inner range

UNIFIED VIDEO, ACCESS & SECURITY SYSTEMS

INCEPTION

Release Notes 7.0.0
January 2025

INNERRANGE.COM

Contents

How to Upgrade 3

Version Information 4

Version 7.0.0 5

Version 6.3.0 9

Version 6.2.0 15

Version 6.1.0 20

Version 6.0.1 25

Version 6.0.0 26

Version 5.2.0 29

Version 5.1.2 34

Version 5.1.1 36

Version 5.1.0 37

Version 5.0.1 40

Version 5.0.0 41

Contact 47

How to Upgrade

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

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

How to Upgrade

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

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

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

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

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

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

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

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

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

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

Version Information

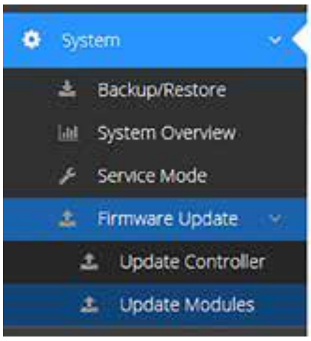
Minimum Required Versions

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

Expansion Module	Firmware Version
8 Input LAN Expander	**3.2.0**
UniBus 8 Input Expander	**1.0.3**
UniBus 8 Relay Expander	**1.1.2**
Standard LAN Access Module (SLAM)	**4.0.7**
Intelligent LAN Access Module (ILAM)	**4.1.0**
SIFER Reader	**1.16.0**
T4000 Security Communicator	**2.1.4**
Inovonics RF Expander	**1.1.0**
EliteX Keypad	**3.1.0**
LAN Ethernet Bridge	**1.2.0**
Inner Range Mobile Access Reader	**1.34.40**

How to Update Modules

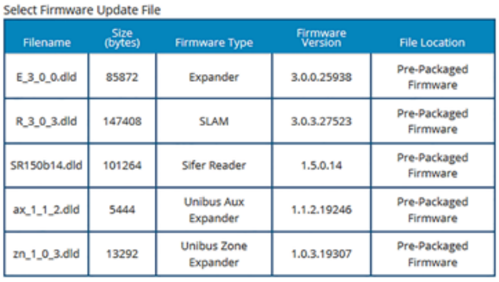
How to check your expansion module versions and update them:



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 of the file. 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 7.0.0

January 2025

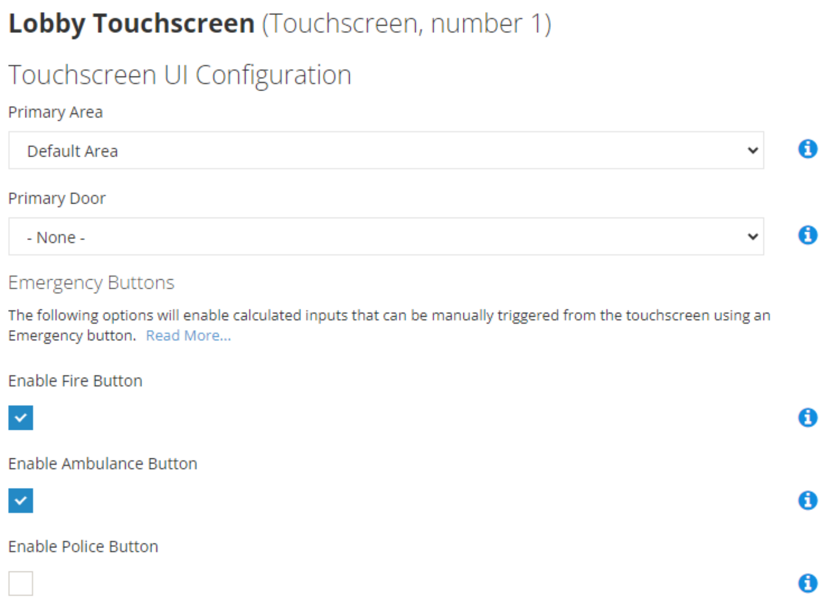
Inception 7.0.0 adds support for the Touchscreen and IR Video, as well as several feature updates and resolved issues.

New Features

Touchscreen Support

Inception is now capable of connecting to and configuring the Inner Range Touchscreen, providing another option for interfacing with the Inception system for Users, like other terminals with a fully capable touchscreen interface and some new capabilities. They can be configured and added like any other hardware module by going to **[Configuration > Hardware]**.

Certain elements of the Touchscreen's UI can be configured via Inception, including lists of Areas, Doors, Inputs, Outputs and other Hardware modules that the Touchscreen can display state or offer control options for, as well as the ability to show 'Emergency Buttons'.



Lobby Touchscreen (Touchscreen, number 1)

Touchscreen UI Configuration

Primary Area: Default Area

Primary Door: - None -

Emergency Buttons

The following options will enable calculated inputs that can be manually triggered from the touchscreen using an Emergency button. Read More...

Enable Fire Button: ☑

Enable Ambulance Button: ☑

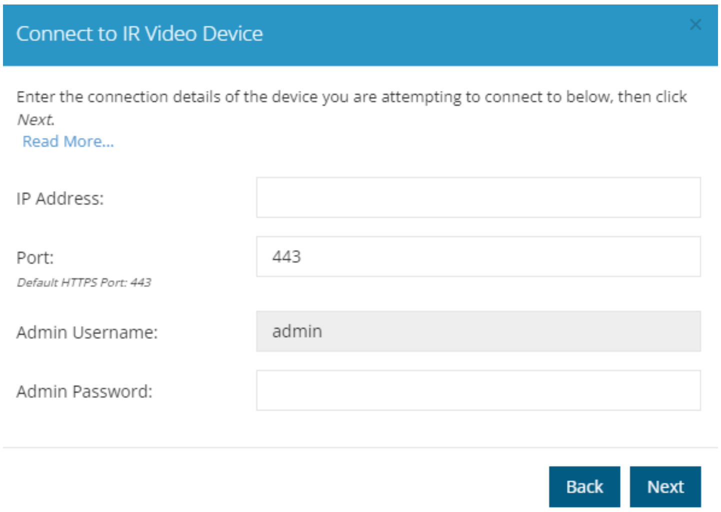
Enable Police Button: □

Enabling a given Emergency Button will allow it to appear and be pressed in the Touchscreen and generate a Calculated Input for the button in question. Actions on button press can then be configured by adding the input to an Area and using an appropriate process group.

IR Video Support

Inception now supports the IR Video Integration, allowing connection to and configuration of CCTV Cameras from an Inception system. While this does not provide the ability to view video, Commands, Inputs and Outputs can all be managed from Inception once connected. You can begin connecting to an IR Video NVR at the 'Integrated Connections' page: **[Configuration > Integrations > Integrated Connections]**.

Clicking ‘Add’ will prompt you for the connection details of the NVR you wish to connect.



Connect to IR Video Device

Enter the connection details of the device you are attempting to connect to below, then click *Next*.

Read More...

IP Address:

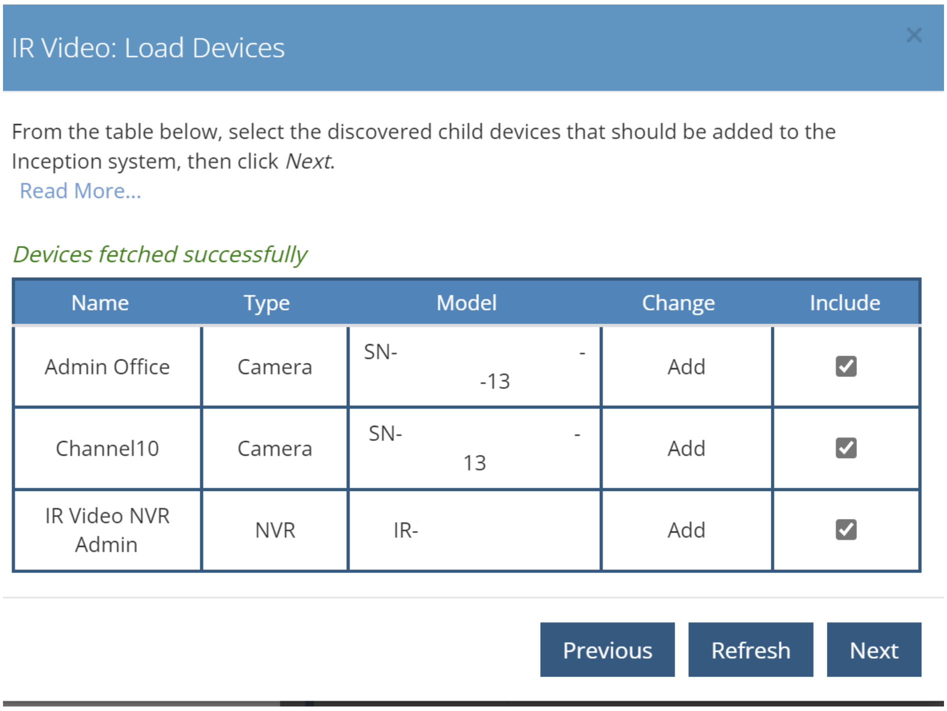
Port: 443

Default HTTPS Port: 443

Admin Username: admin

Admin Password:

Once these details have been entered, Inception will connect to the NVR and display a list of available Cameras which can be selected to be imported into Inception.



IR Video: Load Devices

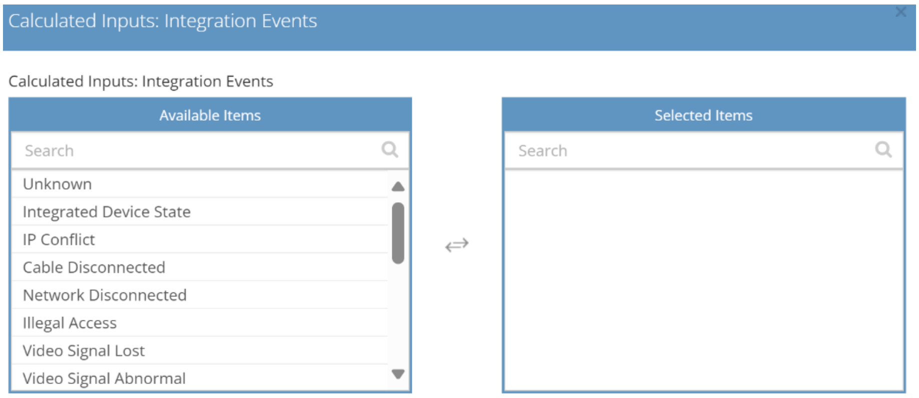
From the table below, select the discovered child devices that should be added to the Inception system, then click *Next*.

Read More...

Devices fetched successfully

Name	Type	Model	Change	Include
Admin Office	Camera	SN- - -13	Add	☑
Channel10	Camera	SN- - 13	Add	☑
IR Video NVR Admin	NVR	IR-	Add	☑

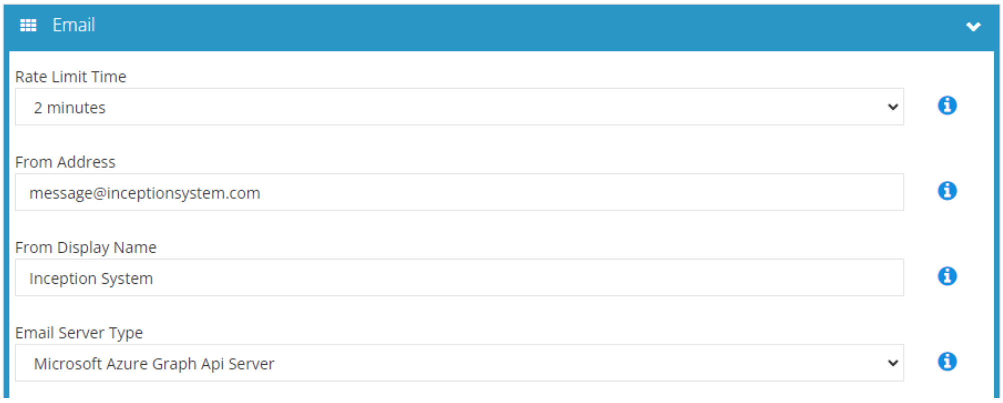
Once selected, further configuration of these devices can be performed at **[Configuration > Integrations > Integrated Devices]**. This includes generating Calculated Inputs for desired Integration Events supported by a given device.



Feature Updates

Email Sender

The Email Sender has been updated to support sending emails via Microsoft Azure and Gmail. These options can be selected and configured in the ‘Email’ tab in **[Configuration > General > System]**.



