For many routers, type the router's IP address into the address bar on your internet browser.
2. Choose port 80 as the forwarded port.
3. Enter the IP address of the Server PC running SmartLock Surf as the destination IP address.
4. Save the changes.

EXAMPLE: Using Linksys WRT54G Router

1. In your browser's address bar, enter the router's IP address.
2. Enter the username and password and press **OK**.
3. Click the **Applications and Gaming** tab.
4. In the **Port Range Forward** section, enter the following information:
 - Application Name = **Surf**
 - Start = **80**
 - End = **80**
 - IP Address = **[IP Address of the Server PC]**
5. Check the **Enable** box and click **Save Settings**.



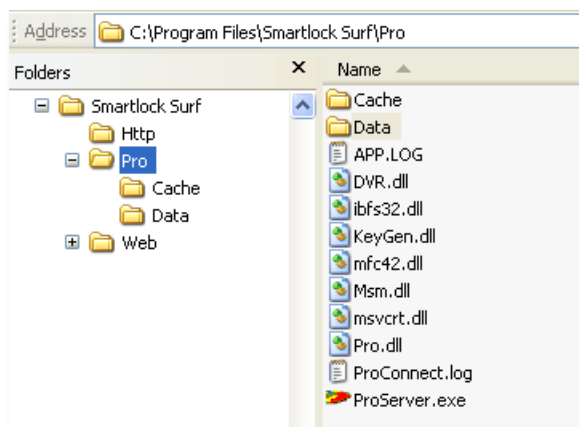
The screenshot shows the router's configuration interface with the 'Applications & Gaming' tab selected. Under the 'Port Range Forward' sub-tab, there is a table for configuring port forwarding. The table has columns for Application, Start, End, Protocol, IP Address, and Enable. A single entry is shown for 'Surf' with Start and End ports set to 80, Protocol set to 'Both', and IP Address set to '10.0.0.62'. The 'Enable' checkbox is checked.

Port Range					
Application	Start	End	Protocol	IP Address	Enable
Surf	80	to 80	Both	10.0.0.62	<input checked="" type="checkbox"/>

Step 5. Server Setup

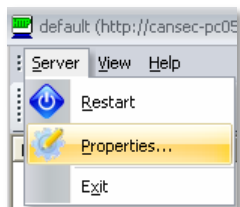
This section describes the initial steps to configure the SmartLock Surf system. These steps are typically done by the installation company or system administrator.

Software settings are saved to the default location C:\Program Files\Smartlock Surf\Pro\Data. *It is good practice to backup this data folder on a regular basis and when any significant changes have been made.*

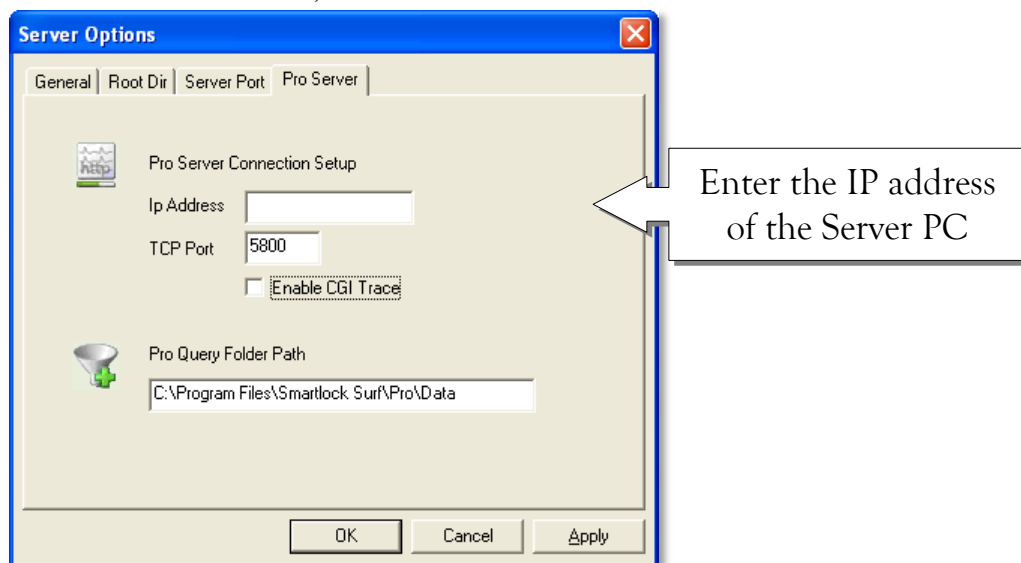


SURF SERVER

1. Go to **Start > All Programs > SmartLock Surf > Launch Surf Server**.
2. From the main menu, go to **Server > Properties**.



3. On the *Pro Server* tab, enter the **IP address** of the Server PC.



NOTE: if you do not know the IP Address of the Server PC:

1. Go to **Start > Run**.
2. Type **cmd** and press **OK**.
3. At the command prompt, type **ipconfig** and press enter.
4. The IP Address will be displayed as shown.

```
C:\Documents and Settings\Heather.Scott>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : cansec.local
    IP Address. . . . .               : 10.0.0.62
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 10.0.0.1
```

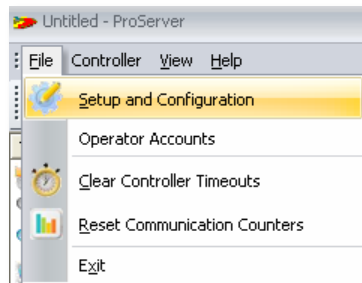
4. Enter **5800** in the **TCP Port** field.
5. Enter the path to the SmartLock Pro Server data folder.
Example: C:\Program Files\Smartlock Pro Server\Data.
6. Click **OK**.

PRO SERVER

7. Go to **Start > All Programs > SmartLock Surf > Pro Server**.
8. If you get an error message, port 5800 is not free. Repeat the instructions in *Step 3. Port Listening*.



9. From the main menu, go to **File > Setup and Configuration**.



10. If you are using a CLAUSB communications device, choose a communications port from the drop-down menu.

NOTE: If you do not know the port number:

1. Go to **Start > Control Panel > System**.
2. Click on the **Hardware** tab and choose **Device Manager**.
3. Expand the **Ports** section to display the port number (shown in brackets). *Refer to the CLAUSB configuration guide for jumper settings.*

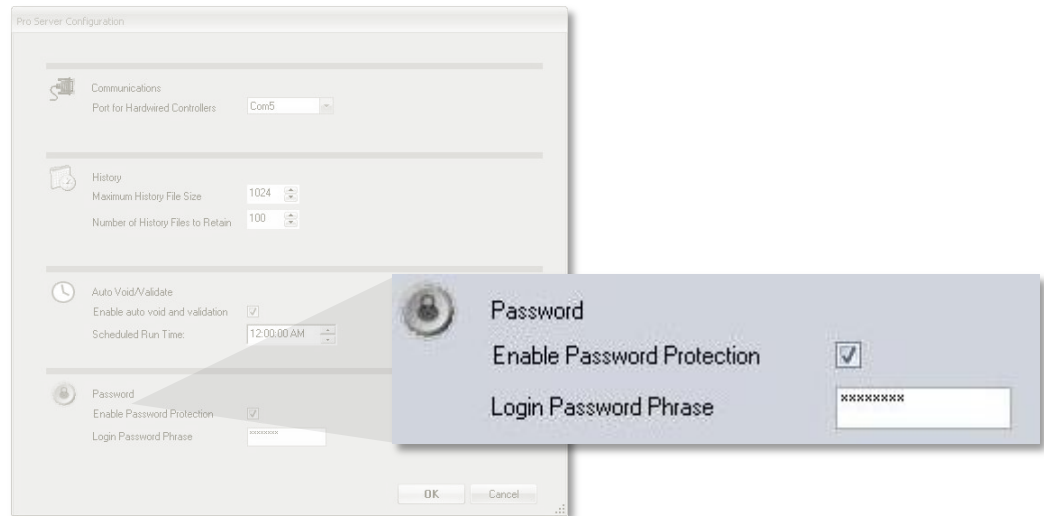


11. If you are finished configuring the system properties, click **OK**.

PASSWORD SETUP

To restrict access to the Pro Server software, follow the instructions below to require a system password when the software is run. *This section is optional.*

