

Introduction

The following additional features have been made available in Director Software v4.75 and main controller firmware v4-56 and greater:

- Authorities by Site.
- Support for R2 DVR's.
- Void User on maximum incorrect User ID/card + PIN attempts.
- Restore all doors to their scheduled state after a fire alarm has unlocked them.
- Full 1000 HSC-IP receiver reporting accounts support in Director Software.

Director Software v4.75

Authorities by Site

This added functionality allows you to:

- Define authorities that are system wide. *System wide* authorities exist in all panels in the account.
- Define authorities for each panel group defined in the account. *Authorities* that are added to each panel group are unique to that panel group.

In the software, the panel group is considered a site. The operator will be allowed to assign a system wide authority to the user's authority/authority plus or a site specific authority for each of the panel groups in the account. Authorities by site cannot be selected for a site that has shared users and cannot be used with pending user edit operations.

Important: The number of authorities that can be defined for the account is *equal* to the sum of the system wide authorities *plus* the number of panel groups *multiplied by* (the number of authorities allowed by the feature set *minus* the system wide authorities). Feature Sets 5 to 7 will support 10 System Authorities, Feature Sets 8 to 10 will support 50 System Authorities and Feature Sets 11 to 14 will support 100 System Authorities.

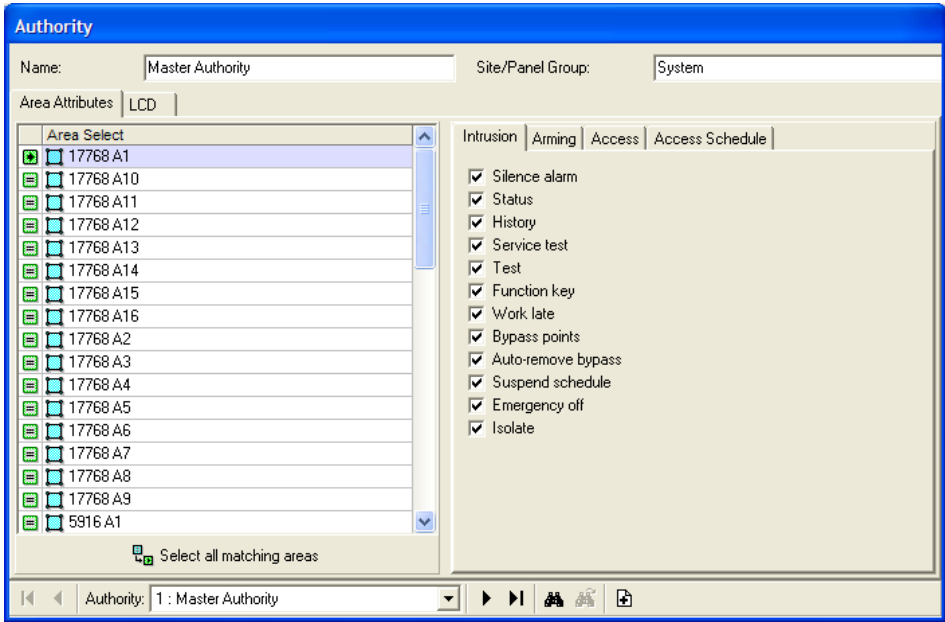
Enabling Authorities by Site

Authorities by Site is enabled by selecting the **Authorities by Site** check box on the Account Information form. This check box will be enabled only when the Feature Set is 5 or above and the Panel Version is set to "Version 4.56 and greater".