Rate Limit Time
2 minutes

From Address
message@inceptionsystem.com

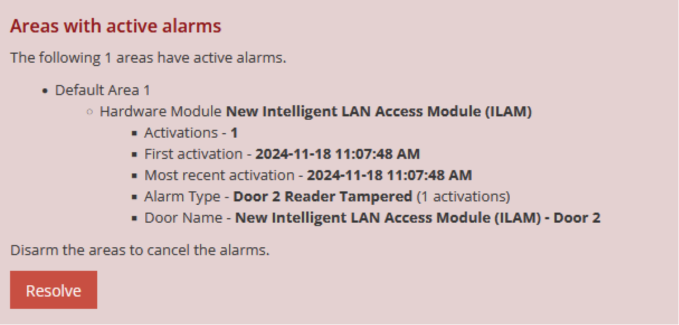
From Display Name
Inception System

Email Server Type
Microsoft Azure Graph Api Server

Existing configurations will use the ‘SMTP’ option and do not require any changes to continue working.

SIFER Tamper Alarms

Tamper Alarms reported in Inception involving SIFER Readers now include the name of the Door related to the Reader.



Areas with active alarms

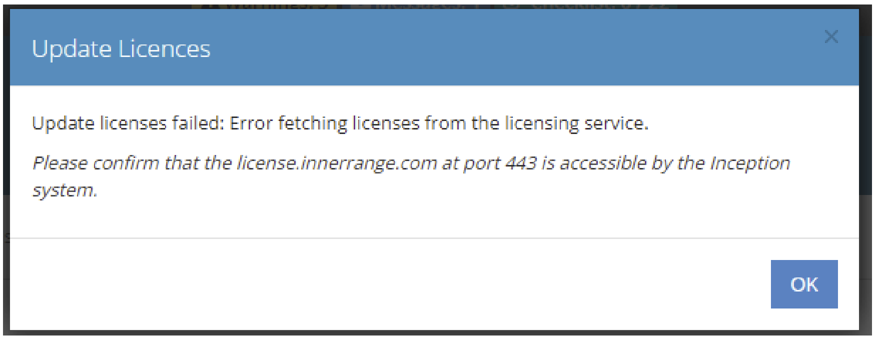
The following 1 areas have active alarms.

- Default Area 1
  - Hardware Module **New Intelligent LAN Access Module (ILAM)**
    - Activations - **1**
    - First activation - **2024-11-18 11:07:48 AM**
    - Most recent activation - **2024-11-18 11:07:48 AM**
    - Alarm Type - **Door 2 Reader Tampered** (1 activations)
    - Door Name - **New Intelligent LAN Access Module (ILAM) - Door 2**

Disarm the areas to cancel the alarms.

Licensing Page Error Messages

Error messages displayed in the Licensing page when a connection error occurs has been improved, including a suggestion for troubleshooting the issue.



Update licenses failed: Error fetching licenses from the licensing service.

Please confirm that the license.innerrange.com at port 443 is accessible by the Inception system.

Issues Resolved

REST API Error Responses

The error reporting from the Inception REST API has been made more robust, providing more information on issues encountered. This includes error reporting for entities sent via POST or PATCH request with GUIDs that do not match an entity in Inception, 400/404 errors now containing bodies in their responses and more descriptive error reporting for invalid parameters provided to the API (eg ‘modifiedsince’ date parameters being invalid).

Entity Editor Locking Up

Resolved an issue where entity editor pages could lock up when adding a new Entity, clicking the new entry in the entity list, then selecting “No” when prompted to save changes. This error was seen effecting the User, Area, Custom Output, Credential Template and Time Period editing pages.

Area Report ID

Resolved an issue where an Area’s ‘Reporting ID’ could be saved incorrectly when updating a newly created Area without reloading the page after initially saving it.

Password Policy

Resolved an issue when creating or changing passwords would incorrectly reject passwords that were valid according to the stated guidelines.

Version 6.3.0

October 2024

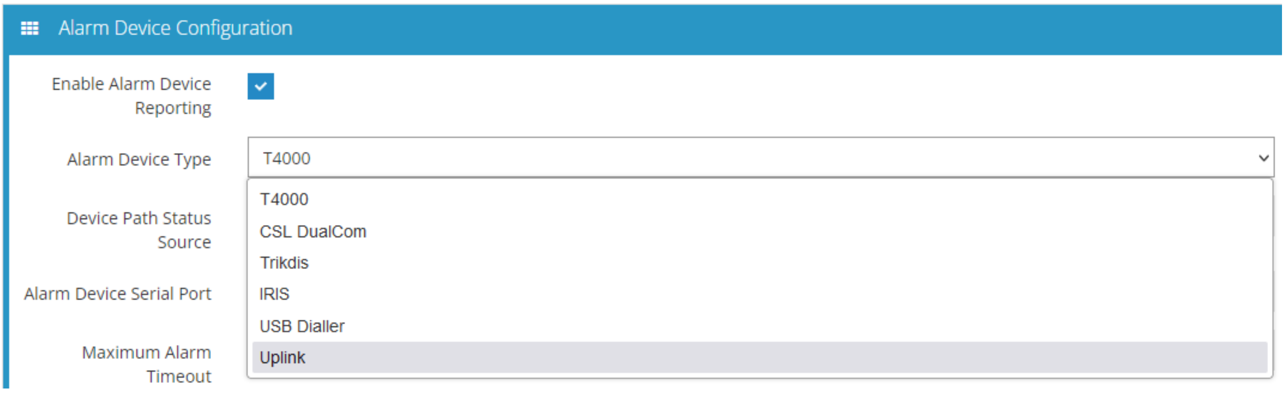
Inception 6.3.0 adds support for the Uplink alarm communicator, storage unit output behaviours, various report and mobile access improvements, and many security and performance improvements.

NOTE: To further secure the Inception system, the TLS 1.0 and TLS 1.1 protocols have been disabled, meaning that any existing connections or email handlers to servers that require these protocols will no longer function. Prior to upgrading to this firmware version or greater, it is recommended to ensure that no such connections are present. Please refer to the *Cyber Security Updates* section for more information.

New Features

New Europe / NA Alarm Communicator Support: Uplink

For European and North American markets, support has been added for the Uplink alarm communicator. This device type is an available option in the *Alarm Reporting Settings*, provided the system region is set to *North America* or *Europe*.



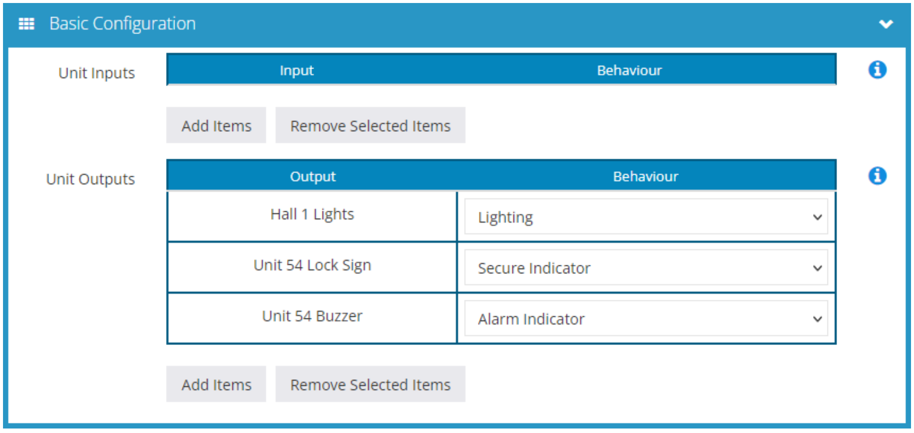
Alarm Device Configuration

Enable Alarm Device Reporting ☑

Alarm Device Type: T4000

Storage Units – Output Behaviours

Storage units can now have different behaviours configured for their outputs, depending on intended functionality. This allows for finer control of when exactly the outputs should be toggled on/off. For example, an accentuator output could be configured to fire when the storage unit moves into the alarm state, by using the *Alarm Indicator* behaviour.



Basic Configuration

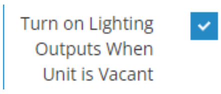
Unit Inputs

Input	Behaviour

Unit Outputs

Output	Behaviour
Hall 1 Lights	Lighting
Unit 54 Lock Sign	Secure Indicator
Unit 54 Buzzer	Alarm Indicator

Additionally, storage units can also turn on outputs with the *Lighting* behaviour when the storage unit is vacant, by ticking the *Turn On Lighting Outputs When Unit Is Vacant* checkbox.

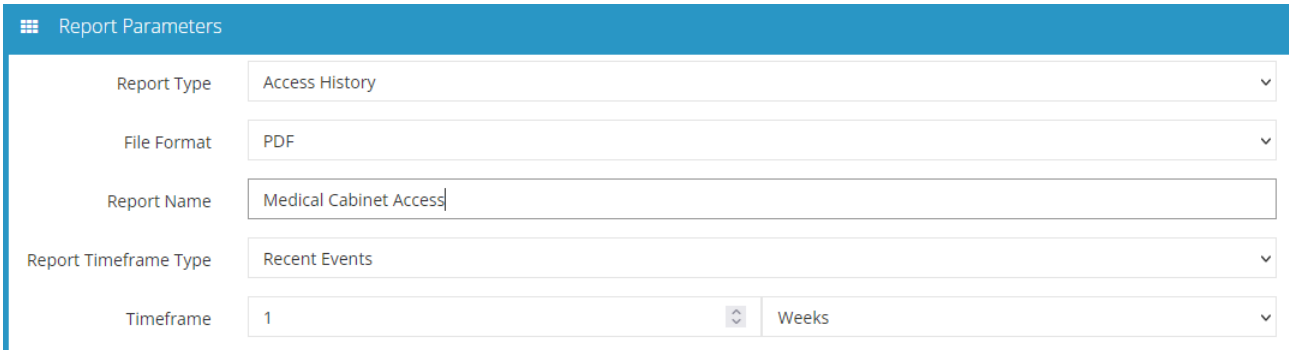


Turn on Lighting Outputs When Unit is Vacant ☑

Feature Updates

Custom Report Names

Reports can now be provided with an optional report name, allowing for easier differentiation between reports and their purposes.



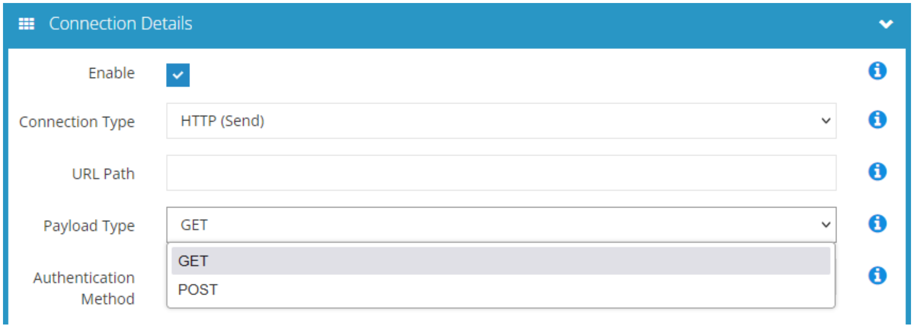
Report Parameters

Report Type	Access History	
File Format	PDF	
Report Name	Medical Cabinet Access	
Report Timeframe Type	Recent Events	
Timeframe	1	Weeks

If a *Report Name* is not configured, the report will generate a report name based on the *Report Type* specified, as per previous behaviour. This new *Report Name* field is present in both the [System > Reports]

Connection POST Functionality

Connections of *Connection Type* “HTTP (Send)” can now be configured to send either POST or GET requests, as opposed to previously just being able to send GET requests. This is represented as a new *Payload Type* dropdown option. When GET is selected, the payload is appended to the URL, while when POST is selected, the payload will be inserted into the body of the request.

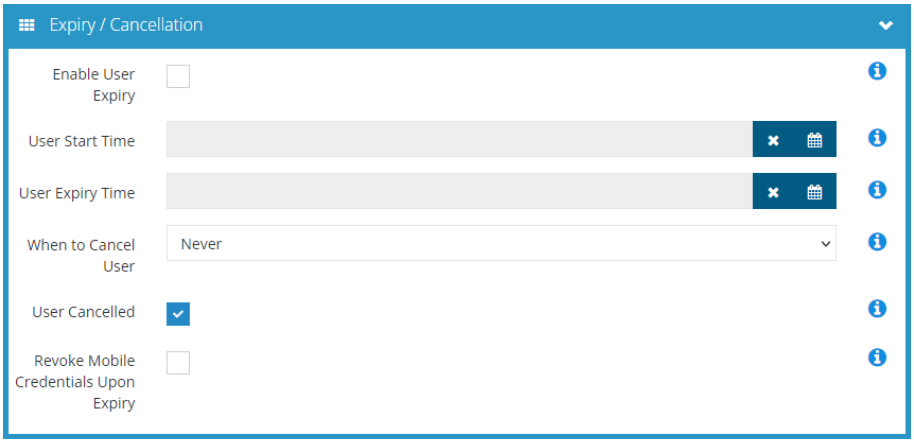


Connection Details

Enable	☑
Connection Type	HTTP (Send)
URL Path	
Payload Type	GET
Authentication Method	

Mobile Access Auto Revoke Credentials Upon User Expiry

A checkbox has been added to the user configuration page to *Revoke Mobile Credentials Upon Expiry*. As the name suggests, when ticked and the user has been marked as expired, that user will have any active mobile credentials automatically revoked.

