TORONTO
Corporate Security

SECURITY ACCESS

C-CURE 9000® PROGRAMMING STANDARDS

Subject	C-Cure 9000® System Programming Standards
Revision No	4.4
Effective	May 29, 2020
Issued By	Corporate Security Corporate Real Estate Management City of Toronto
Approved by	Dwaine Nichol, CPP Director, Corporate Security Corporate Security Unit Corporate Real Estate Management
Approved on	
Supersedes	All previous or existing internal Corporate Security C-Cure 9000® system Programming Standards
Contact Information	Femi Ajayi, CSPM, PSP Supervisor, Building Security Corporate Security Section Corporate Real Estate Management 1050 Ellesmere Road, 2nd Floor Toronto, Ontario M1P 2X3 Tel: 416-397-4224 Fax: 416-396-4225 Andrew Robinson Manager, Infrastructure Unit Corporate Security Section Corporate Real Estate Management

Revision History	Initial Draft – September 10, 2007 Approved – 2008 Revised – January 23, 2013 Revised – March 11, 2014 Revised – May 26, 2015 Revised – January 29, 2016 Revised – March 10, 2017 Revised – September 15, 2017 Revised – June 02, 2020

Document Classification

The information contained in this document is confidential and proprietary to Corporate Security, City of Toronto; and is protected by provincial and federal legislation.

The City of Toronto submits this document with the understanding that it will be held in strict confidence and will not be used for any purpose other than reference for the specification, design, maintenance and implementation of CCure 9000 card access and event management systems.

No part of the document may be circulated or reproduced for distribution outside Corporate Security without prior written approval from the Director, Corporate Security (or his/her designates).

Table of Contents

PREFACE

The City of Toronto owns eight CCure 9000 SAS access control and alarm management systems, linked to a single card database through the CCure 9000 MAS. This unique enterprise solution was so chosen to curtail risk and moderate the impact of system or environmental failures - given the nature and criticality of Corporate Security's services to the City.

This document is intended to highlight security best principles & practices and to serve as a guideline for the configuration of all City of Toronto CCure 9000 systems.

In accordance with industry standards and practices, alarm display and communications should be designed to provide prompt and accurate reporting of all signals and events to a human operator. This is best accomplished when the displayed data is concise, consistent and clear.

To ensure a quality approach, all system programming must be done with the following objectives in mind:

- Efficiency of use
- Ease of Operator understanding
- Effectiveness of data tracking, collection and reporting
- Optimal effect with minimal system load

Although standards are devised for the purpose of ensuring conformity and continuity, pre-packaged "Cookie Cutter" solutions do not always fulfill the protection needs of the facility or the client. In addition, any protective system must be designed, implemented and operated to counter current and emerging threats.

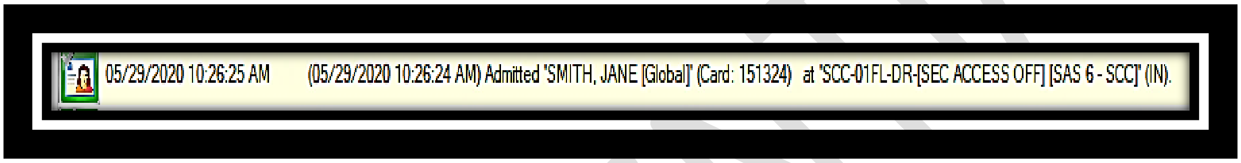
NAMING CONVENTIONS & GENERAL STANDARDS

The following general standards apply to all CCure 9000 programming.

With a few exceptions, all system entries (i.e. names, descriptions, card record entries, etc.) will be made in Uppercase (Capitals). Exceptions will be listed in this document.

There is a finite character limit on a Monitoring Screen line (see below); so the System Programmer will need to balance the device name lengths. Names that are too long with will exceed the available screen space.