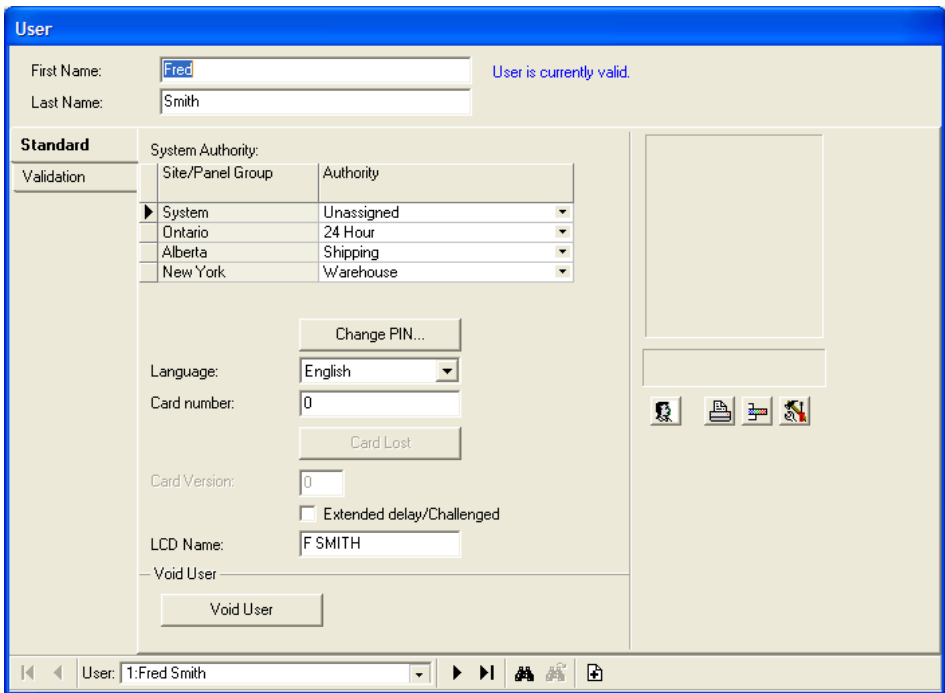
The screenshot shows the 'Account Information' form with the following details:

- Standard:** Master Panel
- Setup:** Change Master Panel... (button), Default Panel Group : Default Panel
- Global Account Options:**
 - Allow PIN duress
 - Display card number
 - Panic token sends duress
 - Synchronize panel time daily
 - Enable User In/Out Status for this Account
 - Authorities By Site** (highlighted with a red circle)
- Pin mode:** Four Digit
- User logon mode:** User ID
- Escort required mode:** ESCORT User
- Point reset time:** 2 seconds
- Dealer ID:** [Redacted]
- Keypad lock code:** [Redacted]
- Arm/Disarm and Tones:** Standard
- Card Action:**
 - Ignore pending enrollment

With Authorities by Site enabled, the Authority form will display a **Site/Panel Group** combobox. This will allow the operator to select the site in which to display/configure authorities. The entries in the **Authority** combobox at the bottom of the form will be filtered according to the selected site. If "System" is chosen for the site, the system authorities will be listed.



The **User** form will be modified in the Standard and Validation tabs for the way user authorities are assigned.



User

First Name: User is currently valid.
 Last Name:

Standard: Valid User Period

Validation Type: Active

Authority Plus:

Site/Panel Group	Authority
System	Master
Ontario	Unassigned
Alberta	Unassigned
New York	Unassigned

Valid on:

Now (Immediately)
 Specified Date/Time:

Invalid on:

Never (Permanent User)
 Specified Date/Time:

User: 1:Fred Smith

Note: If the Global Account Options is not checked for Authorities by Site, then these tabs for the **User** form will remain as they were in the previous version of the Director software.

The **User** gridview will be modified to display the following popup to allow the operator to configure the Authority and Authority Plus data. When in gridview, sorting on the System Authority and the Authority Plus columns will be disabled. Filtering on these columns will still work. There will be a popup allowing the operator to pick the site and authority for which to filter on.

Site Authorities

Site/Panel Group	Authority
System	Master
Ontario	Unassigned
Alberta	Unassigned
New York	Unassigned
Texas	Unassigned

OK Cancel

When a System Authority has been assigned to a user the Site Authorities will be displayed as Unassigned. In order to select a site authority, the operator must first set the System Authority to Unassigned. Then the comboboxes will be enabled for each of the sites.