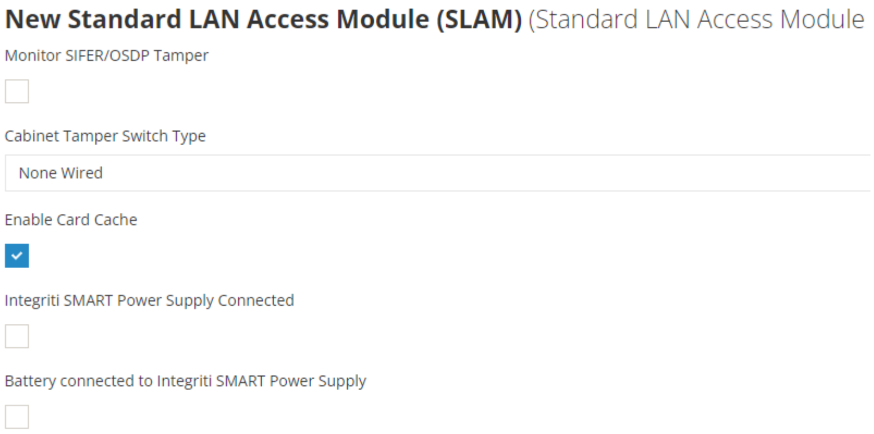


Expiry / Cancellation

Enable User Expiry	□
User Start Time	
User Expiry Time	
When to Cancel User	Never
User Cancelled	☑
Revoke Mobile Credentials Upon Expiry	□

SLAM Card Cache Toggling

The Standard LAN Access Module's (SLAM) offline card cache can now be optionally disabled when configuring the module. When the new *Enable Card Cache* is unticked, the SLAM will not cache card reads and use these cached credentials to grant access in the event the Inception controller falls offline.



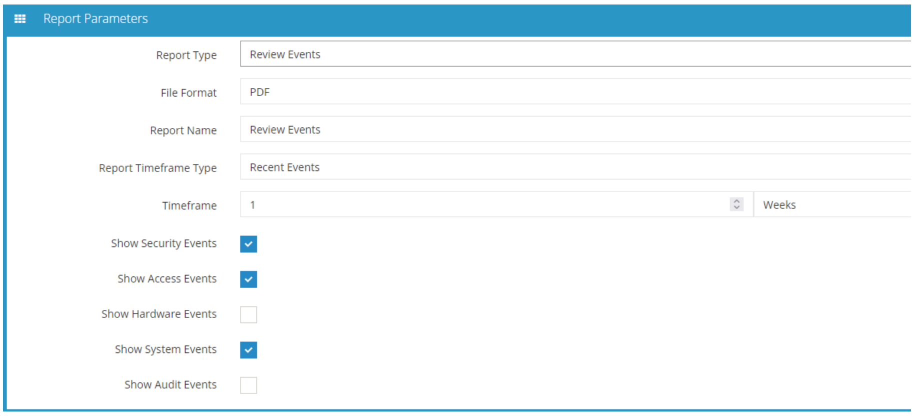
New Standard LAN Access Module (SLAM) (Standard LAN Access Module

Monitor SIFER/OSDP Tamper	□
Cabinet Tamper Switch Type	None Wired
Enable Card Cache	☑
Integriti SMART Power Supply Connected	□
Battery connected to Integriti SMART Power Supply	□

This checkbox is enabled by default, in line per previous behaviour, meaning the SLAM will cache credentials in its offline cache.

Generic Review Event Report Type

A new *Report Type* of “Review Events” has been added, allowing for generic review events to be collated and turned into a report.



Report Parameters

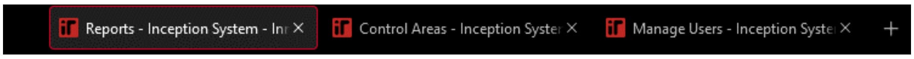
Report Type	Review Events
File Format	PDF
Report Name	Review Events
Report Timeframe Type	Recent Events
Timeframe	1 Weeks
Show Security Events	☑
Show Access Events	☑
Show Hardware Events	□
Show System Events	☑
Show Audit Events	□

Persist Service Mode After System Restart

Service mode will no longer be disabled upon a system restart, preventing situations where the system was restarted due a firmware update or other required restart. This allows for configuration to be done within specified windows of time without any risk of false alarms being raised to monitoring or accentuated.

Dynamic Browser Title

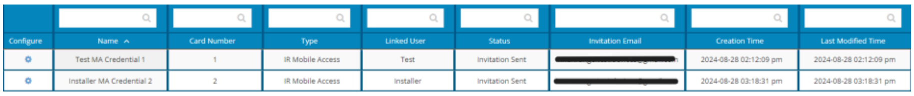
The browser tab’s title will now also display the name of the current page, providing a clear indication to installers and end users of which page each tab is currently showing.



Reports - Inception System - Inı ×
Control Areas - Inception Syster ×
Manage Users - Inception Syste ×
+

Email Field in Mobile Credential Page

The *Invitation Email* column will now be shown in the *Mobile Credentials* page, allowing for clearer visibility of required information within this page.



Configure	Name ^	Card Number	Type	Linked User	Status	Invitation Email	Creation Time	Last Modified Time
⚙	Test MA Credential 1	1	IR Mobile Access	Test	Invitation Sent	[redacted]	2024-08-28 02:12:09 pm	2024-08-28 02:12:09 pm
⚙	Installer MA Credential 2	2	IR Mobile Access	Installer	Invitation Sent	[redacted]	2024-08-28 03:18:31 pm	2024-08-28 03:18:31 pm

3 Minutes Output Timed Control Option

Added a new *3 Minutes* option to the *Output Timed Control* dropdown, allowing this control timeframe without needing to resort to chaining multiple timed control commands.

Access Denied Events with Unknown/Inactive Credentials

Doors will now raise *User Denied Access* events for Unknown and Inactive card reads, in addition to the existing behaviour of when a user is denied access due to being expired, having insufficient permissions, or the door being locked out.

Issues Resolved

EliteX Terminals Not Updating Live State

Resolved an issue with output state changes not being reflected in a connected EliteX terminal when it is on the logged off control screen.

Initial Configuration Timezone Settings Not Saving

The time zone setting selected during the Initial Configuration page will now correctly persist across a system restart.

ILAM System Warning Issues

Resolved multiple issues with system warnings regarding ILAM offline syncing and behaviour. The warnings will now only appear when there is actually an ILAM configured, or there is at least one ILAM being synced to. Additionally, removing the offending user or credential will now correctly clear the corresponding ILAM system warning.

Resending Invitations for Active Mobile Credentials

Active credentials are no longer able to have their invitation resent, preventing scenarios where multiple users could theoretically have the same credential allocated.

Ethernet Bridge IRFast Reporting ID

Ethernet Bridges now have a reporting ID prefix of “P”, as opposed to the previous “?”.

Export Users 'Name' Field Requirement

Exporting Users to CSV now requires that the *Name* column is always present in the exported file, ensuring compatibility when importing the file back into the Inception system.

From and To Review Filters Not Working

Resolved an issue where the *From* and *To* filtering on the *Review Events* page would not correctly filter events when spanning across multiple months.

Dual Credential Access Denied Events

If a user presents a valid credential to a door requiring dual credential access, then a second user presents a valid credential to the same door in quick succession, the Inception system will no longer count them as two separate access attempts. Instead, it will treat them as a single dual credential access event, raising the appropriate Access Denied event.

Cyber Security Updates

Discontinued TLS 1.0 and 1.1 Support

The outdated TLS 1.0 and TLS 1.1 protocols are no longer supported by the Inception system. This specifically applies to outbound connections from the Inception system to external servers, as well as SMTP mail servers. All modern servers and platforms support TLS 1.2 as the new default standard, and connections to these platforms will continue to work as per normal.

Version 6.3.0

Inner Range strongly recommends keeping up to date with the latest firmware. Every release incorporates the latest security and vulnerability patches, helping to protect your devices from known and emerging threats.

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

Version 6.2.0

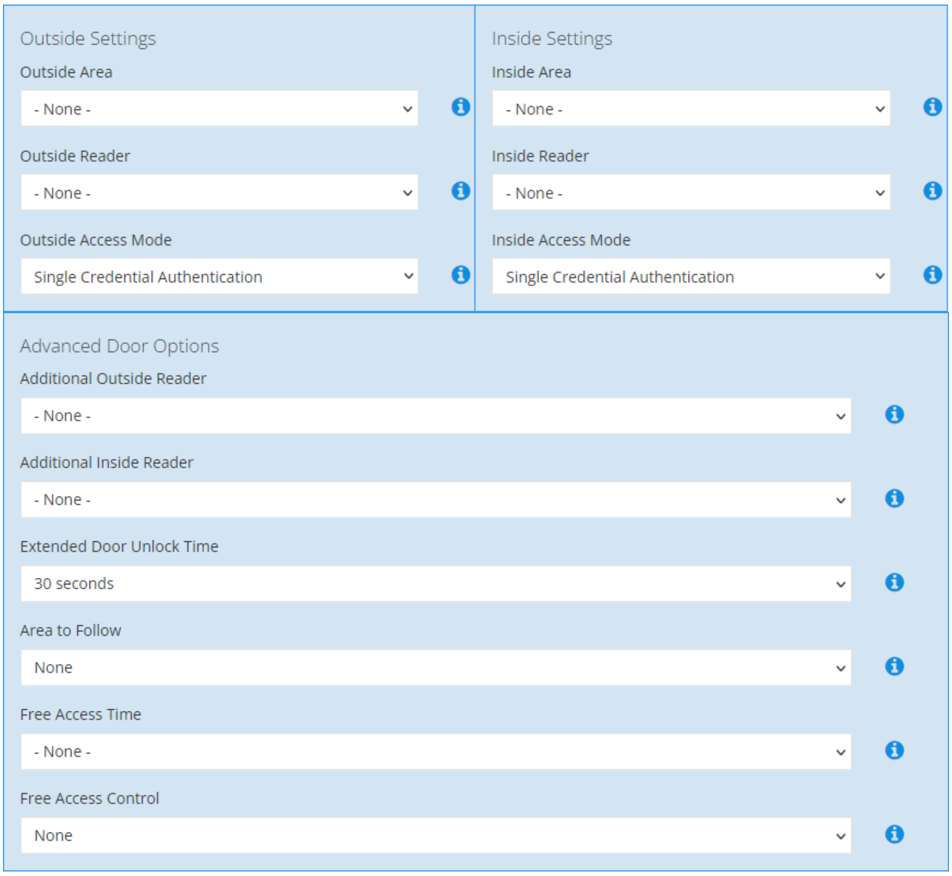
June 2024

Inception 6.2.0 adds the ability to have multiple readers on the same side of a door, multiple new storage unit features, major Mobile Access fixes with various enhancements, and many security and performance improvements.

New Features

Multiple Readers on Same Side of Door

A new *Show Advanced Door Options* checkbox is now available when configuring a door via the hardware wizard. Enabling this will expose additional door options, as well as the ability to select an additional inside and outside reader for the door. This allows for scenarios such as having two readers at different heights (a boom gate with one reader at car height and another at truck height), or two readers of different types (a card reader and a biometric reader), to be placed on the same side of a door.



Outside Settings

Outside Area: - None -

Outside Reader: - None -

Outside Access Mode: Single Credential Authentication

Inside Settings

Inside Area: - None -

Inside Reader: - None -

Inside Access Mode: Single Credential Authentication

Advanced Door Options

Additional Outside Reader: - None -

Additional Inside Reader: - None -

Extended Door Unlock Time: 30 seconds

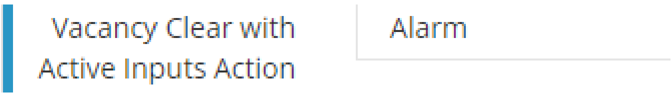
Area to Follow: None

Free Access Time: - None -

Free Access Control: None

Storage Blocks: Vacancy Clear Behaviour

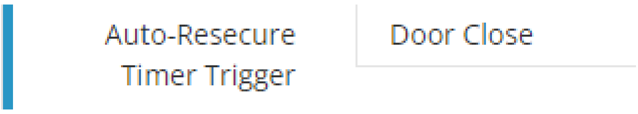
Added a new Vacancy Clear with Active Inputs Action option to storage blocks, allowing installers to choose what happens when a storage unit within that block has its vacancy cleared while it has inputs in alarm.



Vacancy Clear with Active Inputs Action: Alarm

Storage Blocks: Start Auto-Resecure Timer on Unlock

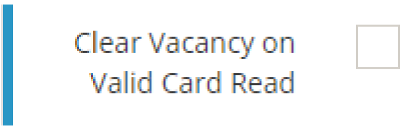
Added a new Auto-Resecure Timer Trigger option to storage blocks, allowing installers to configure when the auto-resecure timer should start for any storage units within that block. When set to Door Close, the timer will start when the storage unit’s door closes. If set to Unlock and Door Close, the timer will start when the storage unit is either unlocked or the door is closed.



