



UNIFIED VIDEO, ACCESS & SECURITY SYSTEMS



INTEGRITI

Release Notes 26.0

May 2026

INNERRANGE.COM

Contents

INTEGRITI

Contents	
Contents	2
Version 26.0	3
Version 25.2.1 Bug-Fix	11
Version 25.2.0	12
Version 25.1.1 Bug-Fix	18
Version 25.1.0	19
Version 25.0.0	24
Version 24.0.1 Bug-Fix	32
Version 24.0.0	33
Contact	47

Version 26.0

May 2026

OSDP Reader Text Support

For Integrity Version 26.0, a new OSDP Reader Text control option has been developed. This allows control of displayed text on readers supporting this functionality, that have been tested by Inner Range (see Controller Release Notes for tested reader models).

Simple LED and Beep patterns can convey a bare minimal level of meaning - both of which require prior knowledge of the site in order to be fully understood.

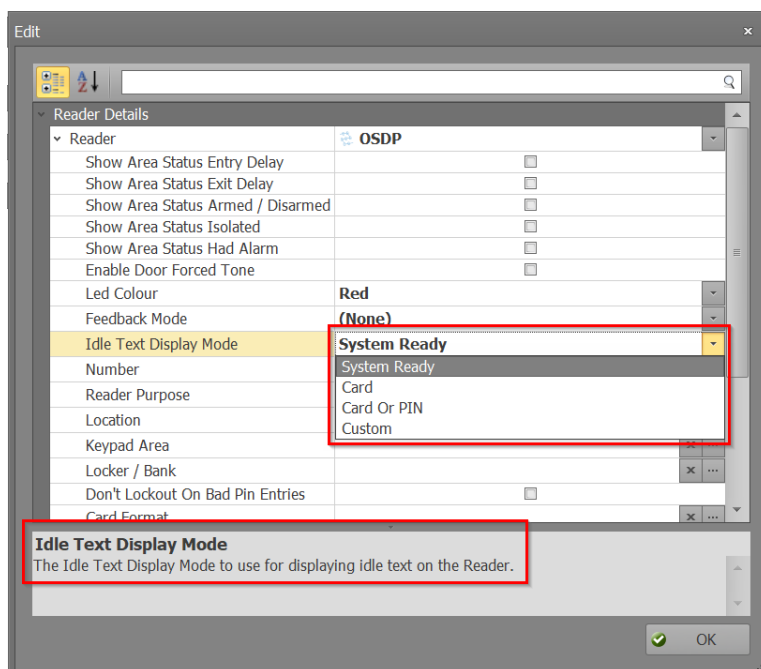
For sites with compatible readers, this new ability to display detailed information to users at individual doors now extends well beyond the traditional reader feedback mechanisms.

By adding text, users at a door may now be presented with precise information related to (for example):

- A **current** individual door state to expand on existing functionality - "Locked", "Unlocked", "Override"
- A **future** door state - "This door will lock at 10PM Daily"
- **Temporary** states - "Door in lockdown!"
- **Emergency** states - "Evacuation in Progress - Entry Denied!"
- **High Security** options - "Dual User Access Only"
- **Multifactor** options - "Present Card then enter PIN"
- **Custom** room functions - "Room Under Hire - Access Restricted"

The total number of custom messages that can be pre-programmed is only limited to the number of LCD Messages a single controller can hold.

Editing what a single door's reader will display can be done via the relevant door's reader settings:



Version 26.0

INTEGRITI

For system integrators that do not require extensive configuration options, readers may be individually configured to have one of many pre-defined text messages displayed to simply match the mode of the reader (Card, Card or Pin, System Ready). To display more customized messages similar to the examples above, the message can be sourced from preconfigured LCD messages instead.