The User Report will still function as it did previously with exception of the sorting on the authority data columns. This will be disabled if **Authority by Site** is selected for the account. If either of the authority data columns is included in the report then there will be multiple rows in the report for each user.

Voiding a User on Maximum Incorrect User ID/card + PIN Attempts

If a pre-set number of incorrect entry attempts are made, a user's entry permission can be temporarily suspended until it has been manually restored.

- The Bad Card/PIN tab in the Account Information screen has been revised with check boxes for "Void User on Maximum Bad UID+PINs" and "Void User on Maximum Bad Card+PINs"
- When either of these incorrect entry attempts is made based on the number of attempts allowed, the user will be locked out until they are re-instated and the lockout duration has either elapsed or has been cleared.

Account Information	
Standard	Invalid User Detection
Setup	<input type="checkbox"/> Void User on Maximum Bad UID+PINs <input checked="" type="checkbox"/> Void User on Maximum Bad Card+PINs
Bad Card/PIN	Maximum Bad PINs: 6
Site Address	System Lockout Duration: 2 minutes
Mailing Address	Maximum Lockouts Before Global Lockout: 10
Contact	User Lockout Duration: 2 minutes
Service PIN	
Shared Users	
Shared Holidays	Invalid Card Detection: None
	Maximum Invalid Cards: 10
	<input type="checkbox"/> Transmit Global Lockout Alarm

In order to re-instate the user:

- Proceed to the Users section in the Director and select the user that has been voided. Press the button to re-instate the user.
- If necessary, proceed to the Control and Status section in the Director and press the button to Clear User Lockout.

Voided User Report

- The Voided User report will be selectable in the User Access Report section by selecting “Users Voided by Maximum Bad PINs” in the Report Type combobox:

User Access Report

Report Type:

Report Period

From: To:

Available Current Period: 01/01/1980 12:00 AM - 28/05/2009 1:17 PM
 Available Archive Period: No Data Available

Report Destination

Output to:

NOTE: A “Card Voided-Bad Pin Count” filter will be selectable in the Director Event Priority section to assign a response condition for when the event occurs, example: A Warning Tone.

Restoring Door Schedule after a Fire Alarm

When a fire alarm occurs, all the access doors that are controlled through out the system can be unlocked. When all fire sensors have been restored to normal, the door schedules can be re-instated to lock or unlock doors as required.

- The Special tab in the System Access screen has been revised with a check box for “Relock all doors/re-evaluate door schedules on fire alarm reset”.

System Access

Standard

Alternate

Special

Door Fallback mode:

Unlock all doors on fire alarm

Relock all doors/re-evaluate door schedules on fire alarm reset

Auto Update Card Version

- When this check box is selected, the following warning message will be displayed:

Warning

Warning - by selecting to relock all doors/re-evaluate door schedules on fire alarm reset you may be violating your local fire code. Do you wish to continue with this selection?

NOTE: Persons planning to use this feature should first verify with the local fire authorities that it is acceptable.

Main Controller Firmware v4-58

Firmware v4-58 contains all modifications made in v4-56, and includes one additional important modification. In Firmware v4-58, area exit delay is now forced to 10 minutes for an area that is being remotely armed for a North American regional setting.

Main Controller Firmware v4-56

Similar to the Director Software, the new selections can also be made in the main controller keypad programming.

- Ensure the controller firmware is v4-56 or greater. If it is not, obtain the v4-56 or greater firmware file and use the Director Software flash utility to upgrade the main controller firmware.

Backup the Customer's Database

If it is an existing customer, obtain their system's database and save it to the Director Software on a local laptop. It will be necessary to get the security system's Unique ID (Keypad Advanced Programming Section **S001:02**. 1st selection), Third Party Password (Keypad Advanced Programming Section **S001:03**.) and the main control unit's main circuit board's serial address number (Keypad Advanced Programming Section **S005:10**. 1st selection) for your laptop's Director Software to communicate with the security system and get the database.