12. In the *Password* section on the *Pro Server Configuration* window, check **Enable Password Protection**.



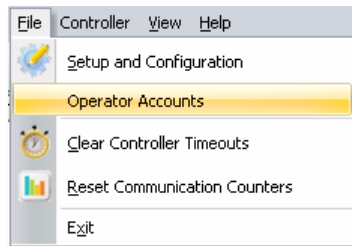
13. Enter a password in the **Login Password Phrase** field.
14. If you are finished configuring the system properties, click **OK**.

NOTE: for more information about configuring the History and Auto Void/Validate options, see *Step 8. History and Audit* and *Step 7. Cardholders*.

USER ACCOUNTS

Specify operator user names and passwords for people who will be managing the SmartLock Surf access control system. An operator must enter his or her user name and password before logging on to the SmartLock Surf software. *There is no default account, so you must set up at least one operator account.*

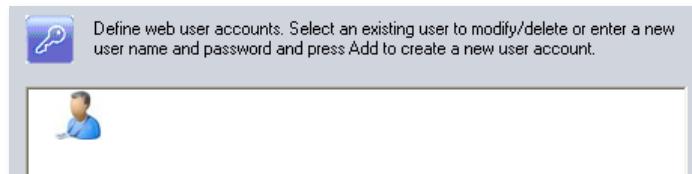
1. Go to **File > Operator Accounts**.




2. Click **New**.

A screenshot of the 'User Accounts' window. It has two input fields: 'User Name' and 'Password'. To the right of the 'Password' field are two buttons: 'New' (highlighted) and 'Delete'.

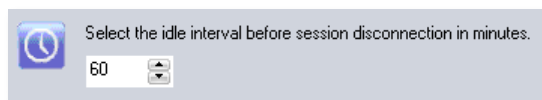
3. A new operator account icon will appear in the *User Accounts* window.



4. Enter a user name and password for the operator account.

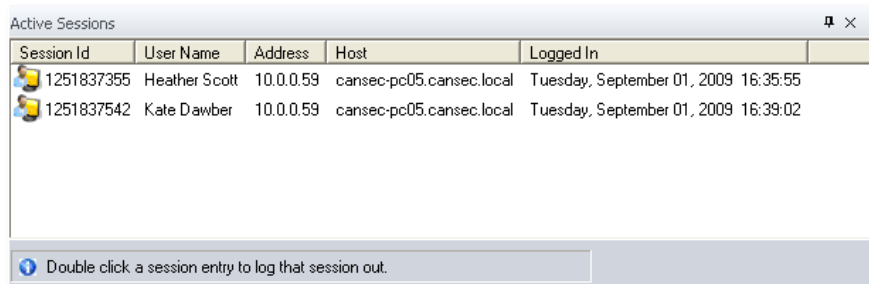
A screenshot of the 'User Accounts' window. The 'User Name' field now contains the text 'Heather Scott'. The 'Password' field is still empty. The 'New' and 'Delete' buttons are still present.

5. Create additional operator accounts if necessary. *There is no limit to the number of operator accounts.*
6. Operators will be automatically logged out of the SmartLock Surf browser after a specified period of inactivity (max. 60 minutes).
7. Enter a new interval if desired.

A screenshot of a dialog box for selecting an idle interval. It has a title bar with a clock icon and the text 'Select the idle interval before session disconnection in minutes.' Below the title bar is a numeric input field with the value '60' and a spin button.

8. Click **OK**.

9. Online users will appear in the *Active Sessions* section of the *Pro Server*.



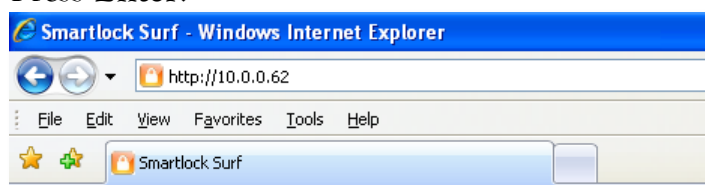
Session Id	User Name	Address	Host	Logged In
1251837355	Heather Scott	10.0.0.59	cansec-pc05.cansec.local	Tuesday, September 01, 2009 16:35:55
1251837542	Kate Dawber	10.0.0.59	cansec-pc05.cansec.local	Tuesday, September 01, 2009 16:39:02

Double click a session entry to log that session out.

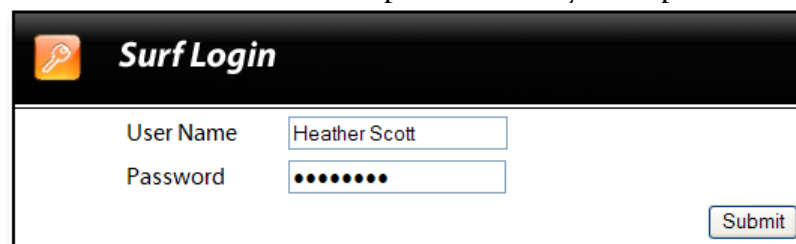
Step 6. Readers

STARTING THE BROWSER

1. Start *Pro Server* and *Surf Server* if not already running.
2. Launch **Internet Explorer 7.0**.
3. In the address bar, type the IP address of the Server PC.
4. Press **Enter**.



5. Enter the user name and password of your operator account.



Surf Login

User Name:

Password:

6. To log off, click the **Log Off** button.



ADD READERS

1. In the *Readers* section, click **Add New Reader**.



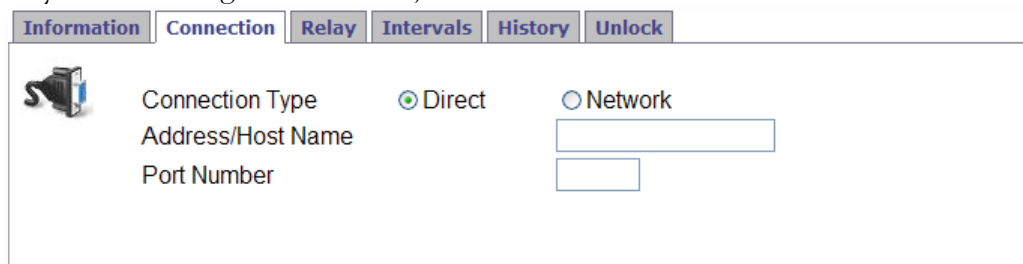
2. On the *Information* tab, enter the panel's unique address (1 to 30).


