inception

WEB POWERED SECURITY

Simple & Easy Installation

Integrated Security - Access Control

Release Notes 3.2.3.4416
11/02/20

www.innerrange.com
inner range
Intelligent Security Solutions

inception
WEB POWERED SECURITY

Table of Contents

Release Notes

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.

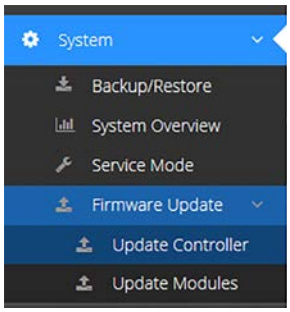
How to upgrade your Inception:

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.

Select Firmware Update File

Filename	Size (bytes)	Firmware Version	File Location
Inception Full 1.0.2.1864-r0.bin	56990917	1.0.2.1864-r0	Onboard Storage

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.

Release Notes

Minimum Required Versions

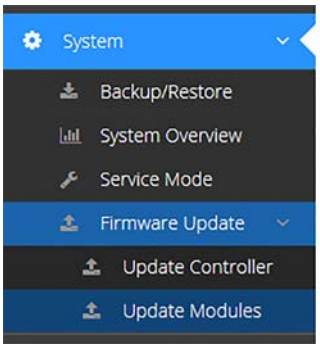
The list below indicates the minimum required firmware versions for several of the expansion modules available to the Inception system. If your expansion modules are using an older firmware version, certain features of the Inception system may work incorrectly or not at all.

Expansion Module	Firmware Version
8 Input LAN Expander	3.0.1
UniBus 8 Input Expander	1.0.3
UniBus 8 Relay Expander	1.1.2
Standard LAN Access Module (SLAM)	3.1.3
SIFER Reader	1.16.0
T4000 Security Communicator	2.1.4
UniBus Lift Interface	1.0.0
Inovonics RF Expander	1.1.0
EliteX Keypad	3.0.13

How to Update Modules

How to check your expansion module versions and update them:

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



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

Updating your module versions

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

Select Firmware Update File

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

Version 3.2.3 - 11/02/20

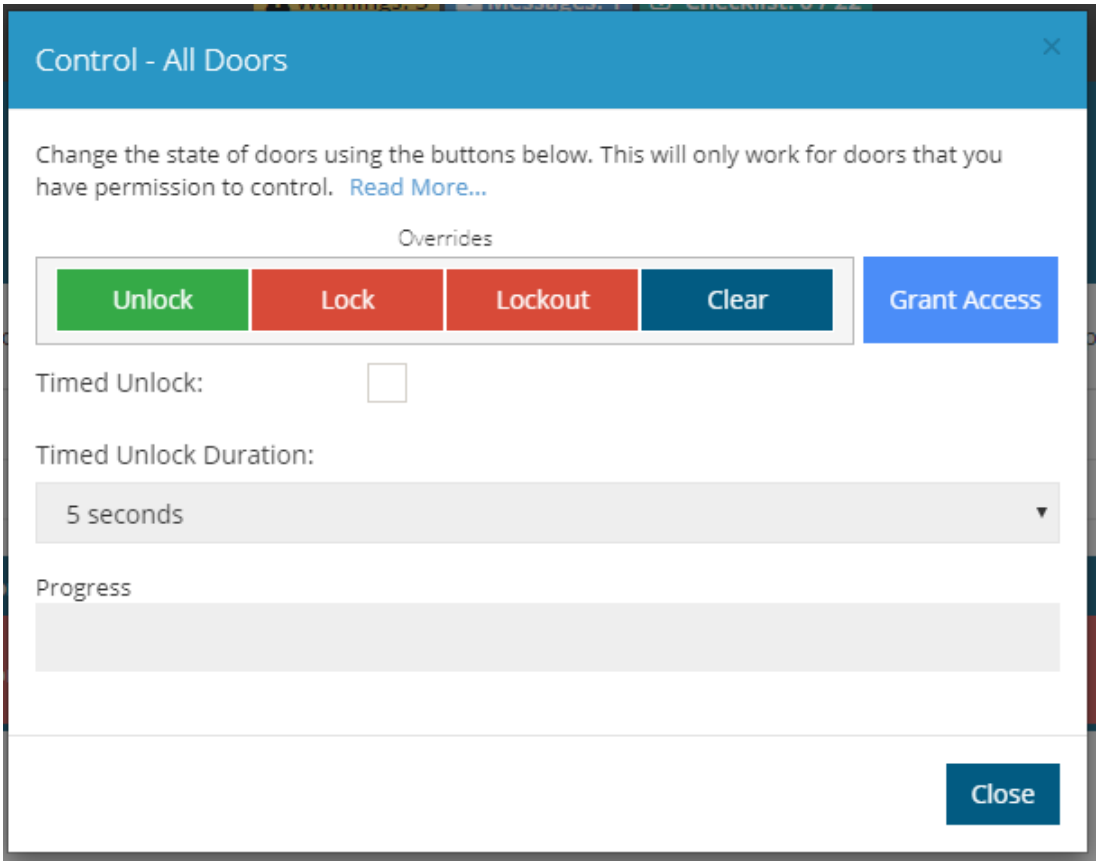
Inception release 3.2.3 allows access to an additional input and output on EliteX terminals and improves door control from the web interface.

Feature Updates

Timed Door Control from Web Interface

The advanced control dialog on the Control Doors page now allows users to unlock doors for a configurable amount of time. This allows doors to be overridden to the Unlock state with a built-in time limit, instead of the override needing to be cleared.

To perform a timed unlock, tick the Timed Unlock checkbox, set the duration, and click the Unlock button.



Additional Input and Output on EliteX Terminals

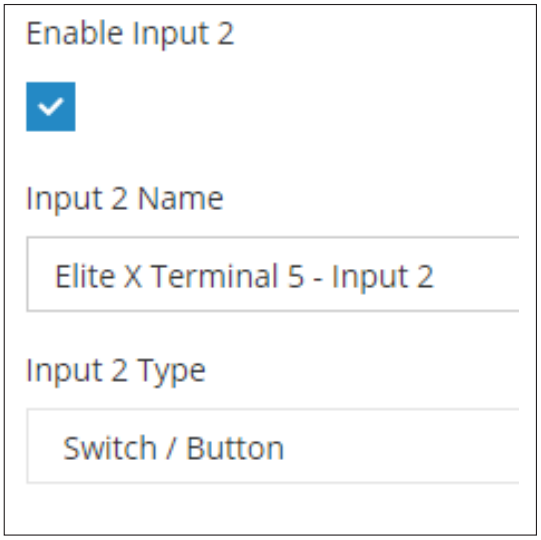
Inception's Hardware Configuration page (**[Configuration -> Hardware]**) can now configure an extra Input and Output for EliteX terminals, allowing for a maximum of 2 configured Inputs and Outputs each. The new hardware points can be found on the EliteX's Terminal Inputs/Outputs section on the Hardware page. Input 2 and Output 2 can be wired to the ZN1/0V and AX2/0V points respectively on the back of the keypad.

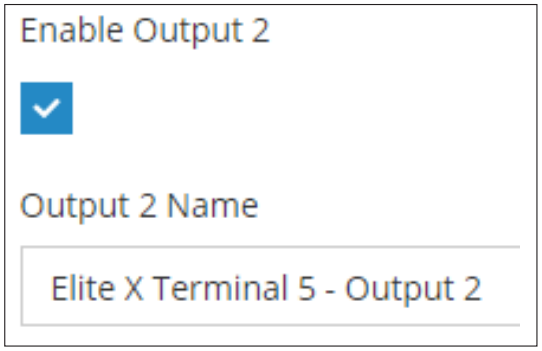
Version 3.2.3 - 11/02/20

Feature Updates (cont.)

Additional Input and Output on EliteX Terminals (cont.)

Additionally, beeper control commands now work by default and no longer require the option to be enabled via the power-up HELP menu on the keypad.

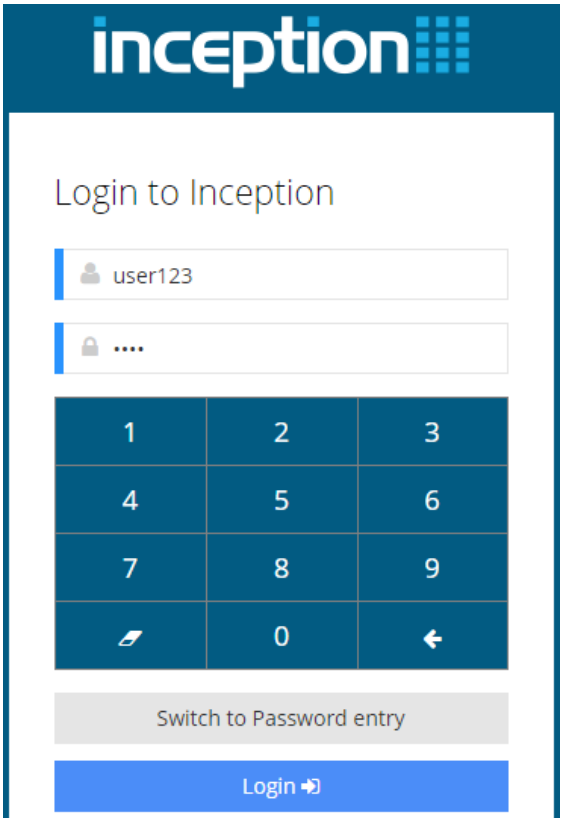




Issues Resolved

Web Login with PIN

An issue introduced in version 3.2.2 has been resolved where logging into the Web Interface with a username and PIN would fail if the username was not lowercase. The login page should now correctly accept valid usernames regardless of case.



Version 3.2.2 - 19/12/19

Inception version 3.2.2 resolves some issues identified in the recent releases of firmware.

Issues Resolved

Case-sensitive User Names

An issue was introduced with 3.2.1 where web login user names were now case-sensitive. This was an unintentional change and is now resolved with this release.

Inactive Credentials Still Working

This release resolves an issue where credentials marked as Inactive were incorrectly still being processed as valid in some circumstances.

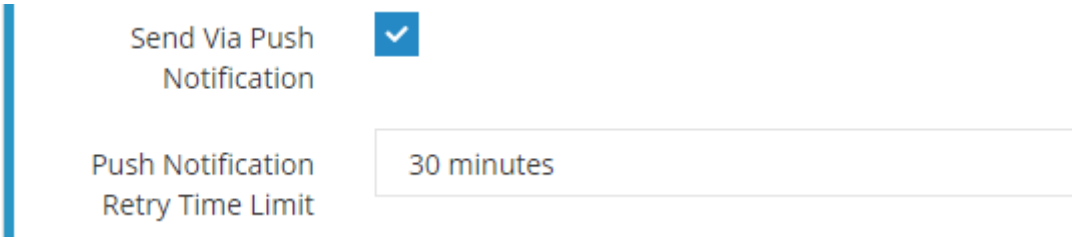
Version 3.2.1 - 12/12/19

The 3.2.1 release of Inception includes some minor feature improvements including SkyCommand notification retries and triggering actions based on area user counts.

New Features

SkyCommand Push Notification Retries

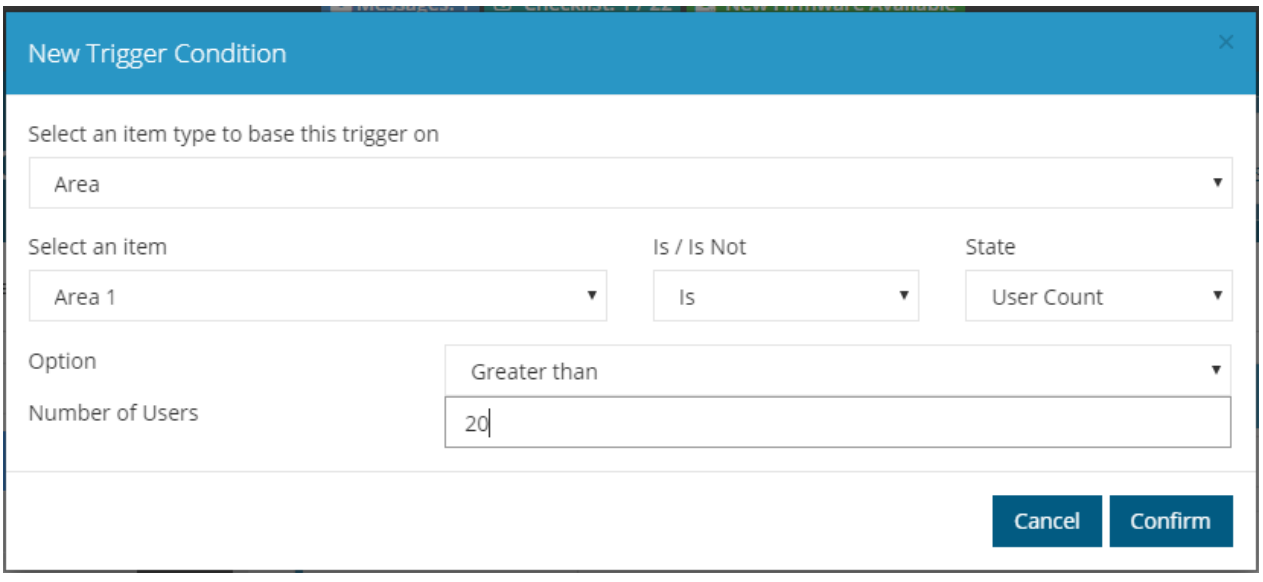
Notifiers can now have a retry time limit configured for push notifications that fail to be sent. The *Push Notification Retry Time Limit* setting determines how long the system will attempt to resend failed push notifications generated by the Notifier before discarding them. This allows Notifiers that send high priority messages to have a longer retry limit while notifications for less important things can be discarded sooner. Note that this only includes messages that can't be sent due to connectivity issues. This option can be set per Notifier on the **[Configuration -> General -> Notifiers]** page.



Automated Actions - Area User Count Trigger

Automated Actions have gained a new trigger condition type that can trigger actions based on the user count in an area. Triggers can be configured to occur when the user count is less than, equal to, or greater than a certain number, for example, Turn On Output 1 when Area 1's User Count is Greater than or Equal to 30.

The new condition can be found when adding a trigger condition to an Automated Action on the **[Configuration -> Automated Actions]** page.

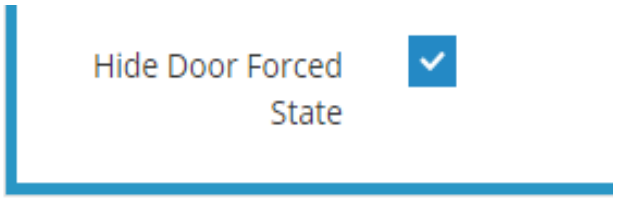


Version 3.2.1 - 12/12/19

Feature Updates

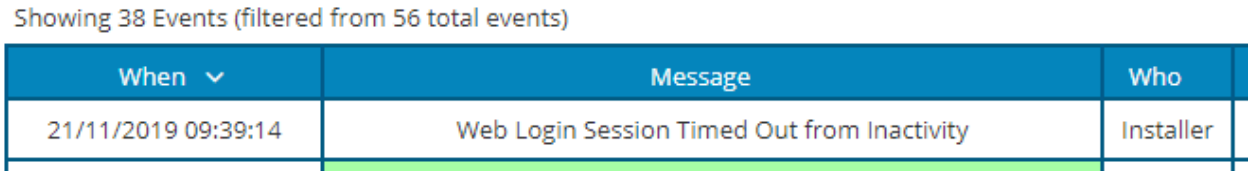
Suppress the Door Forced State

The Door Forced state for Doors can now be optionally disabled if it would be inappropriate or misleading for the door to show up as being Forced. This option is suited for doors with free egress, where the door locked door can be opened from one side. In this case, the door can commonly be opened while locked and shouldn't be highlighted in the interface as Forced. Note that this option does not affect the Door Forced input, which will still activate and can be used for alarm monitoring. This option can be set from the **[Configuration -> Access Control -> Doors]** page.



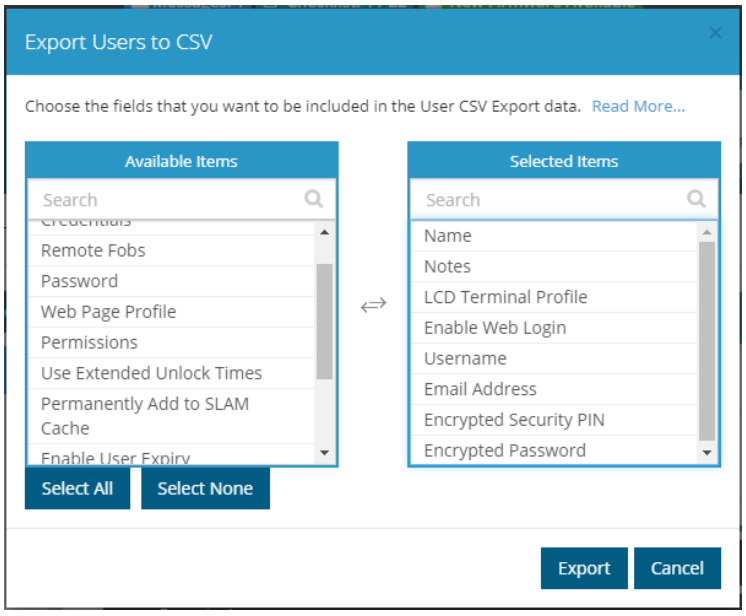
Web Session Timeout Event

A new Review Event type has been added for when a web session times out after 10 minutes of inactivity. Note that an open webpage still counts as activity as all pages regularly check for system state changes. A timeout only occurs when the page is closed without a correct logout.



User CSV Import PINs and Passwords Between Systems

User PINs and Web login passwords can now be exported in an encrypted form through the CSV Export dialog on the Manage Users page (by selecting the "Encrypted Security PIN" and "Encrypted Password" fields), allowing them to be exported and re-imported between Inception systems while retaining sensitive data fields. Previously, PINs and passwords would not be exported at all if the (non-encrypted) "Security PIN" or "Password" fields were included in a CSV Export, the fields would instead be left empty for security reasons.



User CSV data can be exported by clicking the "Export CSV" button on the **[Configuration -> Users -> Manage Users]** page.

Version 3.2.1 - 12/12/19

Issues Resolved

(EU Only) Area Alarm Triggers

Note that this only affects systems using BS8243 standards compliance. An issue has been resolved where the "Detecting Active Alarm Type" area trigger for automation actions would not work for alarms of type "Confirmed Intruder" and "Confirmed Duress".

User CSV Import

Previously, when importing users from a CSV file, the import process would automatically enable options if related options were imported. For example, importing web login details would enable the “Enable Web Login” option and expiry dates would enable the “Enable User Expiry” option.

This caused a problem when exporting a user database, making minor changes, and reimporting the file to update users. In this case, users could have their web login enabled because their web profile was re-assigned, which would then fail validation because no username or password was configured.

If user expiry options or web login details should be imported via CSV, ensure the corresponding “Enable” checkbox is also included and configured in the file (e.g. “Enable Web Login”, “Enable User Expiry”).