NOTE: Refer to the "Entering and Understanding Advanced Configurations" section at the end of these instructions to learn how to obtain the above information from the Keypad Advanced Programming Sections.

Upgrade the Security System's Main Control Board's Firmware

The security system main controller firmware version can be viewed at an LCD keypad connected to it. Use the following procedure to view the firmware version:

- Logon to the system as a service user. E.g. Default ID: "000", service user PIN: "2482" or "7378" if the panel has communicated with the Director Software.
NOTE: If the system Feature Set (S002↓00) is 5 or greater, keypad programming can not be done. The menus can only be viewed using the keypad. Programming can only be done with the Director Software.

LCD Keypad Screen

```
Service
Enter PIN: _ _ _ _
```

- When the control box tamper is activated, a service user has the authority to access system programming using the keypad.

- Using the left and right arrow screen scrolling keys on the keypad, scroll the menus until **Config** is displayed. Press Ok. "Config method" will display. Select "Advanced" with the arrow keys and press Ok.

```
Menu Options
◀ Config ▶ ↓Ok
```

- The screen that begins Advanced programming will display.
S001:00: this is the start of the **System** program section.
The code to the right of S001:00 is the firmware version of the main controller. In this case: "4-49U42". 4-49 is the firmware version. It must be upgraded to 4-56 or greater.

```
S001:00      4-49U42
↓OK          ↓+Group- ↓
```

- The security system main controller firmware must be version 4-56 or greater in order for the two new features to function.
- If the main controller firmware is a lower version number, it must be upgraded. Do e.g. a Direct Connect using a RS485 converter from the Director Software to the main controller to flash the new firmware to the main controller.

Send the Database Back to the Main Control Board or Configure It

Return the database to an existing customer's security system or if it is a new system, configure it according to the customer's requirements.

Programming at the Security System Main Controller for the Two New Features to Function

- The security system can be programmed with the new features using the system keypad instead of the Director Software providing the system's main control board firmware has been upgraded to the 4-56 version or greater.
- Log on to the Security System Main Controller keypad as a Service User and enter "Advanced" Configurations.
- Refer to the "Entering and Understanding Advanced Configurations" at the end of these instructions for further information.
- Make the following entries for the main controller to enable the two new features:

Void a User on Maximum Incorrect User ID/card + PIN Attempts

- Log on to the main controller keypad as a service user and select Menus/Configurations/Advanced.
- Select the following programming location in Advanced Configurations.

	only available with the addition of the Feature Expansion Board.		higher version number automatically. (This setting refers to fixed-ID cards with a version number).
<input type="checkbox"/> (no)	Delay Screen	<input checked="" type="checkbox"/> (yes) <input type="checkbox"/> (no)	(UK ACPO = <input checked="" type="checkbox"/> yes)
<input type="checkbox"/> (no)	Fast Restore	<input checked="" type="checkbox"/> (yes) <input type="checkbox"/> (no)	If a point restore is to be sent within 1 min. (as opposed to siren time-out). UK ver. is 12 sec. (UK ACPO = <input checked="" type="checkbox"/> yes)
<input type="checkbox"/> (no)	Ring Back Required	<input checked="" type="checkbox"/> (yes) <input type="checkbox"/> (no)	If monitoring station will cause keypad tone & siren to confirm area arming (for UL).
<input type="checkbox"/> (no)	Suite Security System NOTE: This feature is only available with the addition of the Director Software and Feature Expansion Board.	0 = Normal, 1 = Different users per area.	
<input type="checkbox"/> (no)	Single Panel	<input checked="" type="checkbox"/> (yes) <input type="checkbox"/> (no)	Yes = Single Panel No = Multi Panel connection.
<input type="checkbox"/> (no)	Enable Wall Tamper	<input checked="" type="checkbox"/> (yes) <input type="checkbox"/> (no)	Main control box back tamper. (UK ACPO = <input checked="" type="checkbox"/> yes)

Full 1000 HSC-IP Receiver Reporting Accounts Support in Director Software

- In the Director Software proceed to the communications setup section for accounts reporting to the HSC-IP receiver.
- The limit for the SIP (HSC-IP) Accounts that can be assigned is now 1000.
- This did not affect the firmware 4-53 or greater.