A screenshot of the "Information" tab in the software interface. It features a tab bar with "Information", "Connection", "Relay", "Intervals", "History", and "Unlock". Below the tabs is a form with three input fields: "Address" (containing "1"), "Reader Name" (containing "Front Door"), and "Exit Reader Name" (empty).

Information	Connection	Relay	Intervals	History	Unlock
 Address: <input type="text" value="1"/> Reader Name: <input type="text" value="Front Door"/> Exit Reader Name: <input type="text"/>					

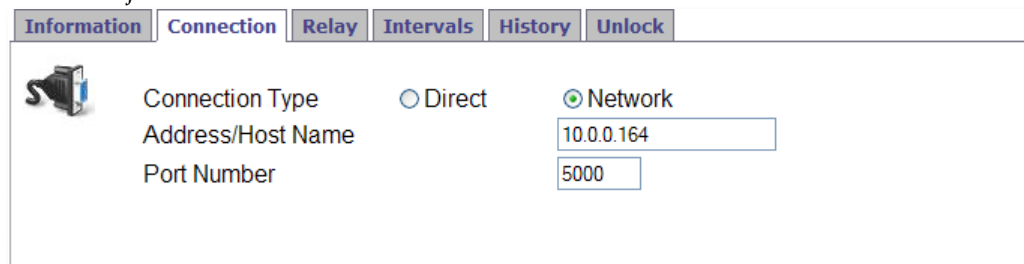
NOTE: the address of the panel is set using DIP switches 1 thru 6. Refer to the *SmartLock Installation Manual* for more details.


3. Enter a descriptive name for the reader and exit reader (if applicable).
4. Click on the *Connection* tab.
5. If you are using a CLAUSB, select **Direct**.

A screenshot of the "Connection" tab in the software interface. It features a tab bar with "Information", "Connection", "Relay", "Intervals", "History", and "Unlock". Below the tabs is a form with two radio buttons: "Direct" (selected) and "Network". Below the radio buttons are two input fields: "Address/Host Name" and "Port Number".

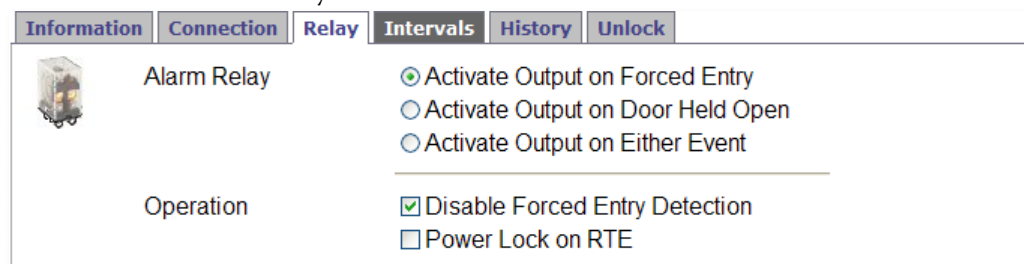
Information	Connection	Relay	Intervals	History	Unlock
 Connection Type: <input checked="" type="radio"/> Direct <input type="radio"/> Network Address/Host Name: <input type="text"/> Port Number: <input type="text"/>					


6. If you are using a Canlan, select **Network** and enter the IP address (or host name) and port number of the Canlan. See the *Canlan Installation Manual* for more details.



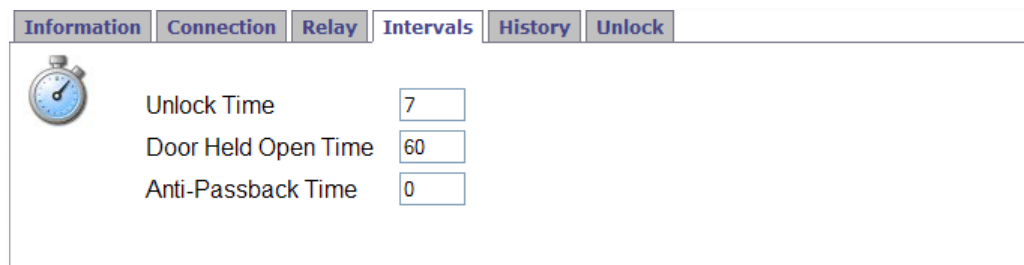
Information	Connection	Relay	Intervals	History	Unlock
	Connection Type	<input type="radio"/> Direct	<input checked="" type="radio"/> Network		
	Address/Host Name	<input type="text" value="10.0.0.164"/>			
	Port Number	<input type="text" value="5000"/>			


7. Click on the *Relay* tab.
8. The SmartLock control panel's built-in OP2 relay can be used to trigger a siren, strobe light, or other device when forced-entry or door-held-open events occur.
9. Select which event(s) will trigger the relay.
10. If door contacts are installed, but there is no request-to-exit button or pushbar at the door, a forced-entry event will occur whenever someone exits the door. To disable forced entry detection in this case, check the **Disable Forced Entry Detection**.



Information	Connection	Relay	Intervals	History	Unlock
	Alarm Relay	<input checked="" type="radio"/> Activate Output on Forced Entry <input type="radio"/> Activate Output on Door Held Open <input type="radio"/> Activate Output on Either Event			
	Operation	<input checked="" type="checkbox"/> Disable Forced Entry Detection <input type="checkbox"/> Power Lock on RTE			

11. If a request-to-exit button, pushbar, or similar device is installed at the door, check **Power Lock on RTE** to activate the lock when a request-to-exit event occurs.
12. Click the *Intervals* tab.

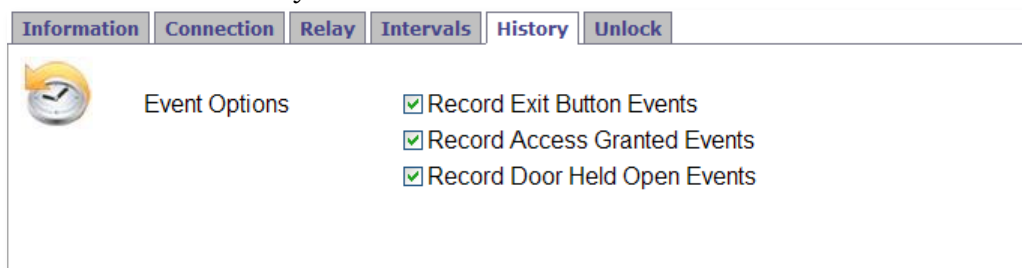


Information	Connection	Relay	Intervals	History	Unlock
	Unlock Time	<input type="text" value="7"/>			
	Door Held Open Time	<input type="text" value="60"/>			
	Anti-Passback Time	<input type="text" value="0"/>			

13. If desired, adjust the intervals.

Unlock Time	This is the number of seconds the door will remain unlocked after an access granted event.
Door Held Open Time	This is the number of seconds the door can be propped open before a door-held-open alarm event is generated at the PC. (Door contact required.)
Anti-Passback Time	This is the number of minutes before a cardholder can reuse his credential at a reader. Default time is 0 minutes (disabled).

14. Click on the *History* tab.



The screenshot shows a web interface with a top navigation bar containing tabs: Information, Connection, Relay, Intervals, History (selected), and Unlock. Below the tabs, there is a section titled 'Event Options' with a clock icon. To the right of this title are three checkboxes, all of which are checked:

- ☒ Record Exit Button Events
- ☒ Record Access Granted Events
- ☒ Record Door Held Open Events

15. Select the events that will appear in the browser's *History* window and stored in the audit file. If the control panel is not online with the PC, the events will be stored in the audit buffer.

