inception

WEB POWERED SECURITY

Simple & Easy Installation

Integrated Security - Access Control

Release Notes 4.2.0

10/03/22

www.innerrange.com

inner range

Intelligent Security Solutions

Table of Contents

March 2022

How To Upgrade

Keeping your Inception system up to date ensures you have the latest feature enhancements and issue fixes available.

Review this document to see what has changed in the latest releases of Inception, as well as any notes and considerations when upgrading.

How to upgrade your Inception:

1. Download the latest firmware from the Inner Range website. This is available from the Technician Downloads section of the website, all that is required is a valid Inner Range user account.

2. Connect your device to the Inception controller's web interface. See the Quick Start Guide for more information on connecting.

3. Log on to the Inception web interface and navigate to **[System -> Firmware Update -> Update Controller]**

*NOTE: If updating a controller with existing programming, it is recommended that a database backup be taken before updating the firmware. This can be done via the **[System > Backup/Restore]** page.*

4. Click the **[Update Application Software]** button in order to display the file upload box

5. The system will now display any previously uploaded firmware files. Click the **[Upload File...]** button to upload the new firmware file.

6. Using the file browser, navigate and select the firmware file, once this is done the file will be uploaded onto the Inception Controller.

7. Once the file is uploaded, it will be verified and then listed in the table of update files. Select the required firmware file by clicking on it in the list and then click **[Apply]**.

8. The system will begin the update process. In rare cases, you may be prompted to default the panel at this point.

9. Once the firmware is updated, the controller will automatically restart and eventually the login screen will be shown. If the login screen isn't shown after 60 seconds, refresh the page.

Minimum Required Versions

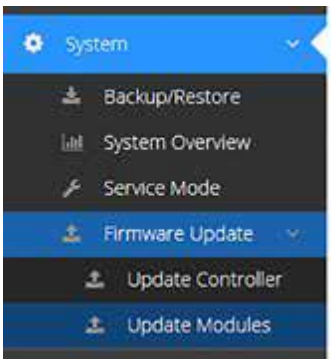
The list below indicates the minimum required firmware versions for several of the expansion modules available to the Inception system.
If your expansion modules are using an older firmware version, certain features of the Inception system may work incorrectly or not at all.

Expansion Module	Firmware Version
8 Input LAN Expander	3.0.1
UniBus 8 Input Expander	1.0.3
UniBus 8 Relay Expander	1.1.2
Standard LAN Access Module (SLAM)	4.0.5
SIFER Reader	1.16.0
T4000 Security Communicator	2.1.4
UniBus Lift Interface	1.0.0
Inovonics RF Expander	1.1.0
EliteX Keypad	3.1.0

How to Update Modules

How to check your expansion module versions and update them:

Note: The T4000 is updated separately, either via the Multipath Bureau software or by the monitoring station.



Checking your module versions and updating their firmware is done from the Update Modules page on the Inception web interface. To view this page, log on to the Inception web interface and navigate to **[System -> Firmware Update -> Update Modules]**. This page will list all of the enrolled modules and peripherals along with their detected version number. Any modules running older firmware versions will be highlighted in orange.

Updating your module versions

1. Inception firmware updates have the latest module firmware files pre-loaded in the system and are ready to be downloaded to the expansion modules.
2. From the Update Modules page mentioned above, click the [Update Module Firmware] button in order to display the file upload box.
3. The system will show all firmware files loaded on the system in a table, including the module type and version number of the file. If necessary, different firmware files can be uploaded using the **[Upload File...] button**. If a file is uploaded, it will be verified and then included in the table of update files.
4. The next window will show all of the configured modules that this file can be applied to. Select the modules that you want to update. Multiple modules can be updated at the same time.
5. Clicking **[Apply]** will begin the update process. Once complete, the modules will automatically restart and reconnect to the system.

Select Firmware Update File

Filename	Size (bytes)	Firmware Type	Firmware Version	File Location
E_3_0_0.dld	85872	Expander	3.0.0.25938	Pre-Packaged Firmware
R_3_0_3.dld	147408	SLAM	3.0.3.27523	Pre-Packaged Firmware
SR150b14.dld	101264	Sifer Reader	1.5.0.14	Pre-Packaged Firmware
ax_1_1_2.dld	5444	Unibus Aux Expander	1.1.2.19246	Pre-Packaged Firmware
zn_1_0_3.dld	13292	Unibus Zone Expander	1.0.3.19307	Pre-Packaged Firmware

Version 4.2.0 – 10/03/22

Inception release 4.2.0 includes a wide range of feature updates and resolved issues.

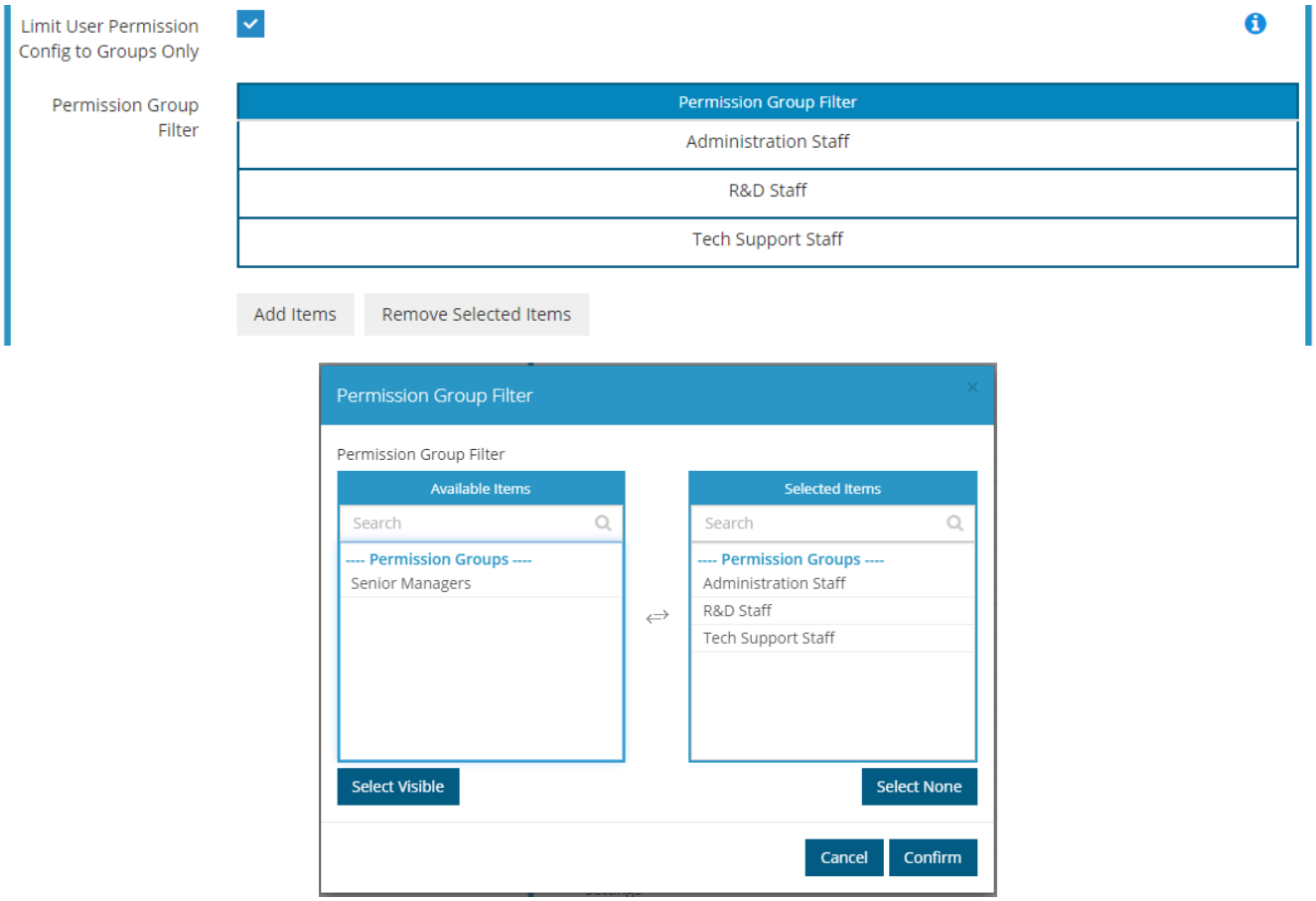
Note: The minimum firmware version for EliteX Keypads has been updated to 3.1.0 due to improvements to module substitution logic.