Auto-Resecure Timer Trigger: Door Close

Storage Blocks: Clear Vacancy on Valid Card Read

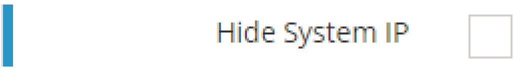
Added a new Clear Vacancy on Valid Card Read option to storage blocks, allowing installers to configure the associated storage units to have their vacancy cleared when a valid entry has occurred, transitioning into the Unlocked state. On a valid exit, storage units will attempt to transition into the Secure state, then the Unlocked state, respecting the Force Secure Units with Active Inputs setting.



Clear Vacancy on Valid Card Read □

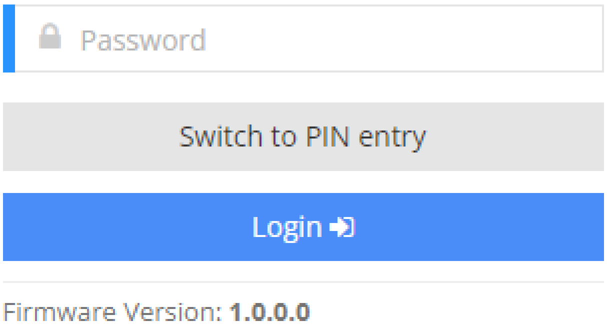
Hide System IP

Added a new Hide System IP option to the system settings under **[Configuration > General > System > Cybersecurity Hardening]**.



Hide System IP □

When enabled, the web interface login screen will no longer have the IP of the Inception displayed under the login button, and will only display basic information about the controller.



Firmware Version: **1.0.0.0**

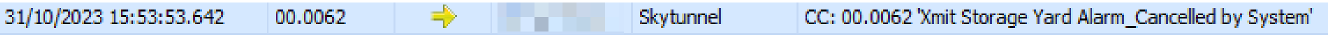
Feature Updates

Better Mobile Access Connection Status

The Mobile Access connection status found within **[Configuration > Access Control > Mobile Access > Mobile Access Connection Settings]** has been updated to give a more accurate display of the current connection status to the Mobile Access portal, and will also refresh with every request made. In addition, occasional flickering should not interrupt the status display.

Storage Unit IRFast Reporting Improvements

The alarm reporting of storage units has had its formatting updated in order to provide more accurate information. When an alarm is cancelled for a storage unit, it will now display "Xmit {AreaName} Alarm_Cancelled by System," indicating specifically that the action performed was an alarm cancel, and specifically pointing out the action being performed by the 'System' rather than 'Schedule'.

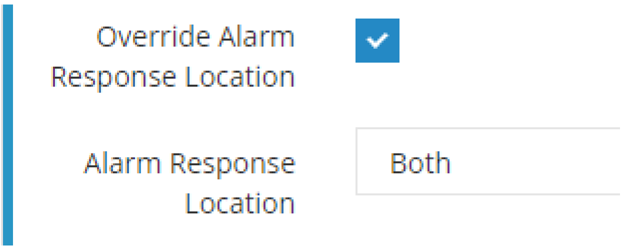


```
31/10/2023 15:53:53.642    00.0062    ➡    [redacted]    Skytunnel    CC: 00.0062 'Xmit Storage Yard Alarm_Cancelled by System'
```

Selecting Specific Siren Outputs in Areas

A new *Override Alarm Response Location* setting has been added to areas, allowing you to configure a custom alarm response location if enabled, rather than from the input location.

Enabling *Override Alarm Response Location* allows for you to select an *Alarm Response Location* of internal, external, or both sirens when sounding an alarm.



Override Alarm Response Location ☑

Alarm Response Location: Both

Issues Resolved

Mobile Access System Name Not Updating

The system name of a linked Mobile Access System should now automatically update as soon as it is updated in the Mobile Access portal, whereas previously it would not update at all.

Mobile Access Session Expiration

Fixed an issue where Mobile Access management functionality on Inception would stop working eventually as the connection would not be renewed until a reboot, resulting in a 'Session Expired' message. Retrying any allocation or editing operation with mobile credentials should now renew the session and work.

Unlinked Mobile Credential Editing

Mobile credentials are now removable even if you are not linked to a Mobile Access system or your Mobile Access system's connection is disabled manually.

Multiple Mobile Credential Removal

Fixed an issue where selecting and removing multiple mobile credentials from a user's mobile credential list at the same time would not result in an automatic save of the user. Now the user is automatically saved after the removal, meaning that the mobile credential changes will not be lost.

Resending Invitations for Revoked Credentials

An update to the Mobile Access portal prevented sending invitations for revoked credentials. As this is now no longer possible, it is not shown in the web interface, as this is not functionality supported by the Inner Range Mobile Access service.

Improved Handling of Mobile Access Invitations

Multiple improvements were made around sending mobile credential invitations to users, focused primarily on properly reflecting various outcomes correctly in the user interface.

Deleting Blank User Mobile Credentials

Mobile credentials that were already removed manually from the system would not be removable from the user's mobile credentials list, and should no longer be prevented by the web interface.

File Upload on iOS Chrome

File upload buttons for the iOS Chrome browser were previously either greyed out of non-functional for each of the instances where an imported file was required. This has been resolved in all locations of the web interface.

Credential REST API Breaking Changes

Resolved an issue present in the REST API after 6.1.0 where the GET and PATCH requests for singular users was no longer returning or accepting 'Credentials' for a user's credential list, and instead was using 'PhysicalCredentials' as the credential list name instead. Either name can now be used for the PATCH request, and user credentials are now returned both under 'Credentials' *and* 'PhysicalCredentials'.

User Deletion and ILAM Syncing

Deleting an expired user would cause issues when synchronising to the offline database of the ILAM, causing it to stop prematurely. The process of offline syncing will be uninterrupted, and will sync the deletion of the user properly.

Two-Factor Authentication QR Codes Missing

When setting up two-factor authentication for a user, the QR code section would appear blank, meaning that the details shown in the 'Manual Key Entry' section had to be used instead. A fix has been applied to allow the QR code to show up again.

Missing LCD Terminal Messages

Resolved an issue where certain LCD terminal messages were intermittently not displaying on the LCD display, such as the logged off idle display message.

DUIM and Hidden Network Share Locations

Inception's DUIM functionality now allows symbolic characters to be provided within the *Network Share Location* field. This is to address scenarios where hidden directories (denoted with a *$*) were not accessible due to this limitation.

Version 6.2.0

Cyber Security Updates

A large update has been done to the firmware and various frameworks within the Inception controller. General software vulnerabilities have been patched while also updating many underlying security frameworks within Inception. Changes were also done to secure the web traffic and content of Inception.

Inner Range strongly recommends keeping up to date with the latest firmware. Every release incorporates the latest security and vulnerability patches, helping to protect your devices from known and emerging threats.

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

Version 6.1.0

January 2024

Inception 6.1.0 introduces support for Inner Range Mobile Credentials, License Management, System Regions, and various security updates.

Note: Changes have been made to make regional settings more accessible in this firmware version through an initial landing page. This landing page does not require a login and appears on first access of the web interface, and so it is recommended that the installer accesses the web interface themselves right after upgrading to this version to configure the system.

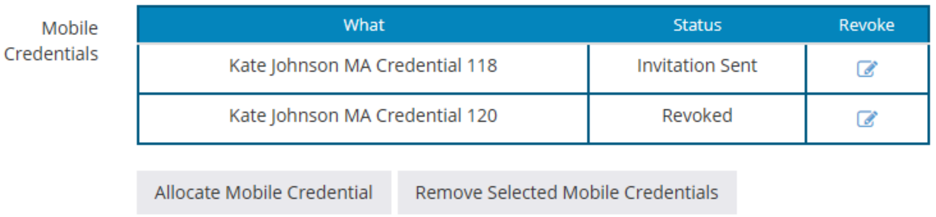
New Features

Inner Range Mobile Credentials

NOTE: Inner Range Mobile Access is only available in beta at the time of release, only systems that are part of the beta program will be able to create an Inner Range Mobile Access account on the portal and generate mobile credentials. Sites running this version of Inception will be able to take full advantage when the Inner Range Mobile Access platform has been launched, expected for release in Q3 2024.

Inception systems can now be linked to Inner Range's Mobile Access service through **[Configuration > Access Control > Mobile Access > Mobile Access Connection Settings]**.

Once the Inception system has been linked to Mobile Access, you may allocate mobile credentials through a user's credential list to be claimed by the Mobile Access app on that user's phone. The credential can then be managed either through the user's mobile credential list directly:

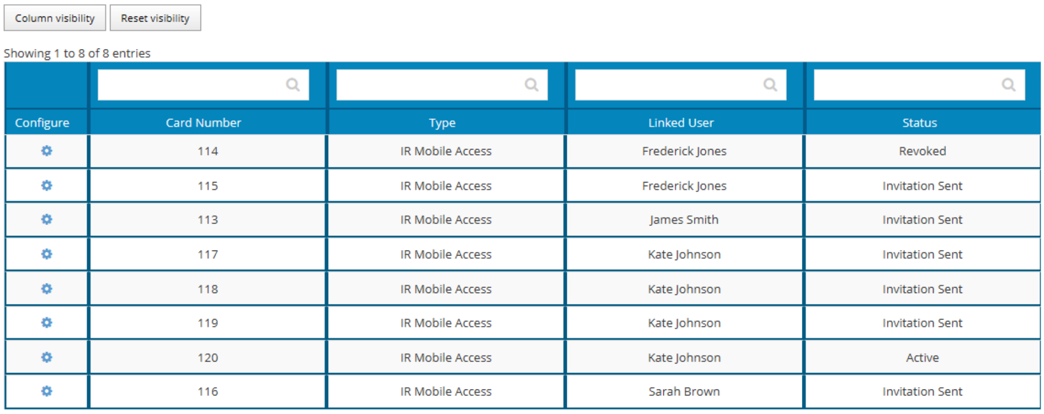


Mobile Credentials

What	Status	Revoke
Kate Johnson MA Credential 118	Invitation Sent	✎
Kate Johnson MA Credential 120	Revoked	✎

Allocate Mobile Credential
Remove Selected Mobile Credentials

Or through the **[Configuration > Access Control > Mobile Access > Mobile Credentials]** page, allowing you to revoke credentials or resend invites for any credential in the system (but not allocate them).



Showing 1 to 8 of 8 entries

Configure	Card Number	Type	Linked User	Status
⚙	114	IR Mobile Access	Frederick Jones	Revoked
⚙	115	IR Mobile Access	Frederick Jones	Invitation Sent
⚙	113	IR Mobile Access	James Smith	Invitation Sent
⚙	117	IR Mobile Access	Kate Johnson	Invitation Sent
⚙	118	IR Mobile Access	Kate Johnson	Invitation Sent
⚙	119	IR Mobile Access	Kate Johnson	Invitation Sent
⚙	120	IR Mobile Access	Kate Johnson	Active
⚙	116	IR Mobile Access	Sarah Brown	Invitation Sent

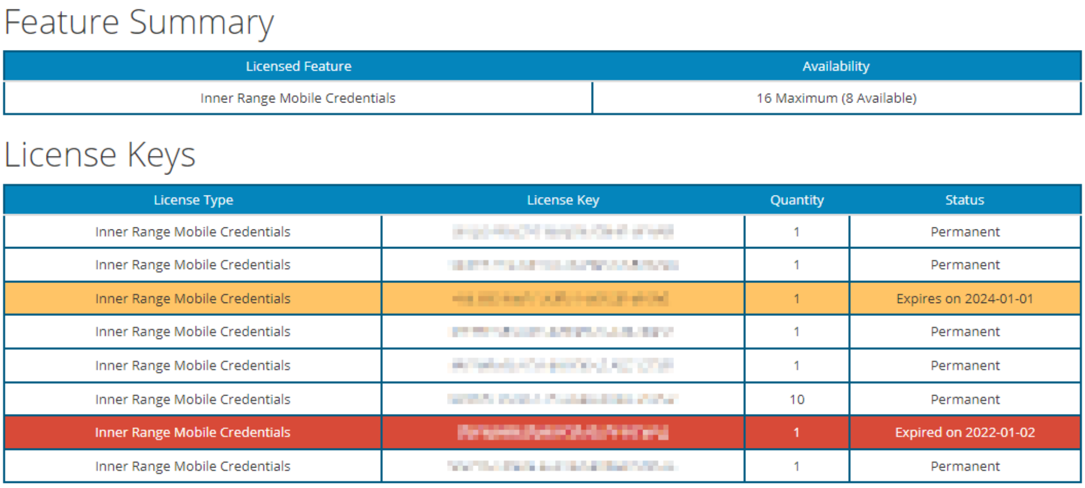
For full information on all the Mobile Access features on Inception and an overview on using other related products like the Mobile Access App or Mobile Access Reader Configuration, please refer to the *Inception Tech Guide – IR Mobile Access*, which is now available on the Inner Range website.