16. Click **Save** to save the reader settings.

17. Repeat for all readers.

18. Refresh your browser to view the changes.

NOTE: for more information about configuring the *Unlock* settings, see the *Door Unlock Schedules* section on page 26.

EDIT AND DELETE READERS

To edit a reader's settings, click the reader you wish to edit and click the **Edit** icon on the sidebar.



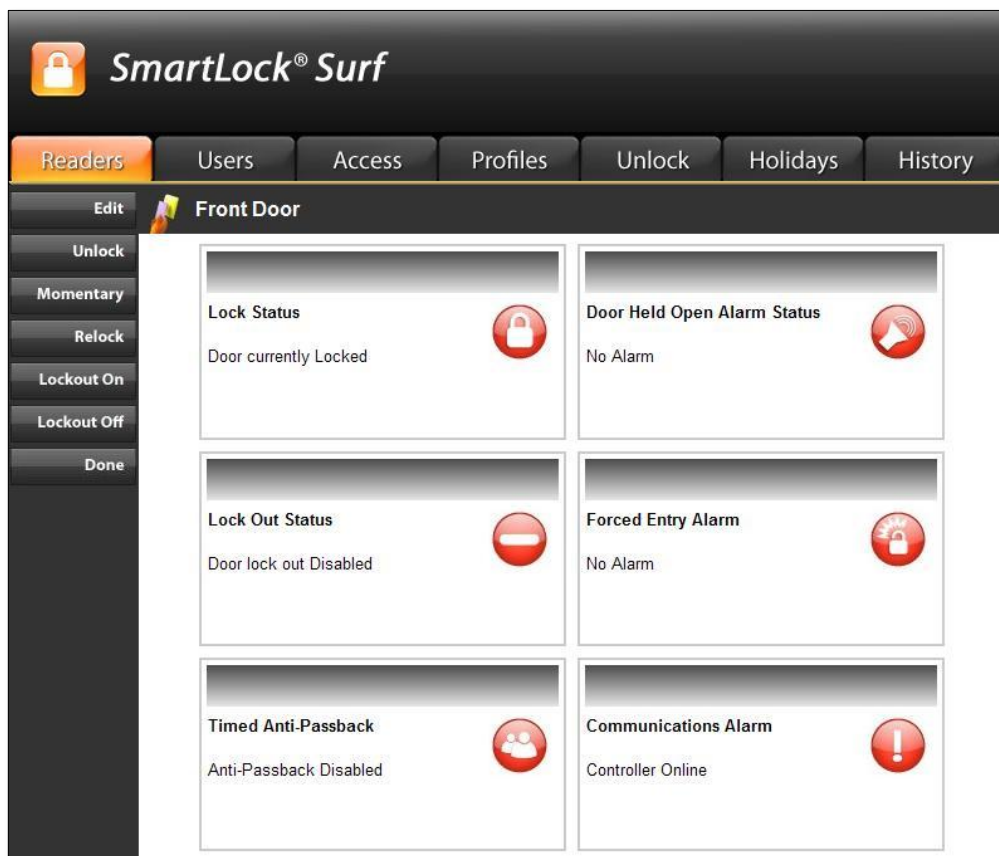
To delete a reader, click the reader you wish to delete, click the **Edit** icon on the sidebar and then click **Delete**.



Refresh your browser to view the changes.

READER STATUS

Click on a reader to view its status. Status notifications will be indicated in the appropriate box.



READER COMMANDS

Reader commands are available from the sidebar.

COMMAND	DESCRIPTION
Unlock	Unlocks a door in a maintained state. Door must be relocked by a command or by schedule.
Momentary	Unlocks a door momentarily for the time specified in the reader configuration.
Relock	Relocks an unlocked door.
Lockout On	Disables a reader so that no cardholders can unlock the door. Useful to prevent access to a hazardous area.
Lockout Off	Remove the Lockout condition from a “locked out” reader.
Done	Return to the main menu.

READER COMMUNICATIONS

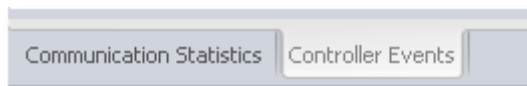
To test communications between the control panel and the communications device (CLAUSB or Canlan) initiate a momentary unlock command from the Server PC:

1. Click on the desired reader.
2. Click **Momentary** from the sidebar.



3. Bring up the *Pro Server* window.

- Click on the *Controller Events* tab.



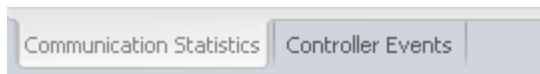
- The unlock event will be shown.

Controller Events						
Date	Time	Event	Name	Id	Location	
June 2...	15:21	Momentary Unlock By Remote	Unknown	0002041000	Controller 1	





COMMUNICATION STATISTICS

You can also test the communications between the control pannel and the communications device by checking the communication statistics from the Server PC:

- Bring up the *Pro Server* window.
- Click on the *Communication Statistics* tab.




- Online controllers are indicated by a **Green** icon and offline controllers by a **Red** icon.

Communication Statistics						
Unit	Name	Network	Net Status	Offline	Polls	Timeouts
 1	Controller 1	No		No	22942	0
 2	Controller 2	No		No	22910	0
 3	Controller 3	No		Yes	12	12
 4	Controller 4	Yes	Connecting	No	0	0

DOWNLOAD CONTROLLERS

If communications is lost with the controllers, you can download user data and reader configuration settings to the controllers manually once communications are restored.


1. Bring up the *Pro Server* window.
2. Click the **Download** icon from the toolbar. 
3. Select which panels will be updated and click **OK**.

UPDATE DATE AND TIME

The SmartLock Surf software synchronizes the date and time of all readers with the date and time of the Server PC. The date and time of all readers is automatically updated once a day if the following conditions are met:

- The readers are online
- The software is running
- A date and time command has not *already* been initiated on that day

To manually update the date and time of all your system's panels:

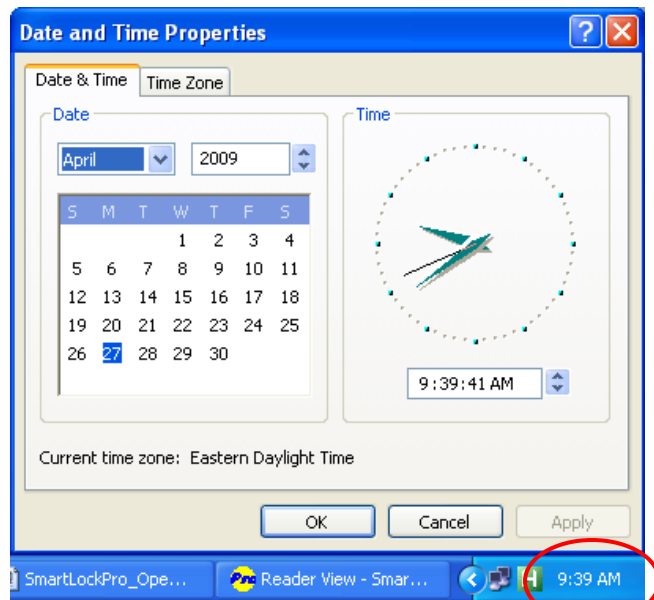
1. Bring up the *Pro Server* window.
2. Click the **Date and Time** icon from the toolbar. 
3. The date and time for all of the panels will be updated with the Server PC's date and time.