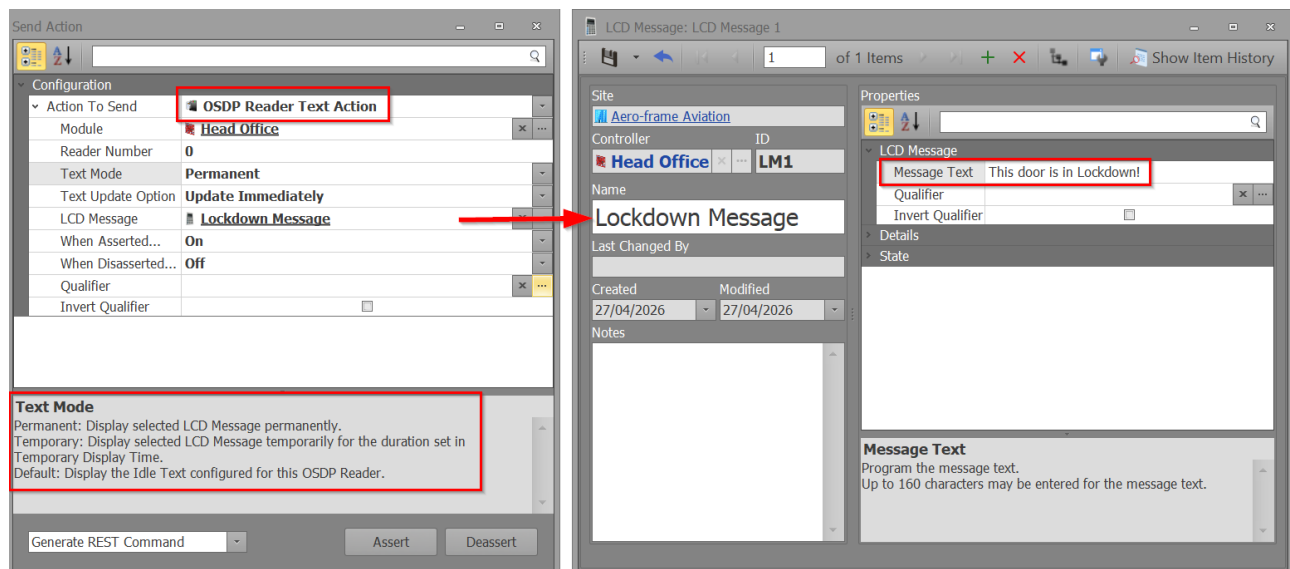
(Requires Integrity Controller Firmware V26.0 or later.)

OSDP Reader Text Controller Action

To allow more granular use of the text display option above, a separate Controller Action has been created to allow dynamic control of a specific reader's display text for automation purposes.

Pre-defined messages are created within standard LCD Messages, and the Action defines several parameters that allow some flexibility of *when* to display the custom text, and for *how long*.

Help Text assists with explaining the various functions supported:



Version 26.0

INTEGRITI

Schindler PORT Integration

Schindler PORT Gateway V1.0: V26.0 now supports the new Schindler PORT protocol via their API V1.0 Gateway for all **new** Inner Range Professional Services Lift HLI deployments. The new PORT protocol is also fully backward compatible with the legacy PORT ID (PORT Technology v1.3.376.1) integration.

Comparison of features:

Administration	Administer Users, Permissions & credentials seamlessly within Integriti.	Legacy Port ID
Floors Status	View Floor State and determine if a floor has been overridden or is following a Time Schedule.	API v1.0 Gateway
Floor Control	Operators can manually override floor(s) if they suddenly need to lock or unlock floor(s). Operators can restore floor(s) back to their last known state if a floor was overridden manually.	API v1.0 Gateway
Access Profiles	Operators have the freedom to program and issue Access Profile permissions without needing to contact Schindler	API v1.0 Gateway
Floor Scheduling	Operators can program floor schedules for unlocking/locking floors between certain times.	Legacy Port ID
Special Operating Mode	Operators can distribute custom Special Operating Modes that trigger automation within Schindler PORT.	API v1.0 Gateway
Access Control Readers	We can nominate any Access Control reader(s) (i.e. QR Code, High/Low Frequency, encrypted etc) to interface directly with the Schindler PORT integration.	API v1.0 Gateway
Receive feedback	Operators can view real time feedback when users present a credential and select a destination floor.	Legacy Port ID
Command	Operators can trigger custom commands from Integriti that trigger actions within Schindler. A great example is the Emergency Lockdown command	API v1.0 Gateway