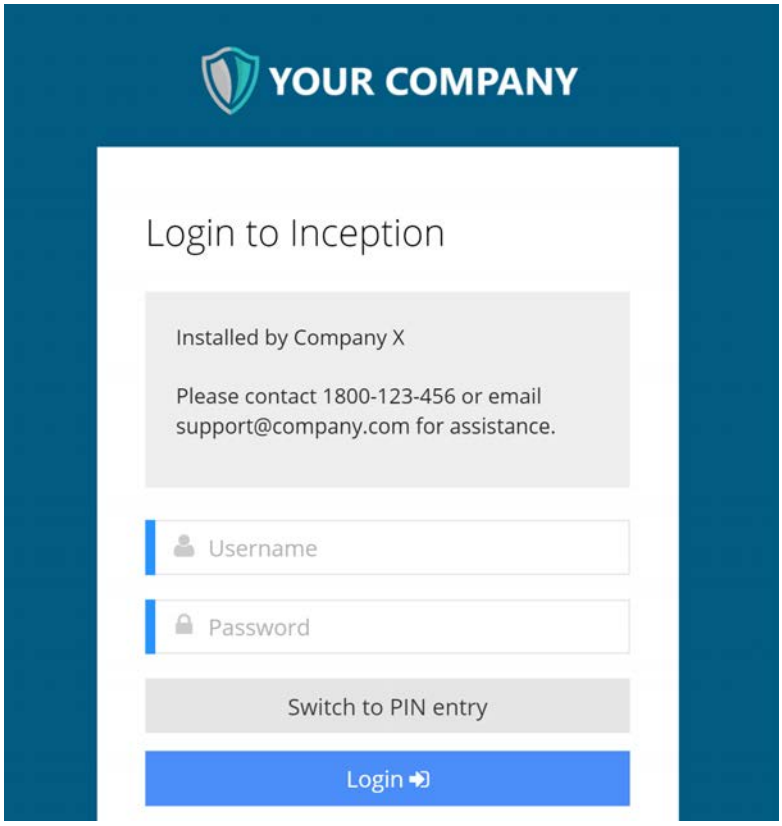
Version 3.2.0 - 15/10/19

Inception release 3.2.0 adds custom branding abilities, improves credential management (with Active/Lost/Stolen states and being identified as card, fingerprint, face and iris) and several other feature updates. It also resolves some issues like a watchdog reset and problems with Review not loading.

New Features

Custom Branding

Inception now provides the ability to set a custom brand logo and text message to be displayed to an end-user when they are logging into the system. The logo will also be included at the top of any PDF or HTML reports that Inception generates. Configuration of these options are on the **[Configuration > General > System]** page.



See the Tech Guide called Inception – Custom Branding for more information on setting it up here: https://www.innerrange.com/Products-Solutions/Inception#Technicians-Resources

Version 3.2.0 - 15/10/19

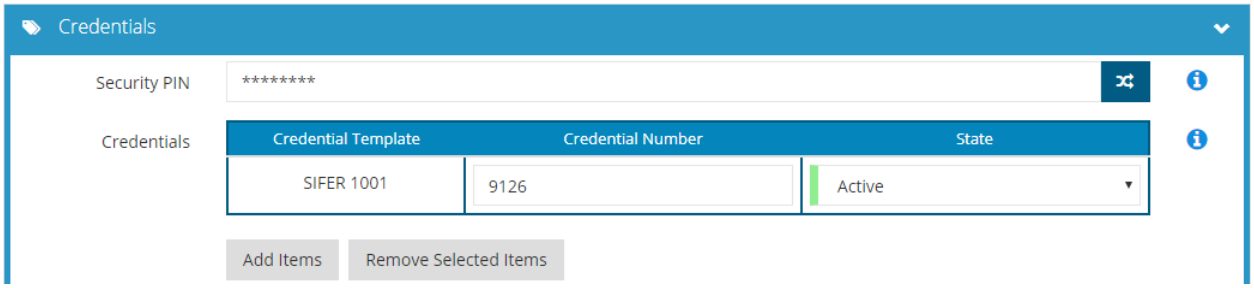
New Features (cont.)

Credential State

Inception user credentials have gained a new “State” property, which allows credentials to be marked as Inactive/Lost/Stolen to prevent them from being used for access, but without having to delete the credential info from the User’s configuration.

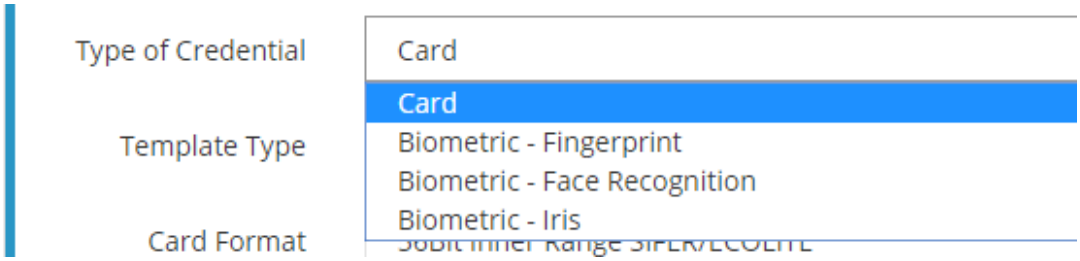
Any credentials set to an “Inactive” state will be rejected by the system when an access attempt is made, and a relevant review event will be logged. A System Message is also created to bring attention to the event and a new Notifier option allows an email or push notification to be automatically sent. This allows the original owner of a lost credential to be easily identified, or notification when a stolen credential has been used.

“Inactive – Lost”/”Inactive – Stolen”/etc behave the same and are only named differently for informational purposes. Existing credentials are set to the “Active” state by default, allowing them to be used as normal. Credential States can be edited on the **[Configuration > Users > Manage Users]** page in the “Credentials” section.



Granular Credential Types

With this release, user credentials are no longer assumed to be card-only. In addition to cards, credentials can now be configured as a facial recognition credential, fingerprint scan, or iris scan data. To reflect this change, “Card Templates” have been renamed to “Credential Templates”. The Credential type can be edited by changing the “Type of Credential” field on the **[Configuration > Access Control > Credential Templates]** page.



Primarily, this allows more advanced access modes to be configured, allowing higher flexibility and security for how a door is accessed. For example, a face scan, card, or PIN may be allowed during the day, but after hours a face scan is no longer allowed and both a card and PIN are required.

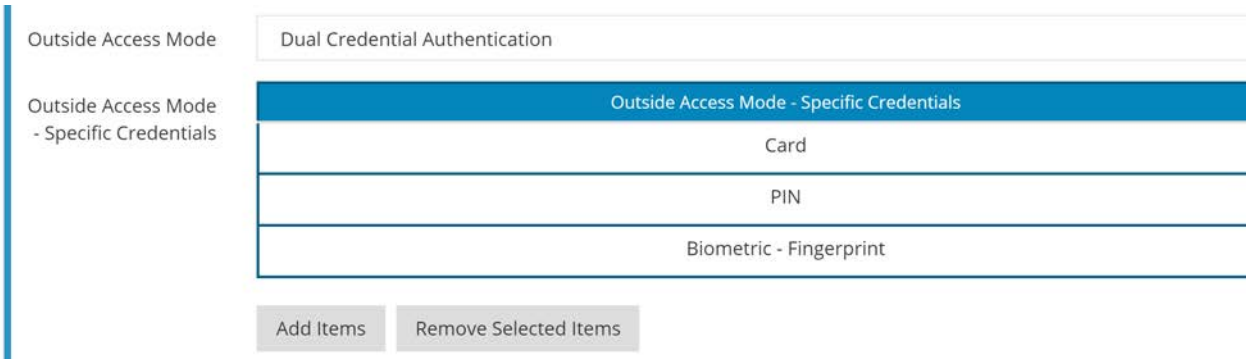
Previously the access modes were limited to combinations of Card and/or PIN. This has now been split into “how many credentials are needed” (Single/Dual/Triple Credential Authentication) and “what types credentials are allowed” (Specific Credentials). So a door can be accessed from a single credential of any type (essentially Card or PIN or Face or Fingerprint or Iris scan), or require two or three credentials of specific types (e.g a combination of card, PIN and fingerprint in any order).

Version 3.2.0 - 15/10/19

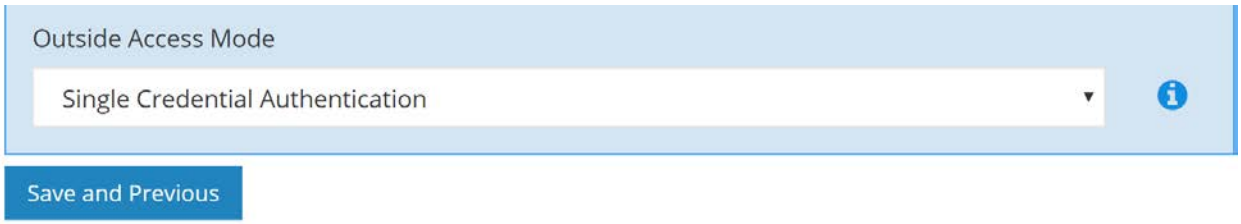
New Features (cont.)

Granular Credential Types (cont.)

Configuration of the access modes are available on the **[Configuration > Access Control > Doors]** page. If no specific credentials are selected, all credential types are allowed from that side of the door (this is the default option). This can be configured for the inside and outside of the door and also works with the alternate door modes feature.



The hardware wizard (**[Configuration > Hardware]** page) has also been updated with this change. By default all credential types are allowed through a door, so the only choice is how many credentials a user needs to present (one, two, or three) to access the door.



REST API

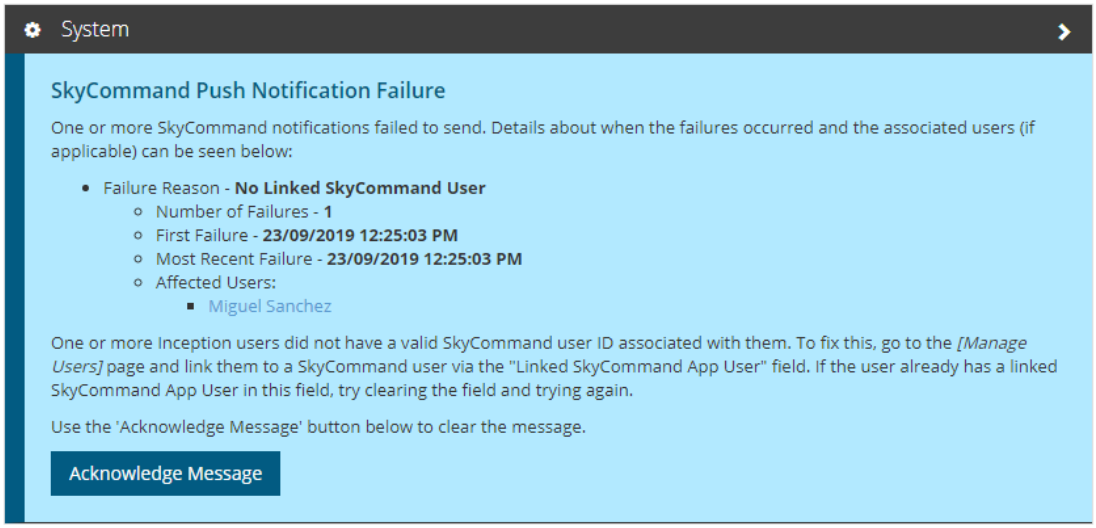
The Inception REST API now provides the ability to “virtually badge” credentials and PINs at readers, which triggers an access event at the door, the same as if the credential was physically badged at the reader. The REST API protocol version has also been increased to version 4. See the latest Inception REST API release notes & documentation for more information on using these features.

Version 3.2.0 - 15/10/19

Feature Updates

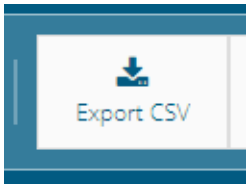
SkyCommand Failed Notification Messages

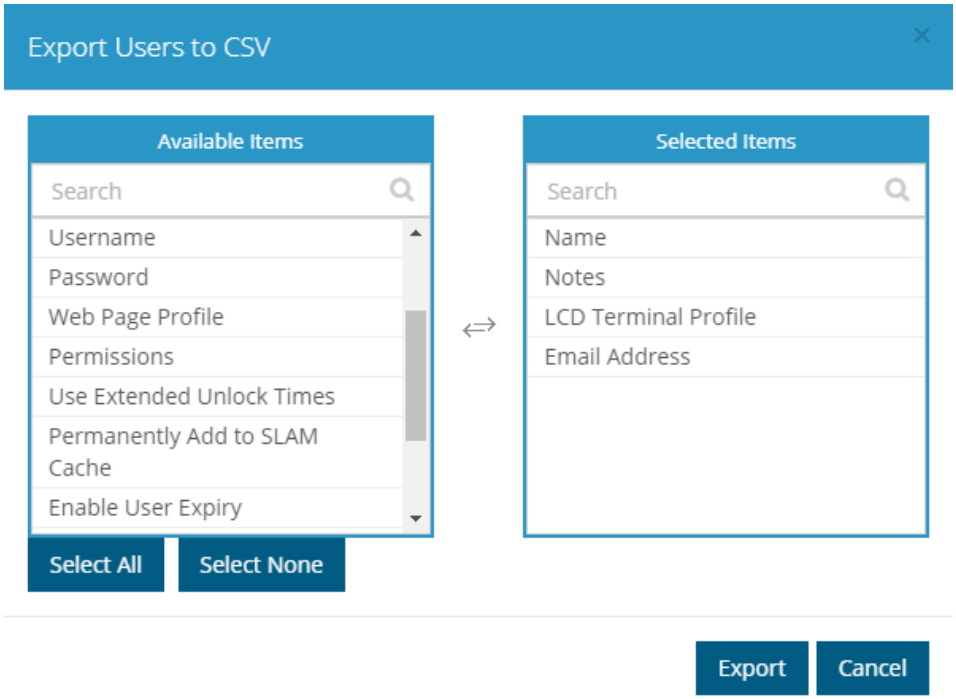
Previously, when a SkyCommand push notification failed to be sent to a user (e.g. a missing subscription, user not linked to SkyCommand, etc), the only indication was a failure event in the review logs. To make push notification failures easier to recognise and for clearer instructions on how to resolve the issues, a new System Message category has been added to bring attention to notification send failures (and the related users if applicable).



User CSV Export

The “Export CSV” button on the **[Configuration > Users > Manage Users]** page now brings up a dialog first to select which user fields or columns should be included in the CSV data, instead of just exporting a fixed set of columns.





Version 3.2.0 - 15/10/19

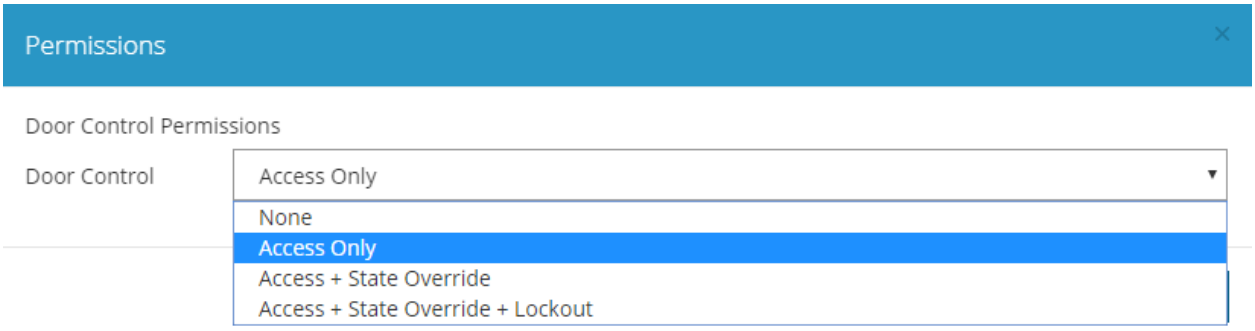
Feature Updates (cont.)

Granular Door Permissions

Door permissions have been split from a single full permission entry into different levels of permission for certain actions, including “Access Only”, “Access + State Override”, and “Access + State Override + Lockout” permissions. This allows finer level control of permissions, allowing users to unlock the door for the normal unlock time (via credential at a reader, web interface or SkyCommand App) while preventing them from overriding the door lock state or locking out the door.

These detailed permission options are only available within permission groups (on the **[Configuration > Users > Permission Groups]** page). If adding the door directly to a user, they will have always have full permission.

These new permission types will also be supported by SkyCommand in a future update.



Issues Resolved

Watchdog Reset Resolved
An issue that could result in a watchdog reset has been identified and resolved in this release.

SkyCommand Notification Timestamp
Push notifications sent from Inception to the SkyCommand App were unintentionally always marked with Melbourne’s timezone. This has been resolved.

Additional Review Events not loading
An issue introduced in version 3.1.0 has been resolved where the Review Events page could enter a state in which it would not load any additional review messages, indicating “all review loaded” even when there were more messages to come.

CSV Import Ignoring User Priority
Previously, CSV Import of users would ignore user priority, allowing someone to modify users with a higher priority than them. With the built-in web page profiles, by default, this would only affect System Administrator users. Also, audit review for a CSV import would indicate the “System” was the one who created/changed the users. Both of these issues are now resolved.

Version 3.1.1 - 08/08/19

Inception release 3.1.1 brings several feature enhancements that help with identifying hardware points and increases the Review amount within Inception to 250,000 events. Also, an issue has been resolve that prevents the Inception from getting into a poor connectivity state.

New Features

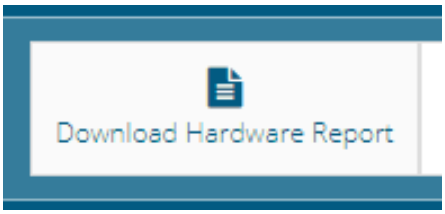
Increased Review Event Limit to 250,000

Inception's review capacity has increased from 50,000 to 250,000 with this release. Review is automatically replaced once the limit is reached, so this change allows a much longer history to be persisted within the system. For sites with higher numbers of users or doors, this larger history becomes important when running reports over the system.

In addition to this change, on the **[State / Control > Review Events]** page, the original *Load All* button in the toolbox has been replaced with a *Load 10000 More* button. These buttons are used to load more review into the browser to interact with.

Hardware Report

The **[Configuration > Hardware]** page has gained a new "Download Hardware Report" button in the toolbox at the top of the page. This button generates a text report containing the details of all the currently configured hardware modules in the Inception system, including their attached Inputs, Outputs, Readers, and Doors (if applicable), and also any additional configuration options such as tamper and power supply/battery monitoring.



Feature Updates

Hardware Points added to Hardware Test Page

The **[State / Control > Hardware Test]** page, used to test the low-level Inputs, Outputs, and modules during commissioning and fault finding, has been updated to include the physical hardware points for inputs and outputs. If there are faults on the inputs or outputs, this information helps when mapping some physical hardware back to the actual input connection on the hardware.

Input Test

Point	Name	Current State
Input 1	Front Door - Reed	Tamper
Input 2	Garage Door - Reed	Tamper
Input 3	Rear Door - Reed	Tamper
Input 4	Study window - Reed	Tamper
Input 5	Hallway PIR	Inactive

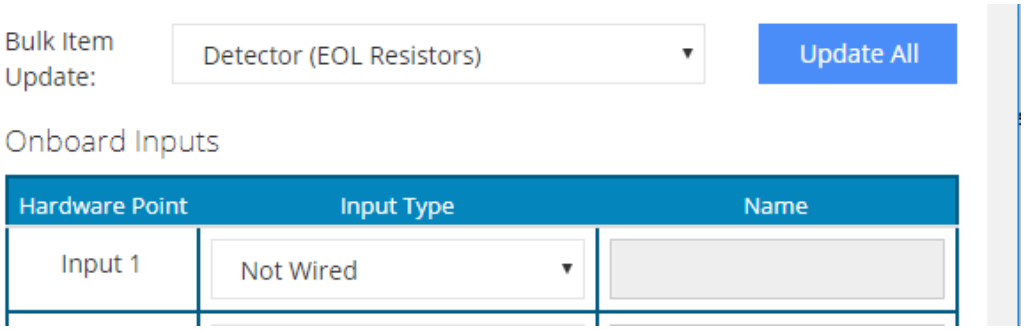
Version 3.1.1 - 08/08/19

Feature Updates (cont.)

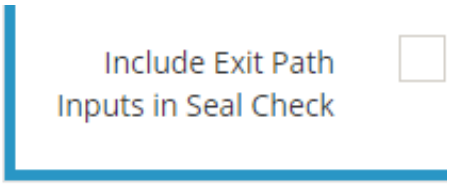
Bulk Input/Output Creation in Hardware Wizard

The Input and Output configuration sections of the Hardware Wizard (**[Configuration > Hardware]** page) has been updated to allow them to be quickly configured. A *Bulk Item Update* section has been added to these sections of the wizard to allow all inputs or outputs on that module to be configured with one click. This speeds up the process instead of manually needing to assign each input type individually.

This is helpful when the cabling for many inputs or outputs have been connected to a module but the cable pairs are unclear. All inputs and outputs can be configured with one click and then the **[State / Control > Hardware Test]** page can be used to identify which hardware point is which.