DAYLIGHT SAVINGS TIME

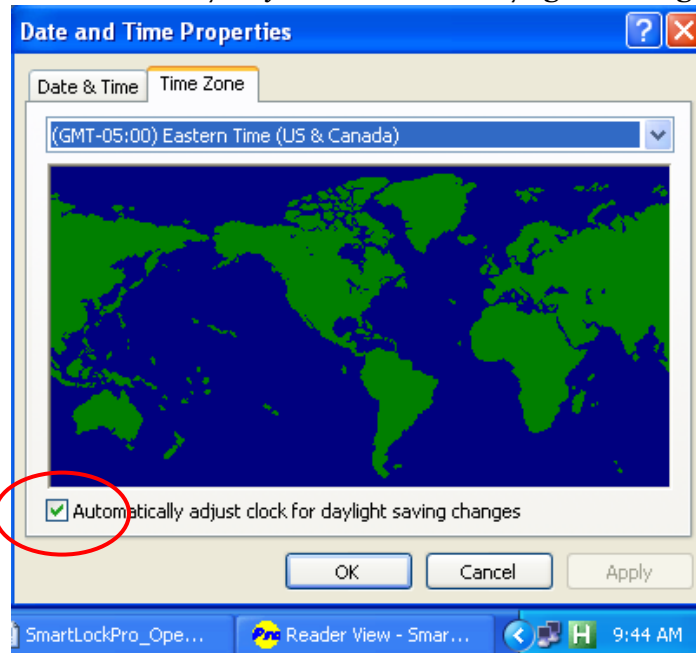
To manually adjust the date and time for daylight savings changes:

1. Make sure the date and time is correct on the Server PC.

2. To adjust the computer's date and time, double-click the time display on the taskbar.



3. To have the computer's time automatically updated when daylight savings changes occur, click the *Time Zone* tab and check **Automatically adjust clock for daylight savings changes**.



4. When the computer's date and time is correct, update the panels' date and time by clicking the **Date and Time** icon in the *Pro Server* window.

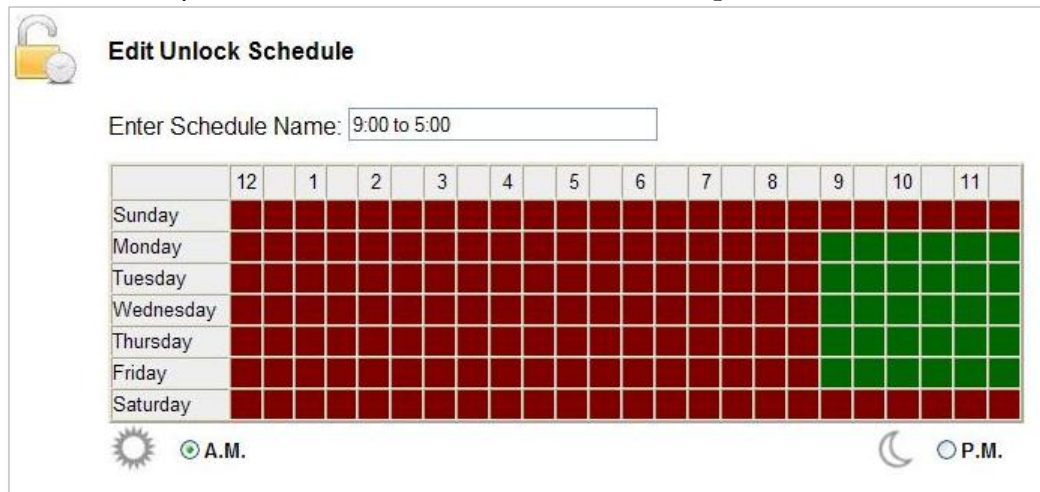
DOOR UNLOCK SCHEDULES

Unlock schedules automatically lock and unlock doors at specific times and days. To create a new unlock schedule:

1. Click the **Unlock** tab from the SmartLock Surf browser interface.
2. Click one of the 60 available unlock schedules.





3. Enter a name for the unlock schedule.
4. Click-and-drag to select the times and days when the door will be automatically unlocked. Selected times will turn green.



Edit Unlock Schedule

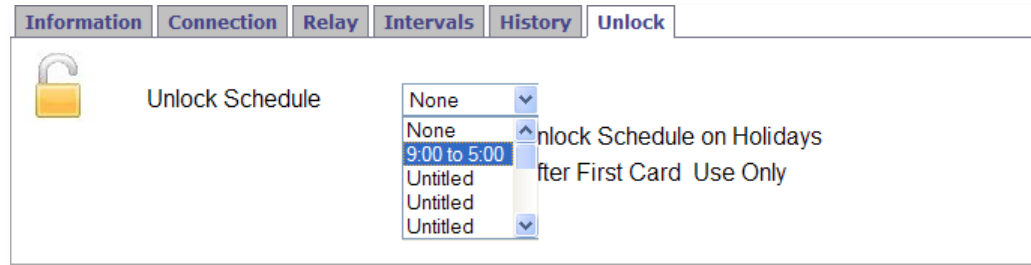
Enter Schedule Name:

	12	1	2	3	4	5	6	7	8	9	10	11
Sunday												
Monday												
Tuesday												
Wednesday												
Thursday												
Friday												
Saturday												


 ☒ A.M. ☐ P.M. 

5. Click **Save**.
6. Now associate the unlock schedule with a reader.
7. Click the **Readers** tab from the SmartLock Surf browser interface.
8. Click the desired reader and click **Edit** from the sidebar.
9. Click the *Unlock* tab.

10. Select the unlock schedule from the drop-down list.



Information Connection Relay Intervals History **Unlock**

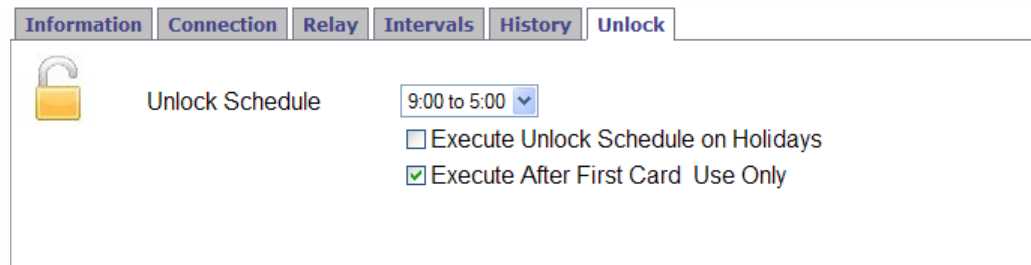
 Unlock Schedule

None
None
9:00 to 5:00
Untitled
Untitled
Untitled


Unlock Schedule on Holidays
After First Card Use Only

11. Check **Execute Unlock Schedule on Holidays** if you would like the door to automatically unlock *even* on holidays (see next section for programming holidays).

12. Check **Execute After First Card Use Only** if you would like the unlock schedule to take effect *only* after a valid access granted event.