Device names that are too abbreviated however will not provide sufficient information to facilitate accurate assessment.



```
05/29/2020 10:26:25 AM     (05/29/2020 10:26:24 AM) Admitted 'SMITH, JANE [Global]' (Card: 151324)  at 'SCC-01FL-DR-[SEC ACCESS OFF] [SAS 6 - SCC]' (IN).
```

FIG. 1 – ADMITTED CARD

All programmed devices, doors, elevators, etc., must include a detailed description with the following information:

Site name: **CITY HALL**
Location of device: **GROUND FLOOR, SUITE 202 NORTHWEST CORNER**
Orientation of device: **HUB ROOM ENTRANCE CARD READER**
Additional Device Data: **INSTALLED WITH FAIL-SAFE ELECTRIC STRIKE**
Date of installation: **INSTALLED MARCH 2020**
Date of warranty expiration: **WARRANTY EXPIRES MARCH 2020**
Facilities door number: (If applicable) **DOOR B5-207**

Put together, it should display like this:

CITY HALL: GROUND FLOOR, SUITE 202 NORTHWEST CORNER HUB ROOM ENTRANCE CARD READER. DOOR B5-207
INSTALLED WITH FAIL-SAFE ELECTRIC STRIKE
INSTALLED BY JCI MARCH 2020
WARRANTY EXPIRES MARCH 2020

CCure 9000 does not allow duplicate names of any device, clearance, schedule, event, or any other user-defined entry on the same partition (i.e., SAS).

This rule does not include data entered onto a card record with the exception of Credential, which does not allow a duplicate card digits.

CCure 9000 will allow you to name both a card reader, a door contact, event and schedule with the same name (i.e., **100QUE-SEC OFFICE), but this is not the best practice and may lead to confusion** for technicians and Security Access Staff working on CCure.

Installed devices which operate as single entity (such as a door) must have similar names to ensure continuity and ease of search. For example, Door **55JOHN-01-WORKS** will have the following components:

- Reader: **55JOHN-01-WORKS DR ®**
- Door Switch Monitor: **55JOHN-01-WORKS DR DSM**
- Door Contact: **55JOHN-01-WORKS DR D/C**
- Door Latch Bolt Monitor: **55JOHN-01-WORKS DR LBM**
- Request to Exit: **55JOHN-01-WORKS DR RTE**
- Electric Strike: **55JOHN-01-WORKS DR STK**
- Forced Open Alarm: **55JOHN-01-WORKS DR – FORCED [E]**
- Held Open Alarm: **55JOHN-01-WORKS DR – HELD [E]**
- Door Open Event: **55JOHN-01-WORKS DR – DOOR OPEN [E]** (to be used with doors with Door Contacts Only)

Programmed events which operate with a schedule will have similar names to ensure continuity and ease of search. For example, Event **1530MAR-UNLOCK MAIN DRS** is controlled by schedule **1530MAR-U MAIN DRS**.

LOCATION CONVENTIONS

Location prefixes **must** be used in the configuration of all device and sub-system names:

The location prefix will precede any other information contained within a device, clearance, and time spec or event name.

A hyphen (-) will separate the location prefix from the remainder of the device, clearance, schedule or event name.

Location prefixes must include the full address minus the street suffix. (i.e., **1530 Markham Road would become 1530MARKHAM)**

Location prefixes must allow a reasonably trained Operator prompt recognition of the location that the device, clearance, schedule or event is affiliated with.

Corporate Sites will follow the same naming convention as above with the exception of the Civic Centres.

Metro Hall, City Hall and Civic Centres will retain their common abbreviations as follows:

- **METRO HALL = MH**
- **CITY HALL = CH**
- **SCARBOROUGH CIVIC CENTRE = SCC**
- **NORTH YORK CIVIC CENTRE = NYCC**
- **YORK CIVIC CENTRE = YCC**
- **EAST YORK CIVIC CENTRE = EYCC**
- **ETOBICOKE CIVIC CENTRE = ECC**

All Toronto Water location naming conventions will follow the same naming as Corporate Sites with the exception of the Water Treatment and Filtration Plants.

For example, Horgan Filtration Plant would become **HORGAN**, whereas the Wastewater Quality Enforcement and Laboratory located at 30 Dee Avenue would become **30DEE**.

Tanks, Reservoirs and Pumping stations will follow the regular location naming convention (**ADDRESS>NAME i.e., Rosehill Reservoir would be named 75ROSEHILL**)

All location conventions are subject to review by the Security Access Team.