New Features

Option to Limit Available Permission Groups

Inception now has the option to limit which permission groups a User can select from when managing other user's permissions. Permission Groups can be filtered by the Web Page Profile that the user is assigned. The feature is configured on the **[Configuration > Users > Web Page Profiles]** page, in the **Item Editing Permissions** section. The *Limit User Permissions Config to Groups Only* option must be enabled to activate the *Permission Group Filter* option. If no items are set, all permission groups are available to the user, otherwise, only the items specified can be used.

This allows common staff permission groups to be available to certain users, while manager permission groups are hidden and need to be set by more senior staff. Or a hierarchy of permission groups could exist for different parts of the building, but the user only sees a small subset for a simpler administration interface.

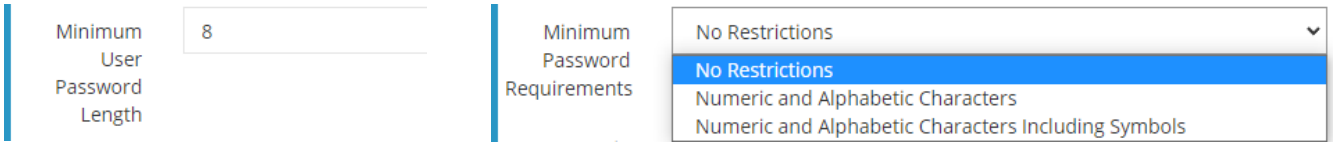


Password Policy

Multiple new features relating to password management have been added to the **[Configuration > General > System]** page in the **PIN / Password Policy** section that allow for the adjustment of system-wide configuration related to login.

Password Policy – Quality and Change Frequency

Various options have been added to enforce different restrictions on passwords. If a user does not meet the specifications set within this configuration, they will be sent to a page to change their password before they can login. Password length can be enforced to make users create passwords with a minimum length, and *Minimum Password Requirements* can require numbers, alphabetic characters and symbols in passwords for them to be valid.



A mandatory password change frequency can also be configured to mandate users to change password in a specified repeating timespan (for example, every 30, 60 or 90 days). After this timespan, users will be sent to a page to change their password.

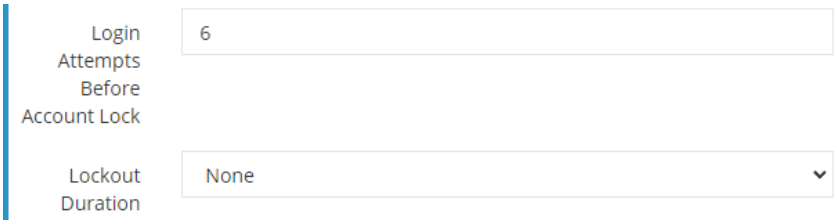
Password Policy - Account Lockout Changes

Changes have been made to how account lockout works and how it can be configured.

Users attempting to login with incorrect credentials will be locked out after a configured number of attempts (default 6), their account will be locked out until the configured 'Lockout Duration' timespan has passed. This is separate to the existing lockout logic, where if the user is unknown (their username is not found), then after 3 failed attempts all login attempts will be blocked for a period of time.

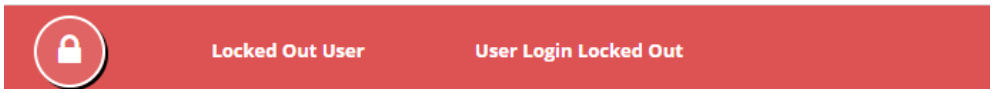
Setting the *Login Attempts Before Account Lock* to 0 disables user-specific account lockout completely and only the existing global lockout logic will apply.

If the *Lockout Duration* is set to 'None', then account lockout will be indefinite – requiring administrator intervention which will be covered in the next section of the release notes.

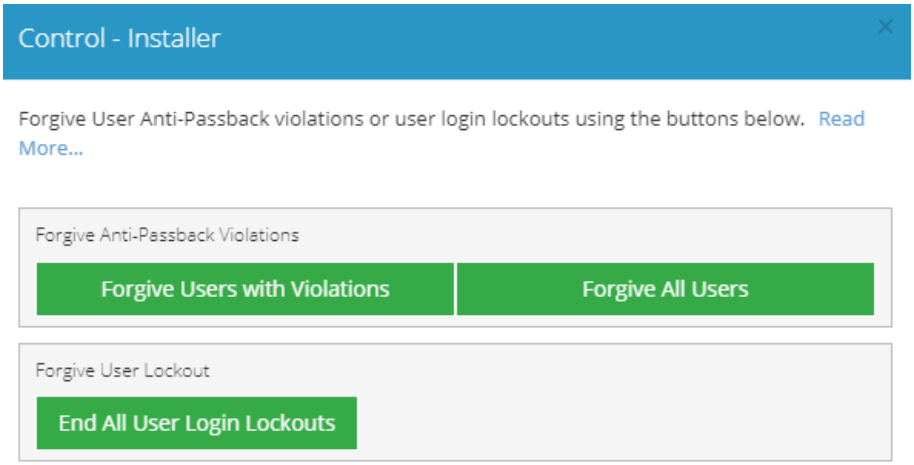


Password Policy – Administrator Intervention

When a user has been locked out for either the specified *Lockout Duration* in the password policy or indefinitely, this can be forgiven through the **[State / Control > View Users]** page. If a user has been locked out, they will be red with the status "User Login Locked Out". That user can be forgiven through the *Quick Control* button to allow them to attempt to login again.



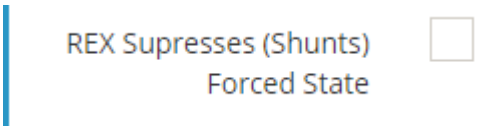
The toolbar *Control All* button in the same page or the **[Configuration > Users > Manage Users]** page can forgive all lockouts in the system with the *End All User Login Lockouts* button.



REX / REN Inputs can Suppress Door Forced

A new option for door configuration has been added on the **[Configuration > Access Control > Doors]** page that changes the way REX/REN inputs behave. When enabled, the door will not unlock when the REX/REN input activates, instead the Door Forced state will be suppressed if that door opens during the *Default Unlock Time*.

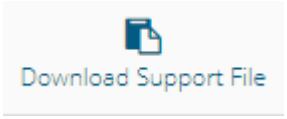
This is commonly used for doors where the Forced state is monitored that can be freely opened from the inside. Instead of using a physical REX button, a motion sensor or an exit bar is used on the inside of the door. As the user leaves, they open the 'locked' door and no alarms activate. If someone walks past the inside of the door though, the door does not unlock which would allow an exterior person to enter.



