# inception

WEB POWERED SECURITY

Simple & Easy Installation

Integrated Security - Access Control

Release Notes 6.0.1

23/11/2023

www.innerrange.com

inner range

Intelligent Security Solutions

# Table of Contents

November 2023

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

# 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.

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## 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.**

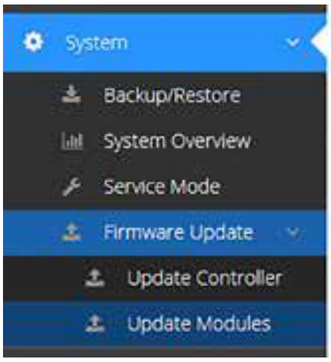
| Expansion Module | Firmware Version |
|---|---|
| 8 Input LAN Expander | 3.2.0 |
| UniBus 8 Input Expander | 1.0.3 |
| UniBus 8 Relay Expander | 1.1.2 |
| Standard LAN Access Module (SLAM) | 4.0.7 |
| Intelligent LAN Access Module (ILAM) | 4.1.0 |
| SIFER Reader | 1.16.0 |
| T4000 Security Communicator | 2.1.4 |
| Inovonics RF Expander | 1.1.0 |
| EliteX Keypad | 3.1.0 |
| LAN Ethernet Bridge | 1.1.0 |

## How to Update Modules

### How to check your expansion module versions and update them:

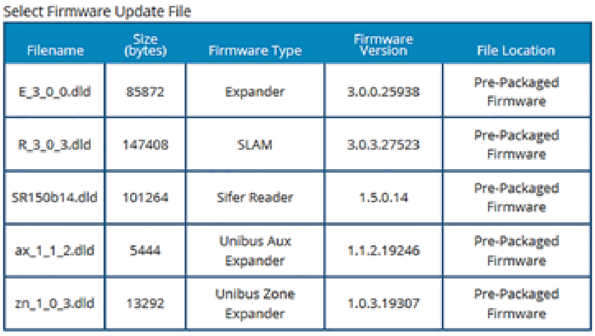
*Note: The T4000 is updated separately, either via the Multipath Bureau software or by the monitoring station.*

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 |

November 2023
The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## Version 6.0.1 – 23/11/2023

**Inception 6.0.1 resolves issues introduced in 6.0.0 surrounding the ILAM and SLAM modules, Aperio wireless locks, and review messages.**

## Issues Resolved

### SLAM/ILAM Generic Outputs Were Not Controllable

Resolved an issue where control of outputs configured as Generic Outputs on an ILAM or SLAM, whether automatic or through a user, would display correctly on the Inception but not be controlled on the actual hardware module.

### Last User Being Missed in ILAM Offline Review

Resolved an issue where ILAM review events from offline mode would not come through for the last listed user in the Inception system if users in the system had more than one credential.

### Aperio Wireless Locks Not Following Free Access

Resolved an issue where Aperio Wireless locks would not follow free access time period functionality of associated time periods.

### Aperio Wireless Locks Manual Control Issues

Resolved an issue where Aperio Wireless locks would not lock or unlock via manual user control.

## Cyber Security Updates

1 cyber security issue has been resolved in this release.

Inner Range strongly recommends keeping up to date with the latest firmware.

Every release incorporates the latest security and vulnerability patches, helping to protect your devices from known and emerging threats.

We do not share the details of security-related issues to avoid compromising clients that are still using previous releases. Inner Range will issue security bulletins detailing any disclosed vulnerabilities to accredited security technicians.

## Version 6.0.0 – 19/10/2023

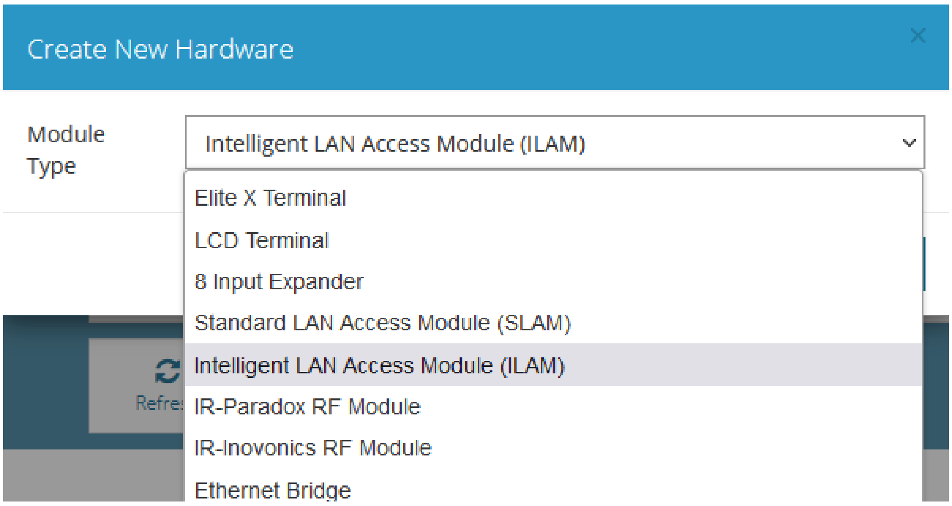
**Inception 6.0.0 introduces support for the Intelligent LAN Access Module (ILAM), which includes support for offline functionality as well as integration with Aperio wireless doors. Additionally, support has been added for the inversion of the active and tamper states on hardware inputs.**

Note: The minimum firmware version for the 8-Zone LAN Expander has been updated to 3.2.0, due to bugfixes to the module's power cycle and siren tamper behaviours.

## New Features

### ILAM (Intelligent LAN Access Module) Support

The Inception system now supports Inner Range's Intelligent LAN Access Module (ILAM). The ILAM is a 2-door access control module, which is expandable up to 8 doors with 2-door UniBus expanders. Up to 8 Wiegand readers, or 16 SIFER or OSDP readers can be connected to the module. Lock outputs, door reed and tongue inputs, door REX and REN inputs, valid and invalid outputs and Door Open Too Long (DOTL) outputs are all on-board for wired doors. The ILAM is now an available option in the list hardware modules on the **[Configuration > Hardware]** page.


Create New Hardware

Module Type: Intelligent LAN Access Module (ILAM)

The ILAM includes an offline operation mode, allowing for limited access control functionality in the event the ILAM loses connection to the Inception system. When the ILAM's status is offline on the Inception, the ILAM will continue to process access requests to its connected doors, allowing/denying entry into the doors, and keeping a record of these events. When connection is regained, these access events will be synchronised back to the Inception system as review events, and the Inception will begin synchronisation of its database with the ILAM's offline database.

For in-depth coverage on the ILAM's offline database functionality and limitations, please refer to the *Inception Tech Guide – ILAM Offline Guide*, which is now available on the Inner Range website.

### Wireless Door Support – Assa Abloy Aperio

Alongside the release of the ILAM, the Inception system now includes a powerful bi-directional interface to the Assa Abloy Aperio wireless locking system, using the ILAM's Reader RS-485 port. This interface provides the full capability of standard hardwired doors to Aperio wireless doors.

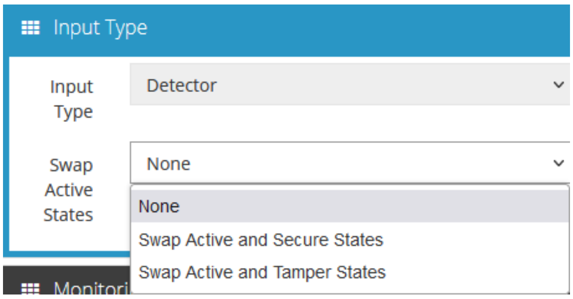
With no need to wire directly down to the door when using Aperio wireless locks, installation costs are dramatically reduced. In addition, a large range of door furniture options are available within the Aperio range to appeal to end-users and architects alike. The Inception system manages Aperio wireless doors in the same way as a traditional wired door, allowing configuration of the wireless doors through the standard hardware wizard. The similar configuration and interaction as hardwired doors mean that there are no additional special training or programming requirements.

A corresponding tech guide *Inception Tech Guide – Aperio Wireless Doors* is now available on the Inner Range website, providing an in-depth overview of this new integration, as well as installation instructions.

## Feature Updates

### Swap Input Active and Tamper States

Hardware inputs can now be optionally set to have their active and tamper states swapped. This option is intended for sites where most inputs follow the standard EOL logic, however some sensors (fire sensors, etc.) behave differently and require that their alarm and tamper state are flipped.


Input Type

Input Type: Detector

Swap Active States: None

To facilitate this change, the existing *Invert Active and Secure* checkbox has been replaced with a dropdown, allowing the input to be configured with one of three options. Note that the option can only be used for standard EOL inputs, it cannot be used for two state inputs (switch/button) as they do not have a tamper state.

## Issues Resolved

### Storage Blocks Stuck in Secure Pending

Fixed an issue where Storage Blocks could potentially not move from “Some Units Secure Pending” to “All Units Secure” when its monitored unit that was in the “Secure Pending” state is marked as “Vacant”.

### SLAM Offline REX/REN Required Powercycle

SLAM offline REX/REN configuration will now be applied instantly, rather than after the module has been initialized again on the Inception LAN.

## Cyber Security Updates

2 issues have been resolved in this release.

Inner Range strongly recommends keeping up to date with the latest firmware.

Every release incorporates the latest security and vulnerability patches, helping to protect your devices from known and emerging threats.

We do not share the details of security-related issues to avoid compromising clients that are still using previous releases.  Inner Range will issue security bulletins detailing any disclosed vulnerabilities to accredited security technicians.

## Version 5.2.0 – 04/07/23

**Inception 5.2.0 adds a range of features, updates and bugfixes for Storage Units and Storage blocks. Other notable additions include a new Alarm Cancel option for Areas, Invalid Certificate handling for HTTP connections, and Door permissions now allowing distinction between Entry and Exit.**

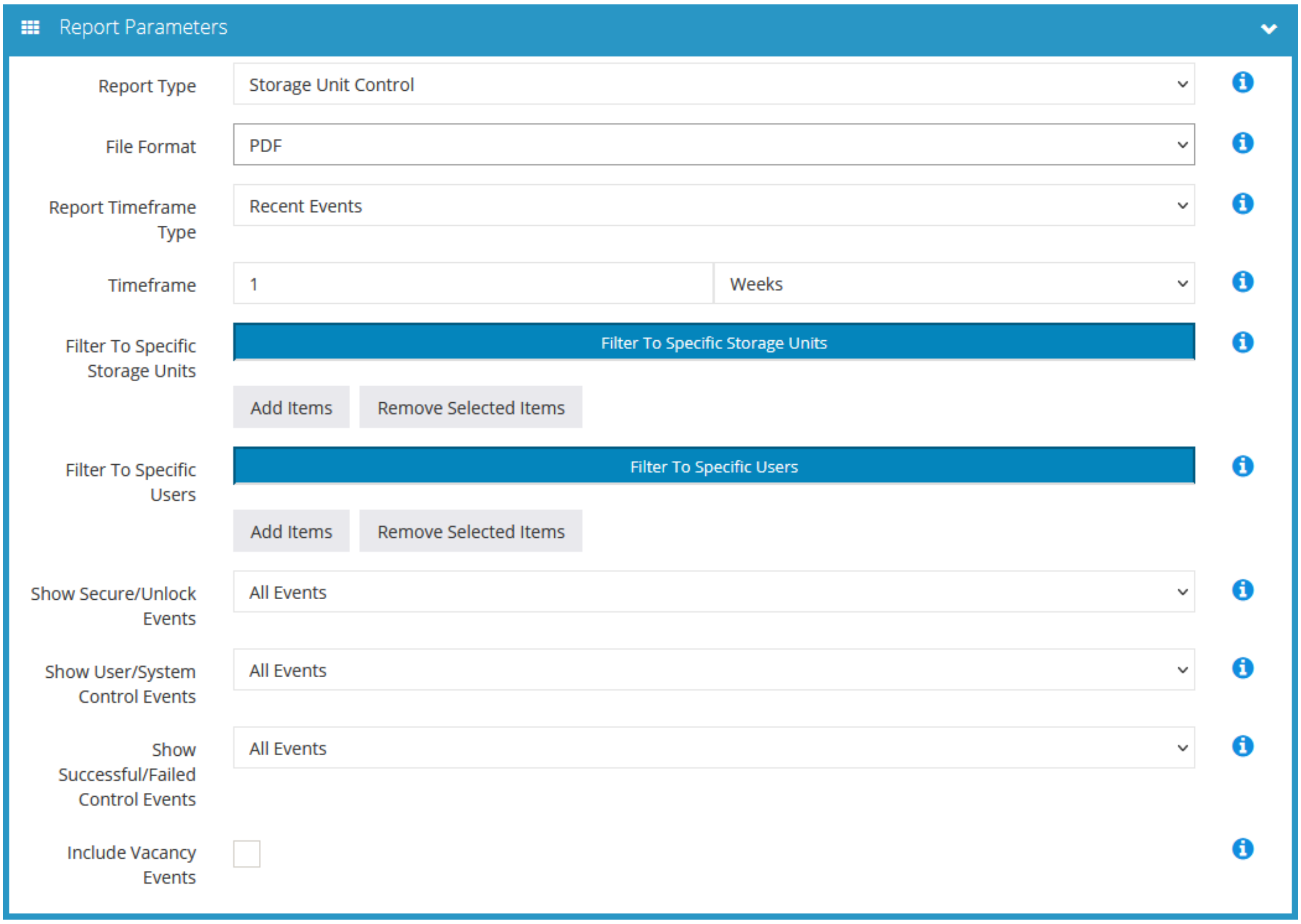
*Note: The minimum firmware version for LAN Ethernet Bridge has been updated to 1.1.0, which improves connectivity between the Inception and the Ethernet Bridge.*

## New Features

### Storage Unit Access Report

A new report type of *Storage Unit Control* has been added to **[System > Reports]**, allowing for the filtering and reporting of Storage Unit access events.

Similar to the Area Access report type, operators can utilize this new report type to differentiate between Storage Units, Users and event types, all within a specified timeframe.