HARDWARE CONFIGURATION

The following standards should apply to CCURE 9000 hardware configuration and programming

GENERAL STANDARDS

All device programming must meet the recommended specifications as outlined by Software House. Unique or ‘one-off’ programming may only be employed if written authorization is given by the Security Access Team.

All device programming must conform to current legislation, regulation, administrative law, by-law or policy.

All device names, descriptions, instructions or notations will be entered in capital letters.

DEVICE NAMING CONVENTIONS

Device names should provide sufficient detail as to the type of device and location of install
All device names are subject to review by Security Access Team.
The following conventions must be used with device names:

- Door: DR
- Double Doors: D/D
- Door Contact: D/C
- Latch Bolt Monitor LBM
- Door Switch Monitor: DSM
- Request to Exit: RTE
- Electric Strike: STK
- Glass Break: G/B
- Maglock: MAG ([M] – No longer used in door names)
- Card Reader (One-Way): ®
- Card Reader (entering): [IN] ®
- Card Reader (exiting): [OUT] ®
- Stair: STAIR
- Office: OFF
- North: N
- South: S
- East: E
- West: W
- North West: N/W
- North East: N/E
- South West: S/W
- South East: S/E
- Elevator: ELEV
- Interior / Inner: INT
- Exterior EXT
- Entrance: ENT
- Room: RM
- Parking: PKG
- Employee: EMP
- Receiving: RECV
- Shipping: SHIP
- Loading Dock: LOADING DOCK
- Administration: ADMIN
- Mezzanine: MEZZ
- Storage: STOR

iSTAR CLUSTERS

GENERAL SETTINGS

The iSTAR Cluster Name should be entered in the following manner:

9LESLIE-ISTAR CLUSTER # 1 (Location prefix, hyphen, and iSTAR Cluster)

iSTAR Clusters should **not** be placed On-Line unless ready to be used and monitored

Encryption Setting: iSTAR EDGE, ULTRA, and ULTRA SE Controllers should be "Encrypted"

Only one iSTAR should be added to a cluster.

Communications
Leave at default settings

Cluster
Leave at default settings

Miscellaneous
Leave at default settings

Area
Leave at default settings

Encryption
Leave at default settings

Triggers
Leave at default settings

iSTAR CONTROLLERS

GENERAL SETTINGS

The iSTAR Controller Name should be entered in the following manner:
9LESLIE-ISTAR # 1 (Location prefix, hyphen, and iSTAR number)

iSTAR Controller should **not** be placed On-Line unless verified by the Security Access Team and ready to be used and monitored

Controller-Type should be iSTAR Ultra SE, Ultra or EDGE

Controller Type**:** Select Controller type at the beginning of programming the Cluster.

If Controller Type is iSTAR Ultra SE, it is extremely important that Security Access Team Member checks off the "Configured" check box under ACM Board 1 to gray out the selected controller type before saving.

Technicians must also confirm that the right type of ACM Board is selected before programming.

Adapter #1 MAC Address: Should be the iSTAR MAC Address

Time Zone: GMT -05:00 Eastern Time (US & Canada)

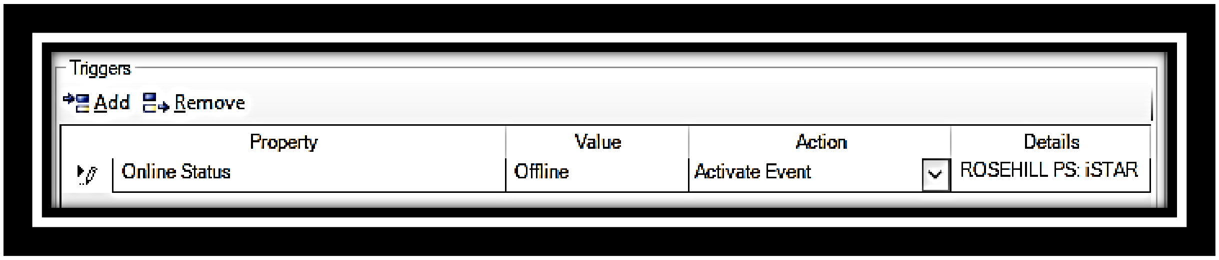
Onboard Ethernet Adapter: Defaults when you enter IP Address.