March 2022

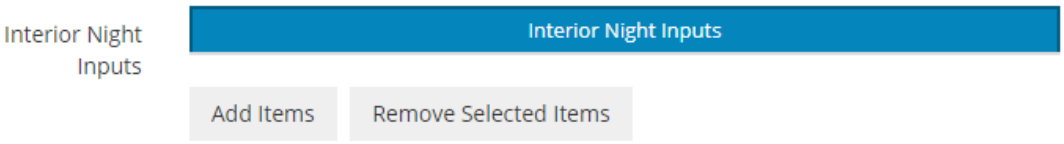
Support File Download Button

A new button has been added to the toolbox on the **[System > Service]** page that allows for the download of a support file that Support can use to diagnose issues. The information in the file is what is often requested by Support when diagnosing issues, so this allows for an easy way to collate that information and allow for faster assistance. The support file will include a database backup, internal system logs, two weeks of review, and various system information.



Additional Monitored Inputs During Night Mode Arm

Added a new list of Monitored Inputs similar to the Perimeter Inputs list on the **[Configuration > Areas > Edit Areas]** page that allows additional inputs to be monitored during the Night arm mode.



When this area is armed in Night mode, the intruder inputs (Primary, Handover, Instant) specified in the list will also be monitored in addition to the Perimeter inputs. Any interior night inputs are treated as Primary inputs, triggering Entry Delay if activated. This allows more of the building to be monitored while everyone is asleep, while not immediately activating sirens if someone enters that section. The Perimeter inputs are unchanged in Night mode, activating sirens instantly if a perimeter input (i.e a door or window) activates.

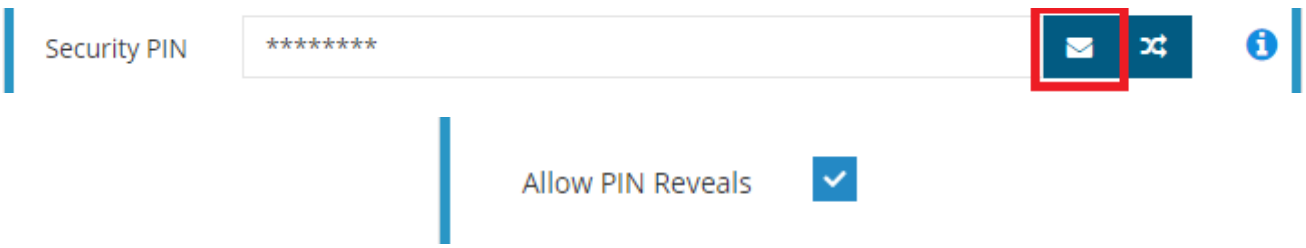
In order to add Inputs into this list, they must first be present in the Monitored Inputs list above it.

Send / Reveal User PIN

Added a new button next to the Security PIN field found on the **[Configuration > Users > Manage Users]** page that lets an email containing the user's PIN be sent to that user. This requires the User to have an email address configured, and an Email Server to be configured on the **[Configuration > System > Settings]** page.

Additionally, a new option has been added to Web Page Profiles that allows a User to reveal another user's PIN. With the option enabled, they can only reveal PINs of users with the same or a lower priority level.

If a PIN is revealed or is sent to a User via email, a review event is logged indicating which user requested the action.



Feature Updates

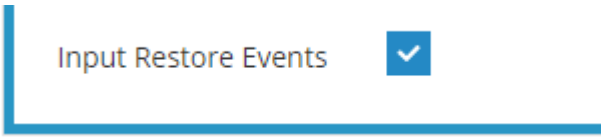
Installer Account on First Login

The first access of Inception's web interface will take the user to a page where they configure the credentials for the Installer user. Setting up these Installer credentials is required and will need to be done before the user is taken to the login page for the first time.

This applies for factory defaulted units, or when the Installer user account has been reset.

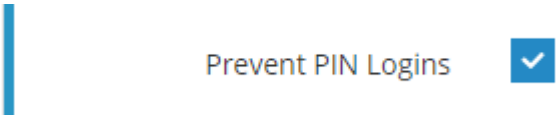
Notification on Input Event Restore

A new option has been added to Notifiers (configured on the **[Configuration > General > Notifiers]** page), that allows notifications to be sent when an input re-secures or restores. This is helpful for environmental sensors, such as temperature or water sensors, as it allows notification when a problem event is restored. Also for door events like Door Held, as a notification can be sent when a door is finally closed.



Prevent Web Login via PIN

Web interface logins using Username + PIN can now be prevented, forcing the use of a password. This can be enabled on the **[Configuration > General > System]** page in the **PIN / Password Policy** section.



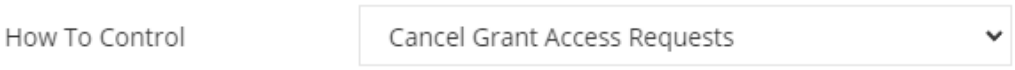
Changed "Limit User Permission Config to Groups Only" behaviour

Previously, the Web Page Profile option *Limit User Permission Config to Groups Only* (configured on the **[Configuration > Users > Web Page Profiles]** page) would affect both User permission editing and Permission Group editing. This was impractical, as it meant Administrators either could not make their own permission groups with specific items, or had a more complicated User management interface.

The change means this option only applies to User permission editing. If a user can edit permission groups, they can edit them without restriction.

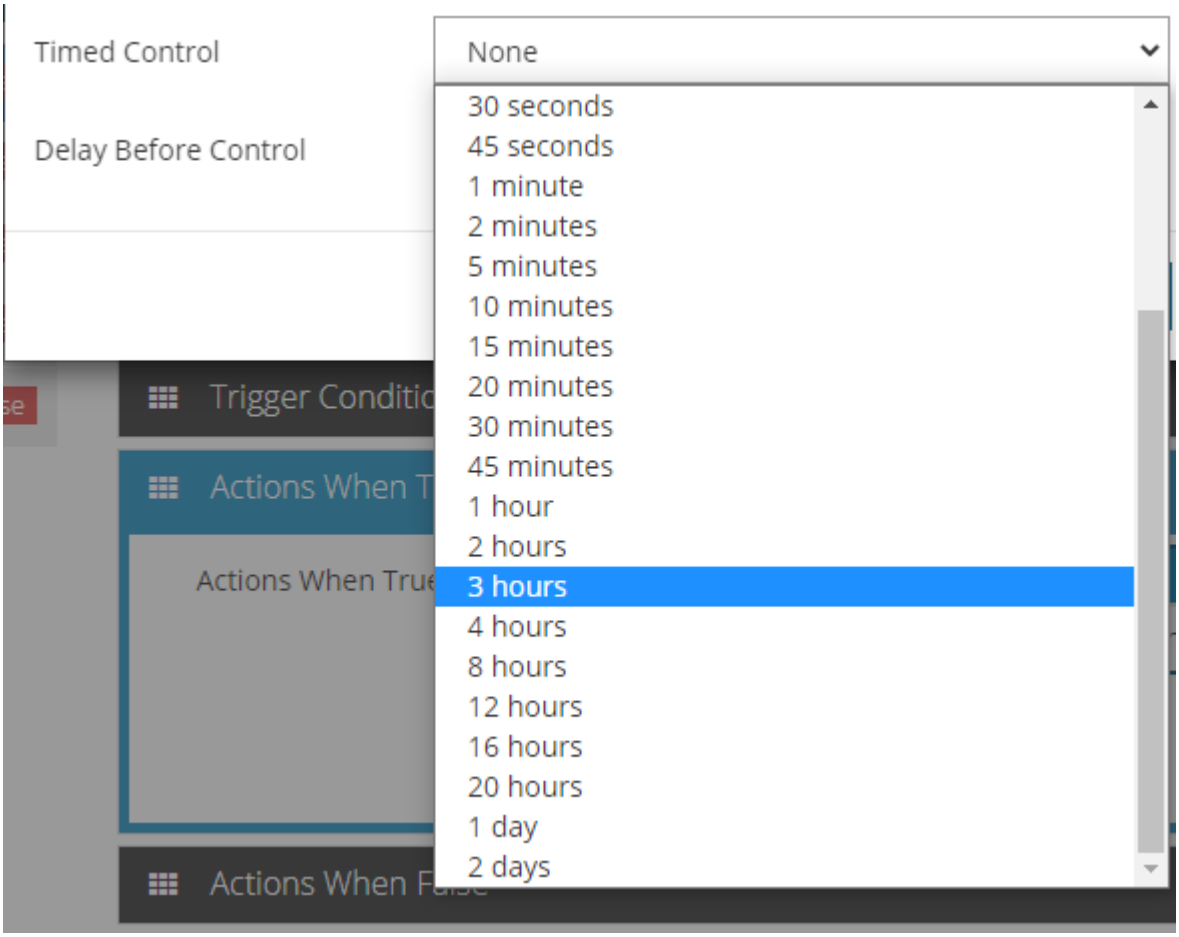
Automated Action – Cancel Grant Access Requests