Report Parameters

Report Type: Storage Unit Control

File Format: PDF

Report Timeframe Type: Recent Events

Timeframe: 1 Weeks

Filter To Specific Storage Units

Filter To Specific Users

Show Secure/Unlock Events: All Events

Show User/System Control Events: All Events

Show Successful/Failed Control Events: All Events

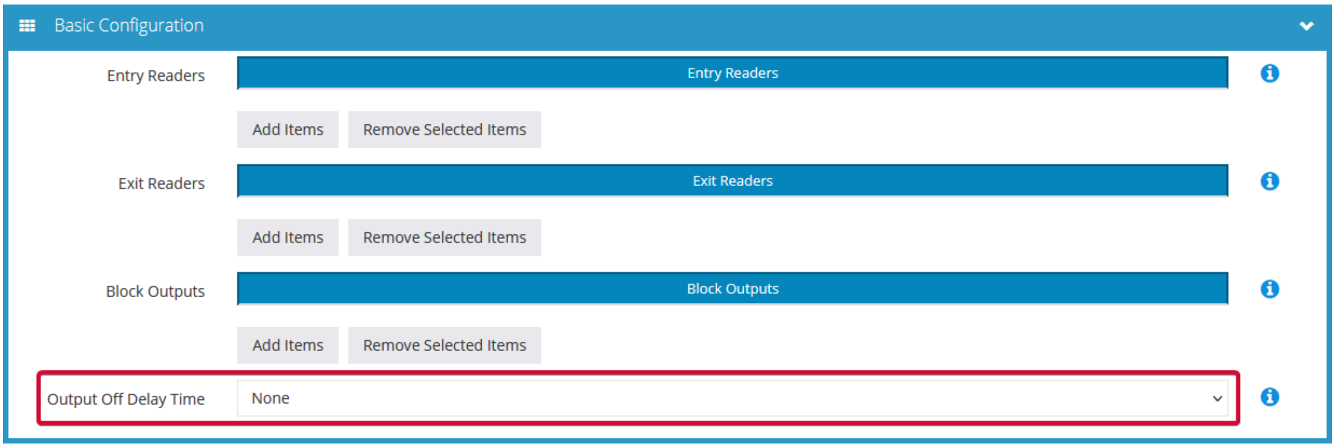
Include Vacancy Events: □

## Feature Updates

### Storage Block Delay for Output Control

A new *Output Off Delay Time* option has been added to Storage Blocks. This option allows a delay to be defined before the Storage Block's outputs are turned off. When set to *None*, these outputs will turn off immediately when all units in the block are secure. When set to any other value, the outputs will wait this amount of time before turning off.

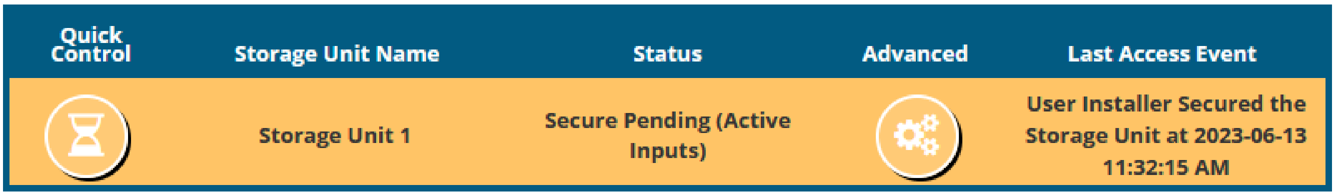
This is useful for scenarios where the final unit was secured at a keypad inside the facility, and some time is required for a person to leave before the interior lights are turned off.



Output Off Delay Time: None

### Storage Units Only Secure with No Activity

Storage Units have had their default behaviour changed to only secure the unit once all its inputs have secured. If any of its Inputs are in Alarm when the Secure command is sent, the Storage Unit will instead move to a *Secure Pending (Active Inputs)* state. The unit will remain in this state until either unlocked, or all its inputs are sealed, in which case it will transition automatically to the *Secure* state.



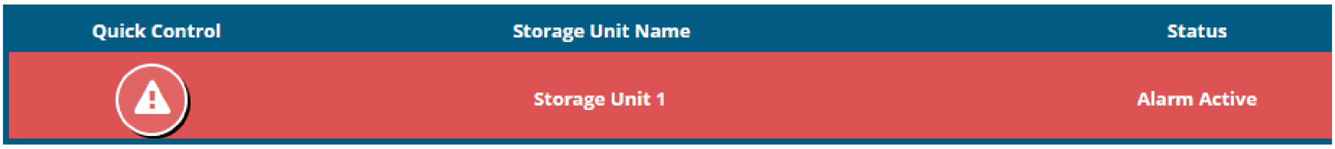
| Quick Control | Storage Unit Name | Status | Advanced | Last Access Event |
|---|---|---|---|---|
| ⌛ | Storage Unit 1 | Secure Pending (Active Inputs) | ⚙ | User Installer Secured the Storage Unit at 2023-06-13 11:32:15 AM |

This behaviour was added to address scenarios where multiple people are in their Storage Unit, then one badges at the exit reader while the other person is still within the Storage Unit. With the original behaviour, the Storage Unit would then instantly go into alarm due to unsealed inputs (door reed, motion sensors, etc.). However, with the new behaviour, the Storage Unit will instead go into the *Secure Pending (Active Inputs)* state, then automatically secure once all the inputs have secured, due to the final occupant having left the Storage Unit.

The original functionality of forcefully securing the Storage Unit regardless of monitored input state can still be enabled within the Storage Unit's parent Storage Block configuration, by checking the *Force Secure Units with Active Inputs* checkbox. Sites with existing Storage Blocks configured will have this option ticked by default upon upgrading their firmware, to retain previous functionality. However, newly created Storage Blocks will have this checkbox unticked.

### Storage Unit Latched Alarm State

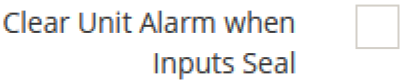
Alongside the *Secure Pending* logic implemented above, Storage Units no longer have the default behaviour of restoring back to the Secure state upon all inputs resealing. Instead, once a Storage Unit has transitioned to Alarm, it will remain in alarm until the unit is unlocked, or a new *Clear Alarms* action is performed on the unit. This *Clear Alarms* action is now the default *Quick Control* action that is performed via **[State / Control > Control Storage Units]** on Storage Units that are in alarm. This action will attempt to move the Storage Unit back into the *Secure* state, depending on whether the unit still has unsealed inputs, or the operator has the appropriate permissions. Additionally, the unit's alarm state can be cleared by the user unlocking the unit.



| Quick Control | Storage Unit Name | Status |
|---|---|---|
| ⚠ | Storage Unit 1 | Alarm Active |

This change was made to address scenarios such as where an intruder would trigger an alarm on a Storage Unit's monitored input (such as a door reed), moving the unit into alarm, but then close the door behind them, causing the unit to revert back to the Secure state despite the unit having been breached. With the new default behaviour, the Storage Unit will remain in alarm even if all inputs are resealed.

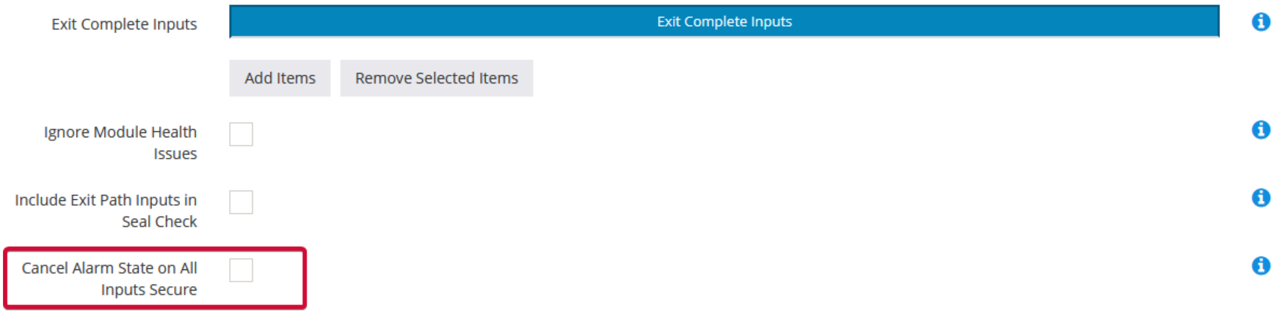
This logic can be toggled using the *Clear Unit Alarm when Inputs Seal* checkbox in the Storage Unit's parent's Storage Block configuration. When enabled, Storage Units that are handled by the Storage Block will retain old behaviour of automatically resecuring the unit upon all inputs sealing. Upon upgrading firmware to this version or later, previously configured Storage Blocks will have this checkbox ticked, preventing existing sites from unwanted changes. However, newly created Storage Blocks will have this checkbox unticked.



Clear Unit Alarm when Inputs Seal □

### Area Option to Cancel Alarm on All Inputs Secure

*Cancel Alarm State on All Inputs Secure* is a new Area option that allows an Area's state to be automatically cleared when all the Area's monitored inputs are sealed. Following this, an *Alarm Cancelled* event will be sent to the monitoring station, and all sirens and strobes will be stopped.



Exit Complete Inputs: Exit Complete Inputs ℹ

Ignore Module Health Issues □ ℹ

Include Exit Path Inputs in Seal Check □ ℹ

Cancel Alarm State on All Inputs Secure □ ℹ

This new option is specifically designed for areas that are monitoring latched inputs, where another action is required to secure the input (duress inputs or emergency exit buttons with a manual release, storage unit alarm inputs with *Clear Unit Alarm when Inputs Seal* set, etc.).

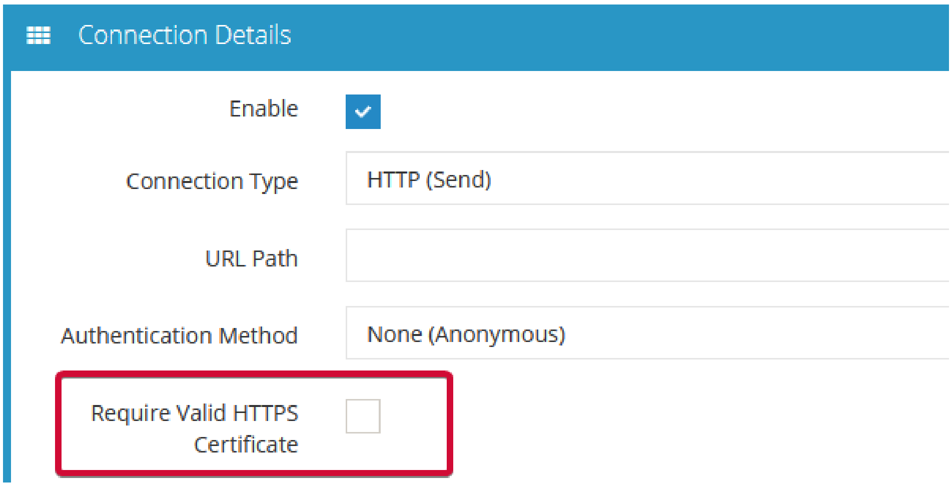
For example, when the calculated input of a Storage Unit this Area is monitoring moves into alarm, the Area will respond according to the input's process group, potentially moving the area into the alarm state, sending an event to the monitoring station, and triggering the appropriate sirens and strobes. The Storage Unit owner can action the alarm on their unit, either by unlocking the unit or performing a *Clear Alarms* action. With *Cancel Alarm State on All Inputs Secure* enabled, the Storage Unit's calculated input will be resealed, and the monitoring Area will send an *Alarm Cancelled* event to the monitoring station, stop its sirens and strobes, and move the area back into the *Armed* state.

This new behaviour was added to address scenarios where the Storage Unit had gone into alarm, then being unlocked by the Storage Unit customer, however monitoring had not received confirmation of the alarm being cleared, so a security guard callout and cancellation of the site's sirens still being required (particularly detrimental for unmanned sites).

## Invalid Certificate HTTPS Support for HTTP Send Connection

The original behaviour of the *HTTP (Send)* connection type, when connecting over HTTPS, was to only accept SSL certificates that had been issued by a certificate authority. This could lead to situations where the Inception system would refuse to connect to a local system with a self-signed certificate, or directly via IP without going through a secure DNS.

To address this, a *Require Valid HTTPS Certificate* checkbox has been added to the *HTTP Send* connection type, configured under **[Configuration > General > Connections]**. This is unchecked by default, meaning the Inception system will perform HTTPS connections to a system, regardless of the remote server's certificate source.



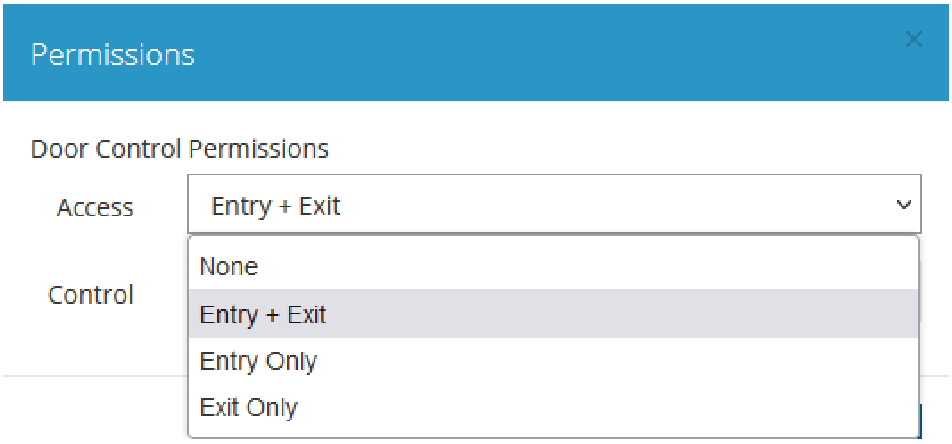
Connection Details

| | |
|---|---|
| Enable | ☑ |
| Connection Type | HTTP (Send) |
| URL Path | |
| Authentication Method | None (Anonymous) |
| Require Valid HTTPS Certificate | □ |

Checking this option forces the Inception to only make HTTPS connections to remote servers with a trusted, certificate authority provided, SSL certificate.

### Separate Door Permissions for Entry vs Exit

The *Access* door permission has been broken into two separate permissions, *Entry* and *Exit*, which can be assigned separately or together to Permission Groups.