Inner Range Mobile Access portal: https://mobileaccess.innerrange.cloud/

License Management

With the introduction of licenses to Inception, license management has been added under **[Configuration > General > Licensing]** to allow you to view the licenses applied to the Inception system through Inner Range's licensing service. If required, this page will also allow you to trigger a manual fetching of all system licenses or to apply a license key manually.

The licensing page will summarise the features available to your Inception system based on the licenses applied to it, along with a list of all license keys and their status.



Feature Summary

Licensed Feature	Availability
Inner Range Mobile Credentials	16 Maximum (8 Available)

License Keys

License Type	License Key	Quantity	Status
Inner Range Mobile Credentials	[redacted]	1	Permanent
Inner Range Mobile Credentials	[redacted]	1	Permanent
Inner Range Mobile Credentials	[redacted]	1	Expires on 2024-01-01
Inner Range Mobile Credentials	[redacted]	1	Permanent
Inner Range Mobile Credentials	[redacted]	1	Permanent
Inner Range Mobile Credentials	[redacted]	10	Permanent
Inner Range Mobile Credentials	[redacted]	1	Expired on 2022-01-02
Inner Range Mobile Credentials	[redacted]	1	Permanent

For further information on Inner Range's licensing service and instructions on how to manage licenses, refer to the *Inception Tech Guide – Licensing* document, available on the Inner Range website. The licensing guide also includes general troubleshooting and information on handling licensing when there is no connection to the Inner Range licensing service.

Inner Range Licensing Service: https://license.innerrange.com

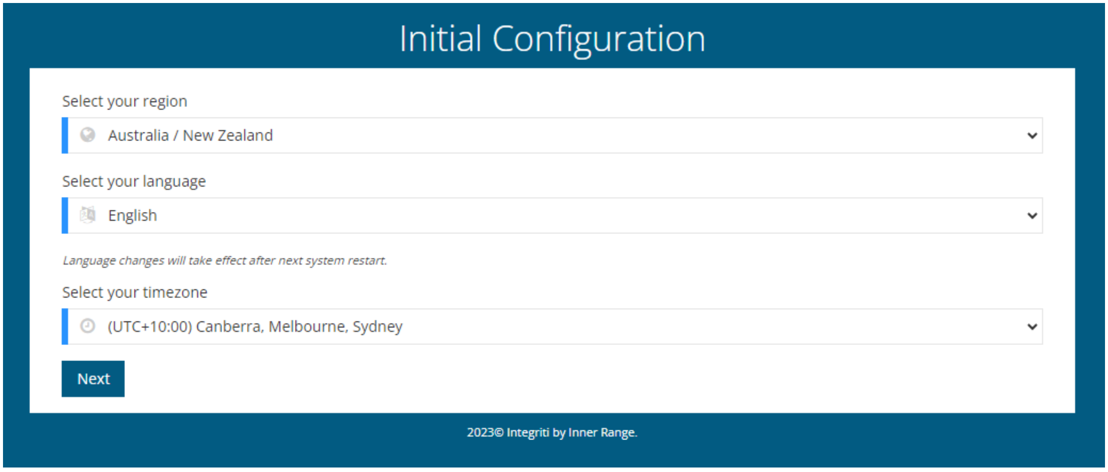
System Regions

System regions have been added to Inception which can enable region specific functionality for the Inception system, such as specific device types (either for Europe or North America), or certain reporting settings.

When accessing the web interface for the first time or when upgrading, a landing page will allow you to immediately choose the appropriate system region.

Initial Configuration Landing Page

When accessing the Inception system through the web interface either for the first time or the first time since upgrading to this firmware version, an initial configuration landing page will appear to allow you to set your system region, language, and time zone.



Select your region: Australia / New Zealand

Select your language: English

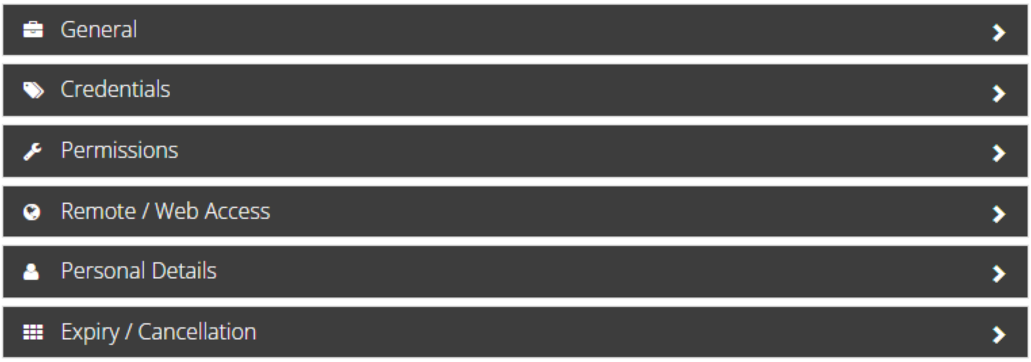
Language changes will take effect after next system restart.

Select your timezone: (UTC+10:00) Canberra, Melbourne, Sydney

Feature Updates

New User Configuration Page

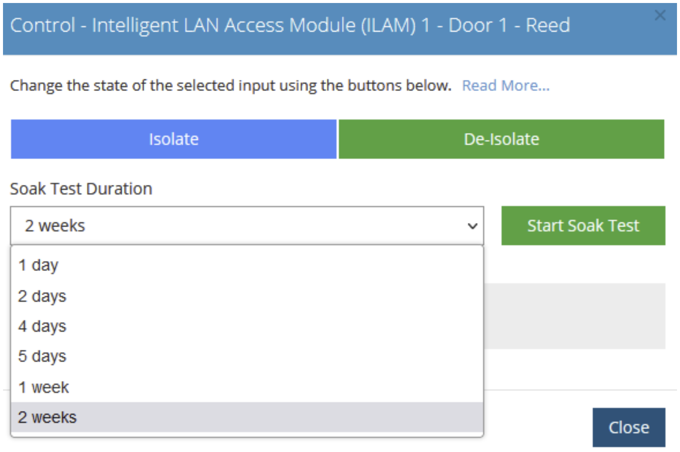
The User configuration page has now been updated with a better look and more accurate categorisations for configuring different features for that user. With the increasing complexity of user configuration, the new categories ‘Remote / Web Access’ and ‘Personal Details’ were added to make it easier to configure web login, reduce clutter of the credentials section, and allow for a more direct user configuration experience.



The guided tour to ‘Add a New User’ has been updated to match the new user configuration experience.

New Soak Test Duration

When performing soak tests, two weeks is now selectable as an option in order to meet recommended EN standards.


Control - Intelligent LAN Access Module (ILAM) 1 - Door 1 - Reed

Change the state of the selected input using the buttons below. Read More...

Soak Test Duration: 2 weeks

ILAM Offline Clash Warnings

When configuring raw cards that may clash with an existing credential template when synchronising to a connected ILAM's offline database, the system will now inform you of the clashing credential(s).

Issues Resolved

Self-Signed Certificate Expiration Resolution

Self-signed certificates that have expired will now be automatically generated and applied to the Inception with a System Message to indicate that this has happened. If the certificate was manually uploaded, there is also a warning that appears when the certificate expires.

Failure to Randomly Generate PINs

An issue has been resolved where the button to randomly generate a PIN for a user would fail if the PIN/Password Policy in Inception's System Settings had a defined maximum user PIN length over 9.

Security PIN Email

The security PIN email sent when sending user their security PIN has had unnecessary and irrelevant information removed from it to provide clarity to the recipient of the email.

Incorrect Support File Review

Fixed an issue present in 6.0.1 where support file review would fetch the events starting from 14 days ago, rather than the current time up to 14 days ago. This would cause issues where large amounts of review would start from 14 days in the past ascending.

User Duress Functionality for Onboard Readers

User duress events are now supported for onboard readers. Any readers connected directly to the Inception controller will now be able to report user duress.

Unknown Card/PIN Feedback on Invalid Auxes

Unknown credentials or PIN access at a Wiegand reader will now trigger VAL/INV feedback, in order to be consistent with OSDP reader feedback.

Duplicate LAN Module Disconnected Messages

Review messages no longer log duplicates of LAN module disconnection events.

Cyber Security Updates

2 issues have been resolved in this release.

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

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

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

Version 6.0.1

November 2023

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

Issues Resolved

SLAM/ILAM Generic Outputs Were Not Controllable

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

Last User Being Missed in ILAM Offline Review

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

Aperio Wireless Locks Not Following Free Access

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

Aperio Wireless Locks Manual Control Issues

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

Cyber Security Updates

1 cyber security issue has been resolved in this release.

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

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

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

Version 6.0.0

October 2023

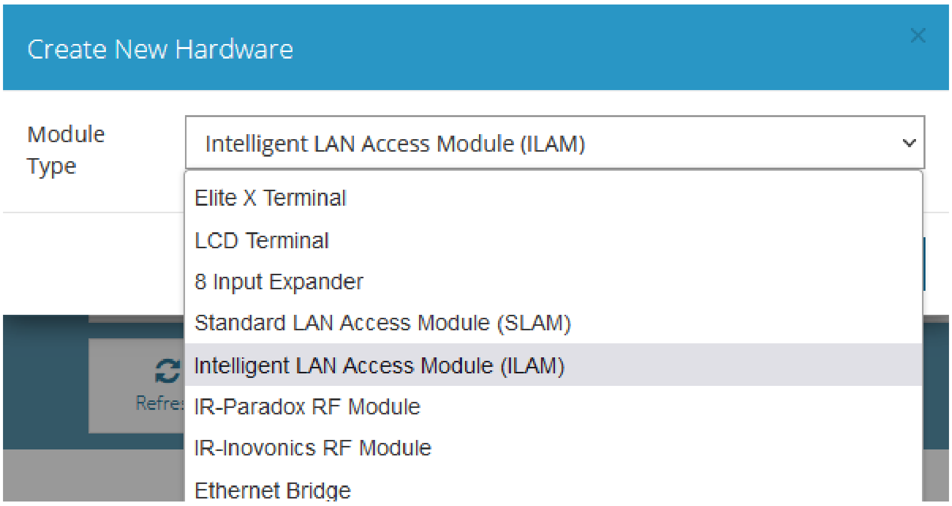
Inception 6.0.0 introduces support for the Intelligent LAN Access Module (ILAM), which includes support for offline functionality as well as integration with Aperio wireless doors. Additionally, support has been added for the inversion of the active and tamper states on hardware inputs.

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

New Features

ILAM (Intelligent LAN Access Module) Support

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


Create New Hardware

Module Type: Intelligent LAN Access Module (ILAM)

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

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

Wireless Door Support – Assa Abloy Aperio

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

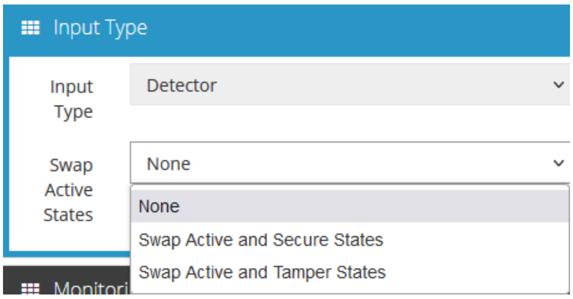
With no need to wire directly down to the door when using Aperio wireless locks, installation costs are dramatically reduced. In addition, a large range of door furniture options are available within the Aperio range to appeal to end-users and architects alike. The Inception system manages Aperio wireless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

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

Feature Updates

Swap Input Active and Tamper States

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



Input Type

Input Type: Detector

Swap Active States: None

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

Issues Resolved

Storage Blocks Stuck in Secure Pending

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

SLAM Offline REX/REN Required Powercycle

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

Cyber Security Updates

2 issues have been resolved in this release.