Include Exit Inputs in Area Arm Seal Check



Areas have gained a new *Include Exit Path Inputs in Seal Check* option in the Inputs section of the **[Configuration > Areas > Edit Areas]** page. This causes Entry/Exit path inputs to also be included in the Seal Check performed whenever an Area is armed with an Exit Delay (i.e. if an Exit path input is active during the seal check, the check will fail and cancel the arm). By default, exit path inputs were always excluded from the seal check as they may be active when arming from a terminal. For example, this option allows the exit inputs to be included in the seal check where, on a site with multiple exit doors, you want to be notified if one of the other doors is open during an arm attempt so you can go and close it.

Limit User Permissions to Permission Groups Only

To help simplify user management for end-users, a new option has been added to Web Page Profiles. If enabled, users with that profile will only be allowed to assign permission groups to other users and will have the individual areas, doors, outputs and so on hidden. This allows the detailed site permissions to be configured by a technician or a system administrator, while a user responsible for the day to day management has a simpler interface. Also, if a site has complex permissions (i.e permission is only allowed during working hours etc), it prevents a user from assigning permission to the item directly.

This option is enabled with the *Limit User Permission Config* to *Groups Only* checkbox added to the **[Configuration > Users > Web Page Profiles]** page, and is enabled by default for the User Admin and Control and User Admin web page profiles.

Version 3.1.1 - 08/08/19

Feature Updates (cont.)

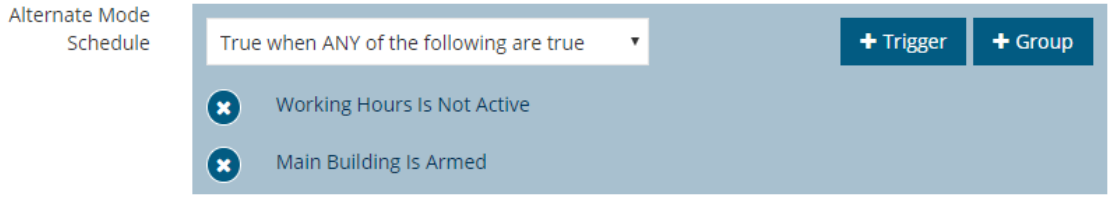
CSV File Format for Reports

System Reports (accessed from the **[System > Reports]** page) are now able to exported in CSV (comma-separated value) file format. This allows the variety of reports available in Inception to be more easily modified or processed by external applications.

Enhanced Alternate Door Behaviour Scheduling

Version 3.1.0 saw the introduction of alternate door programming, allowing the access modes of doors to be changed based on a schedule. This would allow a door to allow Card or PIN during the day but requiring Card and PIN after hours for higher security.

This feature has been extended in this release, replacing the simple schedule with a more advanced option that allows multiple conditions to be specified. Now, for example, you could require Card or PIN for normal usage. Outside of working hours, or if the area is armed, you could require Card and PIN. This would provide additional security for the Disarm on Access feature as the armed area would require both Card and PIN to disarm before accessing the door.



Single 1k EOL

Support for the single 1k EOL configuration has been added as a built-in option. Note that, as with other Single EOL options, all inputs must have EOL resistors wired. This includes switch/button type inputs.

Improved User CSV Import

CSV Import of users has been extended with this release, allowing all options of a user to be imported. This allows additional items of a user to be configured via import, like their web login settings, RF fobs and the less commonly used options. Import files created before this release that use the old format (the 8 fixed-order columns) are still supported. See the CSV Import dialog for more information.

Issues Resolved

Connectivity and Performance Issue

An issue has been reported where, in rare cases after several months of operation, the Inception system would have connectivity issues with modules before rebooting after some time. During this time the web interface may also be unresponsive. After rebooting the system would return to normal operation. This release attempts to prevent the issue from occurring, however, if it does occur, the unit will automatically reboot itself instead of going through an unresponsive phase.

IRFast Reporting over SkyTunnel

Several system events (system reset, test reports, comms failure) were not including their text in IRFast with Text mode when being reported over SkyTunnel. This is now resolved.

Permission Reports

An issue was resolved where User Permission Reports and Item Permission Reports would not contain a title/header line before the document content.

Version 3.1.0 - 09/05/19

Inception release 3.1.0 includes a wide range of new features and improvements to the system. Inception gains a dedicated App, can be integrated with the Milestone Access platform and many other improvements.

New Features

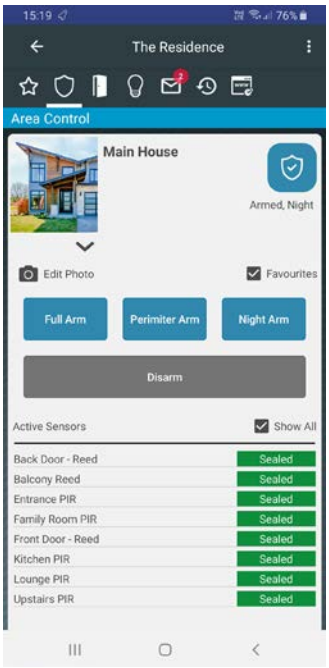
SkyCommand App (Due Q2)

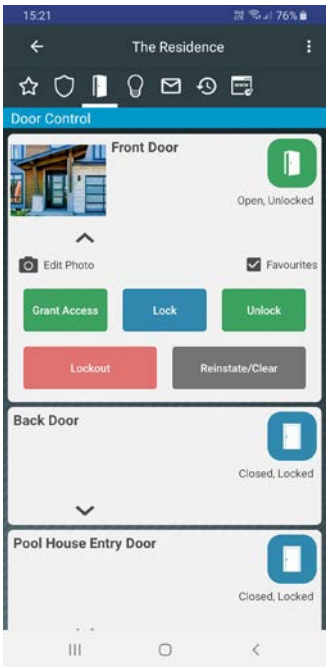
Included in this release, end users can now control their Inception system remotely using the SkyCommand app. The App update supporting these changes is expected to be released late May or June. SkyCommand provides fully interactive control of security areas, doors, and outputs. The visual styling and layout have been updated to accommodate the new functionality. The Inception must have Internet connectivity to enable the App to connect and control the system, this is direct control and a T4000 is not required. The SkyCommand App is free* for up to 10 app users to download and use, with full access to the new features and functionality.

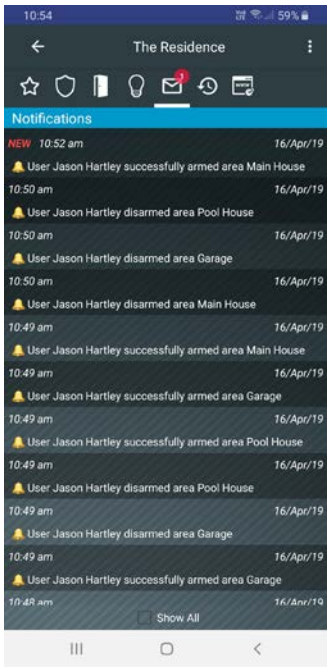
Key features include:
- Interactive control and live status of areas, inputs, doors, and outputs
- Simple or multimode area arming options (Full, Perimeter and Night modes)
- User-selectable timed output control
- Simple and convenient one-touch control, or expand an item for advanced options
- Push notification alerts to users smartphone*
- No T4000 required

*A SkyCommand app subscription is required to enable the Push Notification service an increase the number of app users.

For more information, including guides on how to start using the App, see the SkyCommand App section of the Inner Range website:
https://www.innerrange.com/Products-Solutions/Inception#SkyCommand-App







Version 3.1.0 - 09/05/19

New Features (cont.)

Milestone XProtect Access Integration (Due Q2)

This release includes support for the upcoming Milestone XProtect Access integration, expected to be released late May or June 2019. This integration allows the Inception controller to become the security and access system supporting the Milestone XProtect VMS system. Multiple Inception systems can be integrated with a single Milestone system for multi-site monitoring.

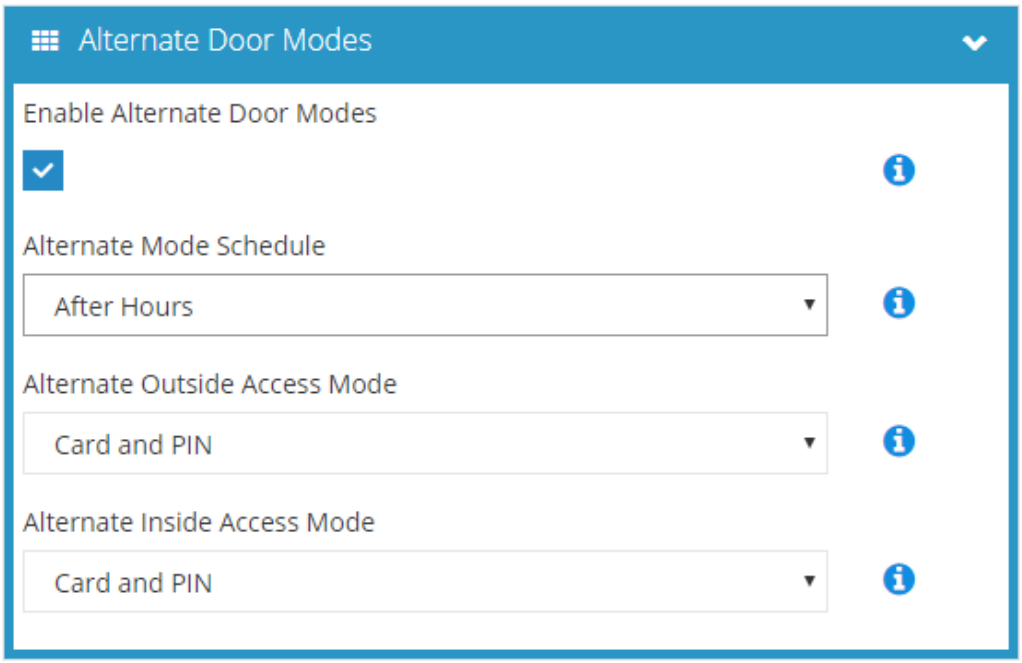
Key features include:

- Live syncing of Door, Area and Output states to Milestone. These items can be displayed on site maps in Milestone with full control abilities
- Live access and alarm events are sent to Milestone, allowing a wide range of actions to be triggered in Milestone based on these events.
- Operator processed access requests can be shown where an operator compares video footage to a user's photo before granting access through a door
- Users are dynamically synced into Milestone with new users and changes automatically appearing in the Milestone interface
- Inception's web interface can be shown directly within the XProtect client

For more information, see the Inception Integrations page on the Inner Range website:
https://www.innerrange.com/Products-Solutions/Inception#Integrations

Alternate Door Programming

A new section has been added to Door programming (the **[Configuration > Access Control > Doors]** page), allowing alternate door modes to be used if a schedule is active. This allows some of the access options for a door to change based on the time of day. For example, during the day, a user could use their Card or PIN to access a door for convenience. However, after hours, the site could require that both Card and PIN are used for higher security. Similarly, access modes could differ based on weekdays vs weekends and so on.

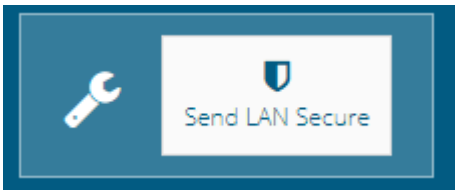


Version 3.1.0 - 09/05/19

New Features (cont.)

LAN Secure

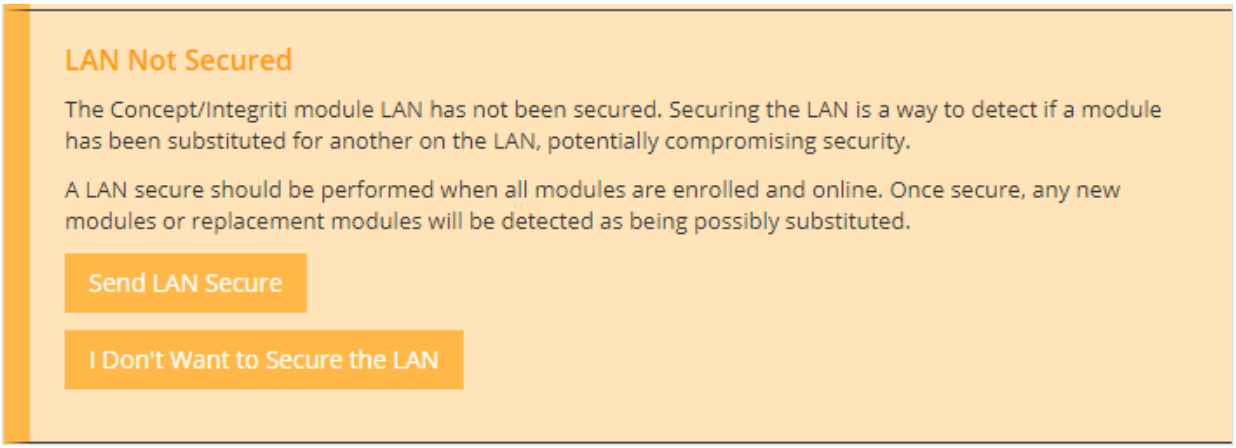
This Inception release includes the ability to secure the LAN. Sending a LAN secure is a way for Inception to detect if a module has been substituted for another on the LAN, potentially compromising the security. After this update, a new Warning will be shown indicating that the LAN is not secured.



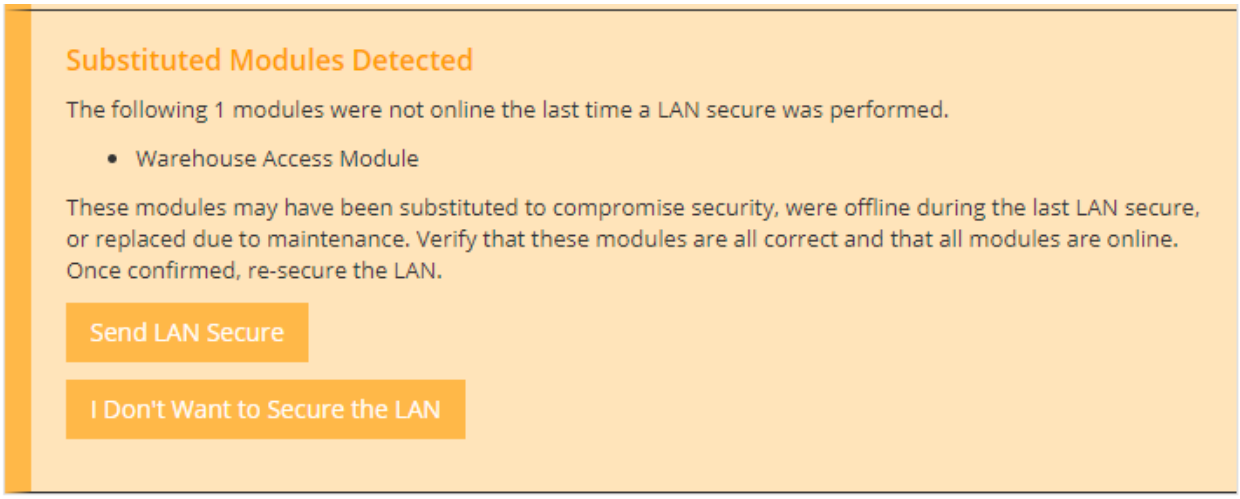
A new reporting event has also been added that is sent whenever a module substitution is detected.

If you don't want to monitor for substitutions and don't want events to be reported, the *I Don't Want to Secure the LAN* button will hide the warning. Otherwise, the *Send LAN Secure* button will secure the LAN. LAN Secure requests can be manually sent from the **[State / Control > Hardware Test]** page too.

Note that this should only be done once all modules are enrolled and online. Once sent, any new modules that connect are considered as potentially substituted.



If a substituted module is detected (a module comes online that wasn't connected when the last LAN secure was sent), an alarm event is generated and a warning is shown listing the detected modules. If the module was replaced due to maintenance or wasn't online during the last LAN secure, a new LAN secure can be sent. Or, you can set the system to stop monitoring for LAN secures from this warning too.

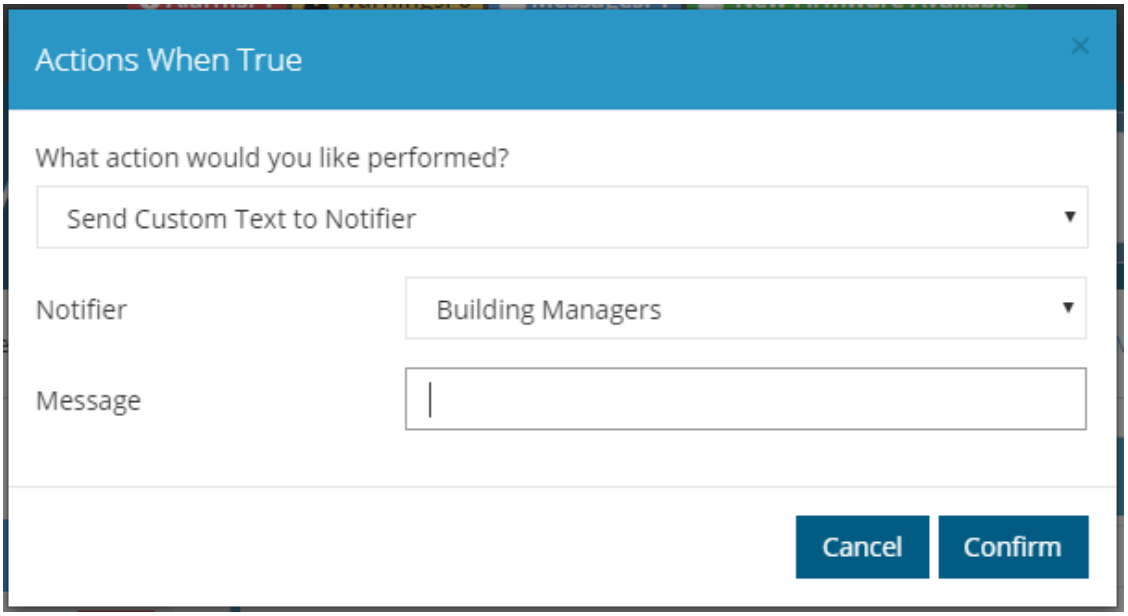


Version 3.1.0 - 09/05/19

New Features (cont.)

Notify Custom Text via Automated Action

The Notifiers section (configured on the **[Configuration > General > Notifiers]** page) allows a wide range of events to be notified to users via email and push notifications (soon, when the SkyCommand App is available). For custom scenarios or messages though, automated actions have been updated to include a new action where custom text can be sent to the recipients linked to a notifier. This allows custom scenarios or scenarios not included by default in the Notifiers section to also send notification messages.



Anti-Passback Report

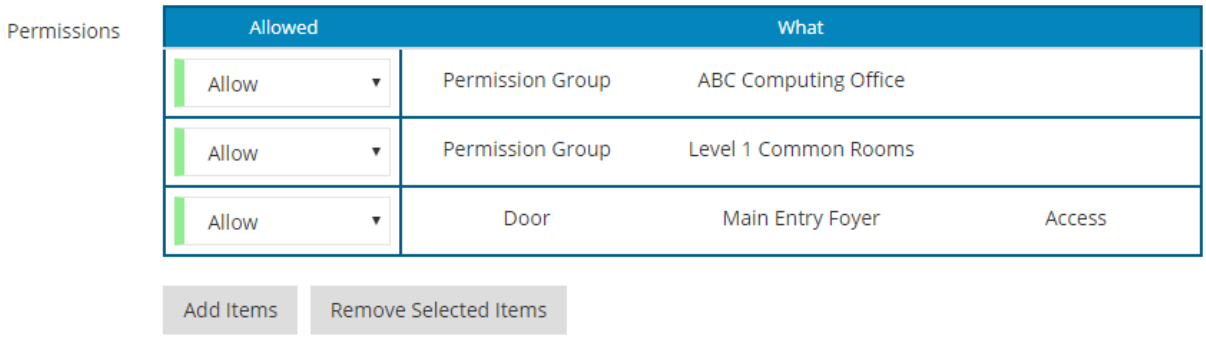
A new report has been added to the **[System > Reports]** page that can detail user Anti-Passback violations. The report can be filtered to include only events related to specific areas, doors or users over a timeframe. The report can also optionally include both violations and forgiveness events. Violations will include when the event occurred, who violated the anti-passback rules and where the violation occurred. Forgiveness will include who was forgiven (either a specific user or group of users) and who granted the forgiveness.