Permissions

Door Control Permissions

Access: Entry + Exit

- None
- Entry + Exit
- Entry Only
- Exit Only

Control

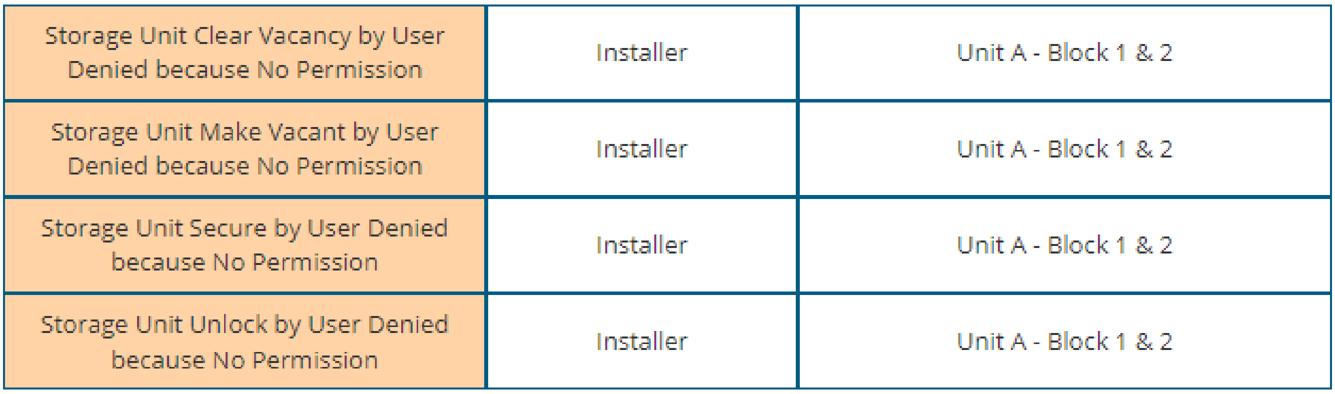
This allows for greater flexibility when configuring access through a door, as it allows for the configuration of *Entry* only permissions to a door without *Exit* permission, or vice versa. Alternatively, this more granular control could then allow the configuration of *Entry* permissions to be set to *Always* in one permission row, and then another permission row that grants *Exit* permission only between working hours, etc.

Existing Door *Access* permissions will be automatically converted to *Entry + Exit* permissions upon upgrading to this firmware version or later.

## Issues Resolved

### No Review for Storage Unit Failed Control

Review events are now logged for scenarios where the operator attempts to secure a Storage Unit that they do not have permission to. Additionally, these events have been broken down into 4 separate event types, depending on the action that was performed.



| | | |
|---|---|---|
| Storage Unit Clear Vacancy by User Denied because No Permission | Installer | Unit A - Block 1 & 2 |
| Storage Unit Make Vacant by User Denied because No Permission | Installer | Unit A - Block 1 & 2 |
| Storage Unit Secure by User Denied because No Permission | Installer | Unit A - Block 1 & 2 |
| Storage Unit Unlock by User Denied because No Permission | Installer | Unit A - Block 1 & 2 |

### Ethernet Bridge Connection Reliablity

The LAN Ethernet Bridge can now re-establish TCP connections to the Inception Controller without its attached modules briefly dropping offline.

## Version 5.1.2 – 08/06/23

**Inception 5.1.2 resolves some issues in the 5.1.1 release with reports, storage blocks, Wi-Fi hotspot, and Service Mode. Additional Door Timed Unlock options have also been added, as well as a floating save button on editor pages.**

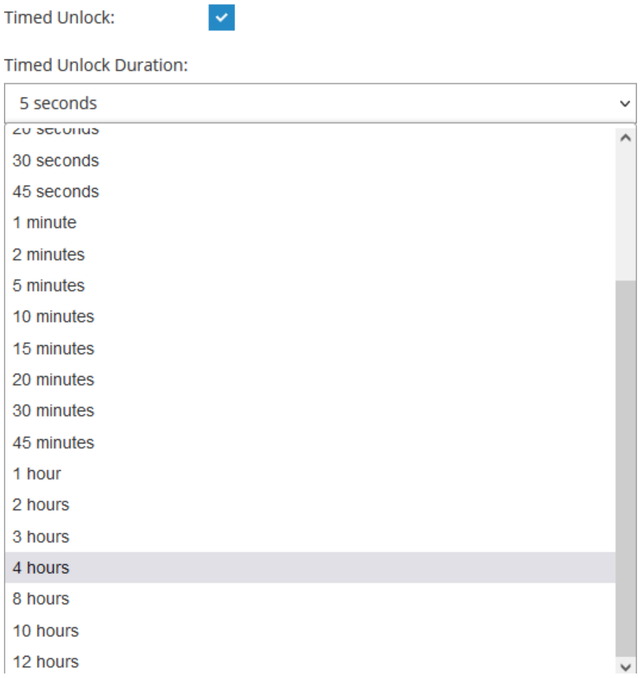
*Note: The minimum firmware version for Standard LAN Access Modules (SLAMs) has been updated to 4.0.7 due to updates to support additional card packets.*

## Feature Updates

### Door Control Timed Unlock Options

Doors can now be timed unlocked for longer durations, with support being added for 8/10/12 hour durations. These additional times have been added to both **[State / Control > Control Doors > Advanced > Timed Unlock Duration]** and **[Automated Actions > Automation > Automated Actions > Control Door Action > Timed Duration]**.

This allows for greater flexibility when controlling doors over longer time periods, such as occasional events lasting most of the day.



Timed Unlock: ☑

Timed Unlock Duration:

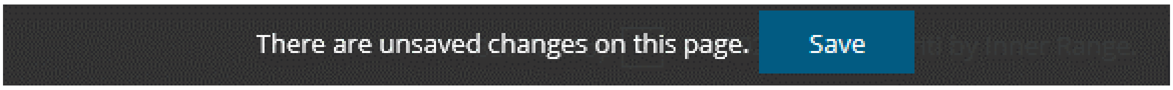
5 seconds

- 20 seconds
- 30 seconds
- 45 seconds
- 1 minute
- 2 minutes
- 5 minutes
- 10 minutes
- 15 minutes
- 20 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 2 hours
- 3 hours
- 4 hours
- 8 hours
- 10 hours
- 12 hours

### Floating Save Button

A floating save button will now show at the bottom of the window when there are unsaved changes on the page. The button will always be visible at the bottom of the window, even while scrolling down the page.

This provides the convenience of being able to save configuration on a page without having to scroll back to the top of the page and save from the toolbar, especially when editing from mobile devices.



There are unsaved changes on this page.

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## Issues Resolved

### History Reports in Negative UTC Timezones

An issue was identified where history reports could not be executed on systems with a negative time zone. All reports can now be generated correctly, regardless of the system's time zone.

### Storage Block Time Values

Storage units will now correctly have their "Unit Unlocked Too Long Time" and "Unit Auto-Resecure Time" logic disabled when the corresponding field in their parent storage block is set to *None*.

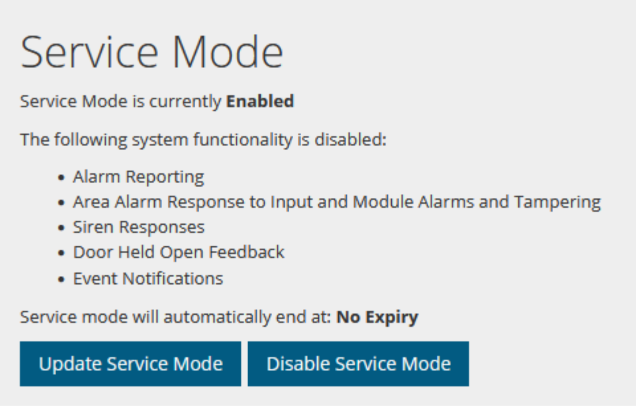
This was to resolve an issue where storage units would instead go immediately into the "Unlocked Too Long" state upon unlocking a unit, or immediately be resecured upon being unlocked, opened then closed.

### WiFi Hotspot Reliability

Improved reliability of WiFi Hotspot mode, especially in situations where the "WiFi Connection Type" was being changed from "Wireless Hotspot" to "Personal" and back to "Wireless Hotspot" in quick succession.

### Service Mode Feature Text

If Notifications are disabled as part of Service Mode, both the service mode summary text and the System Warning for Service Mode now correctly list that Notifications are disabled.



Service Mode

Service Mode is currently **Enabled**

The following system functionality is disabled:

- Alarm Reporting
- Area Alarm Response to Input and Module Alarms and Tampering
- Siren Responses
- Door Held Open Feedback
- Event Notifications

Service mode will automatically end at: **No Expiry**

## Version 5.1.1 – 25/01/23

**Inception release 5.1.1 resolves issues related to editing entities through the web interface in the 5.1.0 release.**

## Issues Resolved

### Date and Time UI Issues

An issue was identified when editing dates and time on any item in the Inception System through the web interface where the incorrect value may be shown compared to what is in the Inception system database. If that item is edited while the display is wrong, the incorrect value would be saved.

### Time Period Editing

An issue was identified where adding a new item to a Time Period’s list of weekly recurring times would only apply the start and end time to the first day selected and added, while the rest would have the default start and end times. All selected days should now be added with the same start and end times.

## Version 5.1.0 – 13/11/22

**Inception release 5.1.0 resolves some issues identified in the 5.0.1 release, and includes updates for OSDP reader management, reports, output control, area arm notifications, calendars, Ethernet Bridges, and many other feature updates and fixes.**

## New Features

### French Canadian Translation

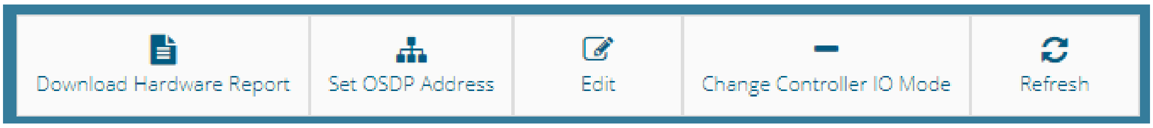
A vendor-supplied French Canadian language pack has been added to Inception and can be chosen when selecting a language pack to use.

## Feature Updates

### OSDP Address Change Option

A new option to change addresses of OSDP readers has been added, accessible under the toolbar in the hardware configuration page at **[Configuration > Hardware]**. When selecting a module with attached readers, the button can be pressed to list all connected 3rd party OSDP readers that can be re-addressed, and a prompt can be followed to select one of the readers to have its address changed.

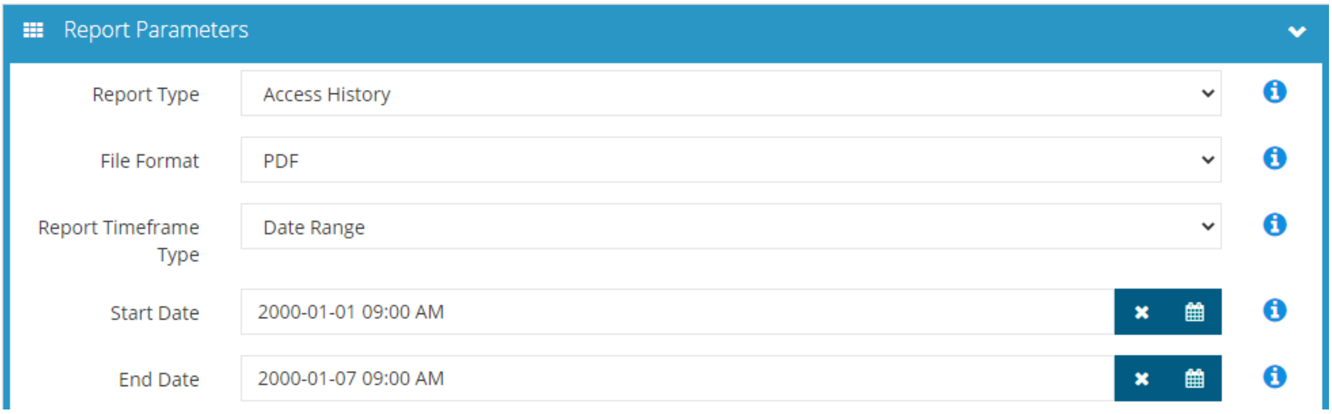
This feature can be used to resolve address clashing by having one of the clashing address readers connected at a time and re-addressing it (if there are multiple readers still connected with the same address, the re-addressing command sent by Inception will not function).



### Custom Time Range for Reports

Reports may now be generated based on a custom time range instead of the most recent events. A new 'Report Timeframe Type' option has been added to allow the selection of a 'Start Date' and 'End Date' where all events in-between will be included as part of the report.

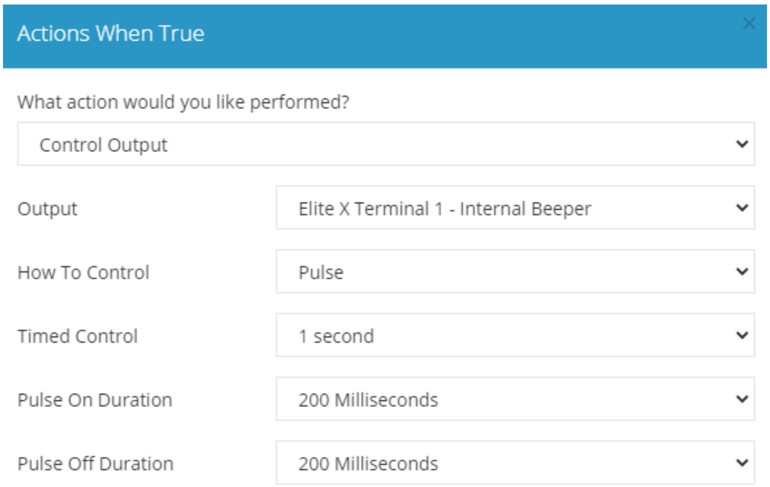
Reports generated through Scheduled Tasks will also have this functionality.


Report Parameters

| | |
|---|---|
| Report Type | Access History |
| File Format | PDF |
| Report Timeframe Type | Date Range |
| Start Date | 2000-01-01 09:00 AM |
| End Date | 2000-01-07 09:00 AM |

## Pulsed Output Control for Automated Actions

A new type of control has been added when controlling outputs in Automated Actions at **[Configuration > Automation > Automated Actions]**. The new option 'Pulse' can be selected under 'How to Control' – allowing the output to be switched on and off continually for a specified period (or indefinitely until another action changes the output if 'Timed Control' is set to none). Each pulse can also have its on and off duration altered to allow for longer or shorter on/off times.