Version 26.0

INTEGRITI

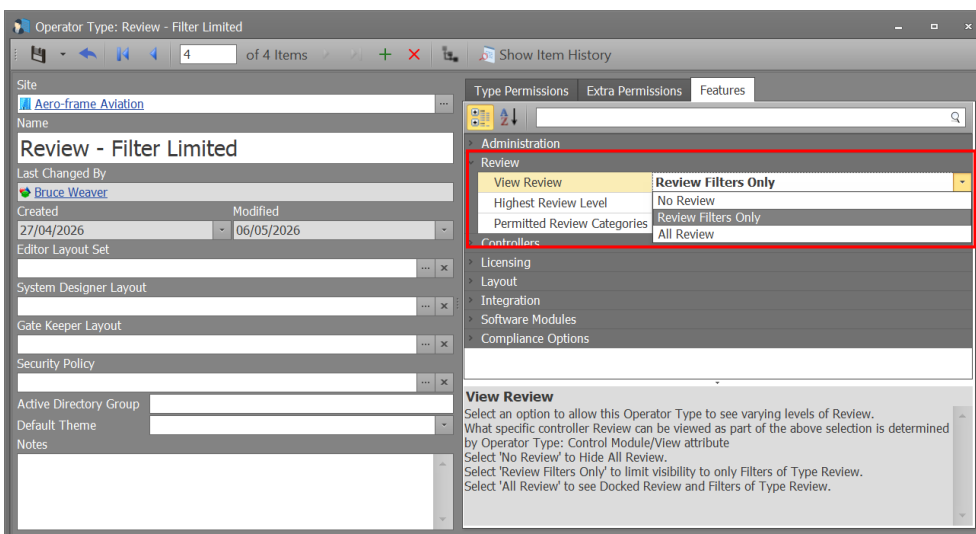
Floor states and status messages are now fully populated and descriptive, and floor actions now support the “Restore” function:

ID	Name	Status	Controlling Time Pattern	Notes
Type	Type here to search...	Type here to search...	Type here to search...	Type here to search...
LF1	LR Level B1 - (LR B1)	Secure (Unexpected)	LR Free B1	Imported from Schindler
LF2	LR Ground + LR Turnstile Entry - (LR G)	Secure (Unexpected)	LR Free G	Imported from Schindler
LF3	LR Level 1 - (1)	Secure (Unexpected)	LR Free 1	Imported from Schindler
LF4	LR Level 2 - (2)	Free (Unexpected)	LR Free 2	Imported from Schindler
LF5	LR Level 3 - (3)	Secure (Forced)	LR Free 3	
LF6	LR Level 4 - (4)	Free (Forced)	LR Free 4	
LF7	LR Level 5 - (LR 5)	Free (Unexpected)	LR Free 5	
LF8	HR Level 6 - (6)	Free (Timed)	HR Free 6	
LF9	HR Level 7 - (7)	Free (Timed)	HR Free 7	
LF10	HR Level 8 - (8)	Free (Timed)	HR Free 8	
LF11	HR Level 9 - (9)	Free (Timed)	HR Free 9	
LF12	HR Level 10 - (10)	Free (Timed)	HR Free 10	
LF13	HR Level B1 - (HR B1)	Free (Timed)	HR Free B1	
LF14	HR Ground + HR Turnstile Entry - (HR G)	Free (Timed)	HR Free G	
LF15	HR Level 5 - (HR 5)	Free (Timed)	HR Free 5	
LF16	LR Turnstile Exit - (LR Turnstile Exit)			
LF17	HR Ground Rear - (HR G)	Free (Timed)	HR Free G	
LF18	HR Level 5 Rear - (HR 5 Rear)	Free (Timed)	HR Free 5	
LF19	HR Turnstile Exit - (HR Turnstile Exit)			

For existing customers wishing to leverage any new Schindler features above, please contact Inner Range Professional Services and Schindler for further information.

Operator Type Option – Review Filters Only

Previous versions of Integrati only allowed *absolute* control of whether Review was available to an Operator or not – via a simple checkbox. This checkbox has been removed and replaced with a menu to select from three possible total options, which now includes a new option – **Review Filters Only**:



Version 26.0

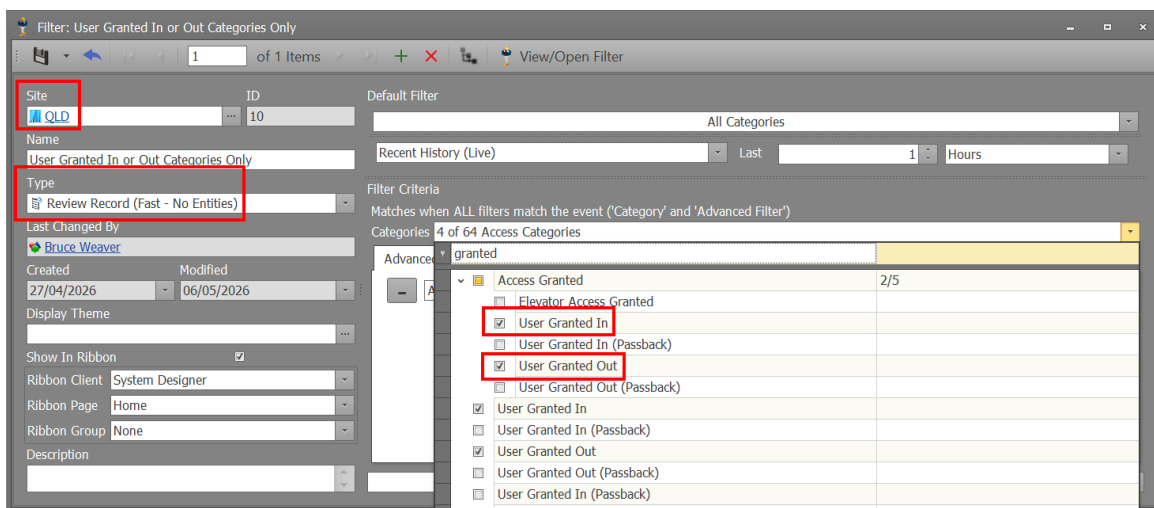
INTEGRITI

The existing “No Review” and “All Review” options behave exactly as before.

The new “Review Filters Only” option will permit Review to be viewable based on pre-defined Review Filters that the Operator has permission to view (based on their Operator Type permissions). Only Filters of type “Review Record” are permitted.

The new feature now allows more granular control of **what** an Operator is allowed to see, without fully exposing **All Review** to the Operator. This can be extremely useful when there is a need to notify Operators of specific granular activity (*particular* door access, area activity, Integration information), without those Operators seeing All Review that may be classified as sensitive.

The rules for what the Operator can see when this new feature is used now depends on the existing granular control already available with the Filter itself:



When the pre-defined filter is subsequently viewed, only Review that is related to the filter logic will be displayed - which will be limited to both the filter logic, and controllers (Control Modules) that the Operator Type allows permission to view:

User Granted In or Out Categories Only (Showing 2)			
Source	Text	Categories	All Categories
Period	Recent History (Live)	Last	1 Hours
Local Time	Source	Text	Category
06/05/2026 1:53:47 PM	Head Office	Unknown User Button Access at <C01:Butt2> out of Front Door	User Granted Out
06/05/2026 1:53:42 PM	Head Office	Unknown User Button Access at <C01:Butt2> out of Front Door	User Granted Out

To use this new feature, an Operator must have (within their Operator Type):

- Ability to view the **specific filter/s** based on the filter's **Site**:

Ability to View the specific items based on the role & site.

Type Permissions						
Extra Permissions Features						
Site Permissions						
Group	View	Edit	Add Sub Site	Add Keyword	Delete	
 Aero-frame Aviation	☒	☒	☒	☒	☐	
▼  NSW	☒	☒	☒	☒	☐	
 Sydney Branch 201	☒	☒	☒	☒	☐	
 Ermington Branch 202	☒	☒	☒	☒	☐	
▼  QLD	☒	☒	☒	☒	☐	
 Brisbane Branch 701	☒	☒	☒	☒	☐	
 Inala Branch 702	☒	☒	☒	☒	☐	
....						
Entity Type Permissions						
Name	View	Edit	Create	Delete		
▼ 	☐	☐	☐	☐		
 Door	☐	☐	☐	☐		
 Door List	☐	☐	☐	☐		
 Dormakaba Controller	☐	☐	☐	☐		
 Filter	☒	☐	☐	☐		
 Holiday	☐	☐	☐	☐		
 Input	☐	☐	☐	☐		

- Permission to view **Control Modules** for each relevant **Site** they wish to have Review content exposed *via* the filter:

Type Permissions

Extra Permissions

Features

Site Permissions

Group	View	Edit	Add Sub Site	Add Keyword	Delete
Aero-frame Aviation	☒	☒	☒	☒	☐
NSW	☒	☒	☒	☒	☐
Sydney Branch 201	☒	☒	☒	☒	☐
Ermington Branch 202	☒	☒	☒	☒	☐
QLD	☒	☒	☒	☒	☐
Brisbane Branch 701	☒	☒	☒	☒	☐
Inala Branch 702	☒	☒	☒	☒	☐

Entity Type Permissions

Name	View	Edit	Create	Delete
c	☐	☐	☐	☐
Lifts	☐	☐	☐	☐
Automation	☐	☐	☐	☐
Hardware	☐	☐	☐	☐
Auxiliary	☐	☐	☐	☐
Control Module	☒	☐	☐	☐
Ethernet Bridge	☐	☐	☐	☐
Expander Module	☐	☐	☐	☐
Graphic Terminal	☐	☐	☐	☐
Input	☐	☐	☐	☐

- “View Review” set to “Review Filters Only” within their Operator Type Features tab.