System Communication		
Configuration	SIP Mode:	SIP over IP
SIA/CID	Full report by area:	Always
SIA/CID Test	SIP Account:	1000
SIP/HSC	SIP baud rate:	150
Paging	HSC timeout:	90 seconds
	HSC SIP Autose	Manual

Entering and Understanding Advanced Configurations

- Logon to the system as a service user. E.g. Default ID: "000", service user PIN: "2482" or "7378" if the panel has communicated with the Director Software.

NOTE: If the system Feature Set (S002↓00) is 5 or greater, keypad programming can not be done. Programming can only be done using the Director Software.

NOTE: Default MASTER (end) USER code is ID 01 or 001, PIN 7793.

LCD Keypad Screen

- When the control box tamper is activated, a service user has the authority to access system programming.

Service
Enter PIN: _ _ _ _

- Using the left and right arrow screen scrolling keys on the keypad, scroll the menus until **Config** is displayed. Press Ok. "Config method" will display. Select "Advanced" with the arrow keys and press Ok.

Menu Options
◀ **Config** ▶ ↓Ok

- The screen that begins Advanced programming will display.

S001:00 F-98U42
↓OK ↓ +Group- ↓

S001:00: this is the start of the **S**ystem program section. Each of the program sections begin with a letter. The next 3 digits (e.g. "001") represent the first program section for System programming. The next 2 digits (e.g. "00" after the colon) represent a sub programming section of this main system program section.

The letters for each of the programming sections are:
S: System; **A:** Areas; **M:** Modules; **P:** Input Points; **E:** Equipment/Pseudo points; **B:** Programmable Outputs; **L:** Authority Levels; **I:** Profile; **W:** User Edit; **U:** Users; **H:** Holidays; **D:** Schedules; **T:** Custom Pt Type; **R:** DooRs; **G:** Area Group; **Z:** Shared Data Groups (Users and Holidays).

F-98U42: the version of the main controller firmware.
 ↓ **+Group-** ↓: Using the middle or right down arrow keys this term's arrows are pointing to will scroll forward or backward through the various program sections (Groups). It will change the program section letter & display that section's program selections for the same programming and sub programming section.
 ↓ **OK:** Pressing the keypad button below OK will enter the programming section displayed.

- A sub programming section can display several defaulted selections that will affect the way the system operates. These selections can be changed to customize the system operation. A box "□" represents that a programming selection has been disabled. A check

□.□.0.□.1.✓✓✓□□
↓Save S002:1

mark "✓" means that it is enabled. With the cursor flashing under a specific selection, the selection can be toggled back and forth from a box to a check mark by pressing any key on the keypad.

Other entries are numerical and with the cursor flashing under them they can be changed by pressing the desired number entry on the keypad from available selections. When entering a sub programming section and all its various selections, the section displayer (e.g. S002:1) appears in the lower right corner of the screen.

When a selection has been changed, always press the keypad button below ↓Save to retain the change. Refer to the Advanced Programming Guide for descriptions for all selections.

- A program section with a down arrow in its section displayer e.g. P001↓0 means if the down arrow keypad button beneath it is pressed, the screen will change to the next input, output etc. and the same program selections for it.
- Pressing the keypad button below "↓?" when it displays in a screen, will cause a momentary screen to display related information. E.g. an input or output number associated with a module will display the module's number (i.e. module # XX), what type it is (e.g. Point Expander module), the module's serial number and its input or output number range. Pressing the button below "↓*" will display information about a specialized module such as RF wireless or a printer module.

201.01.01. . . .
↓Save ↓? P001↓0