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

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

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

Version 5.2.0

July 2023

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

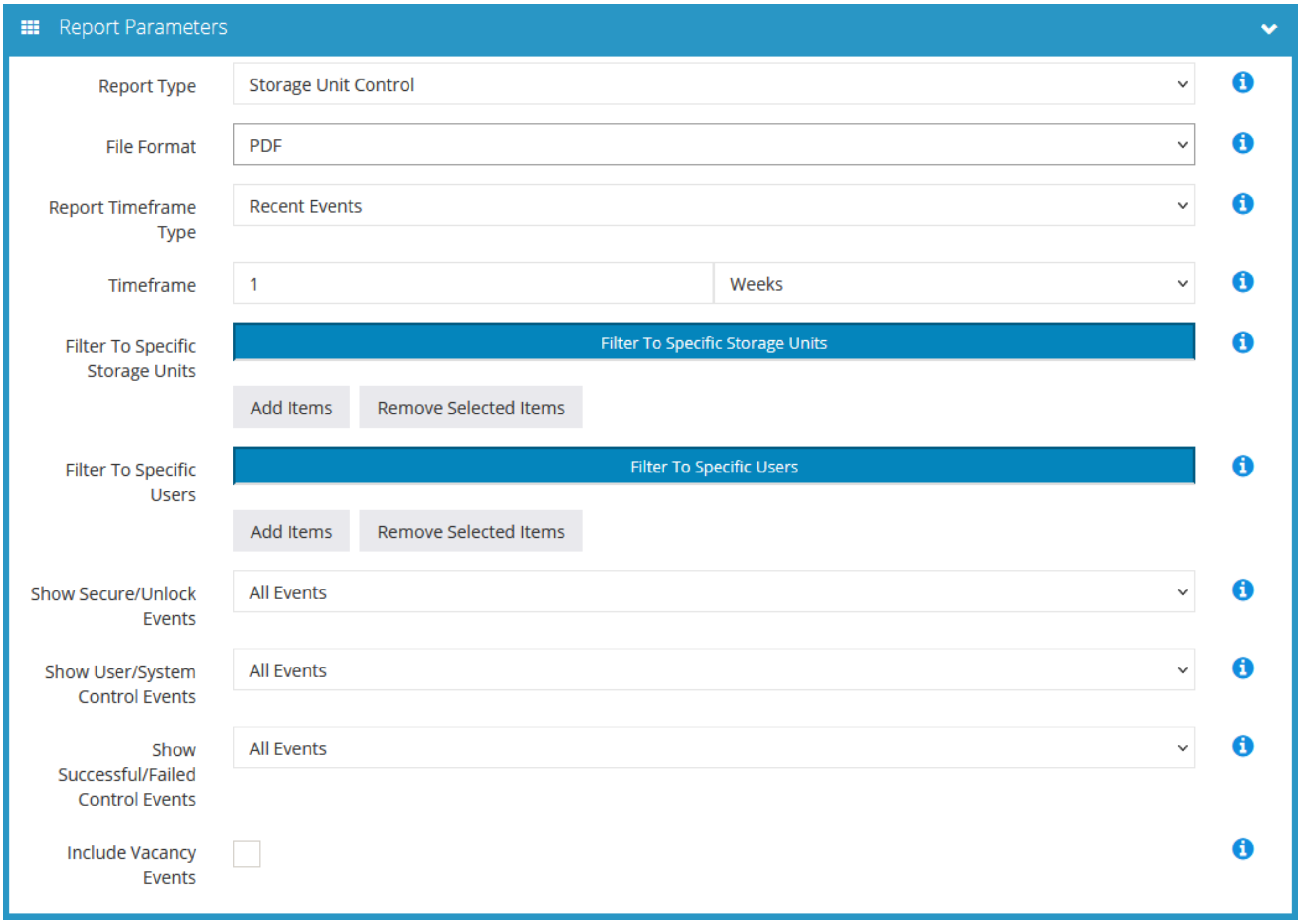
Note: The minimum firmware version for LAN Ethernet Bridge has been updated to 1.1.0, which improves connectivity between the Inception and the Ethernet Bridge.

New Features

Storage Unit Access Report

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

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



Report Parameters

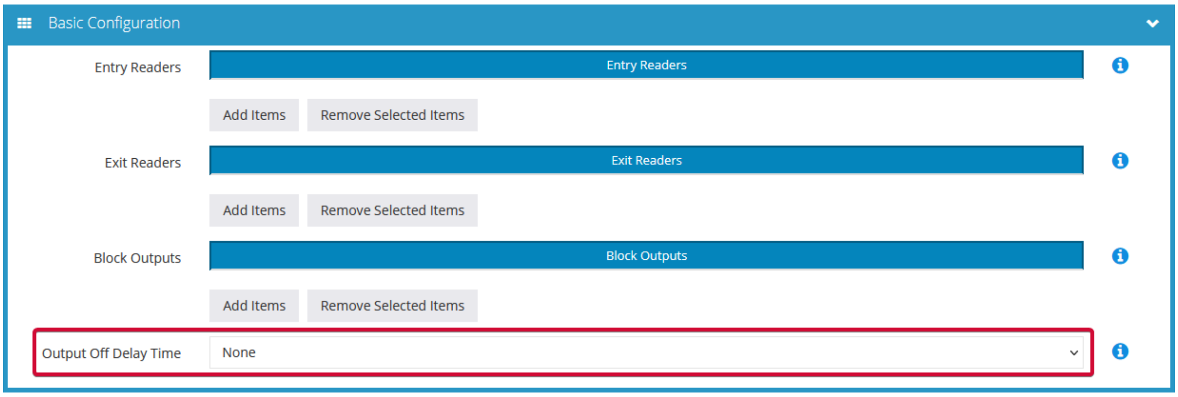
Report Type	Storage Unit Control
File Format	PDF
Report Timeframe Type	Recent Events
Timeframe	1 Weeks
Filter To Specific Storage Units	Filter To Specific Storage Units Add Items Remove Selected Items
Filter To Specific Users	Filter To Specific Users Add Items Remove Selected Items
Show Secure/Unlock Events	All Events
Show User/System Control Events	All Events
Show Successful/Failed Control Events	All Events
Include Vacancy Events	□

Feature Updates

Storage Block Delay for Output Control

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

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



Basic Configuration

Entry Readers: Entry Readers — Add Items | Remove Selected Items

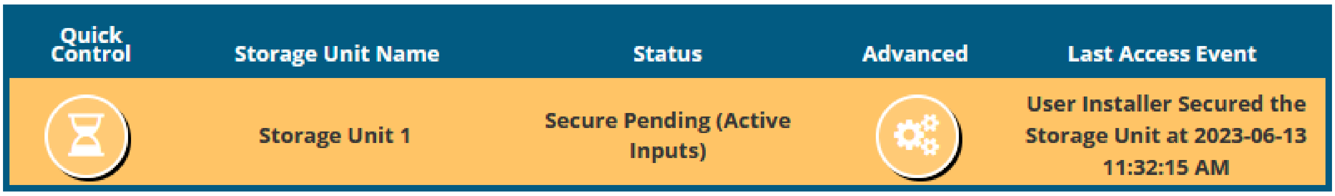
Exit Readers: Exit Readers — Add Items | Remove Selected Items

Block Outputs: Block Outputs — Add Items | Remove Selected Items

Output Off Delay Time: None

Storage Units Only Secure with No Activity

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



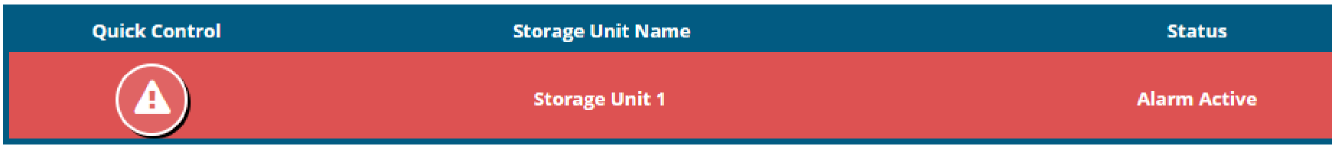
Quick Control	Storage Unit Name	Status	Advanced	Last Access Event
⌛	Storage Unit 1	Secure Pending (Active Inputs)	⚙	User Installer Secured the Storage Unit at 2023-06-13 11:32:15 AM

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

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

Storage Unit Latched Alarm State

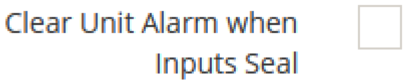
Alongside the *Secure Pending* logic implemented above, Storage Units no longer have the default behaviour of restoring back to the Secure state upon all inputs resealing. Instead, once a Storage Unit has transitioned to Alarm, it will remain in alarm until the unit is unlocked, or a new *Clear Alarms*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



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

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

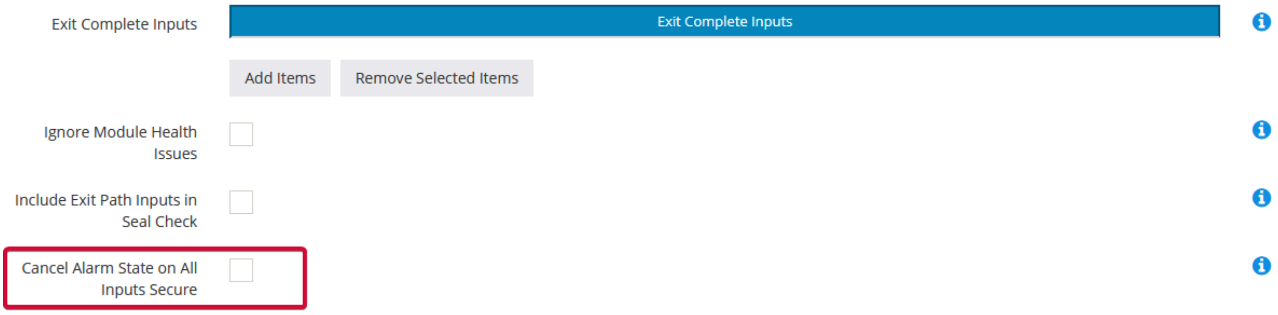
This logic can be toggled using the *Clear Unit Alarm when Inputs Seal* checkbox in the Storage Unit's parent's Storage Block configuration. When enabled, Storage Units that are handled by the Storage Block will retain old behaviour of automatically resecuring the unit upon all inputs sealing. Upon upgrading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



Clear Unit Alarm when Inputs Seal □

Area Option to Cancel Alarm on All Inputs Secure

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



Exit Complete Inputs: Exit Complete Inputs ℹ

Ignore Module Health Issues □ ℹ

Include Exit Path Inputs in Seal Check □ ℹ

Cancel Alarm State on All Inputs Secure □ ℹ

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

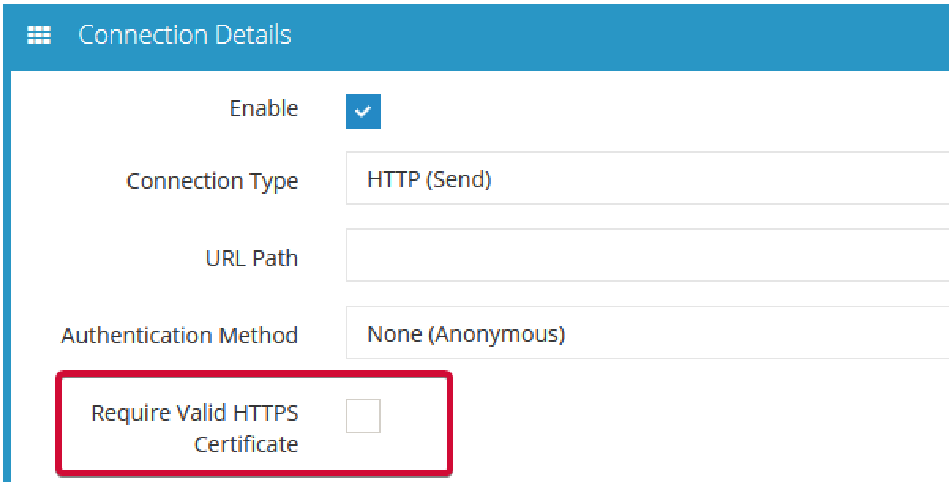
For example, when the calculated input of a Storage Unit this Area is monitoring moves into alarm, the Area will respond according to the input's process group, potentially moving the area into the alarm state, sending an event to the monitoring station, and triggering the appropriate sirens and strobes.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

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

Invalid Certificate HTTPS Support for HTTP Send Connection

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

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



Connection Details

Enable ☑

Connection Type: HTTP (Send)

URL Path:

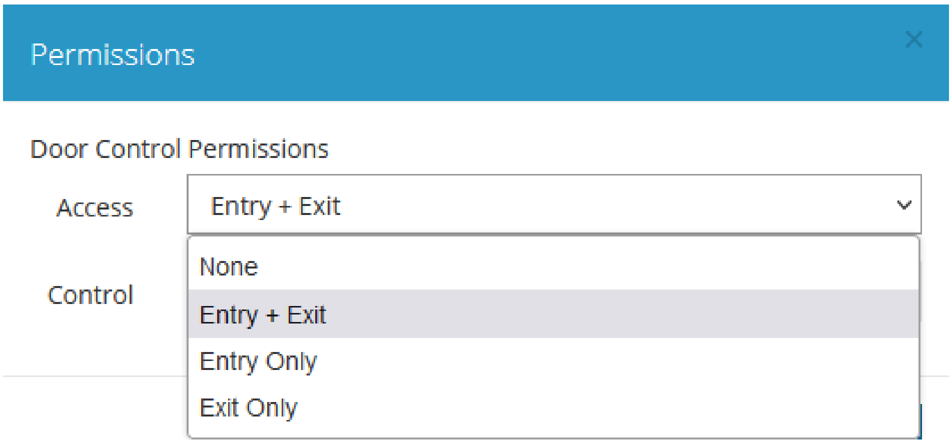
Authentication Method: None (Anonymous)