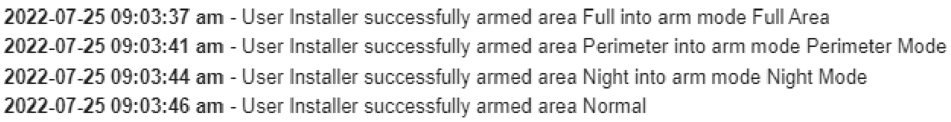
Actions When True

What action would you like performed?
Control Output

| | |
|---|---|
| Output | Elite X Terminal 1 - Internal Beeper |
| How To Control | Pulse |
| Timed Control | 1 second |
| Pulse On Duration | 200 Milliseconds |
| Pulse Off Duration | 200 Milliseconds |

## Multi-Mode Area Arm Notifications

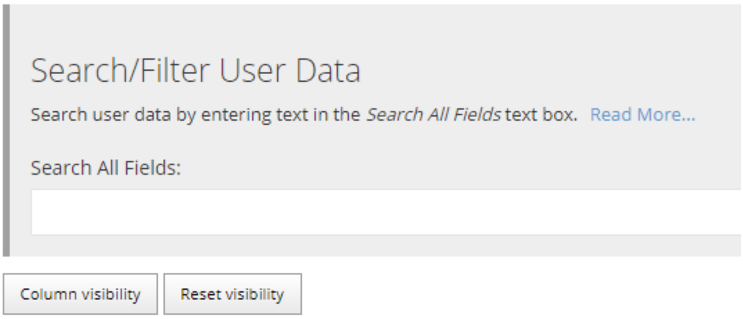
Whenever an area is armed and sends a notification, if multi-mode arming is enabled, the arm mode will now be included in the notification event text.



```
2022-07-25 09:03:37 am - User Installer successfully armed area Full into arm mode Full Area
2022-07-25 09:03:41 am - User Installer successfully armed area Perimeter into arm mode Perimeter Mode
2022-07-25 09:03:44 am - User Installer successfully armed area Night into arm mode Night Mode
2022-07-25 09:03:46 am - User Installer successfully armed area Normal
```

## Persistence of Search Users Page Layout

Changing Column Visibility settings in the **[Configuration > Users > Search Users]** page will now persist even when a user navigates away from the page. Another 'Reset Visibility' button has been added to allow for the settings to be reset.



Search/Filter User Data

Search user data by entering text in the *Search All Fields* text box. Read More...

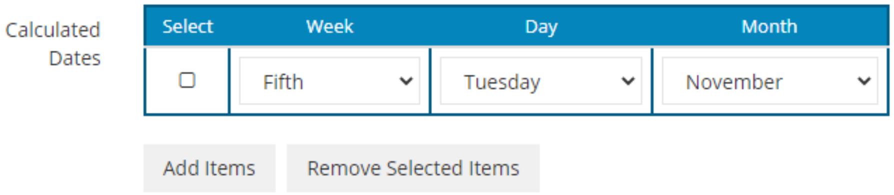
Search All Fields:

## REST API – Door Denied Access in User Info Monitoring

The API User Info Monitoring now also allows a 'DoorDenied' eventType to be specified, which means that when door access is not granted it will be monitored through the request.

### Calendar “Fifth” Week Option

When adding a calculated date to a calendar, the ‘Fifth’ week is now selectable as an option to create an exception for when the calendar should be valid, allowing you to select the Fifth occurrence of the chosen day in the month.



Calculated Dates

| Select | Week | Day | Month |
|---|---|---|---|
| ☐ | Fifth | Tuesday | November |

## Issues Resolved

### Browser Performance (Large Permission Groups)

Browser performance for the permissions group page has been greatly improved for systems with a large amount of items and permission groups.

### LAN Ethernet Bridge Connectivity

Various improvements have been made to Ethernet Bridge connectivity, including stability in scenarios where multiple Ethernet Bridges would cause one or more of them to remain offline perpetually, or with prolonged connection and/or network instability causing dropouts.

### Missing Items in Configuration Report

Issues where newer items in the Inception System were not being picked up when generating a configuration report have been resolved. In addition, all configuration options in items will now appear, giving a comprehensive report of each item.

### OSDP readers with Duplicate Serial Numbers

When there are multiple 3rd party OSDP readers that report duplicate serial numbers, the Inception system will now allow them to connect to the same bus. Connected 3rd party OSDP readers are also given new identification (featuring attached module name, its address, and serial number). Readers being re-addressed or moved to new modules will leave behind the old peripherals.

The Inception system will also now attempt to re-establish connections to readers as quickly as possible to prevent unnecessary downtime (which would also result in the reader temporarily going ‘offline’, with unnecessary review messages and re-connection tones).

### Ctrl+S Save Shortcut

Scenarios where the page needed several presses of CTRL+S to save have been resolved. When using CTRL+S to save on a non-entity page, there will no longer be a ‘Connection Lost’ dialog which interrupts it.

### Send PIN for Duress User

The Duress User’s configuration under the system settings should no longer have a ‘Send PIN’ button shown next to it, as this functionality was not applicable to the Duress User.

## Version 5.0.1 – 23/08/22

**Inception release 5.0.1 resolves some issues identified in the 5.0.0 release.**

## Issues Resolved

### Temporary Disarm could Fully Disarm Area

An issue was identified and fixed where users could perform a full disarm on areas using consecutive temporary disarm swipes.

Whenever a user with temporary disarm permissions swiped with a card at a door once while an area was armed, the area would temporarily disarm as expected. A second swipe would incorrectly set the area to Disarmed indefinitely with no scheduled arm time, even though this would show up in review as a temporary disarm. This should no longer occur and the review messages should accurately reflect the temporary disarms.

### Permissions Limited to 1000

An issue has been resolved where the permission configuration dialog would be empty if there were more than 1000 items that could be added to the Permission Group.

### OSDP / SIFER Reader Periodic Reconnection

An issue was resolved where OSDP and SIFER readers would occasionally disconnect and reconnect with their start-up noise. Readers should now silently re-establish connection in the case of a reader timeout, and unnecessary review messages will not be sent.

### Completed Battery Tests Trigger Item Changed Event

Battery Test completions erroneously triggered an Item Changed event, which would both appear in review and cause notifications to be sent if a Notifier was configured for Item Changes on Hardware. This was unintended behaviour and Battery Test completions are no longer accompanied by Item Change events.

### Module State Does Not Persist Over Power Cycles

When power cycling an Inception controller, all modules would not retain the same state as they had before the power cycle, resulting in Module isolation being reset. This issue has been resolved and Module state will be able to persist between power cycles.

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## Version 5.0.0 – 28/07/22

**Inception release 5.0.0 includes support for OSDP readers, personal storage unit functionality, increased capacity for Inputs and Outputs, improved international experiences, major security improvements like local network HTTPS access and TLS 1.2 support, and many other feature updates and enhancements.**

*Note: The minimum firmware version for 8-Input Expanders has been updated to 3.1.1 due to the DC Siren Support feature.*

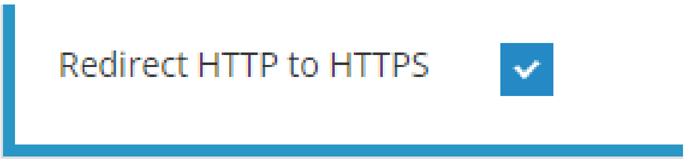
## New Features

### Local HTTPS Support

Though secure access to the Inception web interface has always been available through SkyTunnel, extra support has now been added for local HTTPS web access, accompanied with the ability to disable HTTP access and certificate management.

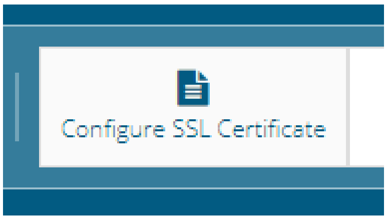
HTTPS web access is enabled by default with this firmware version, and can be navigated to via IP address (https://[ip.address]) or https://[InceptionSerialNumber].local/ in a web browser (where [InceptionSerialNumber] is replaced with your controller's serial number). Inception comes with a self-signed SSL certificate, however browsers may display safety warnings until this certificate is trusted.

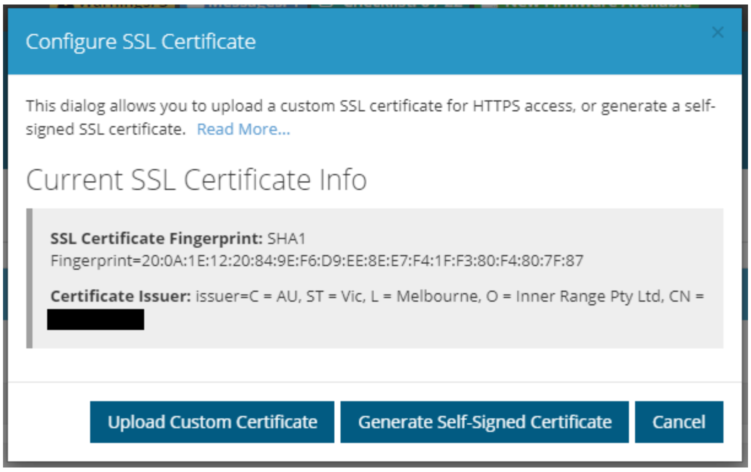
HTTP access can be disabled by selecting the *Redirect HTTP to HTTPS* option on the **[Configuration > General > Network]** page in the Advanced section. This will cause all HTTP requests to be redirected to HTTPS for increased security of web traffic. Note that this feature will also affect the Inception REST API, so any integrations targeting the API should be configured with the HTTPS URL to ensure they continue to work.



Redirect HTTP to HTTPS ☑

A custom SSL certificate can be uploaded to the Inception controller via the *Configure SSL Certificate* toolbox button located on the **[Configuration > General > Network]** page.





Configure SSL Certificate

This dialog allows you to upload a custom SSL certificate for HTTPS access, or generate a self-signed SSL certificate. Read More...

Current SSL Certificate Info

**SSL Certificate Fingerprint:** SHA1 Fingerprint=20:0A:1E:12:20:84:9E:F6:D9:EE:8E:E7:F4:1F:F3:80:F4:80:7F:87

**Certificate Issuer:** issuer=C = AU, ST = Vic, L = Melbourne, O = Inner Range Pty Ltd, CN = [redacted]

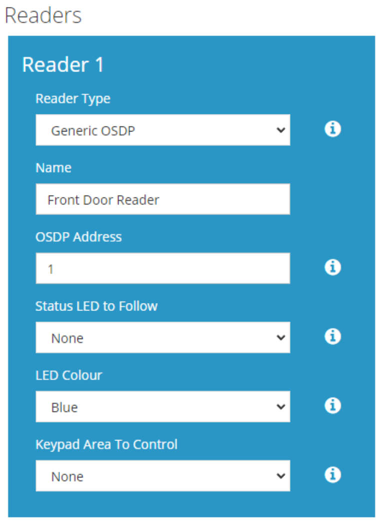
Refer to the **Inception Tech Guide – HTTPS Configuration** for more information on these processes and general setup, including on how to remove the browser safety warning.

## OSDP Reader Support

This release allows 3rd party OSDP readers to be connected to the Inception controller and SLAM expansion modules. These offer similar features to SIFER readers, except for those specific to the SIFER range like multiple LED colours, volume control, etc. When configuring a Reader expansion module in the Hardware Wizard, the Reader Types now have been expanded to include Wiegand, SIFER, Generic OSDP, and OSDP Wiegand Converter.

For OSDP readers connected on the same module bus, ensure they have unique OSDP addresses.

OSDP readers configured in Inception, like SIFER readers, can be detected, enrolled, have state feedback, and be controlled by automated actions to evoke a feedback response.


Readers
Reader 1
Reader Type: Generic OSDP
Name: Front Door Reader
OSDP Address: 1
Status LED to Follow: None
LED Colour: Blue
Keypad Area To Control: None

## 1024 Inputs and Outputs

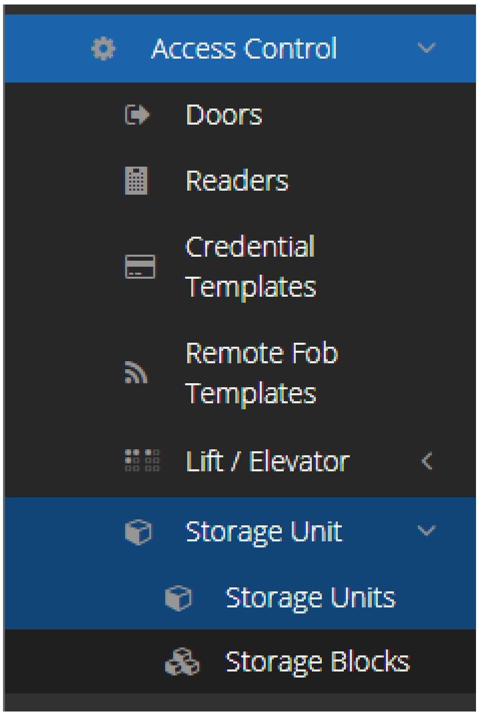
Inception is now capable of supporting up to 1024 Inputs and 1024 Outputs via expansion hardware, increased from the previous limits of 512 of each. These limits apply only to Hardware Inputs and Hardware Outputs. Calculated inputs such as those representing a door's Forced or Held Open states, or a storage unit's Alarm state do not count to these limits.

Note that for ContactID alarm reporting, total input counts above 512 will all report as point ID 999. IRFast can be used for those systems to ensure individually identifiable reporting points.

## Storage Units

Support for personal storage unit facilities has been included in this release. Dedicated Storage Unit items can be created that represent an individual storage space that can monitor door position and motion detector inputs and control outputs for automation. Units can be unlocked or secured to raise an alarm state on access.

There are no limits on the number of Units that can be created, the main limit though is the number of hardware inputs that Inception supports (now 1024). If each unit has a door reed and a motion detector, up to 512 units could be supported. If only one detector is in each unit, then up to 1024 units could be created. For site requirements, keep in mind any additional inputs required for access points, security detectors, fire detectors, and so on that would reduce the number of inputs that Units could use.

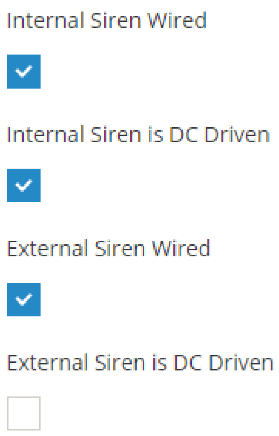


Storage blocks define a group of units and could represent a whole site, a building, or a section of a building. An access request to a block by a customer via PIN or Card would unlock their unit, automatically securing their unit when they exit. They also allow simpler management of automation, controling lighting etc if any unit within a block is unlocked.

See the **Inception Tech Guide – Storage Units** guide for more information on configuring these units.

## DC Siren Support

Inception systems with configured Internal and External sirens should now be able to support blended sirens where one siren is DC Driven and the other is not, as long as the connected 8-Input expander module firmware has support for this feature. This means that when one siren is controlled and the option “Siren is DC Driven” is ticked, it should now use the DC Siren tone.