When adding automated actions in the **[Configuration > Automation > Automated Actions]** page, *Cancel Grant Access Requests* may now be selected under *How to Control* for doors. This cancels any active user access requests a door has.



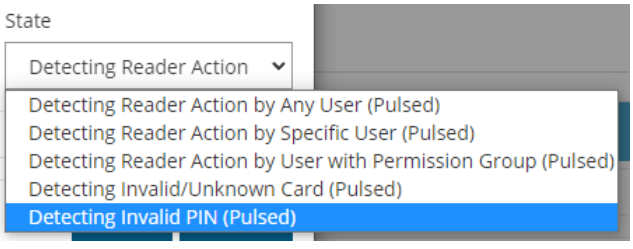
Automated Action - Output Control Time

When controlling an output for time via an automated action, the maximum duration has been extended from 4 hours, with options now available up to 2 days.



Automated Action – Invalid PIN Automated Trigger

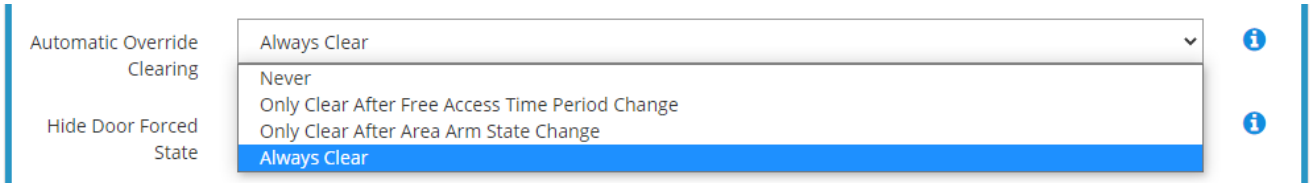
Automated actions with trigger conditions for Card Readers may now use *Detecting Invalid PIN (pulsed)* as a state.



Door Automatic Override Clearing

By default, a Door's Override status (overriding a Door state to Unlock or Lock, but not Lockout) is automatically cleared if the Free Access Time changes state, or if the Area to Follow arms or disarms. This is generally the desired behaviour, preventing doors from remaining unlocked if it should be locked due to the armed area, or remaining locked when the free access time period is active.

For scenarios when this is not desirable, a new option has been added to Doors (configured via the **[Configuration > Access Control > Doors]** page) that can control when this logic applies. It can be disabled completely for a door, or apply only for the Time Period or Arm State change. New doors default to "Always Clear", which is the original functionality.



Issues Resolved

Prevent a Disarmed area becoming Defer Armed

Resolved an issue where if a user only has permissions to temporarily disarm an area (not fully disarm), if they disarm an already-disarmed area, then it would enter the timed disarm state and it would arm soon after. This situation could easily occur with Disarm on Access door logic, where accessing a door automatically disarmed the area on the other side of the door.

This has been changed so that fully disarmed area will not be downgraded to 'temporarily disarmed' state.

Inception Auto Arm Cancel From Input Activity

An issue has been resolved where the "Allow Input Activity to Cancel Auto-Arm Warning" Area option would not trigger if an input activated while another one was already active.

CSV User Import Performance

CSV User Import and DUIM (Dynamic User Import Module) are both much faster to complete. This is more noticeable when importing a large number of users.

Module Poll Time Option Missing

An issue was resolved where the previously visible Module Poll Time field in the Hardware Wizard was hidden. This field should now be visible in the Hardware Wizard for Hardware Modules.

Time Period Edit Display

The Time Period Edit display will no longer have the 'Priority' column take up a large amount of table width, making the Time Periods table slightly easier to edit on smaller screens. The UI for portrait-mode phones is not ideal, but landscape-mode should be improved.

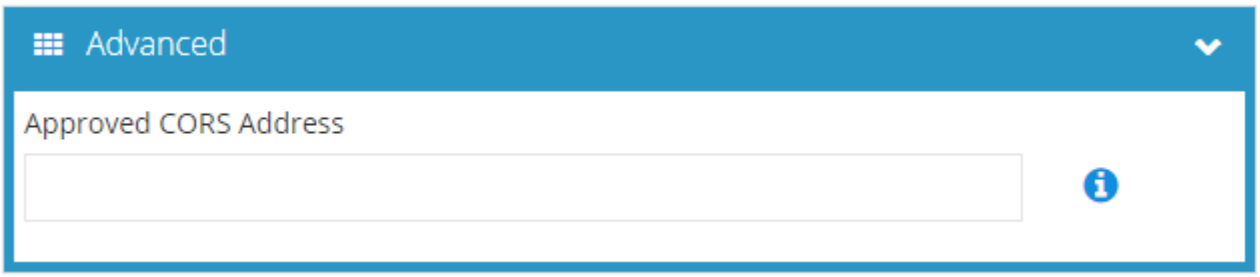
Version 4.1.2 – 29/07/21

Inception release 4.1.2 includes several feature updates and resolved issues.

New Features

CORS Support

Support for Cross-Origin Resource Sharing (CORS) has been added with this release. By default, CORS is disabled on Inception devices, however if the Inception REST API must be accessed via cross-origin requests, the origin address to allow through can be provided in a new Advanced section on the **[Configuration > General > Network]** page.



Feature Updates

Hang Up After Modem Alarm Report

An additional option has been added to the USB Modem configuration that will cause it to hang up the line after reporting an alarm.

By default, the modem attempts to keep the line open after establishing a connection and sending an alarm. This allows multiple alarms to be sent in a single dial, maximising the speed at which alarms can be reported, and is especially useful when connected to a universal transmitter via dialler capture. If the modem is connected to a standard phone line that is shared with other devices though (such as a fax machine), this option will cause the modem to hang up the line after sending an alarm. Note that this means each alarm requires a dial attempt, which can drastically slow down the rate at which alarms can be reported.

Module Substitution Enhancement

The Module Substitution alarm event, which is reported when a new/substituted module is detected after a LAN Secure has been performed, has been upgraded to detect Controller impersonation. This could occur naturally if two controller LANs are connected together, or if the LAN is being tampered with.