Version 3.1.0 - 09/05/19

Feature Updates

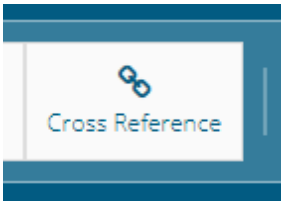
User Permission Simplification

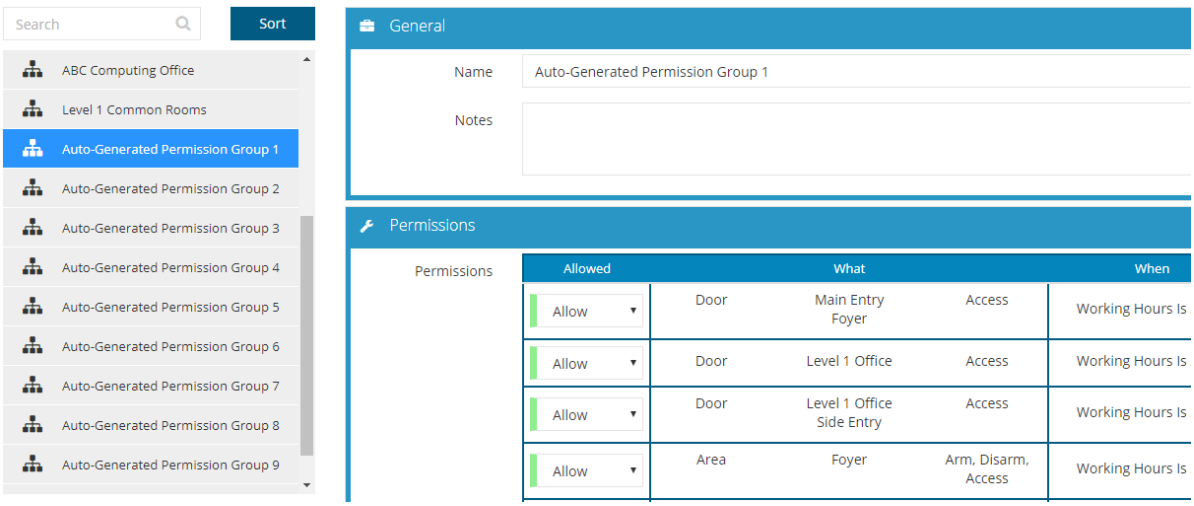
User permissions have been changed in an attempt to be simpler for the end user. In short, the “When” of permissions and customizing of control (like giving disarm abilities but not arm abilities), can no longer be assigned directly to a user. These options can only be set within permission groups.



The main purpose of this change is so when end users (system admins, receptionists, etc) are managing their users, they simply choose the permission groups, areas, doors or outputs that should be assigned to the user. They no longer get prompted with a list of area control questions or a complicated “when” list that they need to remember to set according to the site rules. If a system requires more complicated permissions, such as access only during working hours, or interlocking scenarios with outputs, inputs or other items used as the “when” qualifier, these can all be configured by the integrator within permission groups and the complexity is hidden away from the end user.

NOTE: Auto-Generated Permission Groups –
In order to make this change, users with “complex” permissions (a non-always “when”, or custom area control options) have had their permissions replaced with a permission group. Either an existing one that matched their exact permissions or a new auto-generated one. If auto-generated, these groups should be renamed to explain their purpose, like “Level 2 Office” etc. Note, the “Cross Reference” toolbox button may be helpful in working out who has which permission groups.





Version 3.1.0 - 09/05/19

Feature Updates (cont.)

REST API Improvements

Several improvements have been made to the REST API for 3rd party integrations. In particular, review events can now be retrieved and streamed via the API, and user management has been made improved by being able to fetch user changes from Inception more easily on initial setup and as the changes occur. Many more changes have been included such as more information accessible via new requests.

The Postman sample collection and environment files have been updated, which can be downloaded from the /ApiDocExamples page on an Inception running this release.

For more detailed information about the changes, see the REST Integration API section on the Inner Range website here: https://www.innerrange.com/Products-Solutions/Inception#Integrations

Door Lock after Three-Badge Action

Currently, when performing a three-badge arming action, the first badge will unlock the door, the second badge does nothing, and the third badge arms the area. However, in this scenario, the door still remains unlocked from the first access request for the full unlock time. The user has to wait until the door relocks and in a windy environment, the door could blow open, triggering entry delay and so on.

With this update, the access request will be removed as soon as the three-badge action occurs, relocking the door.

Multi-mode Area Rename (Full, Perimeter and Night modes)

The Multi-mode Area Arming option (added in 2.4.0) adds “Full (Away), Home (Stay) and Sleep (Instant)” arm modes to areas. After feedback, and to be consistent with development being done on other products, these have been renamed to “Full, Perimeter and Night” modes. This will be consistent with what is shown in the SkyCommand App and in updates being made to the Control4 driver.

Version 3.1.0 - 09/05/19

Issues Resolved

Sending Scheduled Reports via Email

An issue has been fixed where if sending a report to many different people via email, only the first batch of users in the list would receive it. This was due to the report being cleaned up too early before all of the emails had been sent.

Internet Explorer Cache Fix

When using Internet Explorer, visual issues could occur when adding items on any of the edit pages where it would appear as if data was lost. After loading the page and adding an item, if the page was revisited then Internet Explorer would show the old list due to a caching issue in the browser. This update forces the caches to be cleared, ensuring the latest information is always shown.

[EU Only] IRIS Communicator Fix

Two issues were identified with the IRIS Communicator integration.

1. ContactID reporting is limited to 4 digit account codes. If a non-4 digit account was entered then it would just fail to send alarms silently. This has been updated with validation.
2. The option to select between ContactID and SIA reporting was not being applied correctly, defaulting to always using the ContactID format. This has been fixed.

Wire Short Update

An issue was identified where a wire short occurring on the Reader or LAN ports of the Inception controller were not being detected by the system or reported. This has now been resolved.

User-Controllable Lock Outputs

In this update, the output linked to a door lock can no longer be configured as end-user controllable. If the lock output was controlled manually, the lock could be in a different state than what Inception believes. For example, Inception could believe all doors are locked, but if the lock output was turned on manually, a door could be pushed open. Also, any lock outputs that are currently user controllable will have that option removed.

If trying to manually test the door lock during initial site commissioning, the preferred way is via the **[State / Control > Hardware Test]** page. This allows low-level control without needing to edit permissions and add unnecessary programming.

If trying to control the door via a T4000 and SkyCommand, a custom output should instead be created that is user controllable and automated actions used to control the actual door. Contact Inner Range support for more information on this. Or, once the new SkyCommand app is released, the door can be controlled directly if the Inception has an internet connection.

Version 3.0.3 - 05/03/19

Inception release 3.0.3 includes a couple of minor feature updates and several resolved issues.

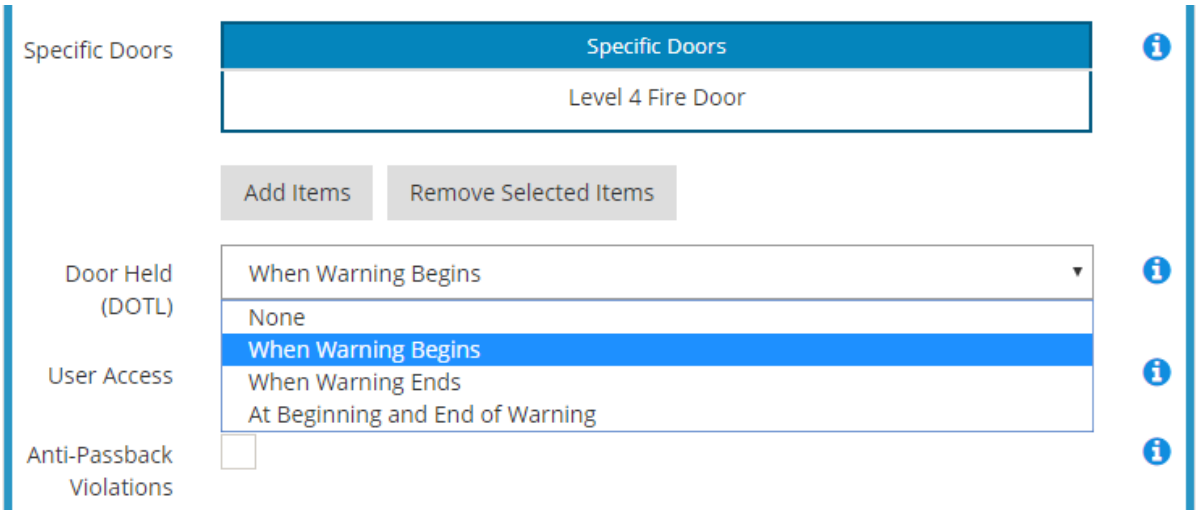
Feature Updates

Door Held Notifications

Within the Notifiers feature, the “Door Held (DOTL)” notifications option has been changed from a simple checkbox to a dropdown option. Previously, notifications could only be sent after the warning phase completed. Now, a notification can also be sent when the warning phase begins for a door being held open.

This allows the event to be escalated multiple times. If a door has been held open for a while, local buzzers can sound and a notification could be sent to people who should be nearby. If no one then closes the door, another notification can be sent to someone else like a building manager and an alarm can be sent to a monitoring station to contact someone.

This change is backwardly compatible. If this option was previously enabled, it will be automatically set to the “When Warning Ends” option.



Item List Focus

When on an edit page with many items, if you scrolled down, selected an item, edit it, and saved it, the item list would return back to the top. This update ensures that after saving the selected item will be focused in the list.

Version 3.0.3 - 05/03/19

Issues Resolved

Email Sending Improvement

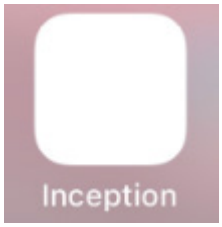
Support for sending emails has been improved in this release. In the past, multiple reports have indicated that over time email sending from Inception can stop. Once stopped, sending test emails or editing settings would be unsuccessful until the controller is restarted. In this release, the email sending logic has improved to help address this issue.

Incorrect SkyTunnel Comms Alarm

In response to a SkyTunnel connection being re-created, even if SkyTunnel was not being used to report alarms, Inception would incorrectly try to report this event as an alarm comms path being re-established. This has now been resolved.

Webpage Icon Update

An issue was identified where on Apple/iOS devices, bookmarking the Inception web interface to create a shortcut on the device would result in a blank box. This has been updated so browsers and devices of various types will have proper a proper IR logo.



Lift Floor Issue

An issue has been resolved that in rare cases could affect the freeing and securing of lift floors. This could occur when multiple floors for a lift car were configured with the same free access time periods. Once the issue occurred, control of the lift floors would be prevented.

Missing Automated Action/Connections State

With Inception release 3.0.0, an issue was accidentally introduced where the Automated Action and the Connections edit pages would no longer show the state of those items within the item list. This release resolves that issue.

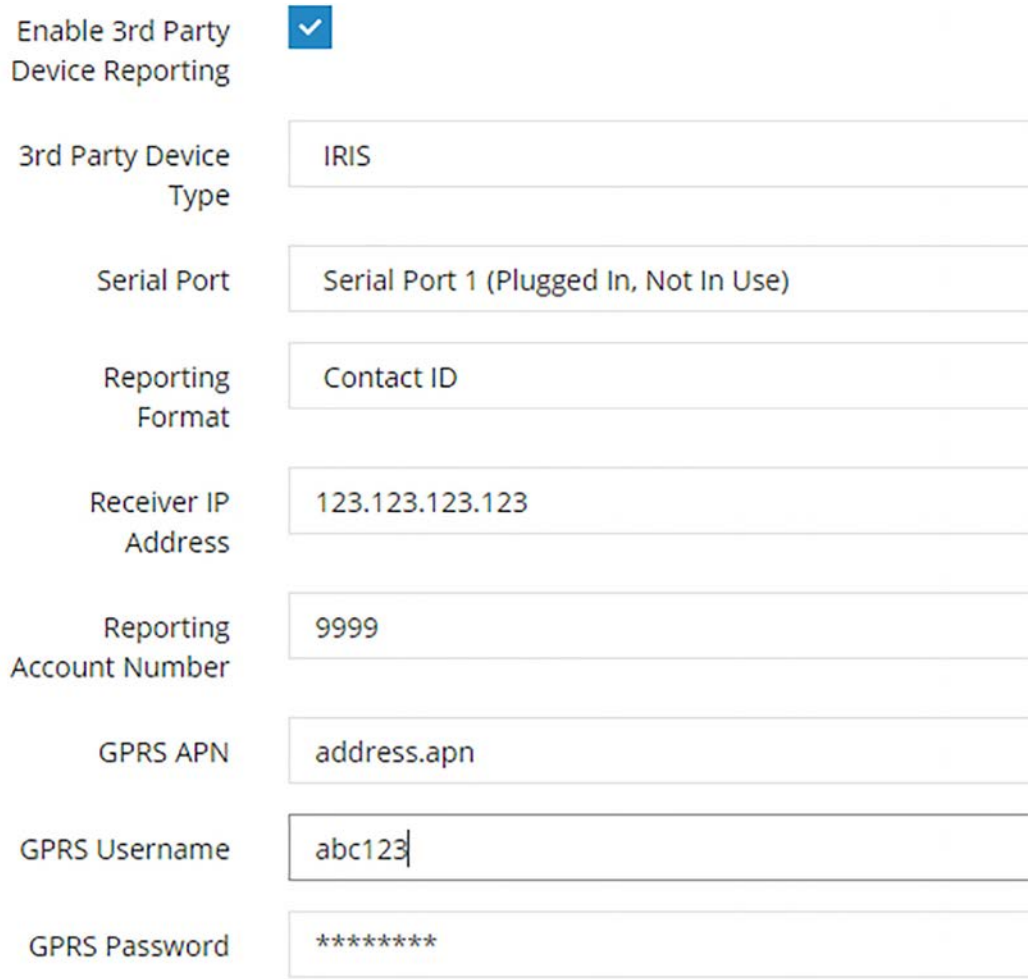
Version 3.0.2 - 31/1/19

Inception release 3.0.2 includes a number of minor feature updates. For the European markets, support for the IRIS alarm communicator is also included.

New Features

[EU Only] IRIS GSM Communicator Support

Support for the IRIS GSM communicator has been added with this release. Only for EU units, the configuration of the communicator is available from the **[Configuration > General > Alarm Reporting]** page. A valid Receiver IP address and Reporting Account Number must be entered for the communicator to work.



Version 3.0.2 - 31/1/19

Feature Updates

Door State Input Types

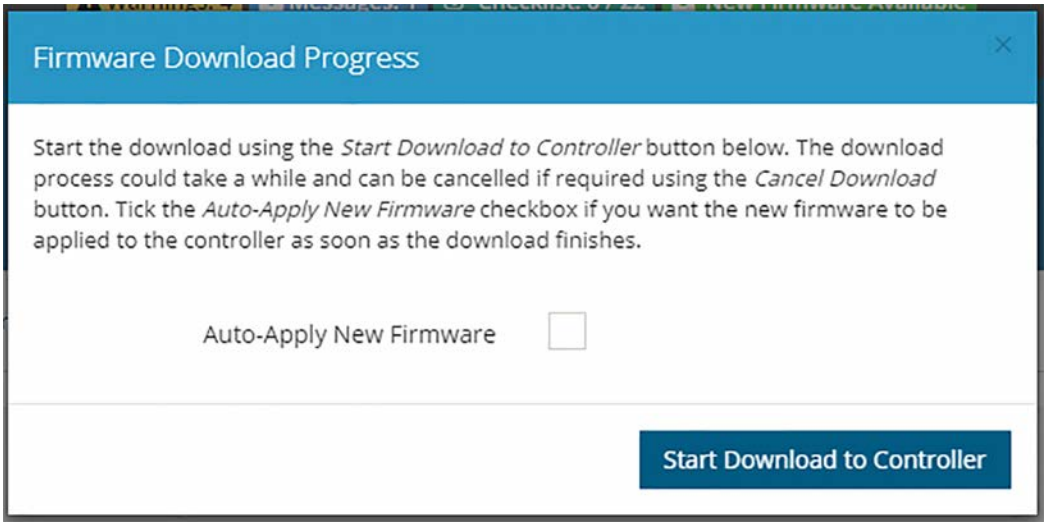
Two new input types have been added that are intended to be used for monitoring and reporting on door states. These are best used with the Forced and Held inputs that the system automatically generates when Reed or Tongue inputs are linked to a door.

- **Door Forced** – When the input is triggered, alarm siren tones are played on internal sirens only, strobes are enabled and a door forced event is sent to the monitoring station. The alarm response will occur regardless of the area's arm state. Used on doors that should only be opened when unlocked, such as after an access request or REX button. Note that doors with free egress (e.g an external door that can be opened from the inside without a REX button or "unlocking" the door) should not be monitored with this input type, as the door will be "forced" during this action.

- **Door Held Open** - When the input is triggered, no sirens or strobes are enabled, but a door held open event is sent to the monitoring station. The event will be sent regardless of the area's arm state. Used as an escalation option when important doors are held open too long. A warning phase can occur with local buzzers to attract attention so that the door can be closed, but if no one is nearby and that phase passes then an event can be sent, allowing the monitoring station to contact someone to ensure the door is closed. Best used with the "Held Open" calculated input that is dynamically created when a door has a reed or tongue input assigned to it.

Auto-apply SkyTunnel Firmware after Download

Updating firmware via SkyTunnel has been made easier by adding an option to auto-apply the firmware once it finishes downloading. If not selected, the firmware can be applied as usual via the *Update Application Software* button when ready.



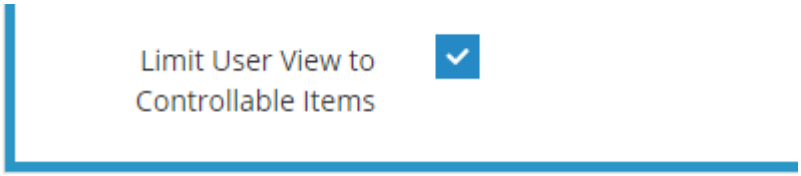
Version 3.0.1 - 20/12/18

Inception release 3.0.1 resolves an issue that primarily affects the Rest API and Control4 integrations.

Issues Resolved

Rest API and Web State Updates

An issue was introduced in Inception release 3.0.0 where users with Web Page Profiles that used the "Limit User View to Controllable Items" option would not be able to see state changes of Inputs and some other items. By default, this would affect users with the "Control and User Admin", "Control Only", "User Admin" and "REST Web API User" profiles.



The intention of this flag was to hide away items that couldn't be controlled; however an unintended change meant that the states of items other than Areas, Doors or Outputs would not be sent.
The results of this issue are that for a user with one of those profiles, they wouldn't be able to see input state or similar pages. Control4 integrations were also affected as they use the Rest API. Areas, outputs and doors could be controlled and their state synced, but input state would not work.
This issue has been resolved in this release.

Version 3.0.0 - 06/12/18

Inception release 3.0.0 includes a new integration API to allow 3rd parties to integrate with the Inception system. The integration allows user management and live state and control of items.

Note: The minimum firmware version for SLAM modules and SIFER readers have been updated, and the firmware files packaged along:

- *SLAM – 3.1.3. Corrected an issue with offline access via Keypad readers. Also resolved an issue with card cache storing last access times in the future.*
- *SIFER– 1.16.0.14. Includes support for the new ECOLITE card format.*

New Features

HTTP REST Integration API

This release includes support for a new HTTP REST-based Integration API. This API allows 3rd party applications to integrate directly with Inception units via a high level interface. A standard Inception user's web credentials are used to authenticate with the API, which also determines the permissions that the API connection has.