Internal Siren Wired
☑

Internal Siren is DC Driven
☑

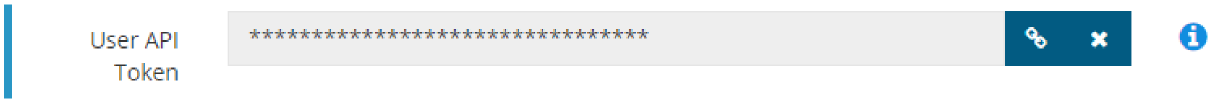
External Siren Wired
☑

External Siren is DC Driven
□

## REST API – User API Tokens

A new REST API authentication method that allows for greater control over API access and eliminates the need for separate login requests has been added, where user-specific API Tokens can be used in requests to make the request on the behalf of the user. These API Tokens can be generated for users on the **[Configuration > Users > Manage Users]** page in the Credentials section and used by adding it to the authorization header of REST API requests (with type 'APIToken' preceding it).

This allows for convenience and management of API authentication, as this token may be unlinked at any time to prevent further usage of the API through that token. Another token can be generated in the future should API access need to be granted to that user again.

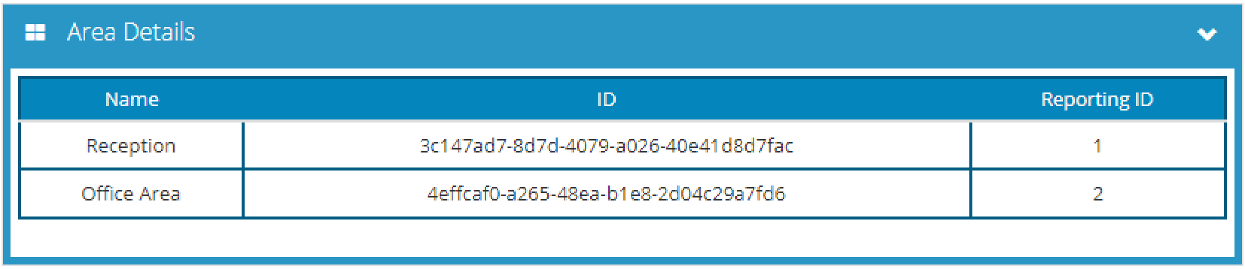


User API Token: ********************************

## REST API – API Details Page

The Inception API Details page under **[System > API Details]** is a quick reference tool that lists all entities that the logged in user can access via the REST API, including their name, ID, and other related information. For integrations configuring Users for example, it allows IDs for items like Card Templates to be seen and entered into the other system, instead of needing that system to fetch the list of options via the REST API and programmatically determine the correct one to use.

It can also be useful in debugging and confirming whether the permissions are configured correctly for a REST API User. If that user’s details are used to log into the Inception web interface, the API Details page will show all items that the user has permission to see.



Area Details

| Name | ID | Reporting ID |
|---|---|---|
| Reception | 3c147ad7-8d7d-4079-a026-40e41d8d7fac | 1 |
| Office Area | 4effcaf0-a265-48ea-b1e8-2d04c29a7fd6 | 2 |

### REST API – SkyCommand User Linking

A new REST API request has been added that allows a user to be linked to SkyCommand by providing their SkyCommand email, rather than having to manually link accounts through the web interface. See the Inception REST API release notes for additional information on usage.

### REST API – Reader Names

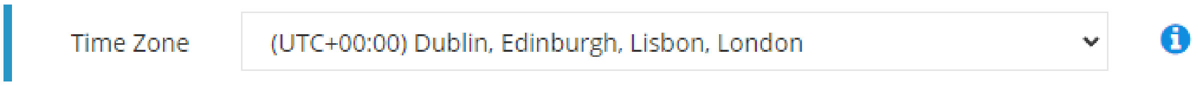
API requests that return a DoorAttachedReader such as Door Summary or Get Door's Associated Reader will now also include the Name property of those readers.

## Feature Updates

### Time Zone Display

The Time Zone display on **[Configuration > General > Date and Time]** now displays the UTC offset of the time zone, and locations grouped to match Windows Time Zone format displays.

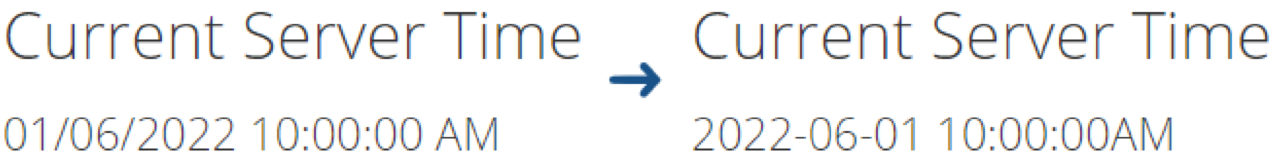
Redundant time zone listings have also been updated and grouped into their respective time zones according to the new time zone names.



Time Zone (UTC+00:00) Dublin, Edinburgh, Lisbon, London

### Time and Date Format

Inception time and date displays will now adhere to a standard international format (YYYY-MM-DD HH:MM:SS), rather than dd-MM-yyyy to avoid confusion in international markets.



Current Server Time
01/06/2022 10:00:00 AM

→

Current Server Time
2022-06-01 10:00:00AM

This change also applies to data input features like User CSV Import, the Dynamic User Import Module, and the REST API. The international format will be checked first, before falling back to the date format used by the Controller's language region (configured on the **[Configuration > General > System]** page, via the Language Options toolbox button.

### Input State Change Review

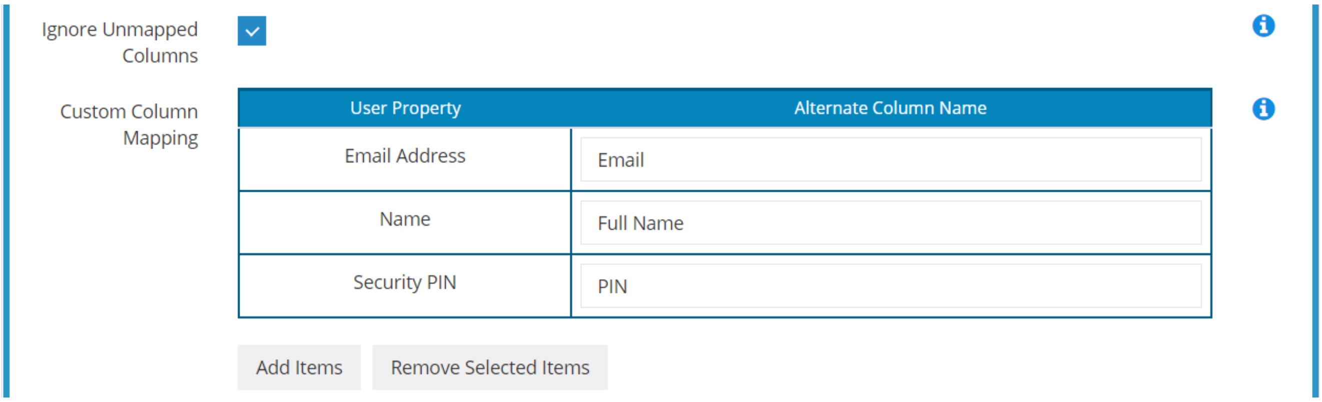
Normally, inputs only log state changes when detailed events are enabled. To support circumstances where an Input requires all state changes to be always logged, such as wanting a review history if certain inputs activate, Inputs now have an "Always Log State Changes" option under their Monitoring Options. This option will create a simplified review message summarising any state changes for that input, and whether the change was Active or Secure.

Always Log State Changes □

## DUIM (Dynamic User Import Module) Custom Column Headers

A new “Custom Column Mapping” option has been added on the **[Configuration > General > System]** page in the **Dynamic User Import Module (DUIM)** section, which allows custom column names from a CSV file to be mapped to Inception user properties. This feature is intended for situations where imported user CSV files have column names that do not directly match Inception’s user properties. This affects all user data CSV imports, whether manually imported or periodically imported through the DUIM service.

When a user property is selected, a custom column name can be entered that matches the CSV file. For example, the 'Name' user property could be mapped to the alternate column name 'Full Name' so that any data in the CSV file under 'Full Name' will be imported into the user's 'Name' property.



Ignore Unmapped Columns ☑

Custom Column Mapping

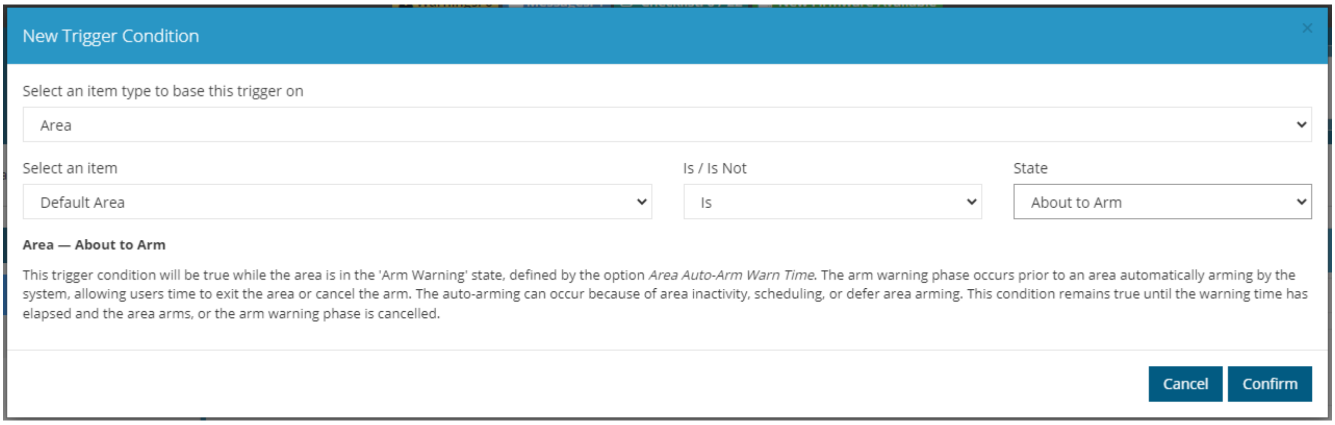
| User Property | Alternate Column Name |
|---|---|
| Email Address | Email |
| Name | Full Name |
| Security PIN | PIN |

In addition, a new “Ignore Unmapped Columns” option has been added that will automatically skip any columns that don’t line up with a field in Inception. Without this option, the import will fail and a System Message will be created with details of the issue.

These changes allow user data exports from one system to be automatically imported to Inception’s via the DUIM service, without needing to modify the CSV headings or remove columns.

## Automated Action Trigger Help Text

Automated Actions can be used to create a wide range of custom automation responses, however it wasn’t always clear when certain trigger conditions would occur. Help text has now been included for every condition state, explaining when that condition can occur and how it could be cleared. Some of these are straight forward, like “*This trigger condition will be true while the selected area is armed*”, but many include detailed information about what options are needed for that state to occur.



New Trigger Condition

Select an item type to base this trigger on: Area

Select an item: Default Area

Is / Is Not: Is

State: About to Arm

**Area — About to Arm**

This trigger condition will be true while the area is in the 'Arm Warning' state, defined by the option *Area Auto-Arm Warn Time*. The arm warning phase occurs prior to an area automatically arming by the system, allowing users time to exit the area or cancel the arm. The auto-arming can occur because of area inactivity, scheduling, or defer area arming. This condition remains true until the warning time has elapsed and the area arms, or the arm warning phase is cancelled.

### Password Display

Passwords have never been retrievable when editing an item that has a password (user web login password, WiFi password, etc). If typing in a new password though it would be shown in clear text until the page was reloaded. Now the password is always hidden even when typing a new one in. when copied. This applies to all password fields in the Inception web interface.

### Web Login No Longer Needed for SkyCommand App Control

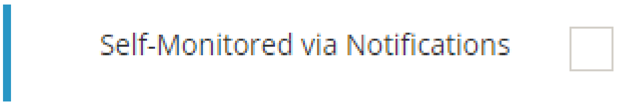
For a User to control and receive push notifications for their Inception system via the SkyCommand App, they previously needed to have Web Login details configured as well. If the User never used the web interface and only required App control, this meant there would be unnecessary username and password details defined for the user. This limitation has now been removed, reducing the number of web user accounts that need to be created to only those who need web interface access.

## Issues Resolved

### Self-Monitoring Review Events

For systems where there may be no monitoring station, and alarm events are instead sent via email or push notification, an option under **[Configuration > General > Alarm Reporting]** is now available to let alarm events be sent even when there are no reporting paths are configured.

This option will suppress the “Alarm Event Failed to Send, No Paths Configured” review event and allow for the configured email or push notification notifiers to send messages.



Self-Monitored via Notifications □

### TLS 1.2 Support

Support has been included for higher levels of TLS, allowing email servers (configured at **[Configuration > System > Email]**) that enforce the use of TLS 1.2 to be used.

### Checkboxes on Mobile Devices

On some mobile devices, including those viewing the desktop version of the Inception web interface, checkboxes would be unresponsive. Checkboxes should now be toggleable on all devices with better responsiveness, and the label of the property can be pressed to toggle the checkbox as an alternative.

### Item Duplication and Password Fields

If an item with password fields is duplicated and saved, it would save an obfuscated version of the password, and would also generate an invalid PIN. Duplicated items with password fields now must have a new password entered for each of these fields before they can be saved.

## Version 4.2.1 – 13/04/22

**Inception release 4.2.1 resolves some issues identified in the 4.2.0 release.**

## Issues Resolved

### Login Issue After Update

If an Inception unit was updated to 4.2.0 from 4.1.0 or earlier, and the Technician’s user had a short password, they would be prevented from logging in. This was due to the short password not meeting the default password policy while also trying to redirect to the EULA page added in 4.1.1.

### EliteX Terminal with SIFER Plugon Module

An issue was identified between the Inception 4.2.0 release and EliteX Terminals running the updated 3.1.0 firmware, where card badges were not being interpreted correctly. This has been resolved.