TRIGGERS

Triggers: Is where you may add the COMM FAIL Event.

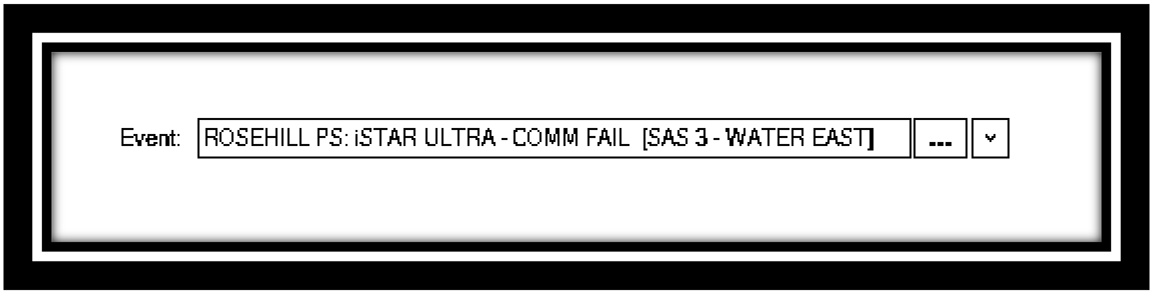
Click Add and set the following:

- Property: Online Status
- Value: Offline
- Action: Activate Event
- Details: Populates when you assign the event to the controller.
- Event: Click … to select an existing event, or click "˅" arrow box to select edit an existing event or select new to create the event.



Property	Value	Action	Details
Online Status	Offline	Activate Event	ROSEHILL PS: iSTAR

FIG.2 – TRIGGERS FIELD



Event: ROSEHILL PS: iSTAR ULTRA - COMM FAIL [SAS 3 - WATER EAST]

FIG. 3 – TRIGGERS FIELD: EVENT SELECTION

DOORS

GENERAL SETTINGS

These are the settings currently used on City of Toronto Doors.

Hardware

- Door Switch Monitor: DSM, D/C
- Door Lock Relay: STK, MAG

Reader

- Inbound Reader
- Outbound Reader
- Readers are continuously active: Box should be checked.

Request To Exit

- Request To Exit Input: Should be selected (RTE).
- Unlock Door on RTE: Should be checked on MAG Doors.
- Shunt DSM while RTE is active: Should be checked for both STK and MAG doors.

Settings

- Send non-alarms input status to the host: Should **not** be checked as this will overload the journal.

TIMING

Timers

Delay Relock (seconds): default setting, to be amended as needed.

Shunt Time: default setting, to be amended as needed.

Unlock Time: default setting, to be amended as needed. Timing can be adjusted by the Security Access Team via request through CMR.

Door Close Debounce Time: Should be configured for vehicle gates, as needed depending on the forced open alarm received.

Door Grace Time: default setting, to be amended as needed.

Door Unlock Grace Time: default setting, to be amended as needed.

Options

Always use Shunt Expire Output: default setting, to be amended by Security Access Team depending on alarm being received.

Delay Relock while Door open after valid access: default setting, to be amended by Security Access Team depending on alarm being received.

Shunt Door for full Shunt Time: default setting, to be amended by Security Access Team depending on alarm being received.

TRIGGERS

FORCED [E] and HELD [E] should be configured with the appropriate HELD/FORCED event for all doors; except for vehicle gates and arm/disarm readers. ****Individual unique events programmed. No generic/shared events. (i.e., each door will have their own forced or held event).**

GROUPS

Doors can be added to door groups through Configuration Menu in CCure 9000.

READERS

General Settings

Readers should **not** be placed On-Line unless ready to be used and monitored.

Reader Technology should be configured as appropriate to the type of reader employed. Most will be either Proximity or Wiegand.

Reader Type should be configured as appropriate to the type of reader employed. Most will be either RM / RM-4E or Direct Connect Wiegand.