Issues Resolved

Tech On Site IRFast Reporting

An issue has been resolved where the Tech On Site reporting event was using a different ID compared to what is documented when using IRFast. The documentation stated this event would be C01:S33, however Inception was sending C01:S32

Inception will now send this event as C01:S33, inline with the documentation.

Version 4.1.1 – 13/05/21

Inception release 4.1.1 includes numerous feature updates based on requests and suggestions over the recent months.

Note: The minimum firmware version for SLAM modules has been updated, and the firmware files packaged along:
SLAM – 4.0.5. Allows Inception to support offline REX/REN functionality. See the below release notes for more information.

New Features

End-User License Agreement (EULA)

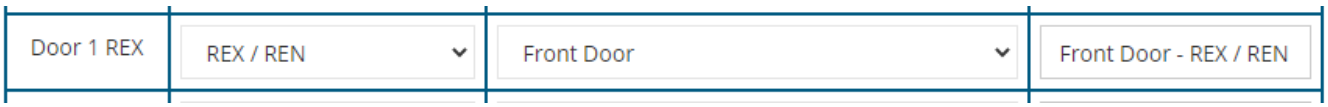
A new EULA page has been added to the web interface. The agreement must be accepted on first login in order to use the web interface.

Feature Updates

Offline SLAM REX Support

Support is now available for REX/REN buttons when a Standard LAN Access Module is unable to communicate with the controller. For this feature to work, the REX or REN button must be wired into the correct input for the correct door on the module and the input must be assigned REX / REN behaviour for that door in Inception's hardware wizard.

Note this requires the SLAM firmware to be updated to 4.0.5 or newer.



LCD Terminal – "LAN Secure" function

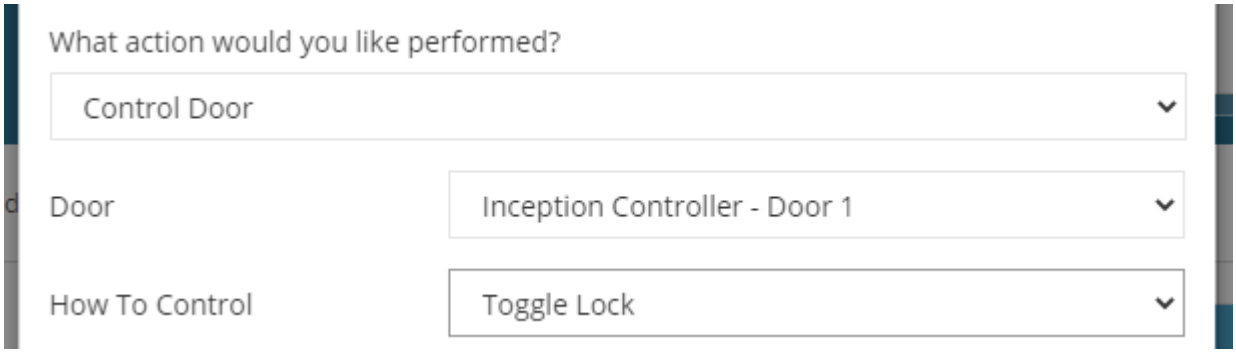
The "LAN Secure" function has been added to the LCD Terminal's Installer menu (keypad shortcut: Menu -> 7 -> 6). This function protects the LAN against module substitution, same as the "Send LAN Secure" button on the **[State / Control -> Hardware Test]** page of the web interface.

Scheduled Tasks – Email Sender

The name of the Inception system is now included in the subject line of emails sent by scheduled tasks to make it easier to identify the sender.

Door Control – Toggle Lock

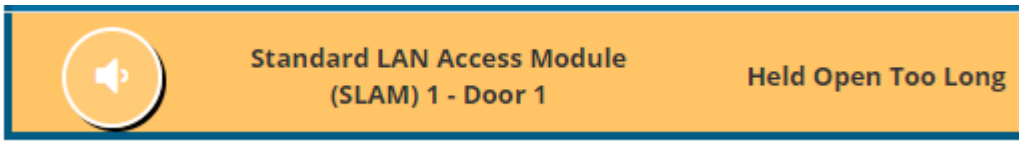
A new “Toggle Lock” door control type has been added for Automated Actions, which locks the door if it is currently unlocked, and vice versa. This new action type can also be triggered from the REST API.



Door Control – Mute DOTL Response

An option has been added to mute the DOTL (Door Open Too Long) response for doors. When a door on the Control Doors page is in the DOTL state, clicking the quick action button will mute the DOTL response. Clicking the quick action button a second time will unlock the door. Logging into an LCD terminal associated with the door will also show the Mute DOTL response screen if the user has permission to control it.

This allows an easier way to let a door stay open when required while silencing any beepers or reader feedback.



REST API – User Config

A new “Generate Unused PIN” function has been added to the REST API to enable a guaranteed valid PIN to be generated for user creation purposes. See the Inception REST API release notes for additional information on usage.

Web Interface – Time Period Editor

The date/time editor control has been improved to allow selection to the exact minute, instead of 5-minute intervals. This affects time editors on the Time Periods page, the Review Events page, the Manage Users page.

Issues Resolved

Connections - TCP (Server)

An issue was fixed where an error in the TCP connection could cause the unit to reset in rare cases.

Login Page

An issue was resolved for a small batch of Inceptions that were produced without ‘IN’ in front of the serial number where the login page would not load in some cases, preventing access to the web interface.

Version 4.1.0 – 03/12/20

The 4.1 release of Inception includes several changes to prepare for compliance with various intruder UL standards. Also included is better support for Single EOL configurations

New Features

USB Dialler Support

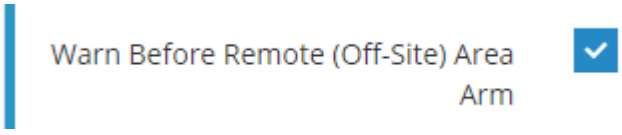
International Markets Only
Inception now supports alarm reporting over USB Dialler connections. This feature is intended for use internationally with universal dialler capture communicators.

USB Diallers can be configured from the Alarm Device Configuration section on the Alarm Reporting settings page.

A new “Device Path Status Source” field for USB diallers has also been added to the Alarm Device Configuration page. The Path Status source field specifies how the device reports its “Path Active” state: “Device Integration” is for devices whose high-level integration reports the status directly to Inception, and “One Input” is for devices that control the state of a hardware output (which is wired to an Inception input) to represent when paths are available.

Remote Area Arm Warning

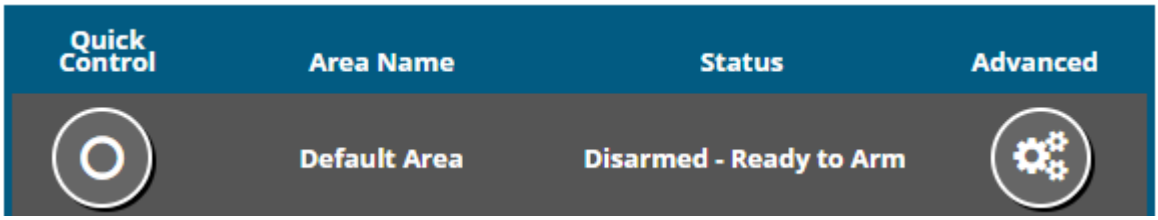
An option has been added to the General section on the System Settings page where if an area is armed remotely it will enter an Arm Warning phase instead of arming straight away, alerting anyone who may be on site.



A “remote” or “off-site” arm is defined to be an arm request that originates from the web interface (i.e. the **[State / Control > Control Areas]** page), the SkyCommand app, or any REST API integrations that signify that their requests are remote.