Information Connection Relay Intervals History **Unlock**

 Unlock Schedule

9:00 to 5:00

☐ Execute Unlock Schedule on Holidays
☒ Execute After First Card Use Only

13. Click **Save**.

Step 7. Cardholders

ACCESS SCHEDULES

Access schedules specify when cardholders can use their credentials to access a door. To create a new access schedule:

1. Click the **Access** tab from the SmartLock Surf browser interface.
2. Click one of the six available access schedules.



3. Enter a name for the access schedule.
4. Select the days and times when cardholders can use their credentials to unlock a door.
5. Click **Save**.


HOLIDAY SCHEDULES

Holidays can be defined so that automatic door unlock schedules and access schedules do not take effect on the day specified. To create a new holiday:

1. Click the **Holidays** tab.
2. Double-click one of the 60 available holiday schedules.



- Use the arrows to select the month, and then click on the desired day.



Edit System Holiday

Select a new holiday date from the calendar, or press Cancel to return to Holiday View window

Holiday Date

June, 2009							
Today							
wk	Sun	Mon	Tue	Wed	Thu	Fri	Sat
22		1	2	3	4	5	6
23	7	8	9	10	11	12	13
24	14	15	16	17	18	19	20
25	21	22	23	24	25	26	27
26	28	29	30				

Select date

- Click Save.

NOTE: Holidays do not repeat and should be updated on a yearly basis.

USER PROFILES

User profiles specify which doors a group of cardholders can access, and link those doors with access schedule that define when those cardholders can access them. To create a new user profile:


- Click the **Profiles** tab.
- Click **Add New Profile**.



- On the *Name* tab, enter a name for the user profile.
- On the *Access* tab, select a reader (or readers).

- Click an access schedule to apply it to the reader.


Name **Access** **Holidays** **Special**

 **Assign an Access Schedule for each Reader**

Readers			Schedules
<input checked="" type="checkbox"/>	Controller 1	24-7	No Access
<input checked="" type="checkbox"/>	Controller 2	24-7	24-7
			Untitled
			Untitled
			Untitled
			Untitled
			Untitled

- Cardholders who belong to this profile will only be able to access the reader during the times specified in the access profile.
- Repeat for all readers.
- On the *Holidays* tab, select which readers cardholders belonging to this profile can access during a holiday.

Name **Access** **Holidays** **Special**

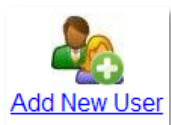
 **Select whether access is granted on a holiday**

<input checked="" type="checkbox"/>	Controller 1
<input type="checkbox"/>	Controller 2


9. On the *Special* tab, select readers cardholders belonging to this profile can lock or unlock in a maintained state by presenting their credential twice (double-bumping).
10. Click **Save**.

ADD CARDHOLDERS

1. Click the **Users** tab.
2. Click **Add New User**.



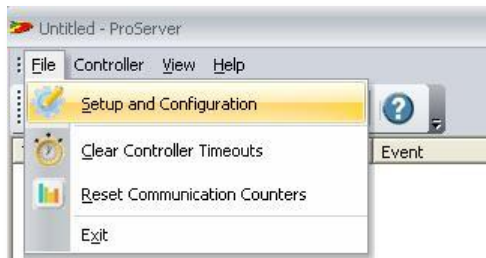
3. On the *Identification* tab, enter the 10-digit User ID number of the cardholder. Add leading zeroes if necessary to make 10 digits.

	Identification	Fields	Notes	Access
	User Id	<input type="text" value="0162122887"/>		
	User name	<input type="text" value="Heather Scott"/>		
	Auto Validate Date	<input type="text" value="June"/> <input type="text" value="23"/> <input type="text" value="2009"/>		
	Auto Void Date	<input type="text" value="January"/> <input type="text" value="1"/> <input type="text" value="2050"/>		
	Limited Use Card	<input type="checkbox"/>		
	Usage Count	<input type="text" value="0"/>		

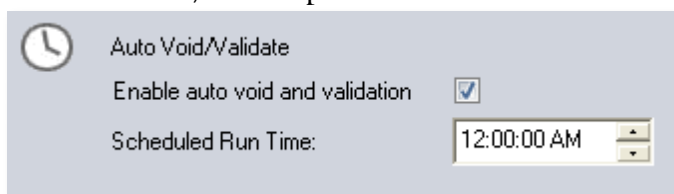
NOTE: The first five digits are the system code and the last five digits are the credential ID number.



4. Enter the name of the cardholder. Keep in mind that cardholder searches are case sensitive, so enter all names using the same convention.
5. If you would like the credential to be automatically validated/voided, (optional) enable Auto Void and Validation by going to **File > Setup and Configuration** in the Pro Server window.



6. Check the **Enable auto void and validation** box.
7. Choose a time you'd like the SmartLock Surf software to do a daily auto validate/void update.



8. Click **OK**.

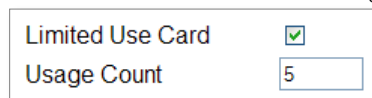
NOTE: both *Pro Server* and *Surf Server* must be running for the auto validate/void feature to take effect.

9. On the *Identification* tab, enter auto validate/void dates.

Auto Validate Date	June	23	2009
Auto Void Date	January	1	2050

10. The cardholder's credential will be automatically validated/voided.

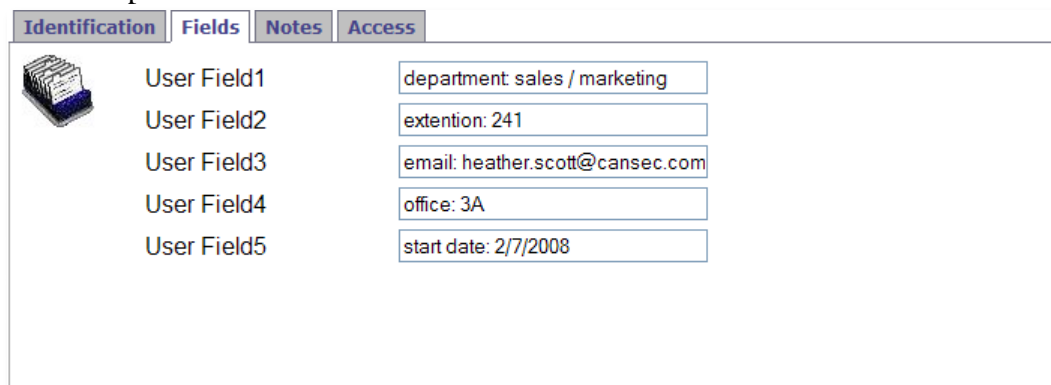
11. To restrict the number of times the cardholder can use his credential, check **Limited Use Card** and enter the maximum number of times the credential can be used in the **Usage Count** field. When the maximum use count is reached, you will receive a *User Voided* event message and the credential will no longer be valid.



A screenshot of a web form. It has two rows. The first row is labeled "Limited Use Card" and has a checked checkbox. The second row is labeled "Usage Count" and has a text input field containing the number "5".

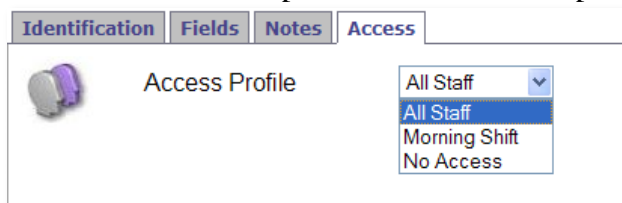
NOTE: To add more uses to the credential after it has been voided, increase the maximum use count, and then select an access profile from the *Access* tab.