Currently, the API offers three main features, however this may be expanded in future:

1. **User Management** – Users can be remotely added and deleted and their details retrieved or updated. This allows 3rd party personnel management systems to integrate seamlessly with the Inception system.
2. **Live Item State** – The state of areas, doors, inputs, outputs and lift floors can be retrieved. The API supports a long polling technique where live, almost instantaneous state change can be retrieved from the system.
3. **Item Contro**l - Areas, doors, inputs, outputs and lift floors can be controlled via the API. Detailed feedback from these control requests can also be retrieved, ensuring the success of the request or providing a detailed reason if it fails.

Dynamic inbuilt help is available on Inception units running this release or above. This can be accessed by opening the Inception web interface and navigating to the "ApiDocExamples" page (e.g modify the URL to be http://[InceptionURL]/ApiDocExamples.

A Postman environment is available with sample requests to exercise the Inception API. The Postman tool can be downloaded from https://www.getpostman.com/, and the latest Postman environment can be downloaded from an Inception unit at the "ApiDocExamples" page mentioned above. Note that this still requires an Inception unit running this firmware or later to use.

More details about the integration can be found on the Inner Range website, including a getting started guide, at the following page: https://www.innerrange.com/Products-Solutions/Inception#Integrations .

Version 3.0.0 - 06/12/18

New Features (cont.)

ECOLITE Card Support (Available Q1 2019)

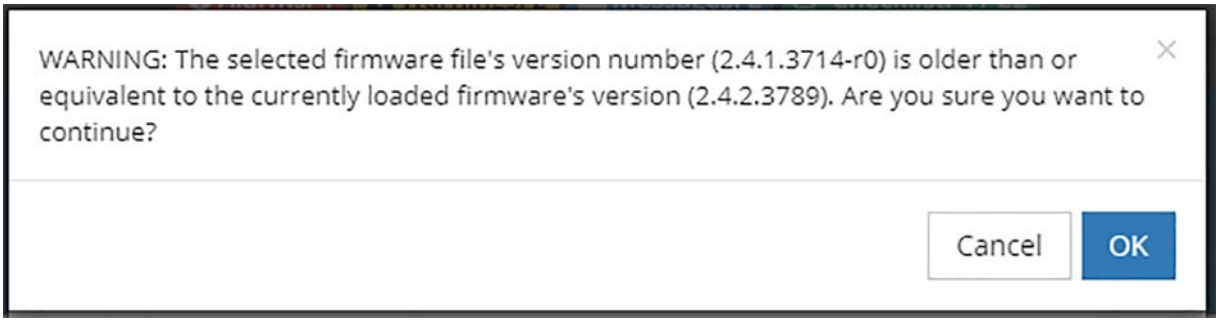
ECOLITE is a range of cards and fobs that Inner Range will be releasing in Q1 2019. These credentials are based on the MIFARE Ultralight EV1 technology and are less secure than the DESFire EV1 technology used in SIFER credentials, but are cheaper option. More details and prices about the ECOLITE cards will be available closer to their release. This Inception and SIFER firmware however includes support for them when they do become available.

ECOLITE

Feature Updates

Controller Firmware Update Validation

When applying a firmware upgrade to an Inception unit, a prompt will be shown if the firmware chosen is older or the same version as what is currently loaded. This can prevent unintended issues from downgrading an Inception, or accidentally applying the same firmware again when intending to upgrade the system.



New Automated Action Triggers

Two new Automated Action Triggers have been added for areas

- **Area in Walk Test Mode** - Automated action responses can now be triggered when an area enters or exits Walk Test Mode.
- **Area Detecting Active Alarm Type** – This is an advanced trigger that activates when alarms of specific types occur in an area. The trigger will activate when the alarm is generated and will deactivate when the alarm restores. The benefit of this trigger is that you don't need separate areas for different alarm types (the main area, the main area (duress), the main area (smoke) etc) and instead, all relevant inputs can be in the same area as intended. This makes area management and control much easier, while still allowing custom automation responses for specific alarm types. Note that this trigger applies only to reported alarms, as opposed to the "Detecting Input Activity" triggers.

Version 3.0.0 - 06/12/18

Feature Updates (cont.)

Single 2k2 EOL Support

Support for the single 2k2 EOL configuration has been added as a built-in option. This EOL configuration is occasionally used in other residential or commercial security system offerings.

[EU Only] Improved WebWayOne / Emizon Support

Support for WebWayOne and Emizon alarm communicators have been improved. In particular, two main changes have been made:

- **Heartbeat Monitoring** – Once a connection is established to the device, Inception will ensure the device is still there by monitoring for heartbeats. If the device stops communicating, the system will respond to the GSM communication error and an event will be logged.
- **Path State Monitoring** – If the device is still online with Inception but indicates that it can't communicate with a monitoring station, Inception will now display this state and log an event.

Issues Resolved

Switch/Button Input Types with Single EOLs

Previously, when using Switch/Button input types (or REX inputs), EOLs could not be used on those inputs so that the open and closed states would become active and inactive. When used in conjunction with a single EOL configuration, these inputs would not work and would always be in the unknown state. In this release, both issues have been resolved.

- For single EOL configurations, an EOL resistor must be used for both detector or switch input types.
- For dual EOL configurations, if EOL resistors are used on a switch/button input, an alarm change will now indicate an active state and sealed will indicate inactive. Tampers in this case will not be monitored; the detector input type should be used if tamper monitoring is necessary.

Version 2.4.1 - 19/09/18

The 2.4.1 release resolves a problem found with the recent addition of Start Time to the user CSV import feature.

Issues Resolved

CSV Import Start Time Issues

Inception release 2.4.0 included the ability to add or update a user's start time via the CSV Import feature, allowing an easy way to manage users in bulk. There was a problem with the release though where the start time wouldn't parse correctly or would use the expiry time instead. This release resolves those issues.

Version 2.4.0 - 13/09/18

The 2.4.0 release of Inception improves the Home installation offering by adding multi-mode area control (Stay / Away / Instant) and support for the Control4 Home Automation system.

Note: Minimum firmware version for the Elite X has been updated, and its firmware files packaged along:

- *EliteX Terminal – 3.0.13. See release notes for more details, but some major changes include resolving some inbuilt SIFER issues, enabling a 12-hour screen inversion to help minimise burn-in and resolving some logged-off clock display issues*

New Features

Control4 Home Automation Support

This release includes support for integration with the Control4 home automation system. Control4 is a smart home platform that brings many of the smart devices in a home together, allowing information and interactions from multiple systems to be coordinated together in one place.

The integration requires a driver plugin for the Control4 system that allows the Inception system to be interacted with. The driver is available on the Inner Range website for now, but once certified can be automatically downloaded from the Control4 online driver database. Some of the key highlights include:

- **Full Area State and Control** – Feedback for entry delay, exit delay, arm warning and area alarms can be shown on Control4 interfaces. Areas can be armed in Away, Stay and Instant modes including prompts and bypass abilities for unsealed inputs.
- **Input State Syncing** – All inputs in Inception can be synced to Control4 with live state changes. These inputs can be simultaneously used for security in Inception and automation in Control4, such as controlling lights when movement is detected or showing the current state of doors and windows.
- **Output Control** – All Inception outputs can be controlled from Control4. These could control any of the physical outputs, or used to trigger custom automation in Inception.
- **Door Control** – In addition to controlling the security features of Inception, the integration allows all doors to also be controlled with state feedback.

The Inception controller implements the Control4 discovery protocol (SDDP) so should be plug and play. Information about who last disarmed an area or accessed a door is also sent to Control4, allowing custom responses like playing a favourite playlist based on who disarmed the system.

For more information about the integration, see the Inception - Integrations section of the Inner Range website here: https://www.innerrange.com/Products-Solutions/Inception#Integrations

Note: Many other automation systems are already supported via the 3rd party automation interface, which allows text strings to be sent bi-directionally over serial or IP. This integration is an explicit integration requiring a driver in Control4.

User Start Time via CSV Import

User CSV Import has been updated to allow user start time to be set via the import. To set a user's start time, the desired date and time should be included in the eigth column of the CSV import. The recommended format for the start date and time is dd/mm/yy hh:mm:ss, however other formats may be accepted. To use a different format, they should be tested with a small CSV first to ensure they are interpreted correctly.

Updating the start time of users is also available with this option. If a value is specified, then the system will enable expiry and set the desired start date and time. If no value is included, similar to the other update options, then no change is made. So if a user was configured to have a start time, they will need to be edited manually to remove it.

Version 2.4.0 - 13/09/18

New Features (cont.)

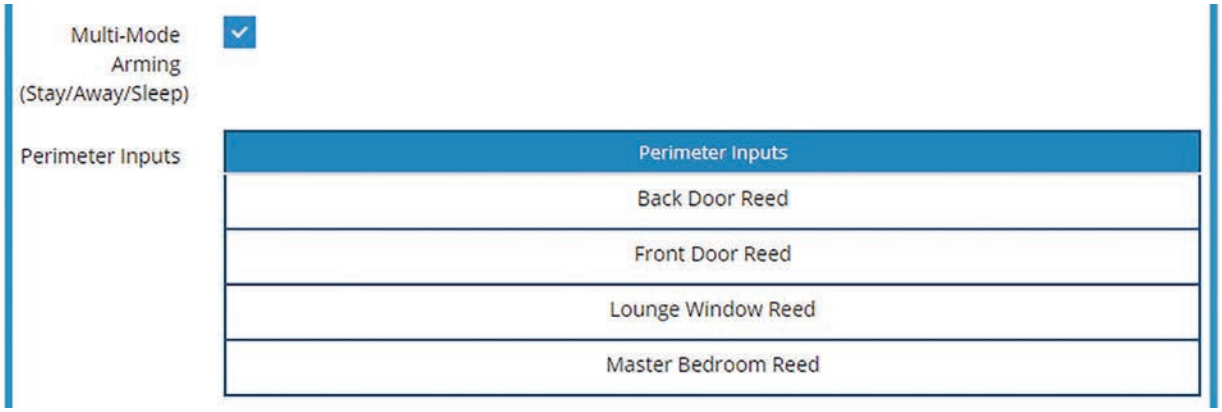
Multi-Mode Area Arming (Away / Stay / Instant)

To help Inception better fit into home installations (especially with the Control4 integration above), areas can now be optionally configured for Multi-Mode Arming. When enabled, the basic “Armed” mode is replaced with “Full (Away) / Home (Stay) / Sleep (Instant)”. These modes are commonly used in home scenarios, where the exterior of the building should be armed while people are inside. This is optional per-area, so a system can be configured with a multi-mode House area, but a standard arm Garage and Workshop for example. Note that these modes only affect Intruder type inputs (Primary, Handover and Instant). Other input types (smoke, duress etc) are monitored regardless of the arm mode.

The arm modes have the following behaviour:

- **Full Area (Away)** - Exactly the same behaviour as the standard Arm mode. The whole area is armed with Exit Delay if required. Intended for use when everyone is leaving the area.
- **Home Mode (Stay)** - Arms the area in Home (Stay) mode. Intended for use when people will remain in the area, securing only the perimeter of the building. No exit delay will activate and only the perimeter intruder inputs are monitored. If a Primary input activates, entry delay will begin (e.g someone opens a door).
- **Sleep Mode (Instant)** - Arms the area in Sleep (Instant) mode. Intended for use when people will remain in the area, but no one is expected to enter or leave. Similar to Home (Stay) mode, no exit delay will activate and only the perimeter inputs are monitored. Unlike Home (Stay) mode though, if any perimeter input activates (including Primary inputs), the alarm will activate immediately. This allows warning if someone breaks into the front door while everyone is asleep for example.

On the **[Configuration > Areas > Edit Areas]** page, in the Inputs section, two new options have been added. If *Multi-Mode Arming (Stay/Away/Sleep)* is enabled, the *Perimeter Inputs* can be specified. Once enabled, the area can be armed in Away, Stay and Sleep modes. Otherwise, any arm requests will only arm the area. This is enabled on a per-area basis.

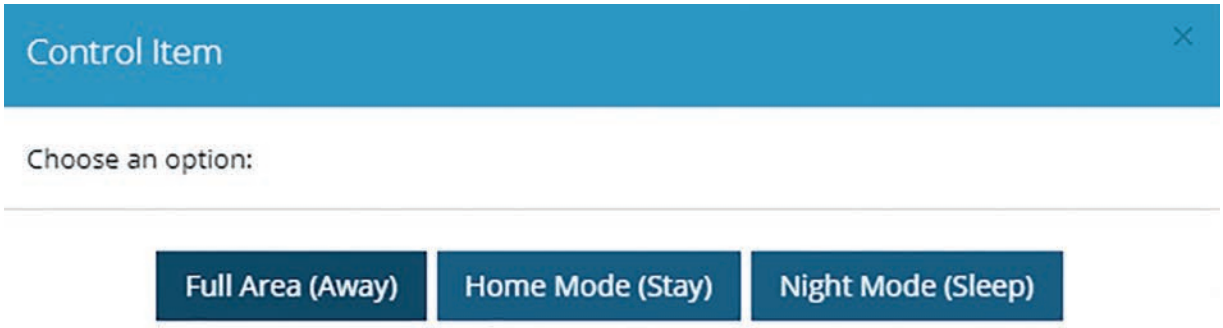


When on the **[Dashboard]** or **[State / Control > Control Areas]** page, the “quick control” button has been updated. For a normal area, quick controlling will arm the area from a disarmed state like normal. For a multi-mode arm area, a dialog will be shown allowing the mode to be selected.

Version 2.4.0 - 13/09/18

New Features (cont.)

Multi-Mode Area Arming (Away / Stay / Instant)



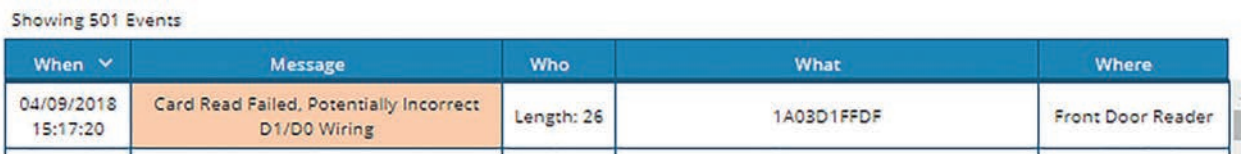
Automated actions can also be configured to trigger on Full (Away), Home (Stay) or Sleep (Instant) modes, and actions can be defined to arm with the new modes.

Feature Updates

Invalid Wiegand Wiring Detection

A common mistake made when wiring Wiegand readers is to reverse the D0 and D1 wires which inverts the card data. The error is not identified until when cards are being assigned to users, where instead of a site-code and card number being shown, raw seemingly random data is displayed. The error could be due to wiring, invalid reader configuration, unsupported formats, poor cards and so on.

With this release, when an unknown card is presented that doesn't match a template, the inverse of the card is checked to see if it is valid. If it is, then instead of the "Card Parity Check Failed" review event that gets logged, a "Potentially Incorrect D1/D0 Wiring" review event is generated.


Showing 501 Events

When	Message	Who	What	Where
04/09/2018 15:17:20	Card Read Failed, Potentially Incorrect D1/D0 Wiring	Length: 26	1A03D1FFDF	Front Door Reader

Issues Resolved

SkyTunnel Connection Reliability

An issue was identified where in rare cases Inception would stop trying to re-establish its SkyTunnel connection when it was lost. This seemed to occur when SkyTunnel was being restarted or updated during maintenance. This release adds extra checking to ensure Inception will keep trying to re-make the connection.

Permanent Input Isolation over Power-cycle

When an input (or hardware module) is permanently isolated, this state should exist until someone manually de-isolates it. This includes over a power-cycle from power loss, firmware update and so on. This originally was the case, however an issue was introduced which prevented Inputs from restoring their permanent isolation state. This issue has now been resolved.

Version 2.3.1 - 12/07/18

The 2.3.1 release of Inception includes Anti-Passback as a new access control feature, as well as some minor bug fixes.

New Features

Anti-Passback

This release adds anti-passback logic into Inception. Anti-passback adds additional validation of user access requests that check whether the user is already in the area they are trying to access. This uses the last known location of the user and is intended to prevent tailgating, moving throughout a building without following access control procedures or passing a card back to allow someone else access to the area.

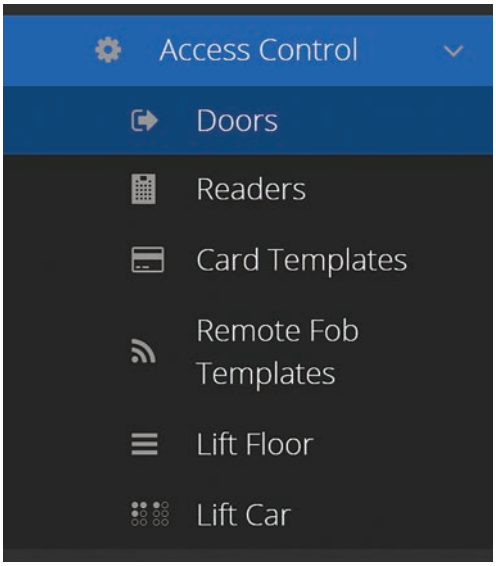
Anti-passback is commonly used on sites whose policies rely on accurate user locations. This could be for time on site reports, accurate muster reports for OH&S compliance and safety, or secure locations in the building. It can also help protect resources such as a carpark, preventing someone driving into the carpark, the access card being passed back and another driver entering with the same credential.

If a user always presents their access credential when accessing doors, even if a colleague is holding the door open for them, then the user's location will always be accurate and they will never be stopped by anti-passback. Violations only occur when the user ends up in a different area than what the system knows. This could be by changing areas without presenting their credential, or presenting their credential at a door but changing their mind and not going through the door for example.

It is recommended that doors with anti-passback logic enabled on them have a credential reader on both sides of the door to allow proper location updating.

Anti-Passback - Configuration

Configuration for this feature is available on a per-door basis, on the **[Configuration > Access Control > Doors]** page. Each door can individually have anti-passback enabled on it. Optionally, a time period can also be specified so the anti-passback restrictions only apply at certain times of the day. This can allow the anti-passback rules to be enforced during the day while others are present to forgive violations, but not be applied at night when a user could become locked in.



Version 2.3.1 - 12/07/18

New Features (cont.)

Anti-Passback – Violations

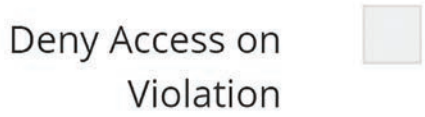
By default, anti-passback logic only checks that the user is not currently in the area they are trying to access. This can be extended with the *Also Verify User Exit Area* option which if enabled, will also check that the user is located in the area they are exiting from.

This allows for more advanced anti-passback logic, ensuring that users always use their access credentials to move around the building. Site security is improved with this option as a duplicated card will not work if the real owner is already on site. Similarly, access to the site through correct entry and exit points can be enforced as internal door access would not work if the users current location is outside.

Anti-Passback – Violation Response

When an anti-passback violation occurs, a review event will be automatically logged, a system message (a blue message on the System Overview page requiring acknowledgement) will be created and optionally notifications to users can be sent.

The *Deny Access on Violation* option then determines if the user is denied access through the door or not due to the violation.

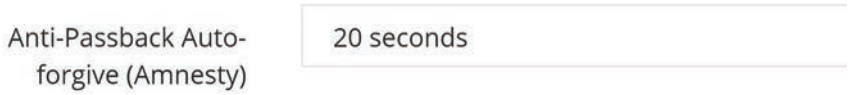


Allowing access may be used on sites where anti-passback is being introduced or where the anti-passback rules shouldn't delay users or affect their productivity. An administrator could, for example, follow up the violation at a later date.

Otherwise, the user will be denied access if they violate anti-passback and they will need to be granted forgiveness or amnesty by an administrator, or somehow move to the location last known by the system.

Anti-Passback – Violation Forgiveness / Exemption

If forgiveness is granted to a user, they will be given an exemption which is a free pass that prevents an anti-passback violation. The purpose of an exemption is to help the user correct their location in the system, so a successful location change through any door will automatically use up the exemption.