To restrict access to “All Review” from this Filter Review stream, the “Investigate Event in All Review” option has been removed from the context menu for users who have “Review Filters Only” selected in their Operator Type.

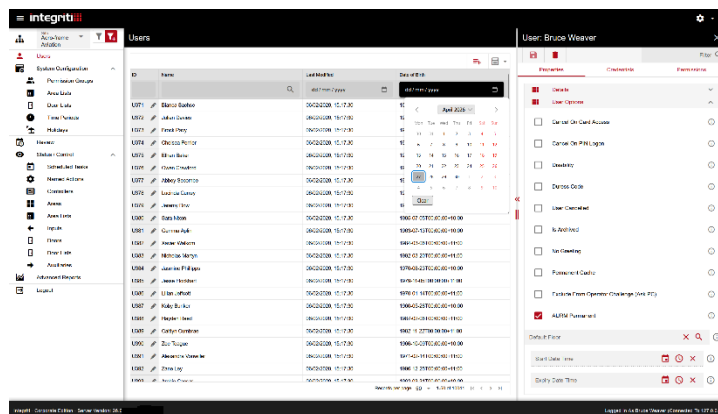
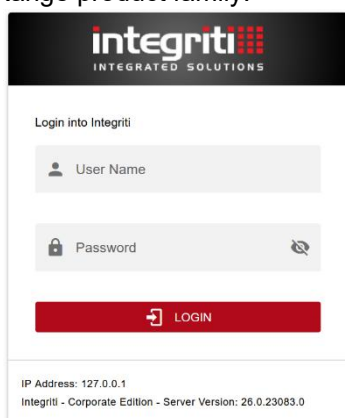
Note: Care should be taken in assigning additional **Create** or **Edit** permissions within Operator Types when using this new feature, as an operator with these extra permissions could create/edit their own filter that has essentially no restrictions.

Version 26.0

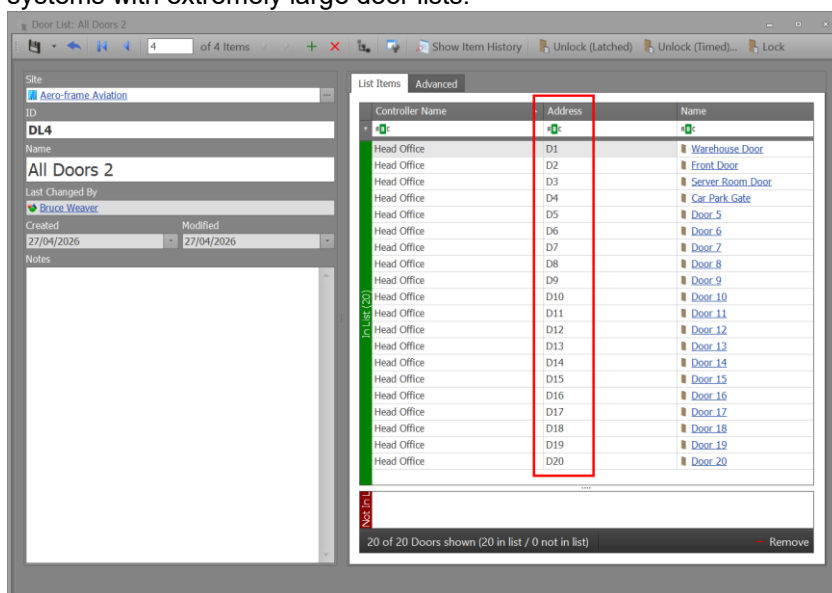
INTEGRITI

Improvements

- **MSSQL 2025 Support:** Integrity V26.0 has now been tested against and formally supports **MSSQL 2025**.
- **Export Review Performance:** When loading large amounts of review (~one million records), on some large systems, the user interface would appear to lock up before eventually displaying the progress bar and offering export options to the user. This has been significantly improved.
- **Show Item History:** Increased performance for larger systems opening the Show Item History dialog and selecting an audit entry from the Audit History list.
- **Web Client Theme:** The web client interface has been re-themed to match that of the greater Inner Range product family:



- **Improvements to REST API v2 interface:**
 - Ability to query user location
 - Updates to online documentation
- **Door List ID Ordering:** Door lists now use “natural” sort order based on the numerical component of the ID number, instead of alphanumeric (lexicographical) sort. This improves visual searching for systems with extremely large door lists:



- **Database Cleanup Purge Help Text:** Updated purge help text to be more descriptive of the actions being executed per purge option.