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## Version 4.2.0 – 07/04/22

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

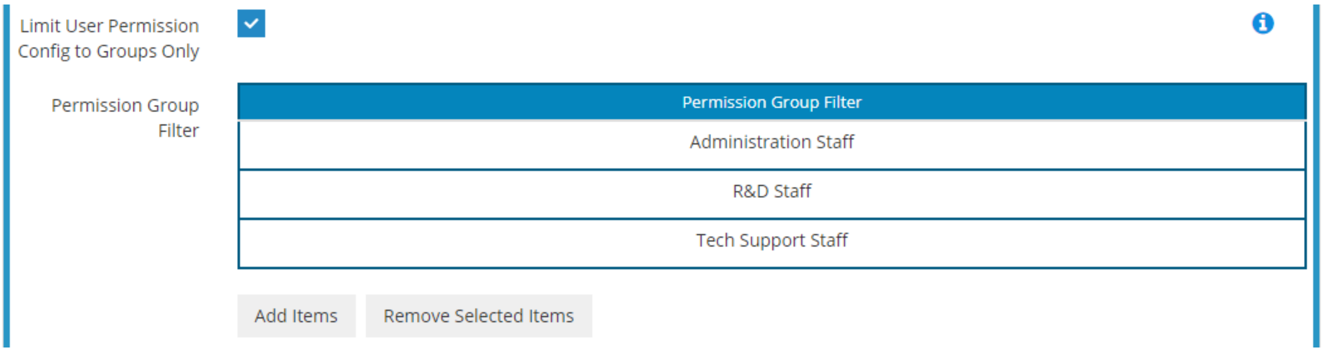
*Note: The minimum firmware version for EliteX Keypads has been updated to 3.1.0 due to improvements to module substitution logic.*

## 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.

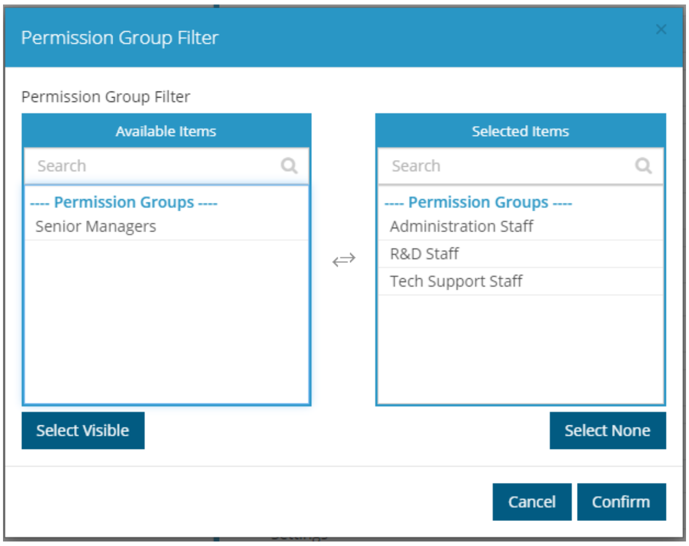
This allows common staff permission groups to be available to certain users, while manager permission groups are hidden and need to be set by more senior staff. Or a hierarchy of permission groups could exist for different parts of the building, but the user only sees a small subset for a simpler administration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



Limit User Permission Config to Groups Only ☑

Permission Group Filter

| Permission Group Filter |
|---|
| Administration Staff |
| R&D Staff |
| Tech Support Staff |



Permission Group Filter

Permission Group Filter

| Available Items |
|---|
| ---- Permission Groups ---- |
| Senior Managers |

| Selected Items |
|---|
| ---- Permission Groups ---- |
| Administration Staff |
| R&D Staff |
| Tech Support Staff |

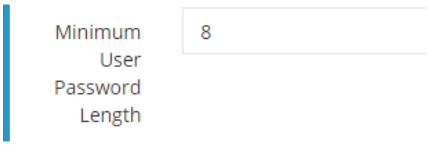
The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## Password Policy

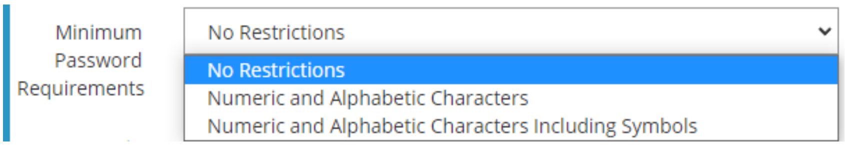
Multiple new features relating to password management have been added to the **[Configuration > General > System]** page in the **PIN / Password Policy** section that allow for the adjustment of system-wide configuration related to login.

### 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.



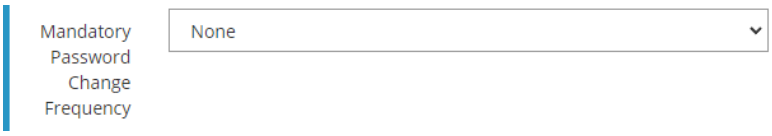
Minimum User Password Length: 8



Minimum Password Requirements: No Restrictions

No Restrictions
Numeric and Alphabetic Characters
Numeric and Alphabetic Characters Including Symbols

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.



Mandatory Password Change Frequency: None

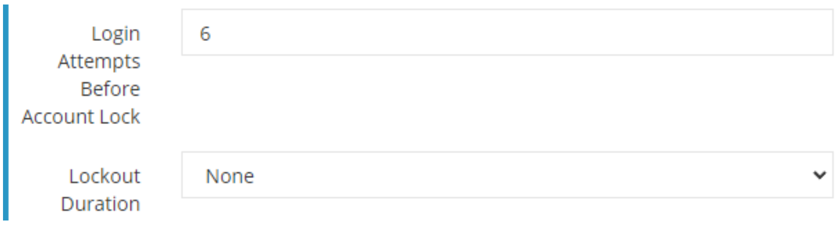
### Password Policy - Account Lockout Changes

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.

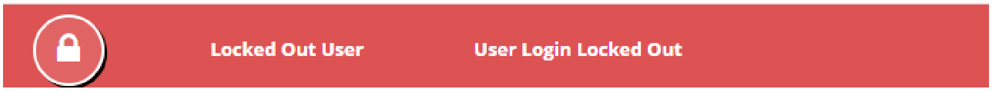


Login Attempts Before Account Lock: 6

Lockout Duration: None

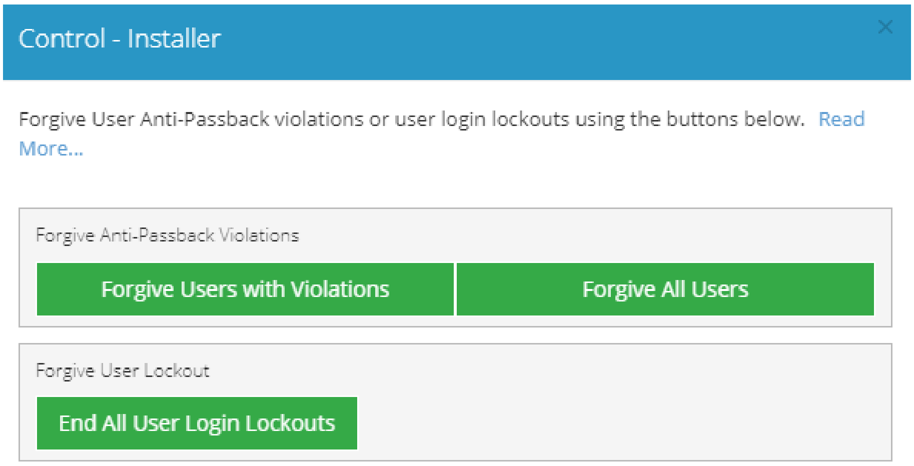
### Password Policy – Administrator Intervention

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.



Locked Out User User Login Locked Out

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.



Control - Installer

Forgive User Anti-Passback violations or user login lockouts using the buttons below. Read More...

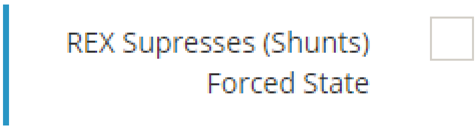
Forgive Anti-Passback Violations

Forgive User Lockout

## 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.



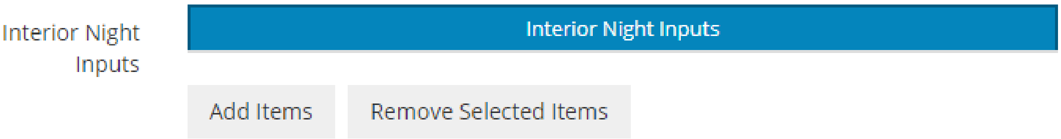
REX Supresses (Shunts) Forced State □

### 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.

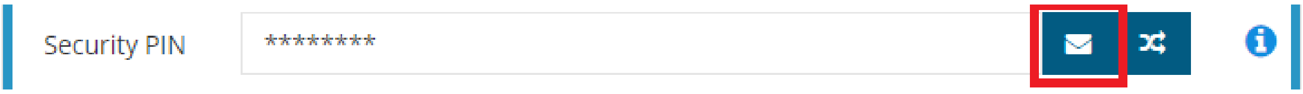
In order to add Inputs into this list, they must first be present in the Monitored Inputs list above it.

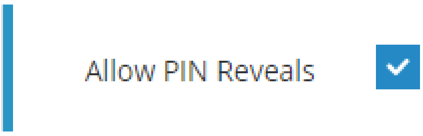
### Send / Reveal User PIN

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.


Security PIN ********


Allow PIN Reveals ☑

November 2023
The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## Feature Updates

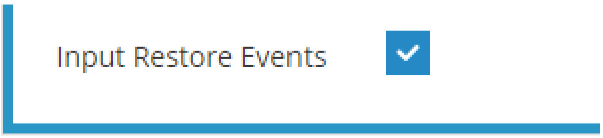
### Installer Account on First Login

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.



Input Restore Events ☑

### 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.

Prevent PIN Logins ☑

### 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.

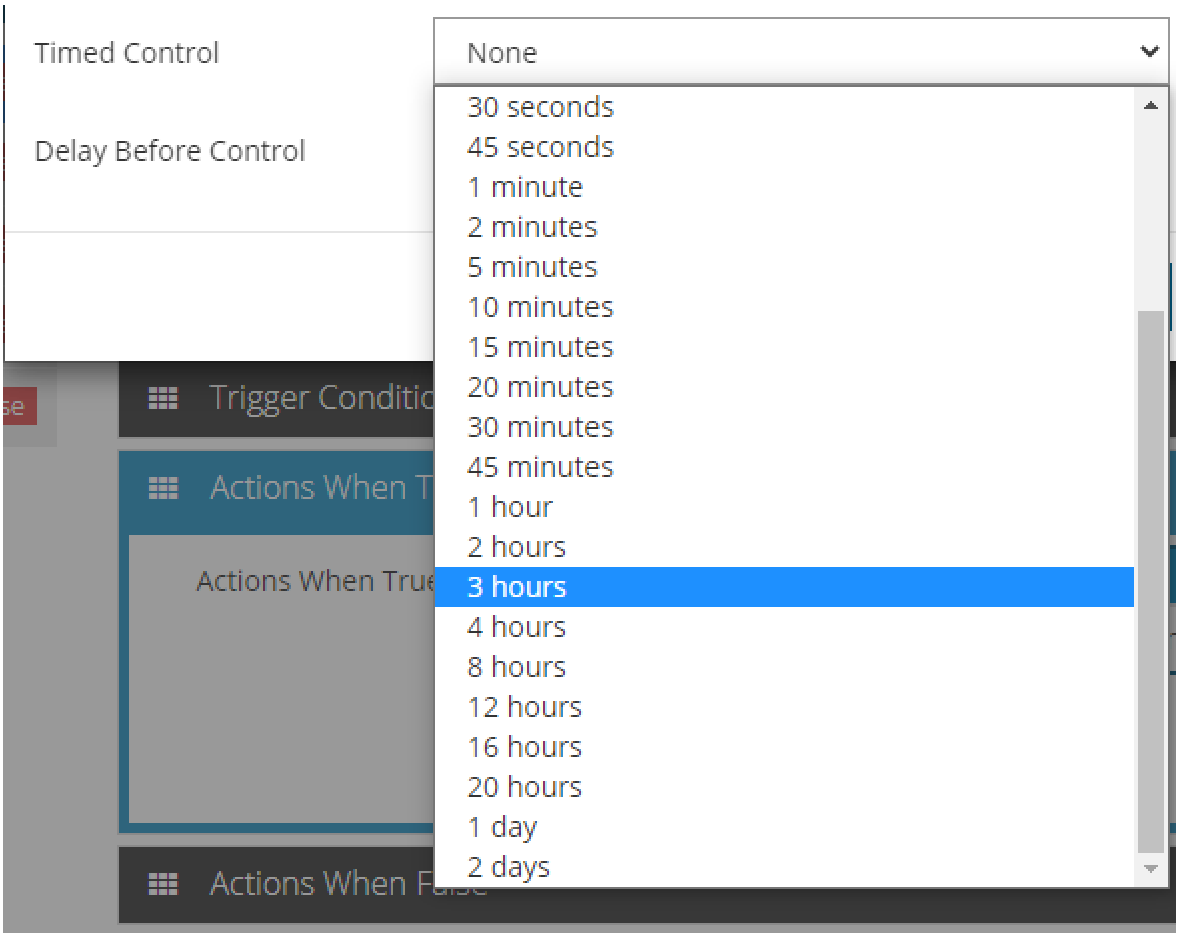
### Automated Action – Cancel Grant Access Requests

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.

How To Control: Cancel Grant Access Requests

## 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.



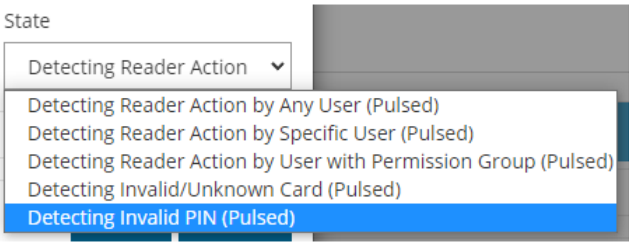
Timed Control: None

Delay Before Control

- 30 seconds
- 45 seconds
- 1 minute
- 2 minutes
- 5 minutes
- 10 minutes
- 15 minutes
- 20 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 2 hours
- 3 hours
- 4 hours
- 8 hours
- 12 hours
- 16 hours
- 20 hours
- 1 day
- 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.