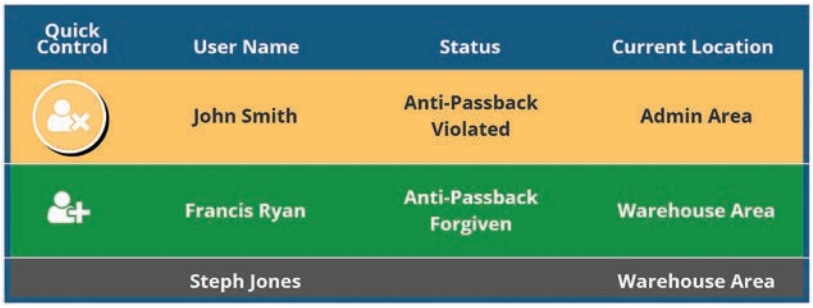


Version 2.3.1 - 12/07/18

New Features (cont.)

Anti-Passback – Violation Forgiveness / Exemption

Forgiveness can be automatically given by the system after a violation occurs, configured on a per-door basis. This is only available if the *Deny Access on Violation* option is enabled for that door. Configuring a short time, like 20 seconds, allows annoyance for the user who caused the violation when they are stopped from accessing the door, without being too inconvenient like having to report to reception or get in contact with someone. Alternatively, longer durations like minutes to hours could be chosen to ensure a violation is forgiven if it remains for too long. An example could be overnight, where the user violated anti-passback when leaving the building. A colleague may have let them out but the violation remains. With long auto forgiveness, this violation will be cleared overnight and the user will be able to access the building the next morning.



The **[State / Control > View Users]** page can also be used to grant forgiveness. This page shows all users and their current location, as well as any users with an anti-passback violations or forgiveness. A user with a violation can be easily forgiven with the quick control button. Alternatively, the Control All button in the toolbox at the top of the page can either forgive all users, or all users with a current violation.

Finally, automated actions can be used to forgive a violation. Similar to the view users page, forgiveness can be given to all users in the system, or all users with a current violation. This could allow a simple button to be added at reception for example that if pressed, would automatically forgive violations. This removes the need for a user to log into the web interface, navigate to the view users page and forgive the violations there.

Issues Resolved

T4000 Reconnection Improvement

The T4000 reconnection logic has been updated to improve the speed of reconnection and prevent alarms being reported unnecessarily. Previously, if connection was lost (heartbeats are sent once per second, if one of these are missed the connection breaks), it would take a minute or so to reconnect and the T4000 would report the disconnection. Inception will now retry the connection several times to restore the link within a few seconds and prevent the unnecessary reporting.

Connection Data Framing

An issue was introduced where the 3rd Party Automation Interface Connections were not framing packets correctly. This primarily affected serial interfaces as they rely on data framing to detect when packets start and end. TCP interfaces on the other hand are generally already framed thanks to the TCP layer. The review events that are logged when discarding data outside of a frame has also been fixed and will now show the actual data instead of “System.Byte[]”

Version 2.3.0 - 07/06/18

Inception release 2.3.0 introduces the ability to translate the Inception web interface and LCD terminals. Two new Time on Site reports have been added, and scheduled tasks can now copy to a network share.

New Features

Inception Translation / Localization

With this release, the Inception web interface and LCD terminal interface can now be translated into other languages. No languages are currently packaged into the controller, however a tool and functionality has been created that allows personalized translations to be made and imported into an Inception. Any translations that are made do not need a special firmware release to be used; they are instead uploaded directly to the Inception web interface.

A basic workflow to translate Inception would involve:

- Downloading a language template from the Inception web interface that includes information about all of the translatable English text in Inception.
- The template is then imported into a new translation tool that can be downloaded from the Inner Range website (web link below).
- Each piece of text is then translated, optionally using the Google Translator Toolkit.
- Once validated, a language pack can be created and imported into an Inception controller.

The same language pack can be used on many Inception controllers and as new firmware releases come out the language pack can be updated to include the new text.

Several documents that explain the process in more detail and the translation tool are available on the Inner Range website in the Technicians Downloads section.
See here for more information: http://www.innerrange.com/InceptionTranslations

Time on Site Reports

Two new reports have been added to Inception, which are two different types of Time on Site reports. Each report is intended to show the amount of time each user spent on site, with the different reports calculating this in different ways, depending on the site requirements. Each report will be generated based on the *Door Access Granted for User* review events.

- **Read In, Read Out** – This type of report is used when there are fixed access points to the site and there is a strict Badge-in, Badge-out policy on site. In this case, users must always present their card or PIN number at specific readers when arriving on site and must present their card or PIN at different specific readers when leaving. The report is generated by matching an access event on a read in reader with an access event on a read and is a more accurate representation of how long a user was on site for. The other mode does not support night shift well (shifts spanning midnight), so this pattern must be used for those users. This report uses an update to the access granted review event, so will only work with access events after this release has been applied.

- **First Badge In, Last Badge Out** – This report will summarize all access events by a user across a day, remembering only the first and last access event that day. The time on site is then the difference between those two events. This option is more flexible than the Read In, Read Out report as any doors on the site can be included, regardless of direction through the door. It is less accurate however, as a user could leave site in the middle of the day for some time without being recorded. This report is broken up into days, with each new day starting at midnight, so if some users work night-shift then the report could be incorrect for them.

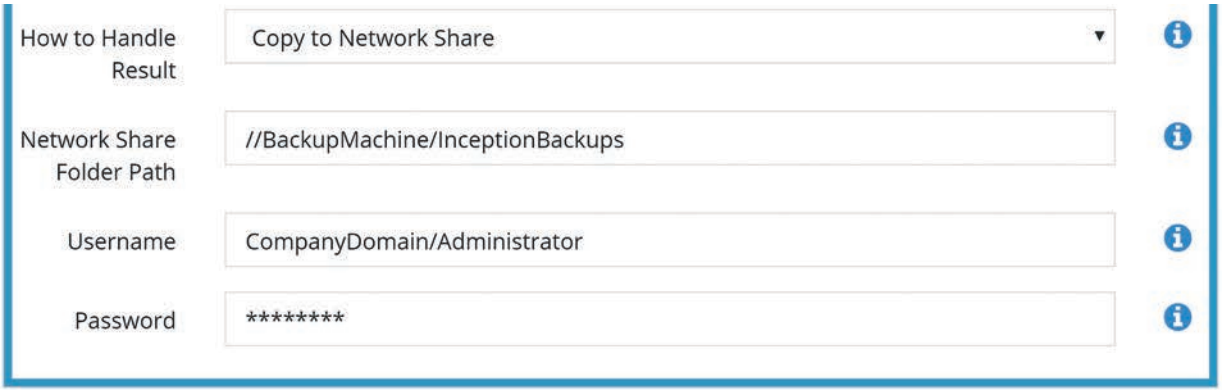
Version 2.3.0 - 07/06/18

Feature Updates

Scheduled Task Copy to Network Share

The Scheduled Task feature introduced in version 2.2.0 has been updated to include the ability to copy the output file to a network share. This allows, for example, regular database backups to be taken that are automatically copied to a shared network folder.

To copy the file, Inception requires the network share location to copy the file to and a username and password to authenticate with.



Alarm Commissioning Report

The Alarm Commissioning Report, available from the **[Configuration > General > Alarm Reporting]** page toolbox, has been updated to include the *Input Event Reporting* area option added in release 2.2.1. This means that if an area will not report input alarms, or only reports non-intruder alarms, then the commissioning report will exclude these events from the report.

The report has also been updated to include the Manual and Periodic test report events. This report is intended to include all possible alarms that can be reported based on the system configuration, so these two events (manual events always, periodic events only if configured) should also be included.

Area Pulse Count with Entry Delay

Previously, area pulse counting did not count the primary or handover input activations while entry delay was active. This meant that even if several inputs were activated along the entry path, when the first instant alarm was activated that would only be counted as the first “hit”. Several other inputs would need to be activated before the pulse counting limit is reached to sound sirens and report the alarm events which would allow an intruder to get much further into the building before a response occurred.

The entry input activations are now counted towards the pulse count limit, however they cannot be the activation that causes the area alarm. This means that activations in the area entry path could cause the pulse count to be much higher than the limit and that a subsequent instant activation is still required to trigger the area alarm.

Other entry delay logic will still apply where alarms and sirens will activate if entry delay ends and the area is not disarmed. This will occur regardless of the pulse count options.

Version 2.3.0 - 07/06/18

Issues Resolved

Improved SIFER Feedback via SLAMs

The SIFER responses for readers connected to SLAMs were inconsistent with those connected directly to the Inception controller. In response to a card read, the SIFER LED flashing would also be unclear if the reader was also showing area state. This has been improved with this release, making the readers more consistent with those directly connected to the controller.

SIFERs Unresponsive on System Time Change

An issue has been resolved where if the system time of Inception was set into the past by a significant amount, then the SIFER readers connected to the controller would become unresponsive. A controller power cycle was required to fix this, or waiting until the system time eventually reached the original time again.

IRFast Reporting IDs

Inception supports the Concept version of IRFast alarm format reporting, however there are several module state alarms that didn't fit into the Concept IRFast format and were instead reported as the same "Unknown" point. This would include states like Power Supply Failure on zone expanders or SLAMs, as well as AC Fail, Battery Test, Wire Short and so on for SLAM modules. These have been changed to report as individual system input points. While still unknown by default to a monitoring station, they can now be mapped and uniquely identified.

Version 2.2.2 - 22/05/18

Inception release 2.2.2 addresses an issue experienced with SIFER readers attached to SLAMS that occasionally causes doors to remain locked on a valid card badge.

Feature Updates

Default Changed for Repeat Alarm Event Limit (Swinger Shutdown)

The default value for the swinger shutdown feature, introduced in Inception release 2.0.0, has been updated from zero to ten. The swinger shutdown feature is designed to limit the number of repeated input activations or module health issues that are sent to a monitoring station.

The previous default of zero disables the limit and allows all alarms to be sent through. This change ensures that the feature is enabled by default for all systems so that if something goes wrong, the monitoring station does not receive endless alarm events until the problem is fixed. In the case of an actual intruder event however, by default up to ten alarm events will still be sent to indicate the issue, followed by a swinger shutdown event.

For existing systems, when this firmware is applied, the swinger shutdown limit will be changed to ten if it is currently zero. The value won't change if it is already configured though. If you don't want this feature enabled, set the value back to zero after the firmware update is applied.

Issues Resolved

SLAM Door Control Issues via SIFER Readers

An issue was reported where when presenting cards or fobs to SIFER readers connected to SLAMs, occasionally the door would not unlock even if access granted feedback was played. The issue was intermittent but when it occurred, the user would have to wait for at least 4 seconds before trying their card again. Repeat card swipes to try and unlock the door within the 4 seconds would be considered part of a "3-badge action" which caused further confusion.

The issue is resolved with this release.

Version 2.2.1 - 10/05/18

Inception release 2.2.1 contains several issue fixes and some minor feature updates. One issue could affect NTP time syncing while the other can appear when the system time is changed.

New Features

Disabling Area Alarm Reporting

A new option has been added to area programming that can be used to prevent the reporting of input events if required. This option only affects the reporting of input events, any siren and other area responses will still occur.

The primary purpose for this option is to allow arming of an area while users will be nearby, securing part of a building or home while other users are present. In an intruder event, sirens will sound to attract attention and allow investigation, but the monitoring station will not be notified and so no alarm procedure needs to be followed.

Three options are available:

- **Report All Alarms -** All input alarms are reported, this is the default option and is normal behaviour.
- **Report Non-Intruder Alarms -** Intruder alarm events (generated by "Instant", "Primary" and "Handover" input types) will not be sent. All other event types (including tamper events from intruder inputs) such as emergency, smoke, duress and environmental input alarms will still be reported.
- **Don't Report -** No input alarm events will be reported. Siren responses will still occur depending on the input type.

Feature Updates

Pulse Counting Review

If pulse counting is enabled for an area, any input activations that count towards the pulse count will now be logged as a Review Event. The event will include the input that caused the pulse count to increase, the current pulse count and the area that the activation occurred in.

03/05/2018 10:39:46	Input Event Created	Admin PIR 1	Alarm	Admin Area
03/05/2018 10:39:46	Sirens Activated in Area			Admin Area
03/05/2018 10:39:46	Input Pulse Detected	Admin PIR 1	Count = 2	Admin Area
03/05/2018 10:39:37	Input Pulse Detected	Admin PIR 1	Count = 1	Admin Area
03/05/2018 10:39:31	Area Armed by User	Installer	Admin Area	

Version 2.2.1 - 10/05/18

Issues Resolved

NTP Sync Error

An issue was identified where in some circumstances, the NTP syncing feature of Inception would stop working and require the unit to be restarted to recover. Time for Inception would typically be synced from the local DHCP server it is connected to, one of the default NTP internet addresses that are provided or a server that has been manually configured. In some cases, an error could occur during the syncing of time, preventing the Inception system from receiving future updates and allowing the system time to slowly drift. This issue has been resolved.

Timer Issue When System Time Changes

An issue was introduced with release 2.1.0 where timers within the system incorrectly relied on the system time. While typically not an issue, if the system time was adjusted backwards it could cause these timers to behave incorrectly, taking longer than they should have to activate. It would be rare for someone to run into this issue, but it has been resolved.

Incorrect Events in "Send All Possible Alarms" Feature

When using the *Send All Possible Alarms* option on the **[Configuration > General > Alarm Reporting]** page, all alarms that the system could send based on the configuration are queued to be reported. Several events were reported incorrectly though, namely the System Reset alarm and restore events and the Communications Failure alarm and restore events for T4000 and SkyTunnel reporting paths. These events would report correctly when generated normally, this issue only affects the *Send All Possible Alarms* feature and has been addressed.

"Terminal Timeout" on Terminal Door Access

If using an Elite or EliteX terminal to access a door, requesting access would show the "Door Access Requested" message, followed by "Terminal Timeout". No functionality has been changed, but the "Terminal Timeout" message is no longer displayed.

Version 2.2.0 - 12/4/18

Inception release 2.2.0 includes several new features and feature updates, the main one being Scheduled Tasks. In addition, a one-click muster report shortcut, several new reports types and some additional user expiry options were added.

NOTE: SLAM firmware 3.1.1 has been included in this release. It is recommended that SLAM expanders are updated as this release resolves an issue with SIFER readers appearing unresponsive and reduces the delay for REX Button presses.

New Features

Scheduled Tasks

This release includes a new Scheduled Task feature which allows actions that produce a file to run on a scheduled basis. The file that is created can then be attached as an email attachment and sent to multiple users, or copied to a USB drive connected to the Inception controller. Many scheduled tasks can be created with their own schedules and they can also be manually triggered or triggered by an automated action if required.

Scheduled Tasks allow regular database backups to be taken, ensuring a recent backup is always available if the controller is damaged or accidental programming changes are made. Weekly reports can be sent to various users that include access history, inactivity, area control or users who will soon expire for example. Reports can also be triggered from automated actions, such as a muster report in response to an emergency event.

Configuration of the Scheduled Tasks is available from the **[Configuration > Scheduled Tasks]** page.

Scheduled Tasks: Schedule Frequency

Three options are available when configuring the schedule frequency, None, Basic or Advanced.

- **None:** This option will cause the task to not run on a scheduled basis. The task would instead either be run manually via the **[State / Control > Control Scheduled Task]** page, or set to run in response to an automated action.
- **Basic:** Allows simple scheduling to be used, running the task daily, weekly, every two weeks or every four weeks. A day of the week can be selected if required and the time of day specified.
- **Advanced:** Advanced scheduling utilizes the Calendar items of Inception (configured via the **[Configuration > Scheduling > Calendars]** page. Multiple calendars can be chosen with a time of day specified, with the days that the scheduled task would run being provided by the calendar.

Scheduled Tasks: Actions to Perform

Currently, two actions are included that can be scheduled to run:

- **Backup Database:** This option will take a backup of the full database at the time of running, producing a file that can be restored at a future date if required.
- **Create Report:** Any of the available reports can be run on a schedule. These are the same reports that are available on the **[System > Reports]** page and can be pre-configured with the desired filters. Reports that include a timeframe filter are dynamic (like the last 2 weeks), with the timeframe applied each time the report is run.

Version 2.2.0 - 12/4/18

New Features (cont.)

Scheduled Task: How to Handle the Result

Once a task has been run, a file is created (currently either a database backup or a report). Two options exist on what to do with the file:

- **Send as Email Attachment:** The file is attached to an email that is sent to one or more users. This requires that an Email Server is configured on the **[Configuration > General > System]** page.
- **Copy to Attached USB Drive:** If a USB drive is connected to the Inception controller, the file will be copied onto it. This drive could also be connected via a Hub if multiple USB devices are required.

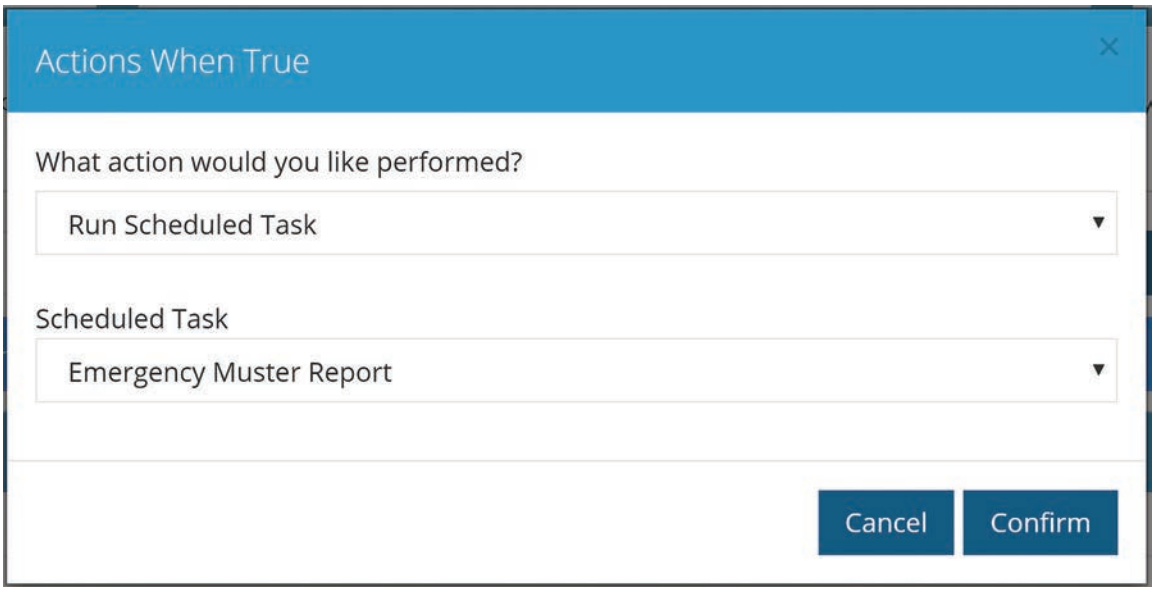
Scheduled Tasks: Other Options for Triggering Tasks

In addition to scheduling the task to run, the task can be triggered manually or by an automated action. When on the Scheduled Task configuration page, a task can be run manually by pressing the *Control* button in the toolbox at the top of the page.

The state of all scheduled tasks can also be seen from the **[State / Control > Control Scheduled Tasks]** page. The tasks can be controlled from here too and show when they were last run, whether their last run was successful and when they are next scheduled to run.

Scheduled Task Name	Status	Advanced	Next Scheduled Run Time	Last Run Details
Database Backup	Last Run Successful		15/04/2018 08:00:00	Completed successfully at 10/04/2018 13:40:45
Access Report	Last Run Failed		16/04/2018 08:00:00	Failed at 10/04/2018 13:17:00

Tasks can also be triggered by automated actions. In this case, running a scheduled task can be configured as an action response when an automated action triggers. This could allow, for example, a muster report to be emailed to multiple users as soon as an emergency event is detected.