Require Valid HTTPS Certificate ☐

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

Separate Door Permissions for Entry vs Exit

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



Permissions

Door Control Permissions

Access: Entry + Exit

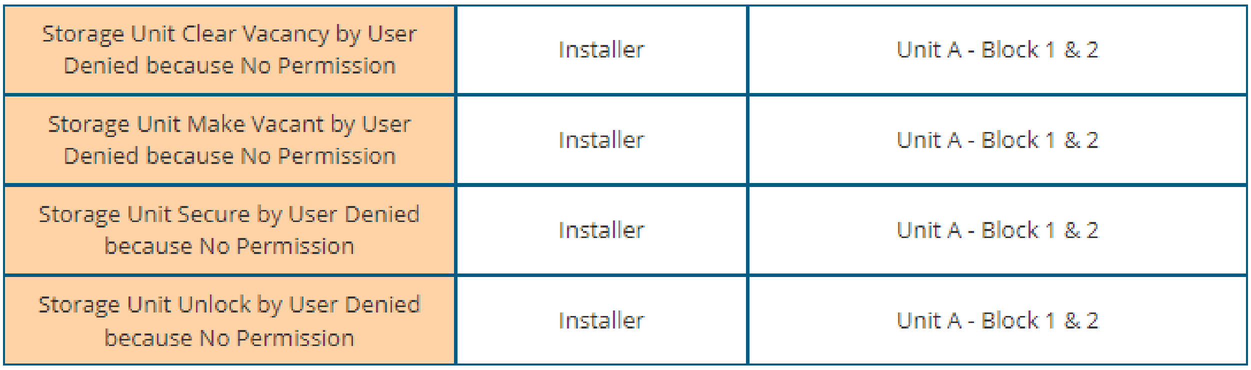
This allows for greater flexibility when configuring access through a door, as it allows for the configuration of *Entry* only permissions to a door without *Exit* permission, or vice versa. Alternatively, this more granular control could then allow the configuration of *Entry* permissions to be set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

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

Issues Resolved

No Review for Storage Unit Failed Control

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



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

Ethernet Bridge Connection Reliablity

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

Version 5.1.2

June 2023

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

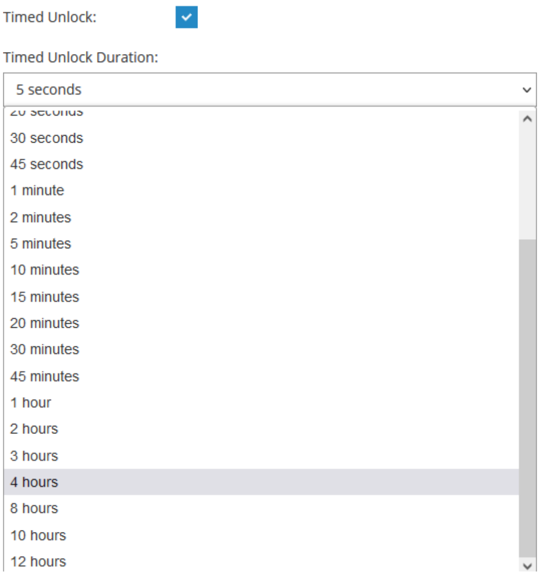
Note: The minimum firmware version for Standard LAN Access Modules (SLAMs) has been updated to 4.0.7 due to updates to support additional card packets.

Feature Updates

Door Control Timed Unlock Options

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

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



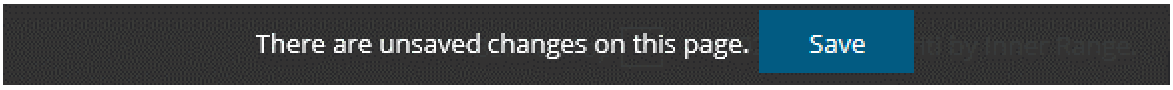
Timed Unlock: ☑

Timed Unlock Duration: 5 seconds

Floating Save Button

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

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



There are unsaved changes on this page.

Issues Resolved

History Reports in Negative UTC Timezones

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

Storage Block Time Values

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

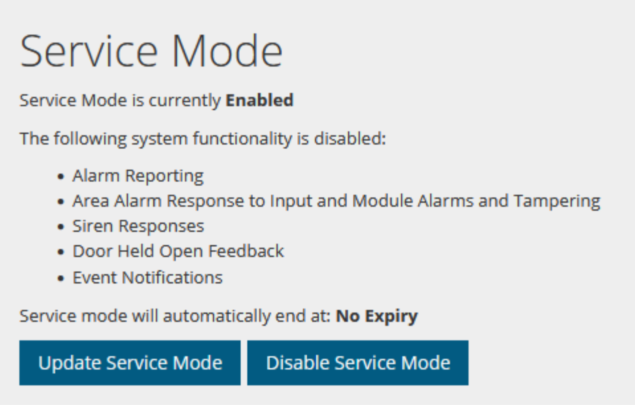
This was to resolve an issue where storage units would instead go immediately into the "Unlocked Too Long" state upon unlocking a unit, or immediately be resecured upon being unlocked, opened then closed.

WiFi Hotspot Reliability

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

Service Mode Feature Text

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



Service Mode

Service Mode is currently **Enabled**

The following system functionality is disabled:

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

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

Version 5.1.1

January 2023

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

Issues Resolved

Date and Time UI Issues

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

Time Period Editing

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

Version 5.1.0

November 2022

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

New Features

French Canadian Translation

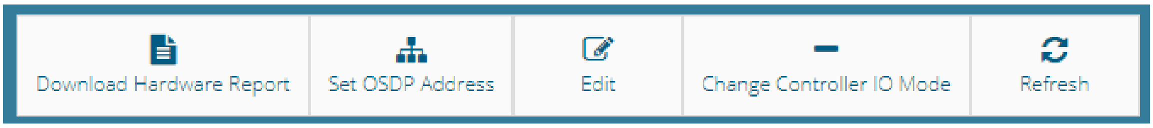
A vendor-supplied French Canadian language pack has been added to Inception and can be chosen when selecting a language pack to use.

Feature Updates

OSDP Address Change Option

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

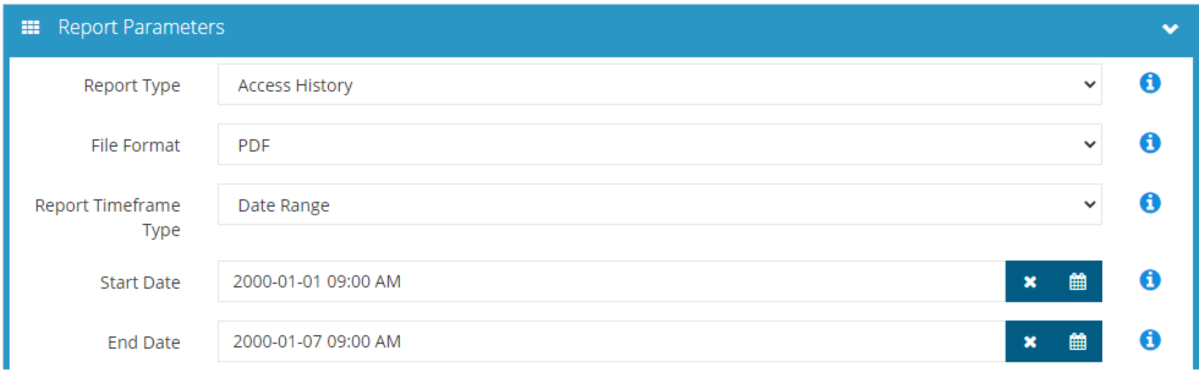
This feature can be used to resolve address clashing by having one of the clashing address readers connected at a time and re-addressing it (if there are multiple readers still connected with the same address, the re-addressing command sent by Inception will not function).



Custom Time Range for Reports

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

Reports generated through Scheduled Tasks will also have this functionality.

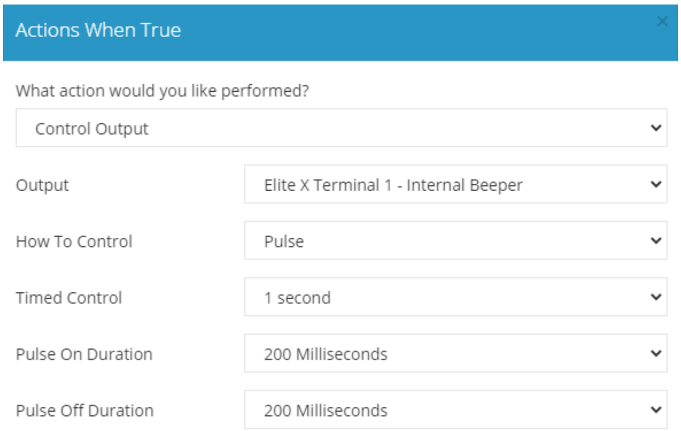


Report Parameters

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

Pulsed Output Control for Automated Actions

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



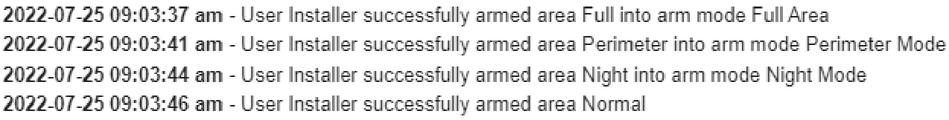
Actions When True

What action would you like performed?
Control Output

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

Multi-Mode Area Arm Notifications

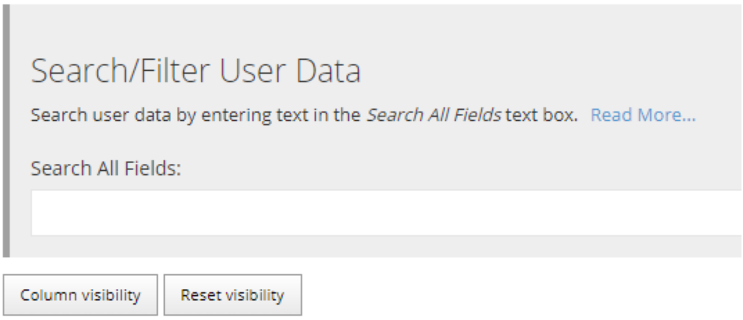
Whenever an area is armed and sends a notification, if multi-mode arming is enabled, the arm mode will now be included in the notification event text.



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

Persistence of Search Users Page Layout

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



Search/Filter User Data

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

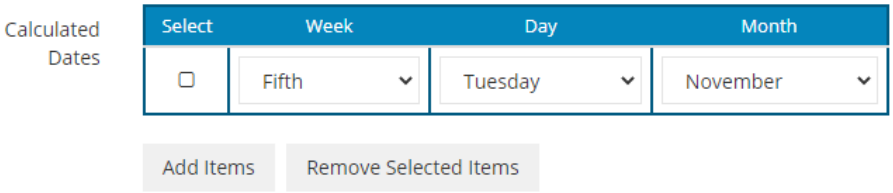
Search All Fields:

REST API – Door Denied Access in User Info Monitoring

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

Calendar “Fifth” Week Option

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



Calculated Dates

Select	Week	Day	Month
☐	Fifth	Tuesday	November

Issues Resolved

Browser Performance (Large Permission Groups)

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

LAN Ethernet Bridge Connectivity

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

Missing Items in Configuration Report

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

OSDP readers with Duplicate Serial Numbers

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

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

Ctrl+S Save Shortcut

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

Send PIN for Duress User

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

Version 5.0.1

August 2022

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

Issues Resolved

Temporary Disarm could Fully Disarm Area

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

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

Permissions Limited to 1000

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

OSDP / SIFER Reader Periodic Reconnection

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

Completed Battery Tests Trigger Item Changed Event

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

Module State Does Not Persist Over Power Cycles

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

Version 5.0.0

July 2022

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

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

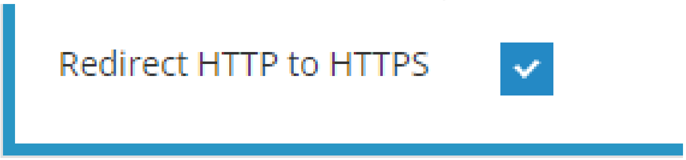
New Features

Local HTTPS Support

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

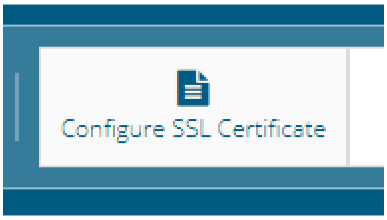
HTTPS web access is enabled by default with this firmware version, and can be navigated to via IP address (https://[ip.address]) or https://[InceptionSerialNumber].local/ in a web browser (where [InceptionSerialNumber] is replaced with your controller's serial number). Inception comes with a self-signed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