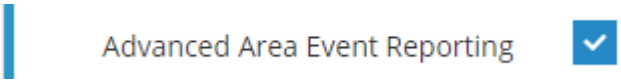
"Ready to Arm" Area Status

Areas will now indicate if they are ready to arm in the web interface or LCD terminal. The "Disarmed - Ready to Arm" state indicates that all non-exit path inputs in the Area are secure. If any of the inputs are not secure, the Area's state will display "Disarmed – Active Inputs" instead.



Advanced Area Event Reporting

A new "Advanced Area Event Reporting" option has been added to the Alarm Reporting settings page in the Reporting Configuration section. This option allows for more granular Area states to be reported via Contact ID and is required for compliance with UL standards.

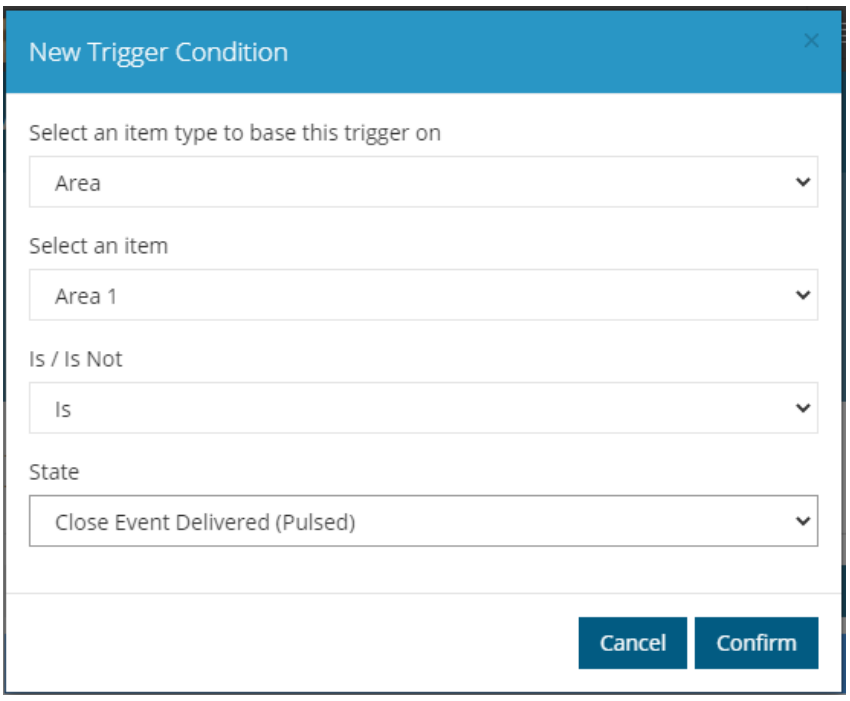


- Areas armed with isolated inputs will report "Partial Arm" instead of a standard Close event.
- Areas disarmed during the Arm Warning phase will report that the arm attempt was cancelled.
- Area arm attempts that fail due to unsealed inputs will report an Unsuccessful Arm Attempt.

Feature Updates

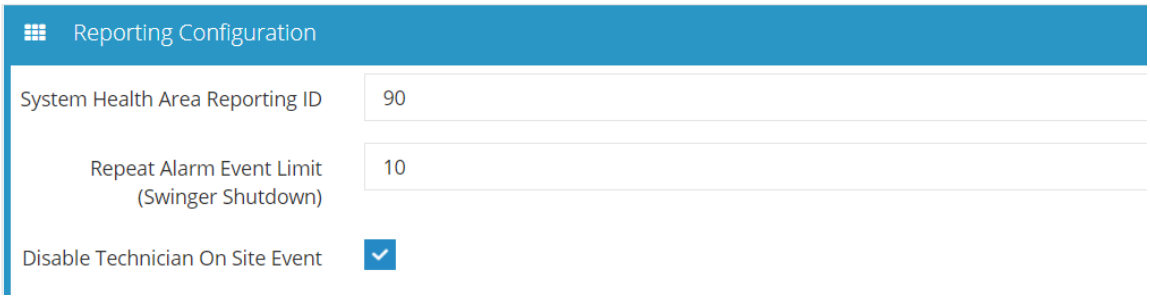
Area Automation – Successful Report of Area Close

To comply with UL2610 standards, a new "Close Event Delivered (Pulsed)" trigger condition type has been added for Areas on the Automated Actions page. This event is triggered when an Area Close event for the area is successfully delivered to a monitoring station.



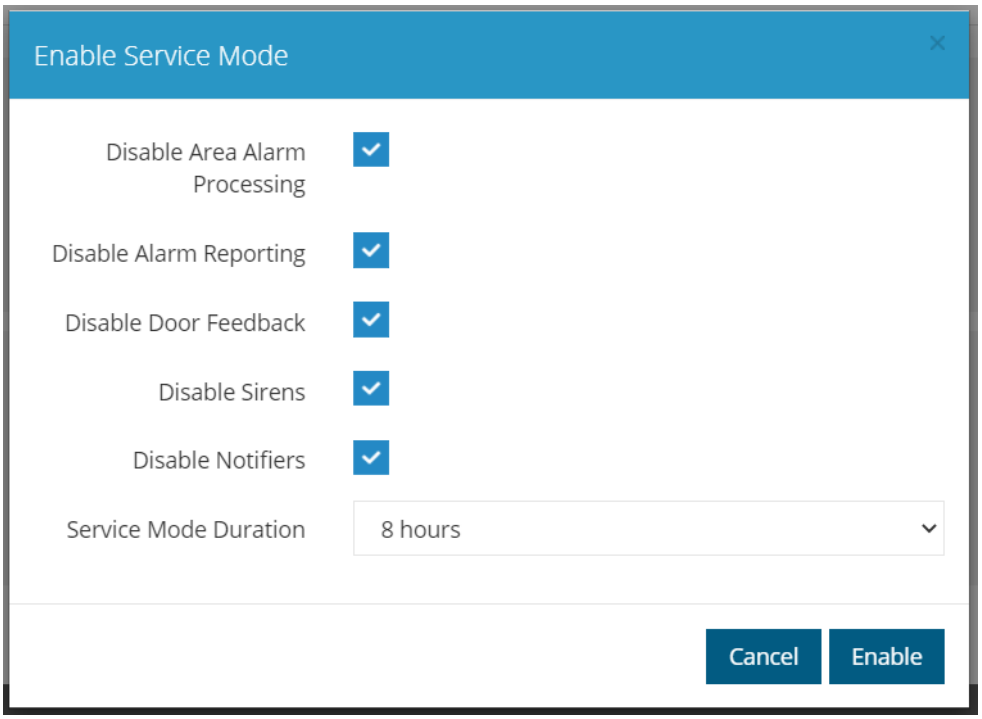
Disable "Tech on Site" Event

A new option to disable the "Technician on Site" event (originally added in release 3.3.0) has been added to the **[Configuration > General > Alarm Reporting Settings]** page. This option is recommended in cases where the monitoring station is having trouble handling the event.



Service Mode – Disable Notifiers

Service mode now has a "Disable Notifiers" option that prevents any email or push notifications from being sent while service mode is active. Previously, notifications for module health and other issues were being sent to users during service mode, despite alarms and sirens being disabled.



Issues Resolved

Improved Single EOL Support for Switch/Button Inputs

Previously the use of a Single EOL configuration required that all inputs required an EOL resistor to work. This included Switch or Button inputs such as REX/REN buttons. This is resolved with this release, no longer requiring an EOL resistor on these input types.

A short on a Switch / Button input causes it to be active, while an open circuit or the sealed resistor is inactive. This can be reversed with the Swap Active and Secure States option on the **[Configuration > Inputs > Hardware Inputs]** page.