All relevant City Card Formats must be entered.

Supervised Inputs should be configured with manufacturer-recommended devices only.

Outputs should be configured with manufacturer-recommended devices only.

Keypad PIN options should be configured as needed.

Keypad Commands options should be configured as needed.

Allow Card Numbers to be Entered via Keypad options should be configured as needed.

Activate this Output During Communication Failures is not currently being used by the City.

Activate this Event During Communication Failures options should be configured as needed Activate this Output While Tampered is not currently being used by the City.

Activate this Event While Tampered is not currently being used by the City, but is recommended for all exterior readers.

Status: default settings.

Reader LED light flashing (RED and GREEN flashing light) when door is in Held Open status.

Reader arm\disarm LED light changing and accepting valid swipe cards. When armed, the LED should show RED, when disarmed, the LED should show GREEN.

Reader LED light changing and accepting valid swipe cards. The LED should change from RED to GREEN with a valid card swipe.

iSTAR INPUTS

General Settings

Inputs should **not** be placed On-Line unless ready to be used and monitored.

The Default State of the input should be armed.

Reverse Sense of Input: should remain deactivated unless the device configuration needs to be inverted.

Activate on Supervision Error: Check box should be unchecked.

Send State Changes to Monitoring Station: Check box should be checked off for inputs not attached to doors.

Send State Changes to Journal: should be activated for inputs not attached to a door.

Triggers: All inputs need to trigger their own Supervision Error event. The event should be named the same as the input itself with – SUPERVISION ERROR [E] at the end.

Example: **55JOHN-01FL-N/E WORKS RTE – SUPERVISION ERROR [E]**

OUTPUT

General Settings

Outputs should not be placed On-Line unless ready to be used and monitored.

Pulse Duration should be configured as needed. Where output pulsing is not required, it should remain at the default setting of 0/10th second.

Send State Changes to Monitoring Station should activated on outputs that are not door related.

Send State Changes to Journal options should be configured as needed.

Normally Energized should be configured as needed; but used sparingly. Outputs that are normally kept energized typically experience more wear and tear.

ELEVATORS / FLOORS

General Settings

GENERAL

Elevators should **not** be placed On-Line unless ready to be used and monitored

Floors should **not** be placed On-Line unless ready to be used and monitored

CCure controls elevator floor access by means of outputs attached directly to the elevator control board.

Elevator Time Schedule must be downloaded to the Controller.

Each floor for each cab must be equipped with its own output. Pressing the floor button in an uncontrolled elevator signals the control board on where to move the elevator cab.

On Controlled Elevator Access, a valid card read must be received first, or CCure will restrict the control board from receiving the floor button activation.

An additional feature of CCure allows the use of inputs to monitor which floor button was activated by a cardholder.

No Input Selection, One Input Selection, or Multiple Input Selection buttons should be configured according to what input design has been chosen for the installation.

BUTTONS

Elevators should be configured in accordance with Software House recommended methods.

Floors must be configured with the correct Elevator Cab + Floor Output to work properly.

Elevator Admitted, Rejected or Duress Access events may be configured as directed by the Security Access Team.

Button Activation Time should be configured to 10 seconds as recommended by Software House.

SYSTEM CONFIGURATION

The following standards should apply to CCURE 9000 system configuration and programming.

AREA / ANTI-PASSBACK

Area/ Anti-Passback is not currently used on CCURE 9000 System.

Configuring Areas enables anti-pass back checking and specifies events to activate when various area-related situations occur.

Doors/readers can be configured to control ingress and egress from a passback-controlled area.

Areas can be defined within a single or iSTAR, or across iSTAR Clusters.

Only Enforce Regular Anti-Passback and Enforce Timed Anti-Passback is use with the city at this time.

Regular Anti-Passback will only permit cardholders to enter an Area an exit swipe was previously registered.

Timed Anti-Passback will reject cardholder entry into an Area if the entry attempt was made within a certain time period. Once the timed rejection has elapsed, entry into the Area will be permitted once again.

Mustering is used primarily for counting personnel during emergency evacuations.

The Access In and Access Out tabs should be configured to accurately reflect those relevant doors/readers that will be used for Area entry or exit.