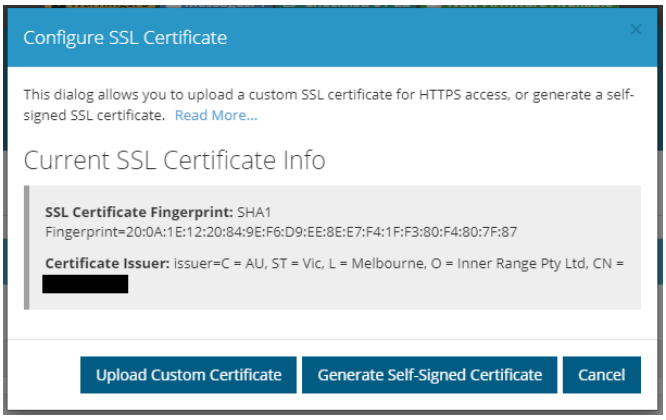
HTTP access can be disabled by selecting the *Redirect HTTP to HTTPS* option on the **[Configuration > General > Network]** page in the Advanced section. This will cause all HTTP requests to be redirected to HTTPS for increased security of web traffic. Note that this feature will also affect the Inception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



Redirect HTTP to HTTPS ☑

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





Configure SSL Certificate

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

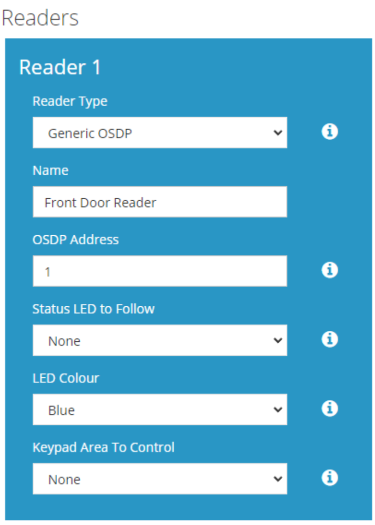
Current SSL Certificate Info

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

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

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

OSDP Reader Support



Readers

Reader 1

Reader Type: Generic OSDP

Name: Front Door Reader

OSDP Address: 1

Status LED to Follow: None

LED Colour: Blue

Keypad Area To Control: None

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

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

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

1024 Inputs and Outputs

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

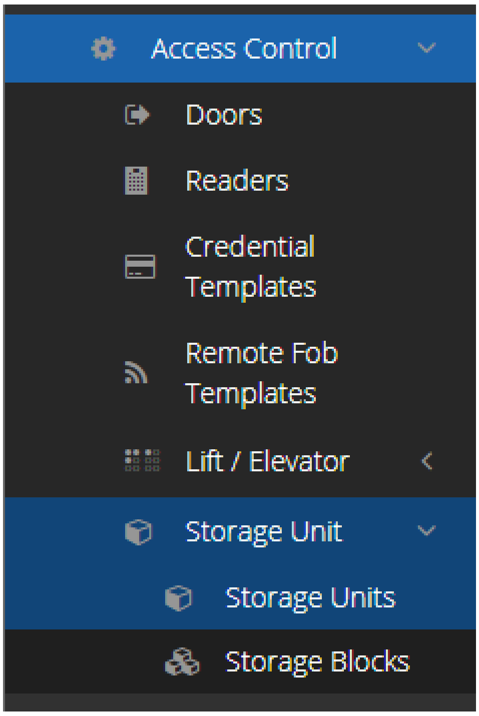
Note that for ContactID alarm reporting, total input counts above 512 will all report as point ID 999. IRFast can be used for those systems to ensure individually identifiable reporting points.

Storage Units

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

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

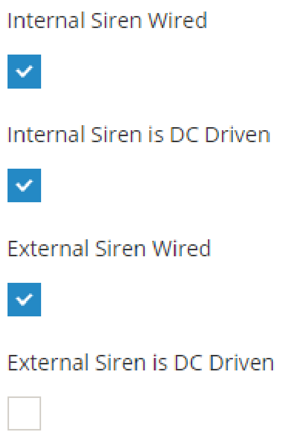
Storage blocks define a group of units and could represent a whole site, a building, or a section of a building. An access request to a block by a customer via PIN or Card would unlock their unit, automatically securing their unit when they exit. They also allow simpler management of automation, controling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



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

DC Siren Support

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



Internal Siren Wired

☑

Internal Siren is DC Driven

☑

External Siren Wired

☑

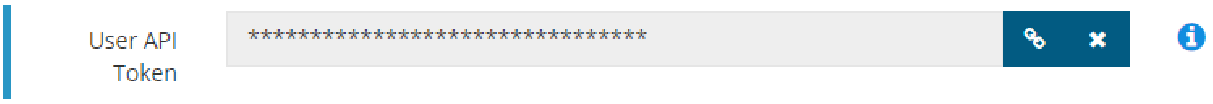
External Siren is DC Driven

☐

REST API – User API Tokens

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

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

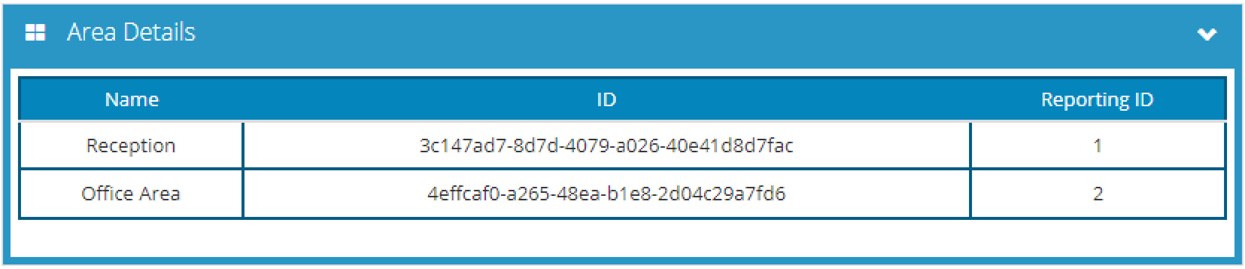


User API Token: ********************************

REST API – API Details Page

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

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



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

REST API – SkyCommand User Linking

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

REST API – Reader Names

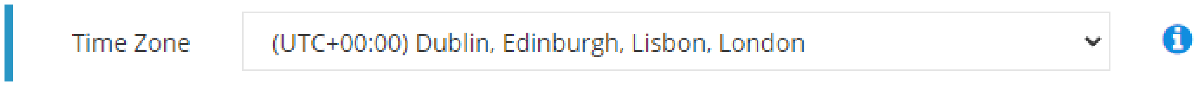
API requests that return a DoorAttachedReader such as Door Summary or Get Door's Associated Reader will now also include the Name property of those readers.

Feature Updates

Time Zone Display

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

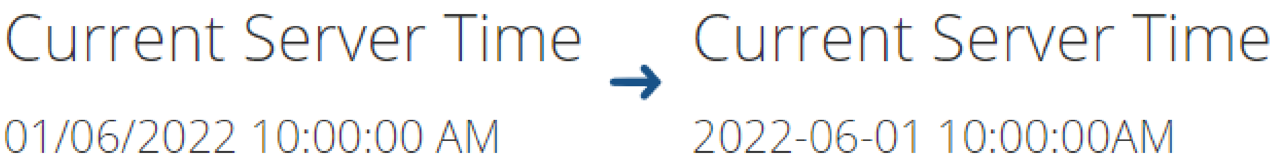
Redundant time zone listings have also been updated and grouped into their respective time zones according to the new time zone names.



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

Time and Date Format

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



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

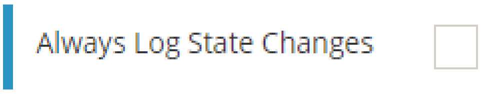
→

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

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

Input State Change Review

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

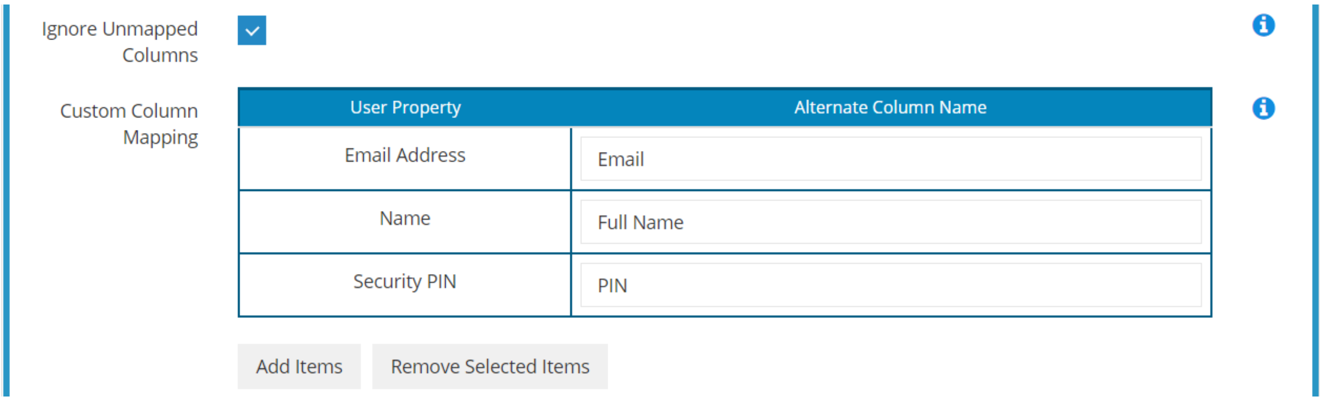


Always Log State Changes □

DUIM (Dynamic User Import Module) Custom Column Headers

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

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



Ignore Unmapped Columns ☑

Custom Column Mapping

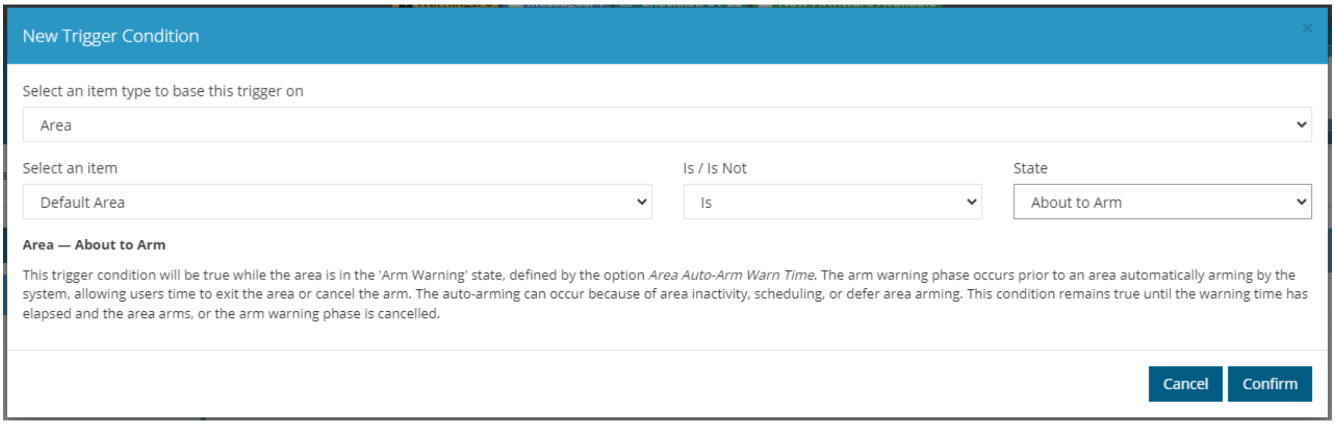
User Property	Alternate Column Name
Email Address	Email
Name	Full Name
Security PIN	PIN

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

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

Automated Action Trigger Help Text

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



New Trigger Condition

Select an item type to base this trigger on: Area

Select an item: Default Area

Is / Is Not: Is

State: About to Arm

Area — About to Arm

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

Password Display

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

Web Login No Longer Needed for SkyCommand App Control

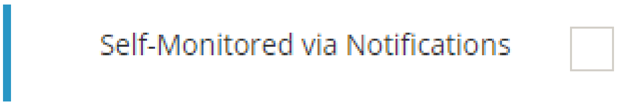
For a User to control and receive push notifications for their Inception system via the SkyCommand App, they previously needed to have Web Login details configured as well. If the User never used the web interface and only required App control, this meant there would be unnecessary username and password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

Issues Resolved

Self-Monitoring Review Events

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

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



Self-Monitored via Notifications ☐

TLS 1.2 Support

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

Checkboxes on Mobile Devices

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

Item Duplication and Password Fields

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

inner range

Global Headquarters

Inner Range Australia

+61 3 9780 4300
anz@innerrange.com

Inner Range United States

+1 (844) 588-0874
usa@innerrange.com

Inner Range United Kingdom

+44 (0) 845 470 5000
uk@innerrange.com

Inner Range Canada

+1 (905) 568-8999
canada@innerrange.com

Inner Range Middle East

+971 4 8067100
middleeast@innerrange.com

Inner Range India

+91 80 4070 3333
asia@innerrange.com

INNERRANGE.COM

January 2025
The specifications and descriptions of products and services contained in this document were correct at the time of publishing.
Inner Range reserves the right to change specifications or withdraw products without notice.