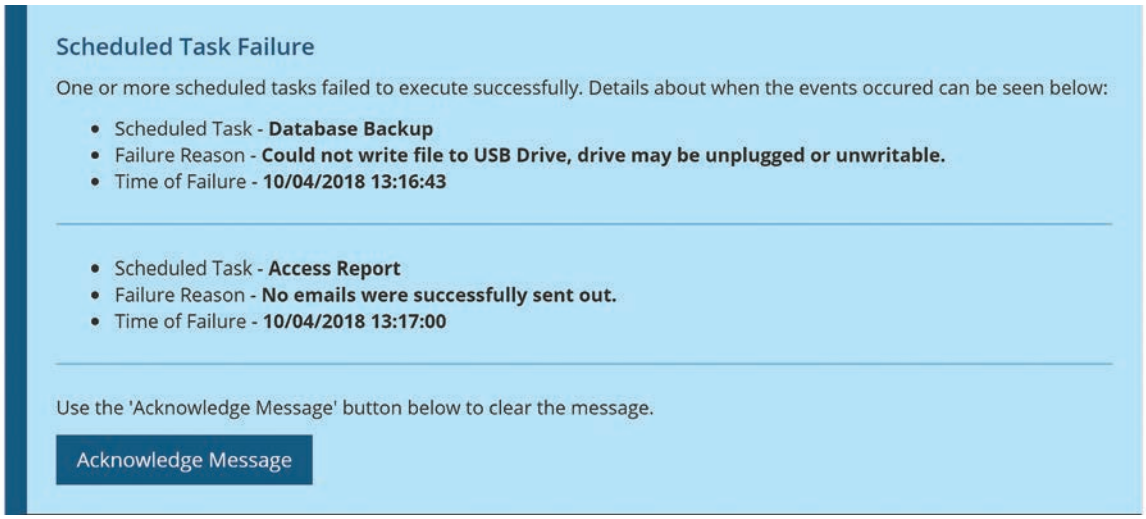


Version 2.2.0 - 12/4/18

New Features (cont.)

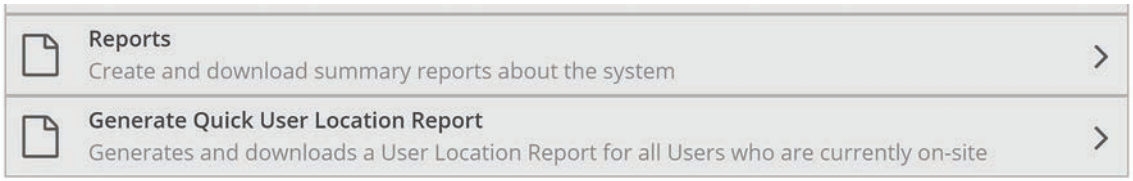
Scheduled Tasks: Task Failed Notification

In the event that a task is unable to run, a system message will be created, with a Messages indicator shown at the top of the web interface. Navigating to the **[System > System Overview]** page will show the message which may help in diagnosing why a task did not run. While a database backup task to a USB drive may have been running correctly for months, if that USB drive fills up and can't be copied to then this ensures that the issue is highlighted.



One-Click Muster Report

A new *Administration Shortcut* has been added on the **[Dashboard]** page that allows a User Location (Muster) report to be downloaded. This removes the need to navigate to the reports page, change the report type, update the filter to exclude users who are not in an area and then download the report. If the report is being used as part of a muster procedure in an emergency, these steps can be excessive, so the one-click shortcut has been added.

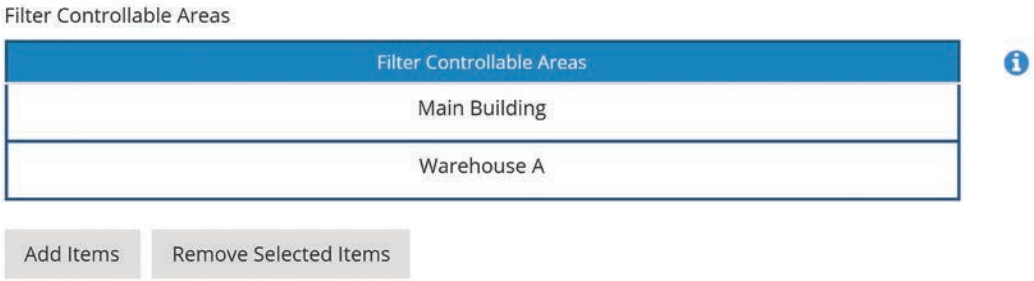


Version 2.2.0 - 12/4/18

New Features (cont.)

LCD Terminal Area Filter

During the Hardware Wizard for an LCD Terminal (Elite or EliteX), a new option has been added to the **Associations** step of the wizard. This allows an area filter to be given to the terminal, limiting what areas that terminal can control. If no filter is provided, all areas that the user can control will be visible on the terminal. On a large site with many areas, it helps to narrow down the area options that a user sees to just those located near the terminal. This can also ensure that if a user should visit each individual building to secure the site, that they can't just arm all areas from a single terminal.



Note that if an area filter is desired and an area is associated with the terminal (via *Associated Area* option), that area must appear in the *Filter Controllable Areas* list. If this is not the case, an error prompt will be shown.

User Details Report

A new User Details report has been added as an option to the **[System > Reports]** page. Unlike the user permissions summary report, which focuses on user permissions, this report includes the other information about a user. Per-user, a table will show their notes, LCD terminal profile, web login profile, email address, expiry information, assigned cards and assigned remote fobs.

The table generated for the user is dynamic, only including information if the user has that information. For example, a notes entry will only be included for a user if they actually have notes.

Area Control Report

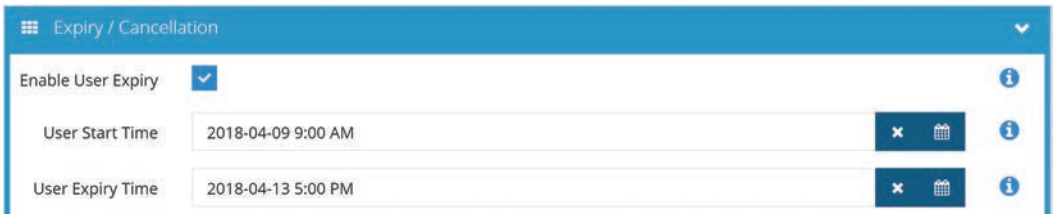
A new Area Control report has also been added as an option to the **[System > Reports]** page. This report includes how the areas in the system have been armed and disarmed recently and details when and by whom they were controlled. The report can include all area events or be filtered to include only specific areas or users, arm or disarm events, user or system control events, successful or failed events. The report covers a configurable period of time from when the report was run.

Version 2.2.0 - 12/4/18

New Features (cont.)

User Start Time (Valid From)

To help manage temporary users at the site, such as contractors and visitors, user expiry options have been expanded to include a *User Start Time* option (or "Valid From" time). This allows users to be programmed in advance with credentials allocated and standard permissions, but the user will not work until the programmed start time. The start time and expiry time are optional, so an expiry can be programmed with no start time and vice-versa.

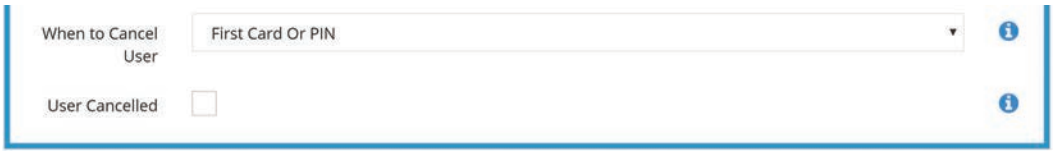


User Cancellation on First Card/PIN

A user cancellation on first credential use feature has been added, where the user will automatically be cancelled once their PIN or Card has been used. This feature is often used where single use credentials are given to visitors to access the site which prevents unlimited access in case the card is stolen.

User expiry times could also be used to manage visitor cards, allowing access for the day only. This option though allows multiple cards to be pre-created and handed out as required, without needing to log into the Inception system and update the expiry time.

Once a credential has been used and the user cancelled, the *User Cancelled* checkbox will be automatically ticked. To reset the user, the checkbox can be un-ticked and the user saved.



Version 2.2.0 - 12/4/18

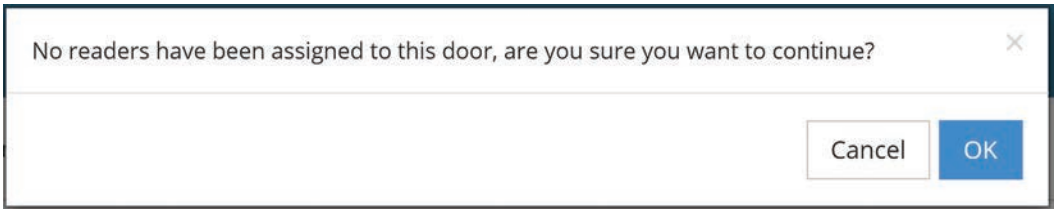
Feature Updates

Hardware Wizard Door Validation

When configuring access control modules in the Hardware Wizard (a SLAM, or the Controller in Access mode), it was easy to forget to program readers to a door as the wizard was stepped through. The result was that even once permission was given to the door, a user couldn't access it and it a visit to the Review Events page was required to diagnose the problem.

When	Message	Who	What	Where
10/04/2018 09:47:30	Door Access Failed, No Door Assigned	Installer		SIFER Reader 740

With this release, a prompt will be shown during the hardware wizard if you are saving a door with no readers assigned, when there are readers available on the module. This should help reduce confusion and make the hardware enrolment process smoother.



Single 3k3 EOL

A new EOL resistance configuration has been included in the system by default, the single 3k3 EOL. This resistance configuration was used by several other products, so if upgrading from one of those systems to Inception, this EOL can save a significant amount of time in rewiring. This EOL configuration treats a 3k3 resistance across the input as Sealed, with any other resistance indicating alarm.

There are also several other EOL configurations pre-packaged into the Inception unit. If the resistance scheme required for the site is not available, Inner Range support may be able to provide an upgrade file that includes a custom EOL scheme.

Issues Resolved

Controller Battery Test after Database Restore

When a database backup was restored to the Inception controller, the system could run into a start-up issue if a battery was configured for the controller and battery testing was enabled. As the next scheduled test time was stored in the database (to persist over a power cycle), the system would see the old test time from the backup and would try to run the test before the system was ready. This issue has been corrected.

Module Failure Time Inconsistency

An issue has been addressed where when a module loses its connection with the Inception controller, a module lost event may not be reported to the monitoring station. In addition, the Module Failure delay feature has been updated to always delay for the configured module failure time when a module is detected to be offline. Previously, the delay may not be used depending on how the module offline event was detected, causing confusion.

Version 2.1.0 - 28/2/18

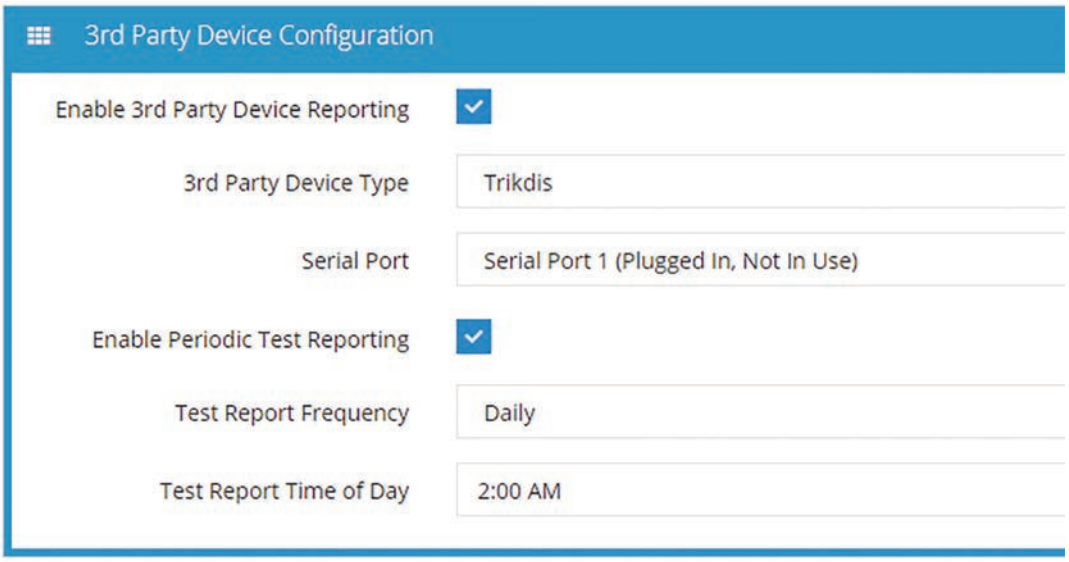
Inception release 2.1.0 includes some improvements to user management with User CSV Export. Support for the Trikdis alarm communicator (European markets only) has also been added along with several Elite Terminal and RF Expander updates.

New Features

Trikdis G16 Alarm Communicator

Note: Applies only to European markets.

Support for the Trikdis G16 alarm communicator has been included in this release. The communicator allows alarms from the Inception controller to be sent with the Contact ID format via the Trikdis communicator.
Connecting the Trikdis unit to the Inception controller requires a USB to TTL cable, such as the Inception to T4000 interface cable. If this cable is used, in addition to powering the unit from one of Inception's VOUT ports, the black wire should connect to the –DC port, the green wire to the CLK port and the white wire to the DATA port.
The reporting path can be enabled and configured from the **[Configuration > General > Alarm Reporting]** page of the Inception web interface. A 3rd Party Device Configuration section has been added to the page where the device type, serial port and periodic test reporting can be configured. See the Trikdis manual for information on configuring the actual Trikdis unit.



Timed Output Control via Elite Terminal

The Output Control menu on the Elite Terminal (**[MENU], [3]**, **[1]**), has been updated to optionally allow timed control. After scrolling and finding the output to control, the **[<]** and **[>]** keys can be pressed to enable timed control. Pressing **[<]** will change to minutes control mode or **[>]** will change to seconds control mode. The duration can be changed with the numeric keypad and then pressing **[ON]** or **[OFF]** will control the output.

```
Admin Lighting ^v
For: 030 Mins
```

Version 2.1.0 - 28/2/18

New Features (cont.)

User Expiry via CSV Import

User CSV Import has been updated to allow user expiry to be set via the import. To set a user's expiry, the desired date and time should be included in the seventh column of the CSV import. The recommended format for the expiry date and time is dd/mm/yy hh:mm:ss, however other formats may be accepted. To use a different format, they should be tested with a small CSV first to ensure they are interpreted correctly.
Updating the expiry of users is also available with this option. If a value is specified, then the system will enable expiry and set the desired date and time. If no value is included, similar to the other update options, then no change is made. So if a user was configured to expire, they will need to be edited manually to remove it.

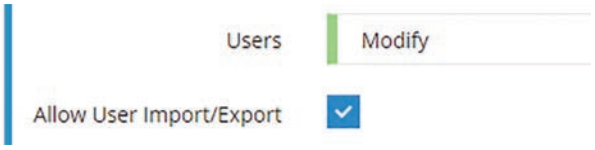
User CSV Export

A new feature has been added to the **[Configuration > Users > Manage Users]** page that allows user details to be downloaded in a CSV format. The format of the CSV matches up with the format required for CSV import feature, which allows it to be used with the Update via CSV feature. This means the exported CSV to be updated and then re-imported to the system, making limited changes to the users.

The export will contain the following information:

- Name
- Permission Group – Name of the first permission group this user has permission to.
- PIN – Never filled in. Only included to line up with the CSV Import format
- Card Number – The number of the first card that the user has
- Notes
- Email Address
- Expiry Date – Only included if the user is configured to expire
-

To help restrict this feature, a new option has been added to web page profiles called Allow User Import/Export. This is only available if the profile allows modification of users. This option is automatically enabled for the Installer and System Administrator web profiles.



Version 2.1.0 - 28/2/18

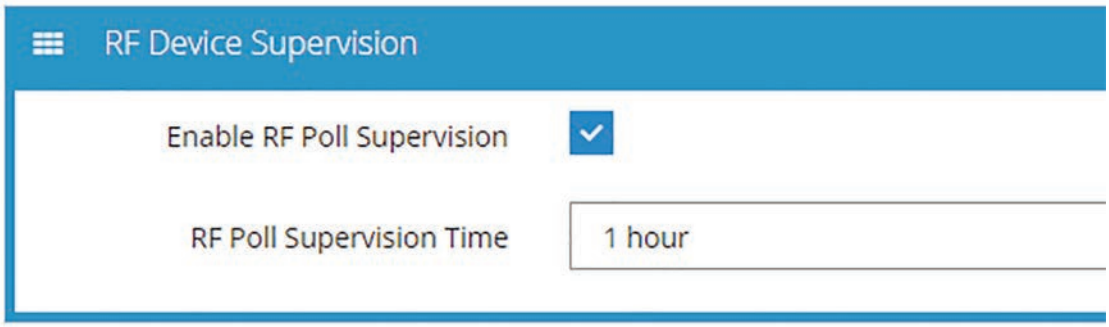
Feature Updates

Live Entity States via Elite Terminal

When viewing the control menus (Areas, Doors, Inputs, Outputs) on the Elite Terminal, the state of those items would not dynamically update and would only change after scrolling. This has now been updated to show live state of the currently focused item.

Optional RF Poll Supervision

In certain cases, monitoring for missed polls of the RF devices on site is undesirable. Each time a device fails to poll in, a poll failure event is raised and communicated to the monitoring station. If occasionally these poll failures are unavoidable, the result is extra work as the monitoring station works through their procedures. For these cases, both the Inovonics and Paradox RF expanders can be configured to disable RF poll supervision. This option can be configured when editing the expander in the Hardware Wizard.



Paradox RF Poll Supervision Time

In Inception release 1.4.1, a configurable RF poll supervision time was added to the Inovonics RF expander. This same option has now been added to the Paradox RF expander too. The poll time determines the amount of time that is allowed to pass before an RF input device is considered to be missing. The time should be set to a value that is several times longer than the default poll times of the devices so that multiple missed polls are needed before raising a poll failed state. This option is available when editing the RF expander via the Hardware Wizard.

Version 2.1.0 - 28/2/18

Issues Resolved

Module Poll Time Options

LAN module poll times should have been limited to between five seconds and four minutes, however those limits were never in place. This introduced an issue where a module's poll time could be set to zero seconds. While most of the supported modules realised this was an unrealistic time, the Concept Paradox RF expander didn't and would instead try to constantly poll in. These limits have now been enforced and any poll times outside of this window have been automatically adjusted.

Entry Delay Lockup

A lockup issue was discovered which could occur as an area entry delay was expiring. The issue could only happen if entry delay was started on an armed area, but the area was not disarmed. At the exact time that entry delay expired, if the primary input for the area re-activated, then this issue could occur. The odds of this issue being experienced on site are very low, as the window of time that the primary input must activate is small as once entry delay starts then the area would normally be disarmed before entry delay expires. Regardless, this issue has been resolved.

Area Walk Test Page

An issue was introduced with Inception release 2.0.2 where the input lists on the Area Walk Test web page would not automatically update. During a walk test, the inputs should automatically move to the "passed" list as they are tested, however this was not occurring. Note that the issue related to updating the web interface itself, the actual test was being performed properly and the test would pass once all inputs were tested.

Module Offline during Firmware Update

When updating the firmware of many modules at once (or the SIFER readers on many modules), it was found that if one of those modules went offline during the update process then the whole update process would fail. This has been improved so that even if a module goes offline, the rest of the modules will succeed and the update only has to be repeated on the offline module once it reconnects.