The Asset In and Asset Out tabs are not currently being used by the City.

CARD FORMATS

The City currently used 9 proprietary 27-bit Wigand card formats:

- **CITY HALL1 (No longer used by the City with the exception of SSLTC)**
- **CITY HALL2 (Not needed in SSLTC)**
- **CITY HALL3**
- **CITY HALL4**
- **CITY HALL5**
- **CITY HALL6**
- **CITY HALL7**
- **CITY HALL8**
- **CITY HALL10**
- **CITY HALL11**

One 35-bit proximity iClass Corp 1000 card format

- **HID CORPORATE 1000**

All specifications under the Card Format should not be changed without **the express authorization of the Security Access Supervisor, and Security Access Team**.

These sections holds the card mechanism of operations and how the system reads the card in CCURE System

HOLIDAYS

Work duties are to be performed by Security Access Team.

There are a maximum of 24 Holiday Lists on iSTAR-equipped CCure systems while there is no practical limit to iSTAR-equipped systems. In a mixed-panel environment, the lowest maximum limit applies.

Only Stat Holidays are entered into CCure. The name should accurately reflect the holiday it represents (i.e., New Year's Day).

The Duration (In Days) should be configured to 1.

The Recurrence feature should be configured to most accurately reflect the nature of the holiday date.

For example, some holiday dates are fixed, so the once radial button should be checked and the relevant date added.

Other dates are relative, so the Yearly radial button should be checked and the relevant (First, Last, First, Second, etc.) weekday of the relevant month should be selected.
To reduce labour costs, the City celebrates weekend Stat holidays on the first weekday thereafter.

Therefore, if Christmas Day falls on a Sunday, the City will shut down during following Monday for this holiday.

HOLIDAY OVERRIDE

Holiday will override the regular schedule and secure the building. However, if the building needs to remain open in spite of the holiday, HOLIDAY OVERRIDE must be configured. This will override the holiday schedule.

EVENTS

An event is a CCure system definition that allows users to link actions, annunciations, and time activations into one component.

Events are used for a wide variety of purposes and thus must be properly named to ensure that any trained Operator can identify it immediately.

Events should **not** be placed On-Line or Armed unless ready to be used and monitored.

All acknowledgeable events must have specific instructions entered in the "**Instructions to Display on Event Monitor**".

These instructions should provide the Operator with the following information:

Type of event: **MOTION ALARM**)
Location of event: **1115 QUEEN STREET WEST**)
Response instructions: **DISPATCH POLICE IMMEDIATELY**), (**CALL A SITE NUMBER**)
Any relevant information: **LOCATION CONTAINS HAZARDOUS CHEMICALS**)

Some important events should have pertinent information entered in the "**Display this Line when Activated**": **MOTION DETECTOR HAS BEEN ACTIVATED IN VAULT**)

The Integrator should consult with the Facility Security Analyst (FSA) or PMO on what to display under the Message Instructions "Instructions to display on Event Details screen"

All acknowledgeable alarm events must be assigned a priority of **75-150** **depending on the sensitivity of the event.**

All non-acknowledgeable events should be assigned a priority of **75-150** (depending on level of importance)

Acknowledgement Tab must have the following checkboxes selected for acknowledgeable alarms:

- Send state changes to Journal
- Send state changes to Monitoring Station
- This event requires acknowledgement
- Allow acknowledgement while causes are active

All other exceptional events will be programmed by the Security Access Team.

Unacknowledged/Un-cleared Events may be configured as needed and appropriate by Security Access Team.

Sounds should be configured to Play Sound Once. Sensitive alarms will be programmed as Play Sound Instead of Beep (which will be a continuous alert).

The following Sounds may be used for alarm activations:

Door Alarms:	Alert
Single Sensor Alarms:	Alert
Intrusion Violations:	Siren
Duress:	Buzzer
Comm Fails:	Buzzer
A/C Fail:	Buzzer
Low Battery:	Buzzer
Tamper Alarms:	Klaxon
AED Removal:	Glass
Glass Break:	Glass
Arm Check:	Laser
Alarm to Intercon:	Siren
Disarm:	Chimes
Fire Alarm:	Siren 1
PIR Alarm	Alarm

The Dialup feature is not currently being used by the City.