Version 4.0.0 – 15/10/20

SLAM 4.0 – The minimum supported firmware for the Standard LAN Access Module (SLAM) is now 4.0. This change includes better support for the SIFER Reader Tampers.

New Features

Two-Factor Authentication (2FA)

Two-Factor Authentication is now supported for Inception web interface login with the use of the Google Authenticator smartphone app or a compatible app that supports TOTP-based 2FA codes. For more detailed information, see the Inception technical note for configuring 2FA (a separate document).

Dynamic User Import Module (DUIM)

The new DUIM feature allows you to automatically import new user data from CSV files copied into a network share folder. This allows user data exported from other systems, such as booking or payroll systems, to automatically be loaded into an Inception controller. Users can be dynamically added, updated, or cancelled , based on the information from another system.

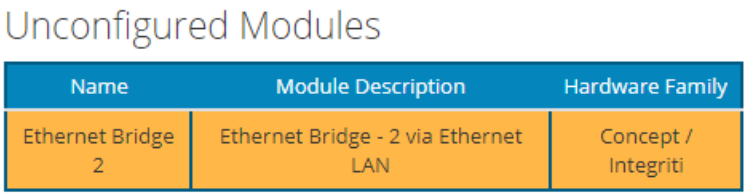
For more detailed information, see the Inception technical note for configuring DUIM (a separate document).

Up to 96 Area Now Supported

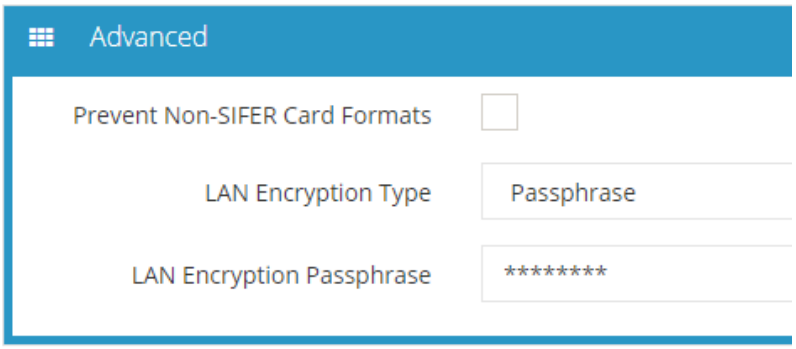
The maximum number of supported Areas has been increased to 96 from the current 32. This allows a granular site setup with more fine-grained security or access control areas. It also allows better support for storage locker sites and other similar scenarios.

Ethernet Bridge Module Support

The Ethernet Bridge LAN module is now supported. The Ethernet Bridge communicates with the controller over a standard Ethernet LAN connection on your local network and allows you to discover and enrol modules that attached to the bridge via the RS485 LAN.



The Ethernet LAN encryption key can be set from the **[Configuration > General > System Settings]** page if a custom key or passphrase is required for additional network security.



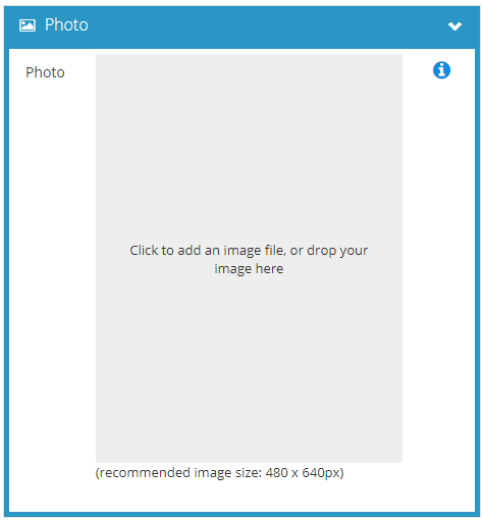
New Features (cont.)

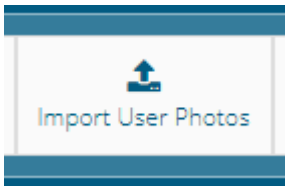
Ethernet Bridge Module Support (cont.)

On the System Settings page, Inception can also initiate a changeover of the Ethernet LAN encryption key to migrate an Ethernet Bridge from an old key to a new one.

User Photos

Photos can now be uploaded for Inception users on the Manage Users page. Photos can be uploaded, cropped and resized for individual users by using the Photo field on the Manage Users page or uploaded in bulk by using the Import User Photos dialog.





User photos are displayed in user-related events on the Review Events page, on the Search Users page, and in the User Details Report. User photos can also be uploaded, modified, or deleted with the Inception REST API, and have been incorporated into the Milestone ACM integration.

It is recommended that user photos be at least 480 x 640 pixels and 3:4 aspect ratio (i.e. portrait) for maximum visual quality in the web interface.

Showing 332 Events (filtered from 512 total events)

When	Message	Who	What	Where
07/09/2020 09:15:04	Web Login was Successful by User	 Installer		
07/09/2020 09:00:00	Time Period went Active		Working Hours	

Showing 6 to 11 of 12 entries

Edit	Name	Photo	Web Page Profile	Email Address	User Expiry Time
	Installer		Installer		
	SCTest		Control and User Admin		

New Features (cont.)

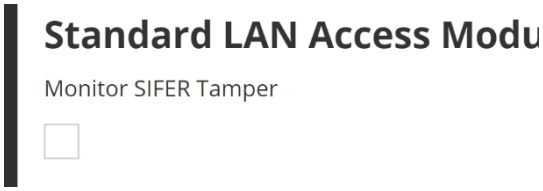
Reader Tampers

The Tamper state for SIFER and Wiegand Readers can now be monitored with this release. If a reader tamper occurs, the system will communicate this hardware event to a monitoring station if alarm reporting is enabled and correctly configured. The event will be based on the Door it is connected to, so a "Door reader tamper event on the Front Door" to help in identifying where the event occurred.

In addition, like other System Tamper states (cabinet, siren), all areas will go into alarm, regardless of whether the area is armed or not and will need to be disarmed to stop strobes and sirens sounding. This response can be disabled on specific areas by using the *Ignore Module Health Issues* area option.

- **SIFER Reader Tampers**

With the SLAM 4.0 update, the Tamper state for SIFER Readers can now be monitored. Like with the other hardware health options, the Hardware Wizard (**[Configuration > Hardware]** page) is used to tell Inception whether to monitor the SIFER Tampers for readers attached to an Inception Controller or a SLAM.



- **Wiegand Reader Tampers**

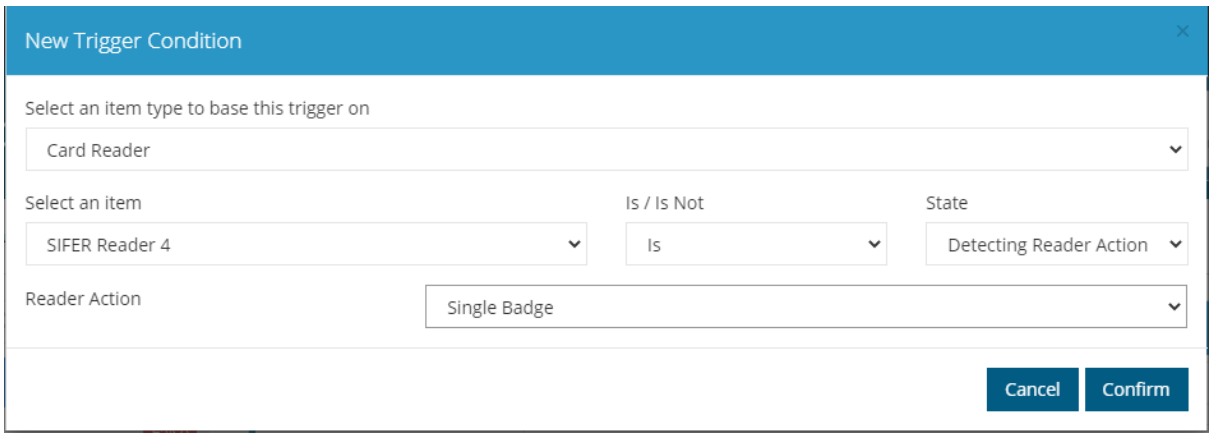
A new Input Behaviour has been added to allow monitoring of the tamper state of Wiegand readers. Note that this input does not need to be monitored directly. By using this input behaviour, the system will have the same response as SIFER reader tampers, triggering a module health response.