12. Click on the *Fields* tab.
13. Enter optional information about the cardholder.



A screenshot of a web interface with four tabs: "Identification", "Fields", "Notes", and "Access". The "Fields" tab is selected. On the left is an icon of a stack of ID cards. To the right are five rows, each with a label "User Field1" through "User Field5" and a corresponding text input field. The fields contain: "department: sales / marketing", "extention: 241", "email: heather.scott@cansec.com", "office: 3A", and "start date: 2/7/2008".

14. Add any additional information about the cardholder or credential on the *Notes* tab.
15. Click the *Access* tab.
16. Choose an access profile from the drop-down menu.



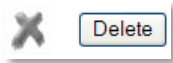
A screenshot of a web interface with four tabs: "Identification", "Fields", "Notes", and "Access". The "Access" tab is selected. On the left is an icon of a card reader. To the right is a label "Access Profile" followed by a drop-down menu. The menu is open, showing four options: "All Staff" (selected), "All Staff", "Morning Shift", and "No Access".

17. Click **Save**.
18. If the system's panels are online, the user data will be automatically downloaded.

EDIT AND DELETE CARDHOLDERS

To edit a cardholder's settings, click on the cardholder you wish to edit.

To delete a cardholder, click the cardholder you wish to delete and click the **Delete** icon.



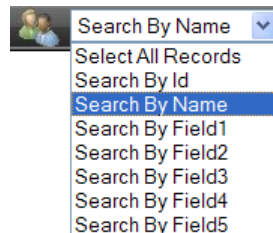
NOTE: only the first 100 cardholders are displayed in the Users section. To display a particular cardholder, search for the user using one of the methods below.

CARDHOLDER SEARCHES

There are a number of options available for searching for a cardholder. These are selected from the search toolbar. Available search options include:

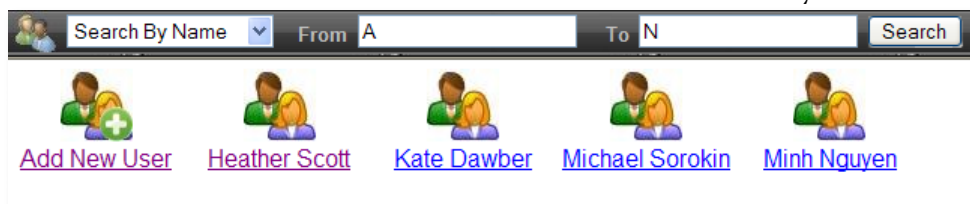
- **Select All Records** - Displays the first 100 records by ID number.
- **Search By ID** - Specify an ID range by entering values in the From and To fields. ID numbers in the range specified will be displayed. To search for a specific ID, enter the ID in *both* the From and To fields.
- **Search By Name** - Enter a user name, part of a user name, or first initials in the From and To fields to display users with that name. Search criteria is *case sensitive*.
- **Search By User Information Fields** - Enter a phone number, department, or other optional data saved in the user information fields to display users with that information.

1. Select one of the search methods from the drop-down menu.



2. Entered the desired data in the **From** and **To** fields.

3. Click **Search** to view the users who match the criteria you entered.



SEARCH TIPS

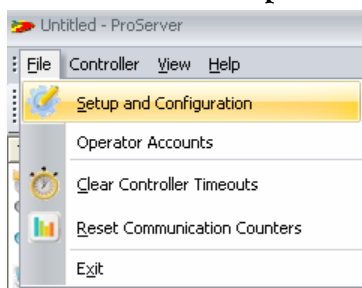
1. Search values are *case sensitive*.
2. If the From and To fields are blank, *all* records are displayed.
3. If you defined names for the user information fields, the field names will be displayed in the search criteria drop-down menu.
4. To return to the default view, choose the **Select All Records** option and click **Search**.
5. Only the first 100 cardholders are displayed in the User section. To find a cardholder not displayed, search for the user using one of the search methods on page 43.

Step 8. History and Audit

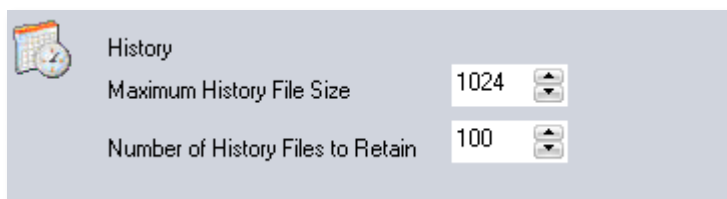
SETUP

The SmartLock Surf software records all events on the Server PC. Because SmartLock Surf is a “real-time” system, these events are constantly being recorded in one file, called the *Current History File*. To specify the size of the current history file:

1. Bring up the *Pro Server* window.
2. Go to **File > Setup and Configuration**.



3. Enter the maximum file size in the **Maximum History File Size** field.



Once the current history file reaches the maximum specified file size, it is archived as a backup file for future viewing and reporting. To specify the number of backup files to store:

4. Enter the maximum number of files in the **Number of History Files to Retain** field.

Once the number of backup files reaches the maximum, the oldest backup file will be deleted to make room for the newest file.

NOTE: the default settings (shown above) will require approximately 100 MB of space.

PANEL MEMORY

The SmartLock control panel holds a maximum of 1,000 events in memory. This is useful to know when the panel is offline and events cannot be sent to the computer. When 1,000 events have been stored in the on-board memory, a new event will replace the oldest event.

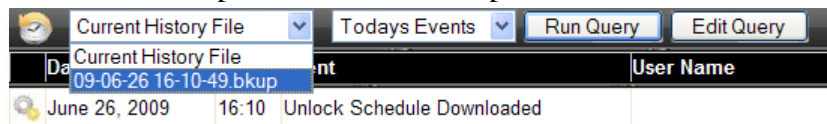
VIEW HISTORY

To view all history events stored in the *Current History File*:

1. Click the **History** tab from the SmartLock Surf browser interface.
2. The current history events for the current day will be displayed.

To view archived history events in backup files:

3. Select a backup file from the drop-down menu.

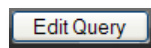


HISTORY FILTERS


History filters make it easy to find specific events. You can use a history filter to search for events based on: date and time, event type, user name, etc. History filters can be saved to make future searches faster.

To create a history filter:

1. Click the *Edit Query* icon.



2. Select a **Starting Date and Time** and **Ending Date and Time**. The filter will retrieve all events that occurred in this range.


Edit History Filter

Starting Date and Time

June, 2009							
Today							
?	<	>					
wk	Sun	Mon	Tue	Wed	Thu	Fri	Sat
22		1	2	3	4	5	6
23	7	8	9	10	11	12	13
24	14	15	16	17	18	19	20
25	21	22	23	24	25	26	27
26	28	29	30				

Select date

Ending Date and Time

June, 2009							
Today							
?	<	>					
wk	Sun	Mon	Tue	Wed	Thu	Fri	Sat
22		1	2	3	4	5	6
23	7	8	9	10	11	12	13
24	14	15	16	17	18	19	20
25	21	22	23	24	25	26	27
26	28	29	30				

Select date

Select the start date from the calendar above and enter the starting time in the edit boxes below.