The General, and Overdue Timing features will be configured as needed and as deemed appropriate by the Security Access Team.

The Event Is Downloaded to Controller: feature is currently being used by the City.

All Scheduled Events on the same server (i.e., SAS) and doors in the same controller can be downloaded to the controller.

CLEARANCES

Clearances are created by the Security Access Team after receiving a detailed Change Management Request from the PMO group.

Clearance names should provide trained Operator reasonably good information as to the clearance timing and location of access.

All clearance names are subject to review by the Security Access Team

Most clearance names will have the following conventions:

- [DAY] = Daytime Access: Monday to Friday during Business Hours (variable)
- [24HR] = 24 Hour Access, seven days a week. (Also known as "Always").
- [EXT] = Extended Access: Used mostly for exterior access or when standard is not followed.

Some clearances may be unique in nature and may require more specific names (i.e., **35S-7 DAYS 0600-2030 for 7 days a week clearance)**

Use Activation Date and Time may be used with temporary clearances (i.e., ones being used by contractors and during labour disruption)

Use Expiration Date and Time may be used with temporary clearances (i.e., ones being used by contractors and during labour disruption)

When configuring elevators, no more than 48 Triplicate Pairs should be used in a single clearance. A Triplicate Pair is a combination of Elevator/Elevator Group, Floor/Floor Group and a Time Specification.

If more than 48 Pairs are needed, another clearance must be created (i.e., **COUNCILLOR** and **COUNCILLOR1**) >>> Not really necessary but it is better not to have too many Triplicate Pairs in a single clearance

SCHEDULES

Schedules are used to provide chronological control over clearances and event activations
Where possible, Schedules should not be configured to span across 2400hrs midnight

The Name should be entered to closely match the event or clearance it is configured with. Exceptions to this standard include generic names, such as: **MON-FRI 0700-1900**; which can be used by multiple clearances. **Generic Names cannot be used for Events.**

HOLIDAY OVERRIDE

Holiday will override the regular schedule and secure the building. However, if the building needs to remain open in spite of the holiday, HOLIDAY OVERRIDE must be configured. This will override the holiday schedule.

iSTAR INTRUSION ZONE

An Intrusion Zone is a user-defined group of doors, inputs, outputs and actions that delineates a physical area monitored for alarms.

Devices within an Intrusion Zone reacts as one when one of its components is affected.

Special-purpose inputs cannot be assigned to an intrusion zone. These include:

- Request to Exit
- Any Power Fail Alarm
- Card Reader Arm/Disarm Input Point
- Any Tamper Alarm

Controller: Select the iSTAR Controller that will have the Intrusion Zone.

Entrance & Exit Doors: Add building doors. **It is extremely important to add all exterior and affected doors.** Every door has to be secured with the exception of the Arm/Disarm door (which has to be in a locked state) and card control box checked to allow arming and disarming of the building.

Inputs: Add all Controlled Inputs
*****All Controlled Inputs must have individual events configured. No generic/shared events are to be used.**

Example of unique event is "1530MARKHAM-S/W EXT DR PIR – MOTION [E]" This should be configured

Arm – Disarm: Arming and Disarming fields should have Card Method to Arm Zone should be configured to "Active Input and Credential".

Arming Input must be selected for Arming and Disarming.

Under the Arm tab, the Readers Sounds during Exit Delay field should be configured as needed and mostly used for Parks, Forestry and Recreation locations.

Under the Disarm tab, the Readers Sounds during Entrance Delay field should be configured according to site and client needs. The default time is **0** seconds.

Allow Disarm While Violated: check box should be checked off.

In iSTAR Intrusion Zones, the door schedule must not activate until the building is disarmed. The schedule should also deactivate anytime the building is armed, regardless of programmed scheduled start time of the event. *** The arming and disarming controls the activation of the schedule of the facility.

All other features of City Intrusion Zones may be configured in accordance with direction from the Security Access Team.

Arm/Disarm readers must have the LED lights change state

Supervision error must be programmed on all devices.