Version 2.0.2 - 07/12/17

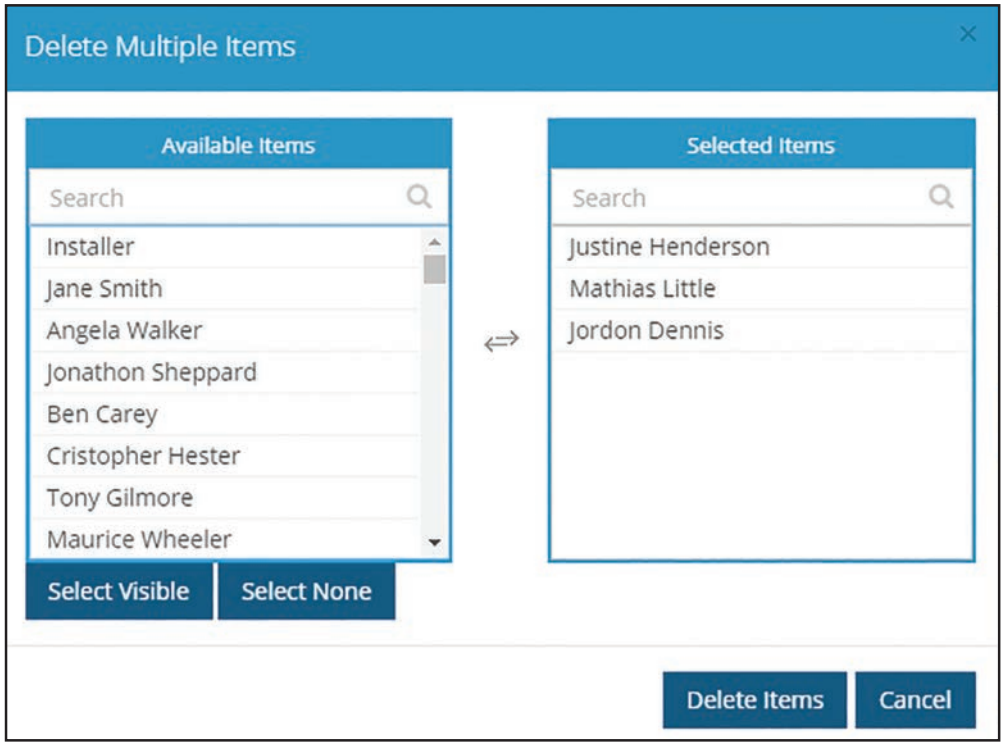
The 2.0.2 release of Inception includes some upgrades to report generation and some other minor upgrades, such as a bulk item delete option.

New Features

Bulk Item Delete

With the recent capacity increases of Inception, the scale of Inception installations can now be much larger (up to 10,000 users for example). Previously, deleting items needed to be done one at a time; the item would need to be selected and loaded, then Delete pressed, then a confirm delete message would need to be acknowledged. This process was fine when there were only a few items to delete, but even though the delete confirmation step could be skipped, deleting a large number of items would be tedious. With this release, a new Bulk Item Delete option has been added.

In order to not fill up the toolbox unnecessarily, this option only appears when there are 25 or more items on the page. Once selected, a dialog will be shown that lists all of the items, which can then be individually selected. These lists can be searched and filtered to find specific items to speed up the process. In addition, the Select Visible button can be pressed to move all unfiltered items across to the delete column.



This option allows a large number of items to be quickly selected out of a long list for deletion. Alternatively, most items can be deleted (e.g after a user CSV import with incorrect data) by selecting all visible items and then moving back the items you don't want to delete (e.g your own user).

Version 2.0.2 - 07/12/17

Feature Updates

HTML and Multi-PDF Report Formats

Two new report formats have been added to Inception, which are configurable when the report is run. These are the HTML report format and the Multi-PDF report format.

- **HTML** – The HTML format is a single file report that is ideal for large data sets. The output file will be a single HTML file that includes all of the desired information and can be as large as you like.
- **Multi-PDF (zipped)** – If the PDF format is still desired that involves a large amount of data, the multi-PDF option can be used. This will split the report into multiple smaller PDFs, generating as many PDFs as required to complete the report. These reports will then be zipped up and the zip file returned to the web interface for download.

Report Size Limits

In the past, reports could be generated that were very large and with the new capacities of Inception, these reports are now even larger. Reports can be generated that can include several thousands of pages, for example a permissions report on 10,000 users who have permissions to many doors, areas and outputs. When trying to render this to a PDF, the Inception controller would run out of memory and reboot, which is obviously undesirable. To prevent this, if a report is started that would be too large for the available memory of the Inception (greater that ~50-100 pages), the report will be stopped.

Instead, a prompt will be shown indicating that the report is too large for a single PDF. From there, a user can either select a new report format (such as those listed above), or the report can be filtered down to show more specific information.

Version 2.0.2 - 07/12/17

Feature Updates (cont.)

RF Fob Signal Strength

The signal strength of an RF Fob is now logged to review whenever a button is pressed. No new messages have been added. Instead, the existing messages (fob button from unknown fob, fob button received from user etc) have been updated to also include the signal strength.

This is useful when assessing a site, as the fob can be used from various locations around a site and the signal strengths recorded in review. Common control locations can be tested to see if the RF signal is suitable; or if receivers need to be moved or extra hardware added. If the review window is open on a phone, these events can be seen live.

Note that if multiple receivers or repeaters are installed on site, the signal strength may not always indicate the closest receiver, as a receiver further away may have received a clearer message first and processed it.

When	Message	Who	What	Where
28/11/2017 15:28:18	Remote Fob Button press received from User	Installer	Button Three (S/N 9930483, Signal 37)	IR-Inovonics RF Module 2
28/11/2017 15:28:16	Remote Fob Button press received from User	Installer	Button Two (S/N 9930483, Signal 18)	IR-Inovonics RF Module 2
28/11/2017 15:28:08	Remote Fob Button press received from User	Installer	Button Three (S/N 9930483, Signal 28)	IR-Inovonics RF Module 2
28/11/2017 15:28:06	Remote Fob Button press received from User	Installer	Button One (S/N 9930483, Signal 27)	IR-Inovonics RF Module 2
28/11/2017 15:28:03	Remote Fob Button press received from User	Installer	Button Four (S/N 9930483, Signal 34)	IR-Inovonics RF Module 2
28/11/2017 15:28:00	Remote Fob Button press received from User	Installer	Button One (S/N 9930483, Signal 32)	IR-Inovonics RF Module 2
28/11/2017 15:26:03	Remote Fob Button press received from User	Installer	Button Two (S/N 9930483, Signal 76)	IR-Inovonics RF Module 2
28/11/2017 15:26:01	Remote Fob Button press received from User	Installer	Button One (S/N 9930483, Signal 74)	IR-Inovonics RF Module 2

Issues Resolved

Older Browsers Supported Again (Internet Explorer, old iOS browsers etc)

In Inception release 2.0.0, older browsers (all Internet Explorer versions, older iOS browsers etc) experienced an issue where the items weren't shown on any edit pages. This has now been resolved, so Internet Explorer 9 and above and other browsers that once worked should work again. Note that it is still recommended to use a more up to date browser.

Time Periods with Long Breaks

An issue was discovered where if a Time Period had more than 6 days before it would next change state, that time would not be calculated and the time period would not trigger again. This could be due to weekly recurring times only on one day of the week, or using exceptions that activate less frequently. This issue has now been resolved and existing time periods will work correctly again. Note that if the next time period change is 7 or more days away, the time period state will show that the next change is "one or more weeks away". This will recalculate once each day until an actual time can be shown.

Version 2.0.1 - 03/11/17

Inception release 2.0.1 resolves an issue introduced in the 2.0.0 release. The issue affects the reporting ID of newly created Inputs and Outputs, causing issues with Contact ID reporting and controlling of outputs via the SkyCommand App.

Feature Updates

Back to Checklist Shortcut

In response to feedback from the field, the Back to Checklist button will now be shown on every page until the checklist is completed. Previously, the button would only be shown in the toolbox when navigating from the checklist. However, if any other navigation occurred, the button would disappear and the user would need to use the navigation bar or the checklist progress indicator at the top of the page to go back.

Issues Resolved

Incorrect Input Reporting IDs

With Inception release 2.0.0, an issue was introduced where any newly created inputs (both hardware inputs and custom inputs) would all be assigned the reporting ID of 1. This would affect Contact ID reporting as the inputs could not be differentiated. Existing inputs are unaffected by this issue, and updating to this release will also fix any affected inputs, giving them unique ids.

Incorrect Output Control IDs

Similar to the issue above, newly created outputs (both hardware outputs and custom outputs) are also assigned control IDs of 1. The SkyCommand App relies on this control ID to differentiate outputs for state and control purposes. Existing outputs are unaffected and updating to this release will fix any affected outputs.

Version 2.0.0 - 26/10/17

The 2.0.0 release of Inception brings increased system capacities, now supporting up to 128 doors and 10,000 users. Also "Swinger Shutdown" functionality, a permanent SLAM card cache option and several other features have also been included.

New Features

Increased Capacities

The maximum capacity of Inception has been increased, now supporting up to 128 doors and 10,000 users (previously 32 doors and 2,000 users). These new limits require no hardware changes or licenses and will be automatically applied with this firmware update.

	Old Inceptions (1.4.3 and below)	New Inceptions (2.0.0 and above)
Doors	32	128
Areas	32	32
Inputs	512	512
Outputs	512	512
Users	2000	10000
Events	50000	50000

With the increased supported system capacities introduced with this release, extensive performance testing was executed to ensure the system could handle these new limits well. Internally, improvements weren't required as the system was still very responsive at and beyond these new limits, but nevertheless several improvements were still made to make the system even faster.

Numerous improvements however were added to the web interface of Inception to support managing and editing of large numbers of items (such as 10,000 users). This resulted in much faster page load times and should result in a much faster and smoother experience when using the web interface, regardless of the size of the system.

T4000 SkyTunnel Passthrough (Due Q1 2018)

While not yet available (due for release in Q1 2018), this release adds support for a feature that will allow a SkyTunnel connection to be established via a T4000's sim cards, using the existing T4000 to Inception interface cable.

This functionality is similar to the soon-to-be released T4000 Router feature which allows a T4000's Ethernet port to act as an internet router and use the SIM data for internet access. The major difference however is the passthrough feature uses the existing T4000 to Inception interface cable, while the router feature requires the Ethernet ports to be connected.

Both options will allow the Inception's web interface to be accessible on sites where for example, the Inception controller is not allowed to be connected to the client's local internet, where local internet does not exist or where being able to remotely access the Inception interface should not rely on the local internet.

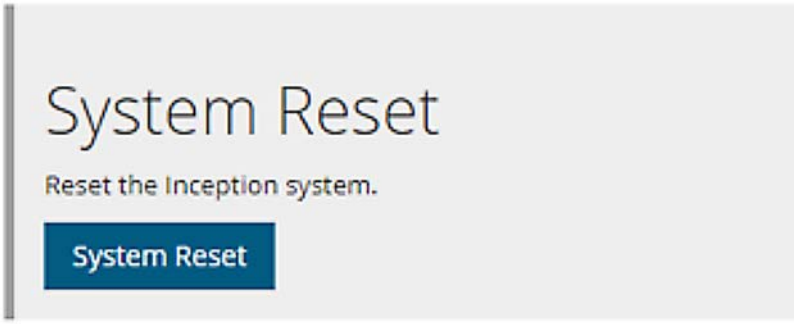
Once this passthrough functionality is made available in SkyCommand and the T4000, any Inception controller running this release or newer will be able to make use of it without any need for cabling changes.

Version 2.0.0 - 26/10/17

New Features (cont.)

System Reset

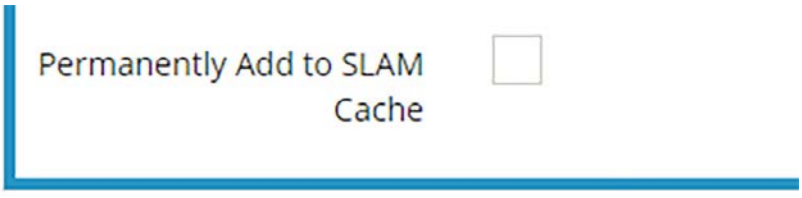
A new section has been added to the **[System > Service]** page that allows the Inception system to be reset from the web interface. Clicking *System Reset* will prompt with a dialog to confirm that you do want a system reset to occur. On accepting this dialog, the Inception controller will reboot and the web page will be unavailable for a period of time while the unit starts up again and reconnects to the network. This option is limited to users who can access the Service Mode page.



Permanent Option for SLAM Card Cache

The Standard LAN Access Module (SLAM) includes a 2000 card cache that is capable of tracking if the last time it saw a card at a reader, whether access was granted or not. This information is remembered for each door on the SLAM in each direction. If communications between the SLAM and the Inception system are lost, the SLAM can use this cache to determine if a user's card should be allowed through the door, allowing offline behaviour.

Cards can be removed from this cache for several reasons; if access is denied to a door when the card is used, after 1 month of inactivity, or if the 2000 limit is reached then as new cards are added to the cache the oldest cards are removed. This feature attempts to allow intelligent offline behaviour where the people who used a door recently will still be able to access the door in the event that the door module loses connectivity with the Inception controller.



Users have now gained an option that can force their cards to remain stored in the cache, even if they haven't been used for a long time. This allows important cards like those belonging to managers, emergency services or fire wardens for example to remain working if something happens to the main controller, even if they are rarely used.

Note that cards are not automatically added to the card cache of each SLAM, the card must be presented at each reader of each door and access be successfully granted for the card to be added to the cache of that module.

Version 2.0.0 - 26/10/17

New Features (cont.)

Repeat Alarm Event Limit (Swinger Shutdown)

The **[Configuration > General > Alarm Reporting]** page has been updated with a new *Repeat Alarm Event Limit (Swinger Shutdown*) option. The swinger shutdown feature is designed to limit the number of repeated input activations or module health issues that are sent to a monitoring station. Often, this option is used in case a detector becomes faulty and begins repeatedly activating, preventing these repeated false signals from being sent through and overwhelming a central station. Similarly, this can prevent module events like low battery from sending repeatedly if the battery capacity is on the edge of detection.

Individual areas, inputs and alarm types are tracked towards repeat event limits, identifying each event separately. In this case, repeated alarm events from an input can trigger swinger shutdown and stop future alarm events from that input from being sent, but if a tamper event is then detected on that input, it will still be reported. Similarly, a module's low battery event could be limited, but a cabinet tamper or AC fail event from that module is different and hence tracked and limited separately and will still be sent through.

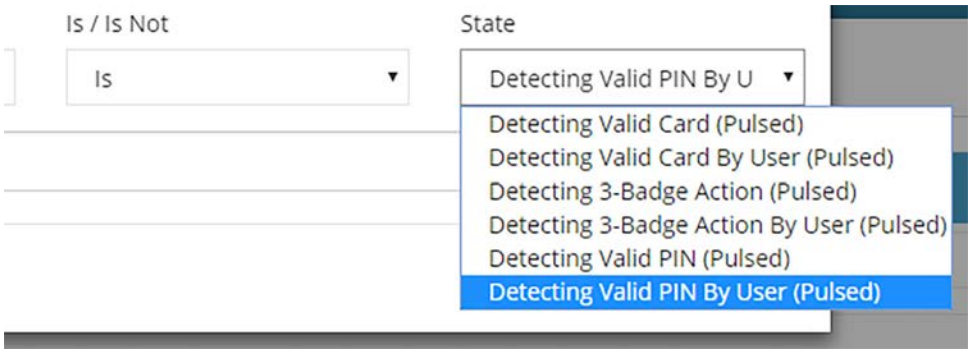
If set to zero, the feature will be disabled and all alarm events will be sent through. If a limit is set, once the event limit is reached for an input or module health event, a separate event is sent to the monitoring station for this input or module to indicate swinger shutdown has occurred. Future activations from that input or module health event will be discarded until the area containing the input is disarmed, or any area is disarmed for module health issues.

Version 2.0.0 - 26/10/17

Feature Updates

Reader Automated Action Trigger on Valid PIN

Inception release 1.4.1 included reader trigger options for automated actions, which allowed actions to be automatically performed in response to a valid card or three-badge action at a reader, by either any user or a specific user. This has now been expanded to include “Valid PIN” as an option, letting actions be performed when a user enters a valid PIN into a keypad reader. Both SIFER and Wiegand keypad readers can be used with this option.



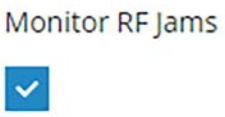
System Messages Removed from Basic Terminal Profile

Based on feedback from the field, the inbuilt “Basic User” LCD terminal profile has been updated to no longer show the System Messages menu by default. Having permission to this menu would cause the system messages and warnings screen to appear after logging on to a terminal, but only if there were any warnings or messages to show. Given the purpose of this profile, being assigned to standard end users who may infrequently use the terminal, this could lead to confusion if their procedure to lock up was similar to “PIN, OK, Choose area, ON” as there was a chance that a different screen would “randomly” appear.

Note that permission to the system messages screen has been removed from the built in Basic User profile from both new factory defaulted systems and existing systems. If showing this screen for basic users is desirable, then make sure to re-allow permission to the menu in the LCD terminal profile.

RF Jam Monitoring Now Optional

RF Jam health events were always monitored and sent through to the monitoring station when they occur, with no way to turn them off. However on sites where there is occasional known interference that can’t be avoided, this could cause RF Jam alarms to be reported that are undesirable. And so, in this release a new *Monitor RF Jams* option has been added to the *Additional Components* section of the hardware wizard when configuring a Paradox or Inovonics RF module.



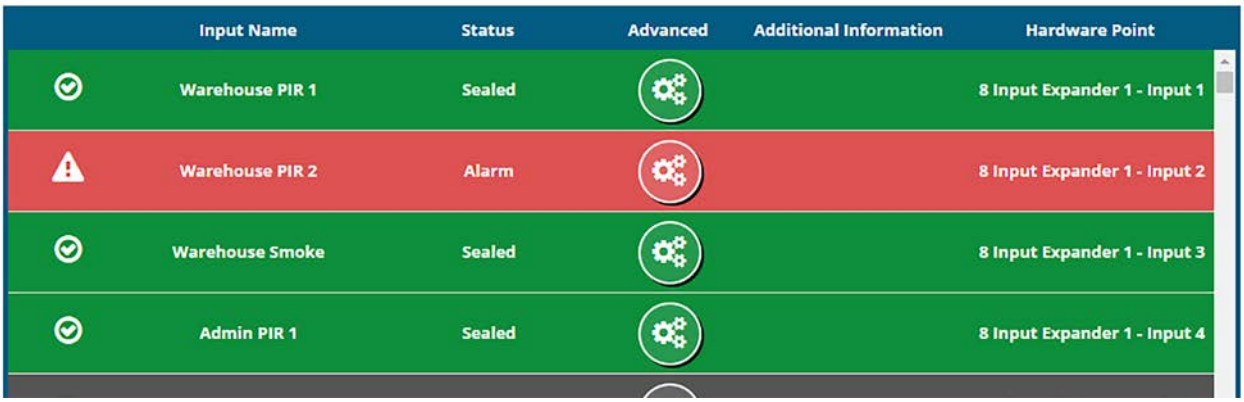
Existing RF Expanders will automatically have this option enabled, so they remain monitoring RF Jams, but it can easily be disabled if undesired.

Version 2.0.0 - 26/10/17

New Features (cont.)

Hardware Points for Input Monitor Pages

The **[State / Control > Control Inputs]** page has been updated to include a new column showing the hardware location of each input. The rest of the Inception system relies on proper names to describe everything where clear names can be entered, instead of a coded numbering or addressing system. When dealing with inputs though, especially when attempting to diagnose faults, it is helpful to know the physical point where the external device connects to the Inception system.



This new Hardware Point column can also be sorted to aid in managing and locating inputs. It is still recommended to use the **[State / Control > Hardware Test]** page though for initial commissioning, as it allows the modules to be fully verified one at a time.

HID 34Bit Card Format

The 34Bit HID Card Format has been included as a built-in card format within the Inception system. Note that if this card format has already been added to a system due to importing a custom item, nothing will change as this is the same card format.

If a card format is required on site that isn't included as a built-in format, please contact Inner Range support to have a custom format created for you that can be uploaded to an existing Inception unit.

Issues Resolved

User Priority Level Issue

Inception release 1.4.3 introduced a user hierarchy feature for managing users, which intended to prevent users of lower "priorities" (e.g basic end users) from being able to edit, create or delete users of higher "priorities" (e.g administrators, installers). However, an issue existed where a lower priority user was still able to edit a higher priority user if the edit involved changing that user's web profile or removing their ability to log in via the web interface. This has now been resolved.

SLAM Cache issue with Wiegand Readers

It was recently discovered that the built in card cache of the Standard LAN Access Modules (SLAMs) was not working if the readers in use were Wiegand. If SIFER readers were being used, then the cache was working correctly. This has been fixed so any supported readers work correctly with the card cache feature.

www.innerrange.com

inner range

Intelligent Security Solutions

Inner Range Pty Ltd
1 Millennium Court Knoxfield, Victoria, 3180, Australia
Tel: +61 3 9780 4300
Fax: +61 3 9753 3499
email: admin@innerrange.com

innerrange.com