Hardware Point	Behaviour	Linked Door	Name
Door 1 REED	Not Wired	No Door	
Door 1 TONG	Not Wired	No Door	
Door 1 REN	Reader Tamper	Front Door	Front Door - Reader Tamper
Door 1 REX	Not Wired	No Door	

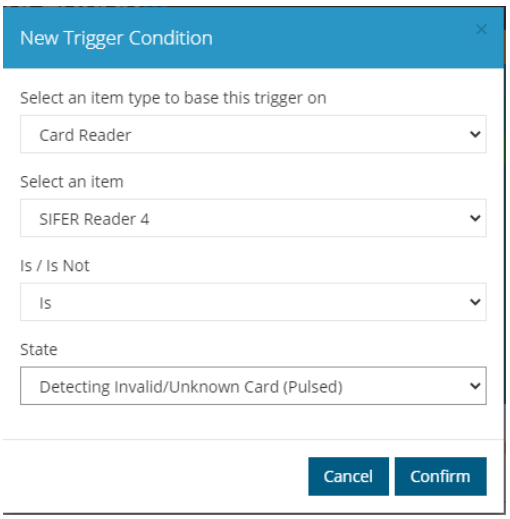
Feature Updates

Automated Actions - Reader Triggers

"Single Badge" has been added as a new Reader Action option for Reader Triggers. This event will only trigger for the first card badge in a multi-badge action performed at a reader, in contrast to the Valid Card event which triggers for every successful card badge.

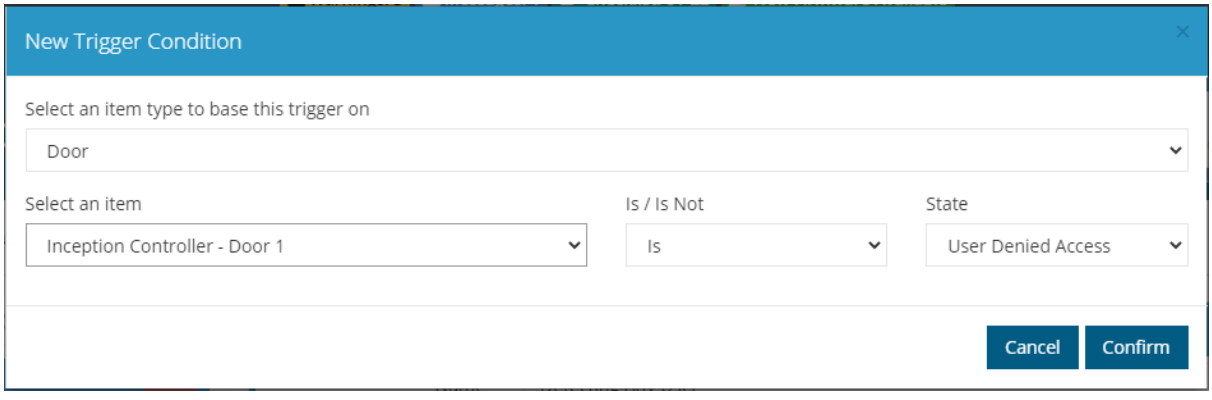


An "Invalid/Unknown Card" trigger event has also been added for Readers. This event triggers when an unrecognised card is presented at a reader, that is, a card that is not assigned to a user. Note that this event will not trigger for a credential that does match a user, but they don't have permission to the door. The new trigger described in the following section should be used in that scenario.



Automated Actions - Door Triggers

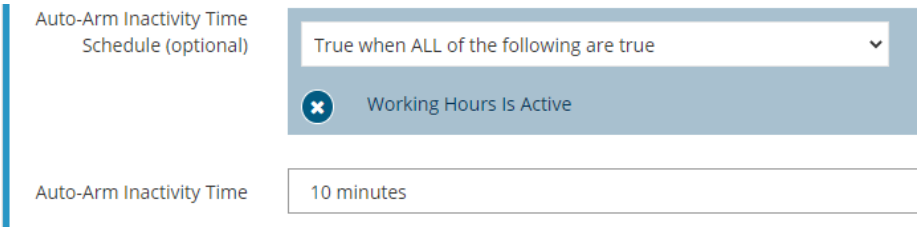
A "User Denied Access" trigger event has been added for Doors. This event triggers when a user is denied access to a door due to insufficient permission, anti-passback logic, or door lockout.



Feature Updates (cont.)

Areas – Auto Arm Inactivity Time Schedule

The *Auto-Arm Inactivity Timer* behaviour can now be qualified by an optional schedule, so that the auto-arm logic will trigger after detecting no input activity for the chosen time interval, but only if the schedule condition is active. An empty schedule is treated as an always-on schedule. This schedule can be configured in the Auto-Arm section on the **[Configuration > Areas > Edit Areas]** page.



Note that if a qualifier schedule is configured, the inactivity time only starts once that schedule becomes true. So, a 30min inactivity time qualified by a time period that becomes true at 7PM would only be able to arm at 7:30PM, even if the area has been empty for a long time.

System Warning – Door Held Open

A new system warning has been added for when one or more doors are in the "Held Open Too Long" state. The warning can be resolved by closing the affected doors or unlocking them.

Access Denied Event

A new system message has been added for when a user is denied access to a door or lift car. The message includes the user's name, the name of the door or lift car, the time of the access attempt, and the reason why access was denied. This message ensures attention is drawn to the fact someone attempted to access something they did not have permission to.

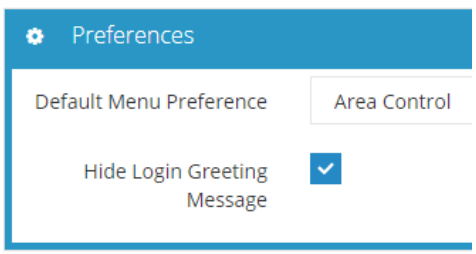
New "Access Denied because User Expired" review events have also been added for doors and lift cars. These events are also included in Access History Reports generated from the Reports page.

LCD Terminal Profiles – Hide Greeting

An option has been added to LCD Terminal Profiles to disable the login greeting message that is usually displayed when a user logs in. To use the option, tick the "Hide Login Greeting Message" checkbox in the Preferences section on the **[Configuration > Users > Terminal Profiles]** page.

LCD Terminal – Jump to Area Control

When a user logs into an LCD terminal while a visible area is in alarm or arm warning mode, they will be taken directly to the Area Control screen if they have permission to control it. Previously the user was only taken to the Area Control screen if the terminal's Associated Area was in alarm or arm warning mode.



Issues Resolved

Inovonics Timeout Error

March 2022

An issue was fixed where setting the timeout to 1 day would actually result in almost immediate timeout.