State: Detecting Reader Action

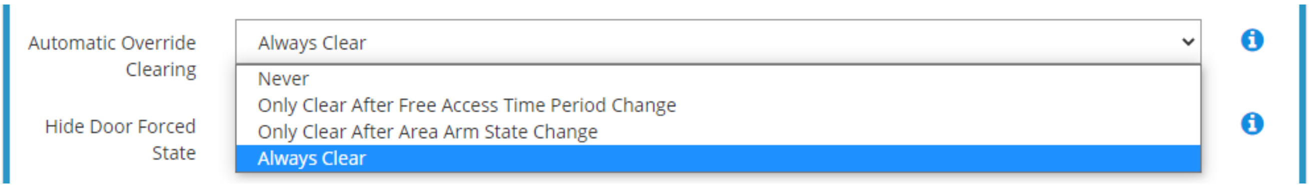
- Detecting Reader Action by Any User (Pulsed)
- Detecting Reader Action by Specific User (Pulsed)
- Detecting Reader Action by User with Permission Group (Pulsed)
- Detecting Invalid/Unknown Card (Pulsed)
- Detecting Invalid PIN (Pulsed)

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

### 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.



Automatic Override Clearing: Always Clear

- Never
- Only Clear After Free Access Time Period Change
- Only Clear After Area Arm State Change
- Always Clear

Hide Door Forced State

## 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.

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

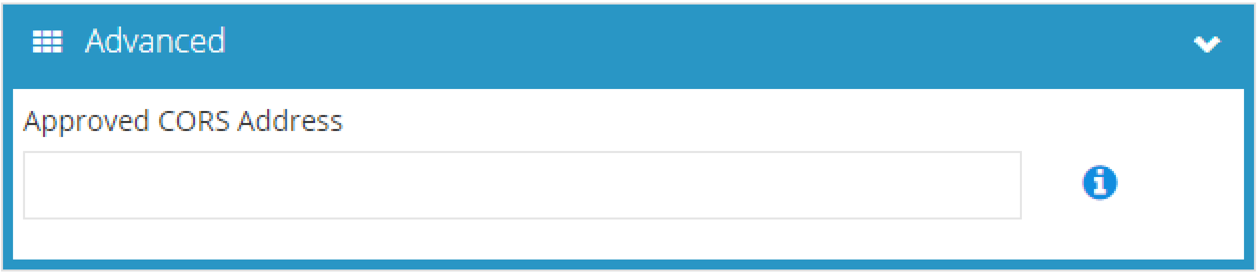
## Version 4.1.2 – 29/07/21

**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.


Advanced

Approved CORS Address

## 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)

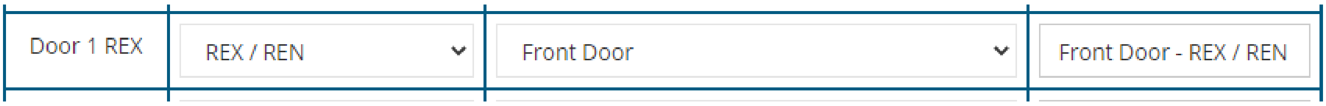
A new EULA page has been added to the web interface. The agreement must be accepted on first login in order to use the web interface.

## 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.



| | | | |
|---|---|---|---|
| Door 1 REX | REX / REN | Front Door | Front Door - REX / REN |

### LCD Terminal – "LAN Secure" function

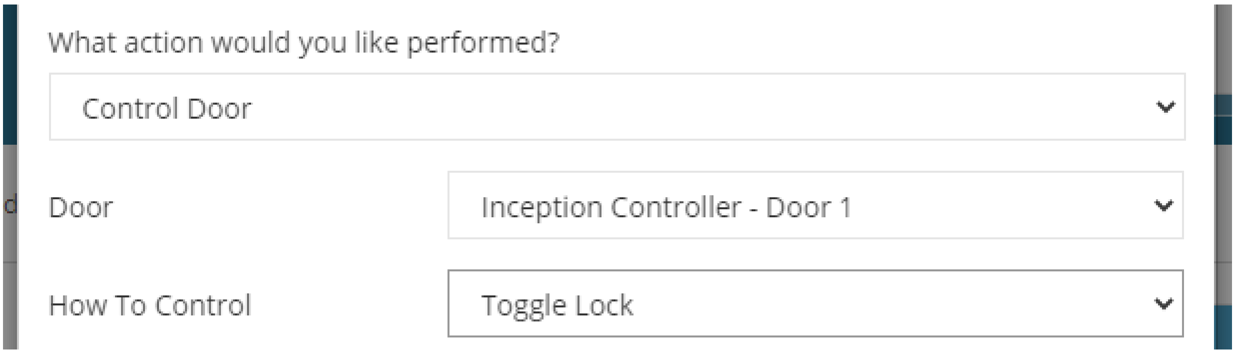
The "LAN Secure" function has been added to the LCD Terminal's Installer menu (keypad shortcut: Menu -> 7 -> 6). This function protects the LAN against module substitution, same as the "Send LAN Secure" button on the **[State / Control -> Hardware Test]** page of the web interface.

### 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.



What action would you like performed?

Control Door

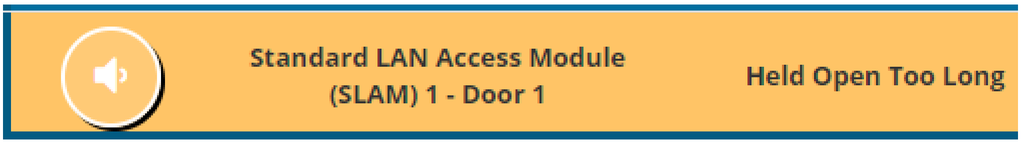
Door: Inception Controller - Door 1

How To Control: Toggle Lock

### 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.



Standard LAN Access Module (SLAM) 1 - Door 1

Held Open Too Long

### 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

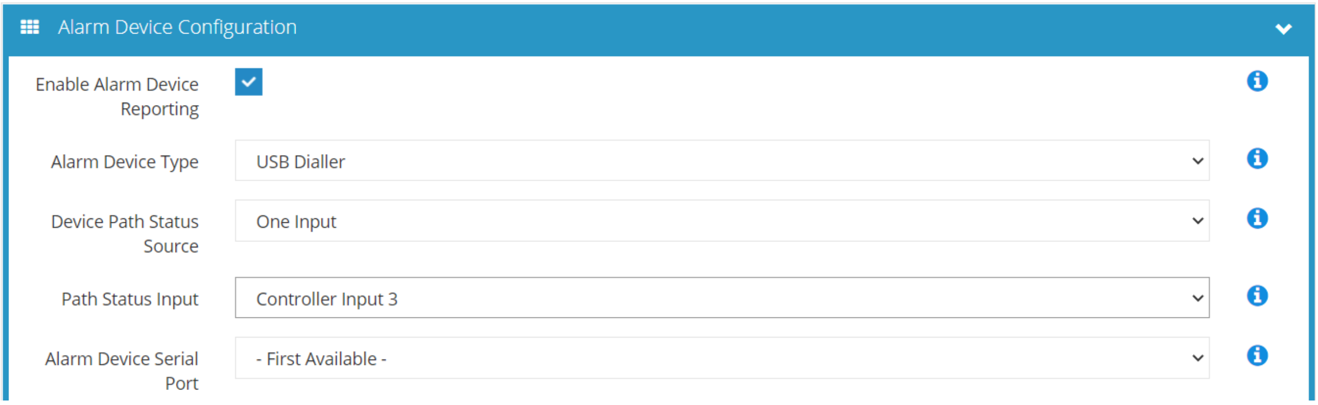
**The 4.1 release of Inception includes several changes to prepare for compliance with various intruder UL standards. Also included is better support for Single EOL configurations**

## 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.



Alarm Device Configuration

Enable Alarm Device Reporting ☑

Alarm Device Type: USB Dialler

Device Path Status Source: One Input

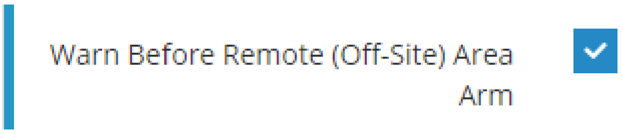
Path Status Input: Controller Input 3

Alarm Device Serial Port: - First Available -

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.

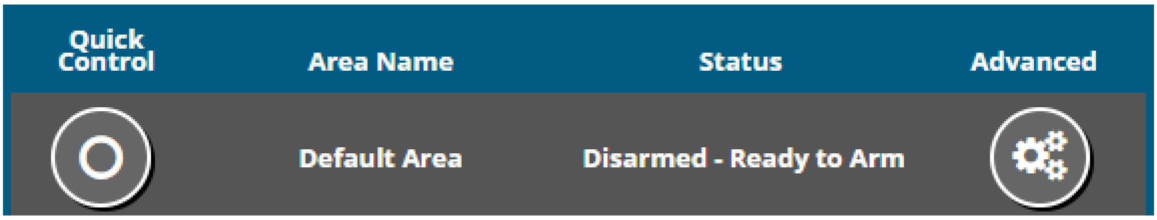


Warn Before Remote (Off-Site) Area Arm ☑

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

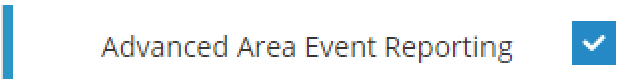
Areas will now indicate if they are ready to arm in the web interface or LCD terminal. The “Disarmed - Ready to Arm” state indicates that all non-exit path inputs in the Area are secure. If any of the inputs are not secure, the Area’s state will display “Disarmed – Active Inputs” instead.



| Quick Control | Area Name | Status | Advanced |
|---|---|---|---|
| ○ | Default Area | Disarmed - Ready to Arm | ⚙ |

### 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.



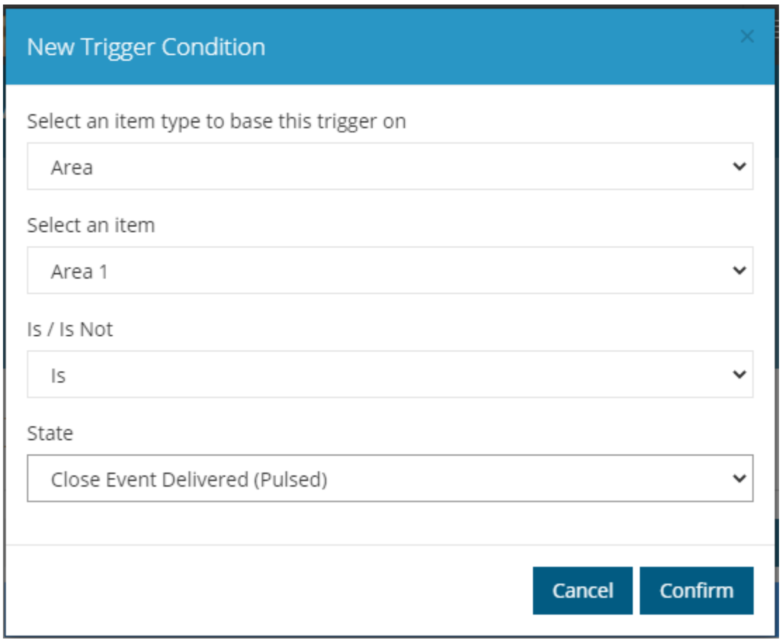
Advanced Area Event Reporting ☑

- 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.



New Trigger Condition

Select an item type to base this trigger on: Area

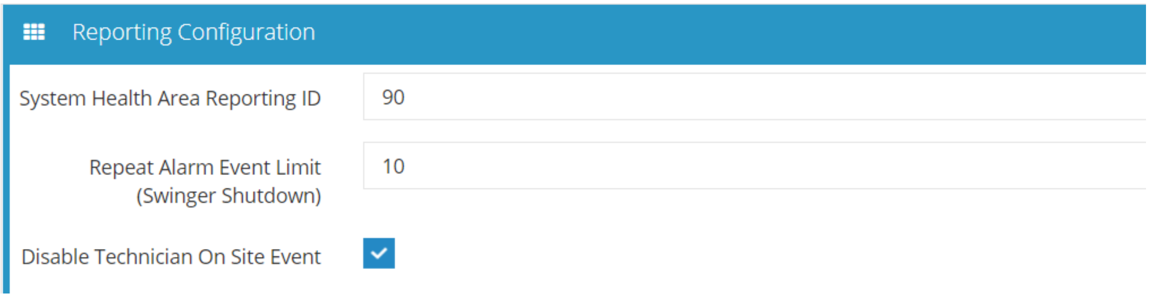
Select an item: Area 1

Is / Is Not: Is

State: Close Event Delivered (Pulsed)

### 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.



Reporting Configuration

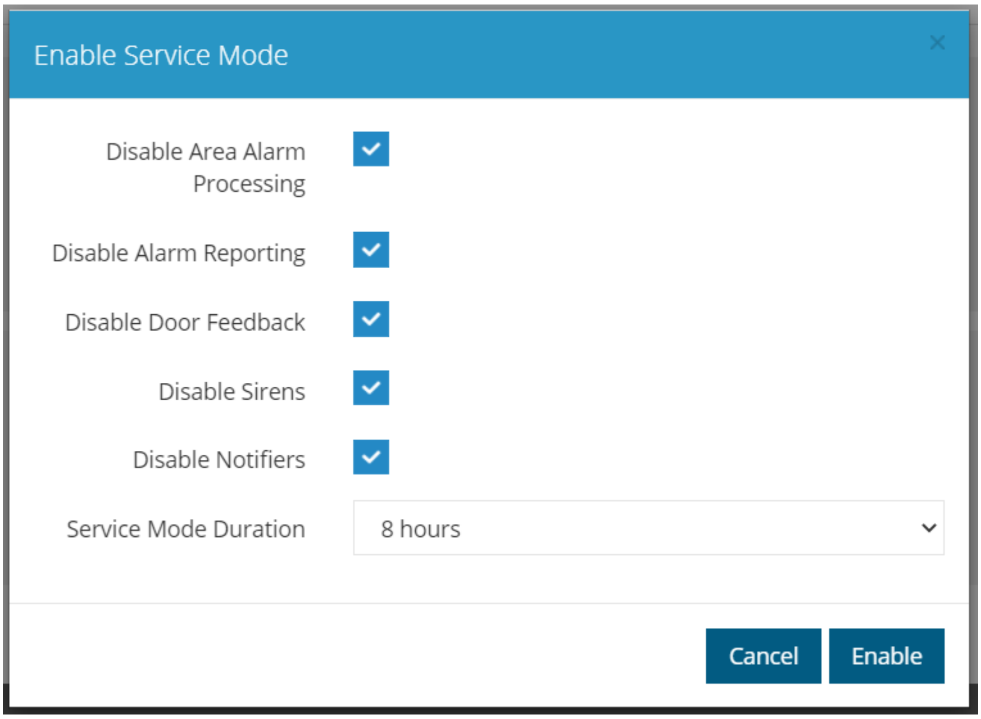
System Health Area Reporting ID: 90

Repeat Alarm Event Limit (Swinger Shutdown): 10

Disable Technician On Site 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.



Enable Service Mode

Disable Area Alarm Processing: ☑

Disable Alarm Reporting: ☑

Disable Door Feedback: ☑

Disable Sirens: ☑

Disable Notifiers: ☑

Service Mode Duration: 8 hours

## 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.

The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.