All Events, Doors and devices naming must start with the building address and abbreviation. Please see previous programming.

Communication Failure, Tamper, AC power Fail, Low battery must be programmed on all iSTARs.

LEGACY MAPS

Legacy Maps are Windows Bitmap files (*.bmp) or PNG files (*.png) which can be associated with CCure to display floor plans of devices and events.

Bitmap/png files should be large enough to recognize map details but not so large that it requires additional time to load onto the screen or the operator to scroll in order to find relevant devices.

A good size is **9000x600** dpi. If the floor plan is too big to shrink into something legible, it should be broken up into two separate files (i.e., **1530MARKHAM-05FL North** and **1530MARKHAM-05FL South**)

Bitmap/png file names must be clear enough to identify them with a facility and specific location

CCure Icons should **not** be placed so that it overlaps other devices on the map. Where more than one device is installed at one point, the icons should be placed in a circle or square around that location.

CCure Map must be clear enough to identify them with a facility and specific location

READER CARD FORMATS

The following Card Formats must be added to all City of Toronto Card Readers, under Reader Card Formats field.

- **CITY HALL1 (No longer used by the City with the exception of SSLTC)**
- **CITY HALL2 (Not needed in SSLTC)**
- **CITY HALL3**
- **CITY HALL4**
- **CITY HALL5**
- **CITY HALL6**
- **CITY HALL7**
- **CITY HALL8**
- **CITY HALL10**
- **CITY HALL11**
- **COT HID ICLASS CORP 1000**

GROUPS

Groups are used to manage related clearances, doors, events, input/output, personnel, elevators, areas, readers and floors to optimize system configuration.

Group Names must be simple and clear.

Group names must include a location prefix, followed by a hyphen and then a simple descriptor (i.e., **1530MARKHAM-DOOR GROUP**)

SUPERVISION ERRORS

Supervision Error reports on the status of communication of CCure 9000 and the device. It may mean there is a fault in the device, or tampering.

An error message is sent to the controller if a Supervision Error is detected and a message should be displayed at the Monitoring Station and entered into historical journal.

All Input devices must be configured with its own unique Supervision Error Alarm event. (i.e., **1530MARKHAM-05FL-ENT DR DSM – SUPERVISION ERROR [E]**) **This is vitally important for diagnosing faulty devices.**

TAMPER DEVICES & SIGNALS

Tamper input switches can provide notification of unexpected or unauthorized access into an iSTAR or card reader. This notification can best be displayed at the Monitoring Station and entered into historical journal by means of a Tamper alarm event.

All iSTARs and card readers (**especially exterior card** readers) should be equipped with Tamper input switches and configured with Tamper alarm events.

Separate Tamper alarms can be configured for each device.

COMMUNICATION FAILURES

CCure maintains bi-directional communications at all time between the host or (server) and its controller and devices.

When communications is lost, CCure will report this condition in accordance with user-defined specifications.

This notification can best be displayed at the Monitoring Station and entered into historical journal by means of a COMM FAIL alarm event.

COMM FAIL alarm events should be programmed with a unique individual event on all Controllers. (i.e., **1530MARKHAM-01FL-ISTAR #1 – COMM FAIL [E]**)

SUMMARY

- All door schedules should be programmed and activates\deactivates only when the building is Arm\Disarm. The Arming must override the building Unlock schedules.

- Arm/Disarm readers must have the LED lights change state

- Each Input not attached to a door configuration must have its own unique events (i.e., Door Open Alarm, Supervision Error)

- Inputs that are part of a door configuration (DSM, RTE) must have its own unique Supervision Error with the matching naming convention that helps easily identify the device.

- All doors must have its own unique Forced, or Held Alarm, but also may have a Rejected Card alarm when requested by FSA, PMO or Security Access Team.

- All Elevator Floors must be programmed with a Scheduled Event which must be downloaded to each controller. Under no circumstances, should uncontrolled elevator buttons be programmed as a group.

- All Controllers must have unique individual COMM FAIL events programmed with matching naming convention.

- Naming Conventions listed in this manual must be adhered to.

- All iSTARs must be encrypted.