Date	Hour	Minute
6/26/2009	00	00

Select the end date from the calendar above and enter the ending time in the edit boxes below.

Date	Hour	Minute
6/26/2009	23	59

3. Select the type of event(s).
4. Enter a user name to retrieve events from only this user. (Optional.)
5. Select a reader or readers. The filter will only retrieve events that occurred at the selected readers.

Events to Include

- ☒ Access Denied
- ☐ Access Granted
- ☐ Reader Unlocked
- ☐ Reader Relocked
- ☐ Door Alarms
- ☐ Request to Exit

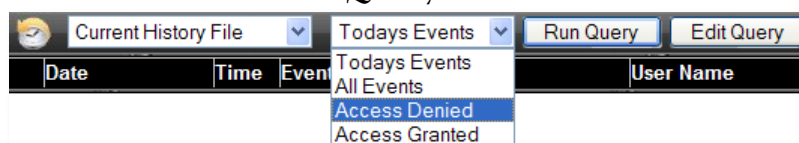
Filter Events by User Name

Readers to Include

<input checked="" type="checkbox"/>	Controller 1
<input checked="" type="checkbox"/>	Controller 2
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

6. Give the filter a name and click **Save As**.

7. Choose the saved filter from the drop-down menu on the history toolbar and click **Run Query**.



8. The filter results will be displayed in the history view menu.

	Date	Time	Event	User Name	User ID	Location
🔴	June 25, 2009	15:31	Access Denied - Not In Database	Kate Dawber	0162122888	Controller 2
🔴	June 25, 2009	15:31	Access Denied - Not In Database	Zaira Shaal	0000100162	Controller 2
🔴	June 25, 2009	15:31	Access Denied - Not In Database	Zaira Shaal	0000100162	Controller 1

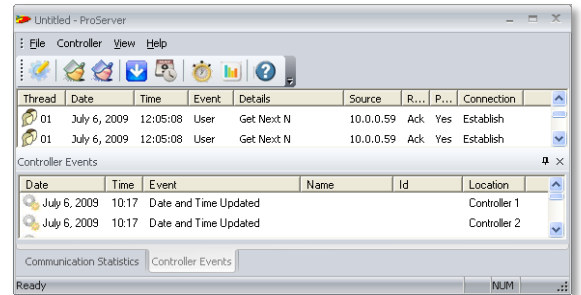
9. To reset the display to show all events in the history file, select **All Events** from the drop-down menu and click **Run Query**.

Appendix

FILE AND SOFTWARE OVERVIEW

SmartLock Pro Server

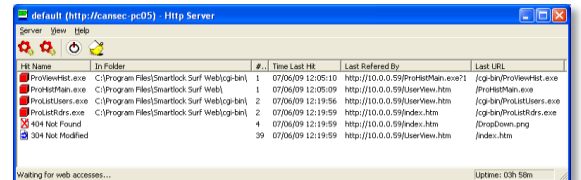
This folder contains user data, reader settings, audit logs and other files that the access control system uses to grant or deny access at the door.



The Pro Server software maintains communication with the control panels.

SmartLock Surf Server

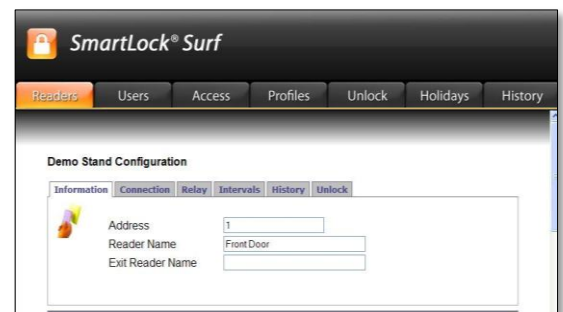
This folder contains the Smart Lock Surf web server.



The Surf Server software is the web server for SmartLock Surf.

SmartLock Web Site

This folder contains the html files and applications used to display the browser interface.



User, reader, and history management is done through the Internet Explorer browser interface.

DATA BACKUP

Back-up your data! Settings defined in the software such as Readers, Users and Profiles are saved to the default location **C:\Program Files\Smartlock Surf\Pro\Data**. Save a back-up copy of your data folder in another location on your computer, on portable memory (flash disk or CD-RW) or another computer or drive on your network on a regular basis and when any significant changes have been made.

Index

Access Privileges		Door	
Assigning.....	33	Automatic Unlock Schedules.....	26
Defining.....	29	Unlock Time.....	19
Holiday.....	30	Door Held Open	
Special.....	31	Interval Time.....	19
Access Schedules.....	28	Relay Setup.....	18
Anti-Passback Time.....	19	Door Unlock Schedules	
Auto Void/Validate.....	32	and Holidays.....	27
Backing up Data.....	41	Defining.....	26
Canlan		Double-Bumping.....	31
IP address.....	18	Events	
Testing Communications.....	22	Displaying.....	20
Capacity.....	5	History.....	38
Cardholders		Features.....	5
Add.....	31	Filters	
Assigning an Access Profile.....	33	Add.....	37
Auto Void/Validate.....	32	Firewall.....	7
History.....	38	Forced Entry	
Search.....	34	Disable Detection.....	19
Search Tips.....	35	Relay Setup.....	18
User Profiles.....	29	History	
CLAUSB		Backup Files.....	36
Choosing Comm Port.....	14	Create a Filter.....	37
Specifying in Reader Properties.....	18	File Size.....	36
Testing Communications.....	22	View.....	37
Client		Holiday Schedule.....	28
Number of concurrent connections.....	5	Holidays	
Communications		Defining.....	28
Testing.....	23	Execute Unlock Schedules.....	27
Control Panel		Setting Access Privileges.....	30
Address.....	18	Intervals.....	19
Memory.....	37	IP Address	
Relays.....	18	Canlan.....	18
Testing Communications.....	23	Server PC.....	13
Updating Date and Time.....	24	Limited Use Credential.....	33
Credentials		Login.....	17
ID Number.....	31	Network	
Limited Use.....	33	LAN.....	11
System Code.....	31	Port Forwarding.....	11
Data		WAN.....	11
Backup.....	41	Operator Accounts.....	16
Folder Location.....	12	Password	
Date and Time.....	24	Operator Account.....	17
Daylight Savings Time.....	24	Pro Server.....	15
Delete		Port	
Cardholder.....	34	80 and 5800.....	8
Reader.....	20	Add Firewall Exception.....	8
		Forwarding.....	11
		Listing Open Ports.....	9
		Scanner Software.....	10

Pro Server	14
Reader	
Add	17
Associate Unlock Schedule	26
Commands	22
Date and Time	24
Edit and Delete	20
Event History	38
Status	20
Testing Communications	22
Relays	18
Requirements	6
Router	
Port Forwarding	11
Schedules	
Access	28
Holiday	28
Search	
for a Cardholder	34
for an Event	37

Software Settings	
Configuring	17
Folder Location	41
Surf Server	12
System Code	31
Time	
Anti-Passback	19
Daylight Savings	24
Door Unlock	19
Door-Held-Open	19
Intervals	19
Updating	24
Unlock Schedules	
and Holidays	27
Defining	26
User Name	17
User Profiles	
Assigning	33
Defining	29
Wide Area Network (WAN)	11

® SmartLock is a registered trademark of Cansec Systems Ltd.

® iButton is a registered trademark of Maxim Integrated Products, Inc.

® Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.