## 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.

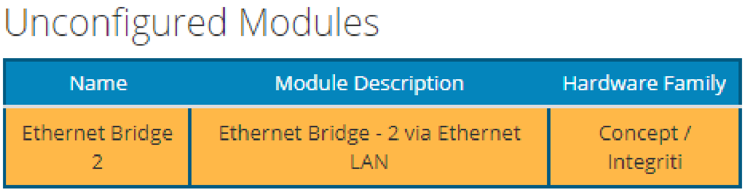
For more detailed information, see the Inception technical note for configuring DUIM (a separate document).

### 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

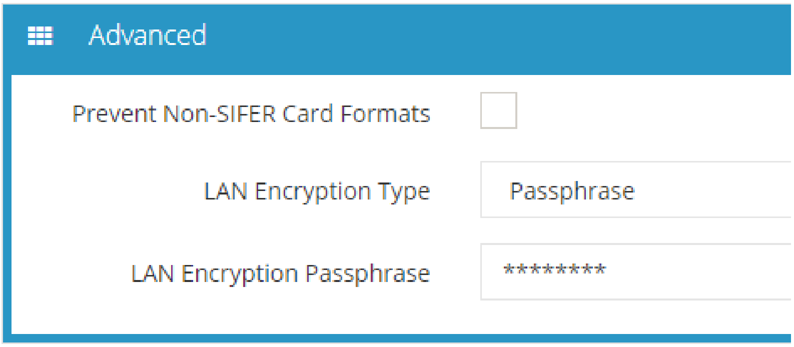
The Ethernet Bridge LAN module is now supported. The Ethernet Bridge communicates with the controller over a standard Ethernet LAN connection on your local network and allows you to discover and enrol modules that attached to the bridge via the RS485 LAN.



Unconfigured Modules

| Name | Module Description | Hardware Family |
|---|---|---|
| Ethernet Bridge 2 | Ethernet Bridge - 2 via Ethernet LAN | Concept / Integriti |

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.



Advanced

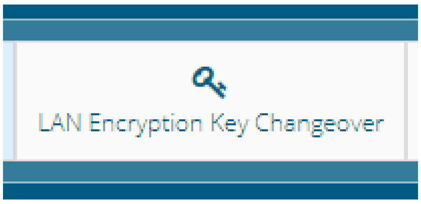
Prevent Non-SIFER Card Formats □

LAN Encryption Type: Passphrase

LAN Encryption Passphrase: ********

## 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.

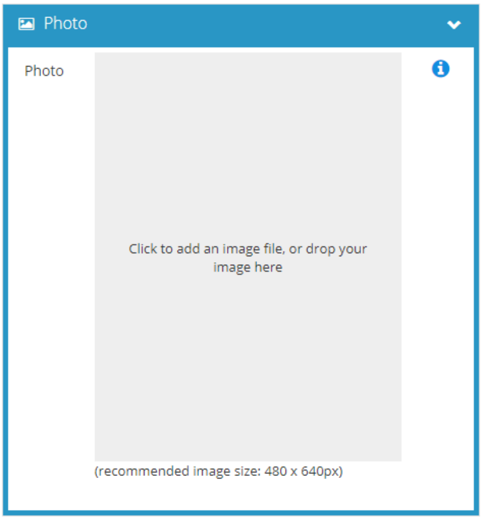
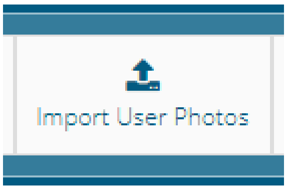
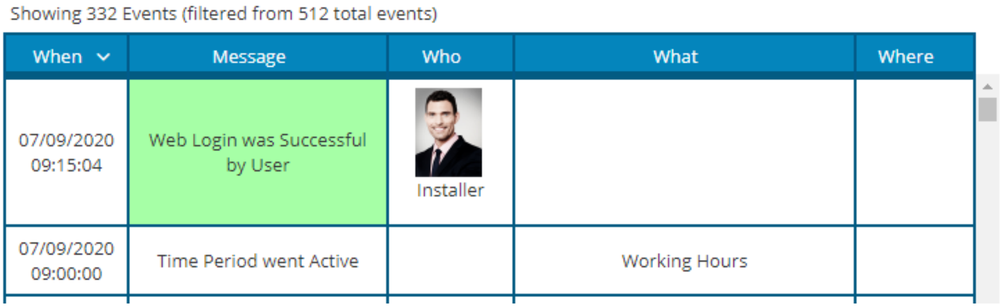


Photo
Photo
Click to add an image file, or drop your image here
(recommended image size: 480 x 640px)



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.

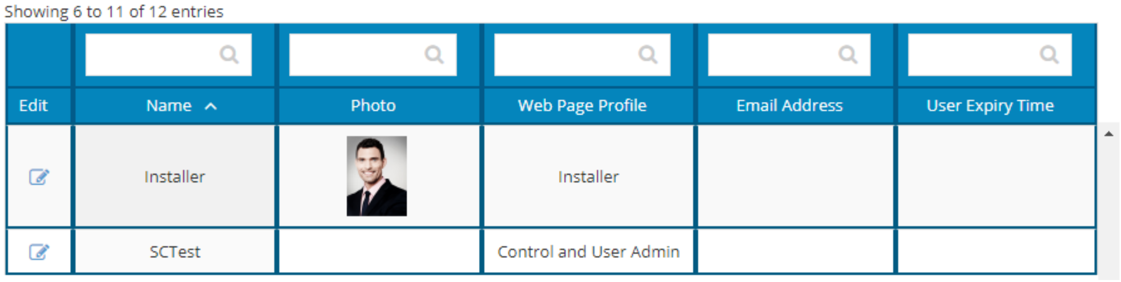
It is recommended that user photos be at least 480 x 640 pixels and 3:4 aspect ratio (i.e. portrait) for maximum visual quality in the web interface.



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 | |

November 2023
The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.



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.)

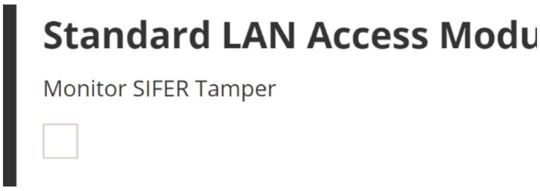
### Reader Tampers

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.



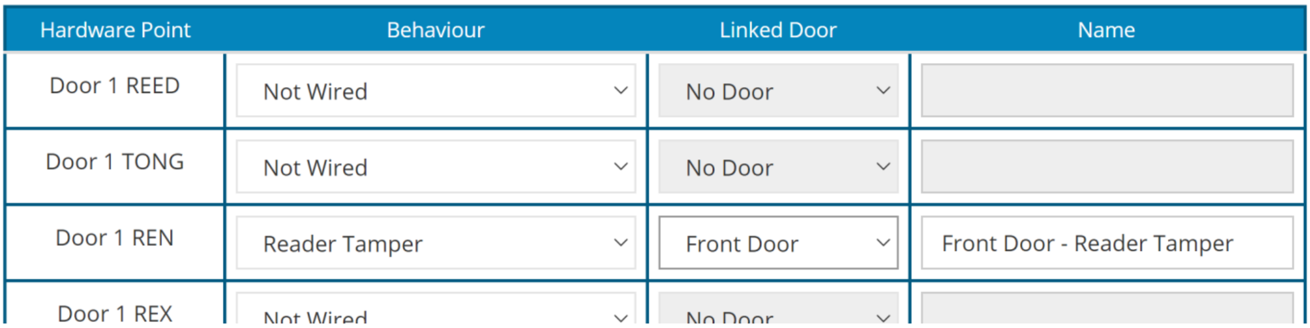
Standard LAN Access Modu

Monitor SIFER Tamper

□

- **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.

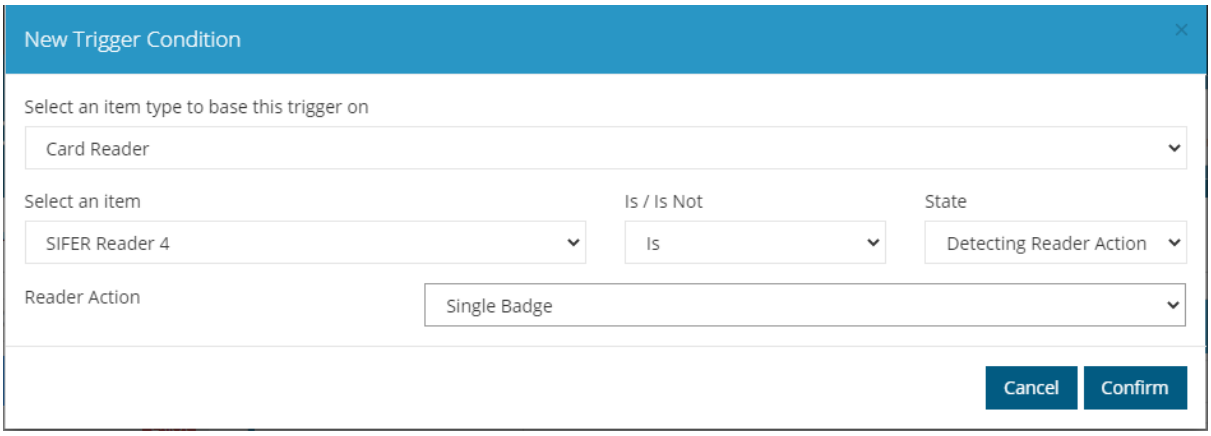


| Hardware Point | Behaviour | Linked Door | Name |
|---|---|---|---|
| Door 1 REED | Not Wired | No Door | |
| Door 1 TONG | Not Wired | No Door | |
| Door 1 REN | Reader Tamper | Front Door | Front Door - Reader Tamper |
| Door 1 REX | Not Wired | No Door | |

# 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.



New Trigger Condition

Select an item type to base this trigger on: Card Reader

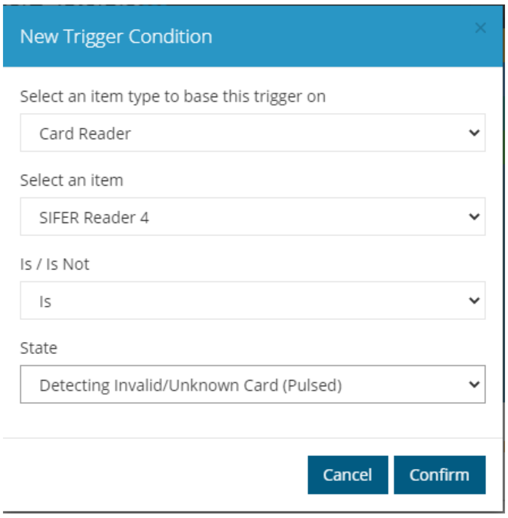
Select an item: SIFER Reader 4

Is / Is Not: Is

State: Detecting Reader Action

Reader Action: Single 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.



New Trigger Condition

Select an item type to base this trigger on: Card Reader

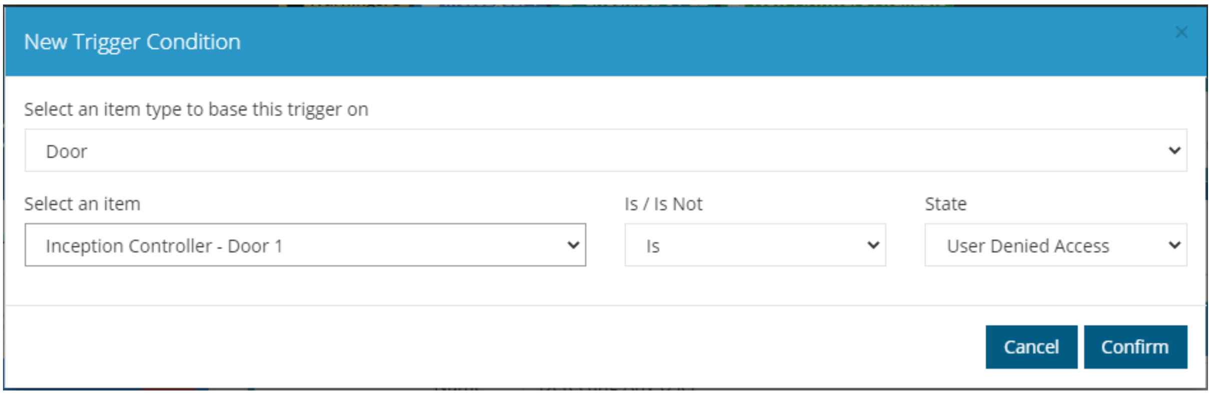
Select an item: SIFER Reader 4

Is / Is Not: Is

State: Detecting Invalid/Unknown Card (Pulsed)

## 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.


New Trigger Condition

Select an item type to base this trigger on: Door

Select an item: Inception Controller - Door 1

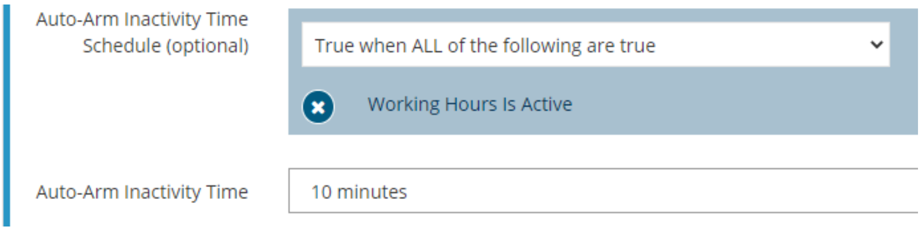
Is / Is Not: Is

State: User Denied Access

## 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.


Auto-Arm Inactivity Time Schedule (optional): True when ALL of the following are true

Working Hours Is Active

Auto-Arm Inactivity Time: 10 minutes

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

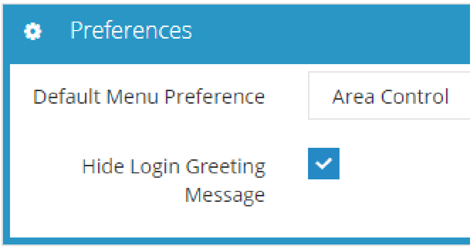
A new system message has been added for when a user is denied access to a door or lift car. The message includes the user’s name, the name of the door or lift car, the time of the access attempt, and the reason why access was denied. This message ensures attention is drawn to the fact someone attempted 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



Default Menu Preference: Area Control

Hide Login Greeting Message: ☑

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

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

inception

WEB POWERED SECURITY

Simple & Easy Installation

Integrated Security - Access Control

Inner Range Pty Ltd
www.innerrange.com
Tel: +61 3 9780 4300
Fax: +61 3 9753 3499
email: support@innerrange.com

www.innerrange.com

inner range

Intelligent Security Solutions