Version 26.0

INTEGRITI

Issues Resolved

- Fixed issue where suspended credential review was visible to all operators regardless of operator type permission.
- Removed ability for an operator to access Server Instances via System Warnings, unless the operator has specific permission to view Server Instances within their operator type permissions.
- Resolved issue where QR credentials could not be automatically generated or revoked via use of filter rules.
- Fixed issue within Export CCTV Footage Dialog which resulted in custom file name and format string editor not being preserved.
- Added GUI limitation within Time Period editor to ensure adding more than the permissible number (16) is no longer accidentally possible per Time Period.
- Added missing help text for Emergency Override function within Send Action/Control Door.
- Resolved behaviour where a map would fail to zoom in to a related entity on first being opened, unless the map was already open.
- Resolved issue where the Database Configuration Tool launched from IntegritiCS would use the "Integriti" registry entry, instead of the correct "IntegritiCS" entry.
- Resolved "Duplicate Error" message within APIv2 when using AddToCollection function.
- Added missing Site Information values when requesting APIv2 controller entities.
- Resolved issue with APIv2 not returning results from XML_ControlAsync command immediately.
- Resolved Operator Auth issue with Auth0 provider due to trailing character.

Documentation

- Hardware and Software Prerequisites: Updated the MS SQL versions supported by Integriti.

Version 25.2.1 Bug-Fix

Version 25.2.1 Bug-Fix

May 2026

Issues Resolved

Controller Sync: Fixed an intermittent issue where entity sync between controller and the software does not always resolve on some systems.

Version 25.2.0

December 2025

OSDP Reader LED Action

For Integrity version 25.2.0, a new Reader LED Action has been introduced, which lets you control the LEDs of SIFER and OSDP readers.

Note that this requires firmware version 25.2.0 and above.

The screenshot shows the 'Send Action' dialog box with the following configuration:

Configuration	
Action To Send	OSDP Reader LED Action
Module	New Controller (AC005383)
Reader Number	1
LED On Colour	Green
LED Off Colour	Amber
Duration	0 hours 00 mins 05 secs
Flash On Period	00.0 secs
Flash Off Period	00.0 secs
Permanent	☐
LED Index	0
When Asserted...	On
When Disasserted...	Off
Qualifier	
Invert Qualifier	☐

Duration
Total Temporary flash period before reverting to permanent settings (ignored for Permanent Actions)

Generate REST Command [dropdown] [Assert] [Deassert]

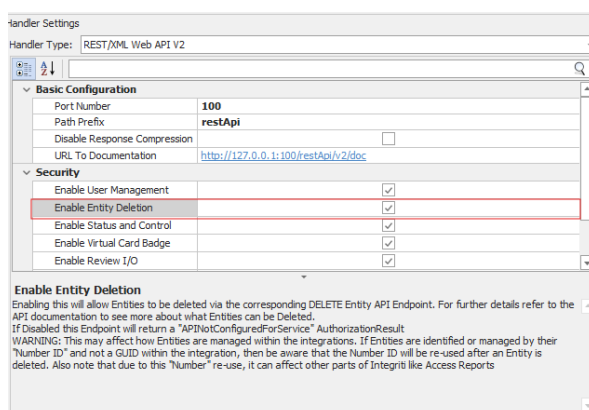
To control the LEDs of the Reader, first select the Module to which the Reader is connected to and enter the Reader Number that you want to send the LED action. Specify the LED On and Off Colour which will be used for setting the colour of the LED. The LED Off Colour is used when Flash On and Off Period is specified. If Flash On and Off Period are specified, the colour of the LED will cycle between the LED On and Off Colours. Use LED Index to specify which LED on the Reader you want to control the colour. Enabling Permanent ignores the Duration period.

Version 25.2.0

INTEGRITI

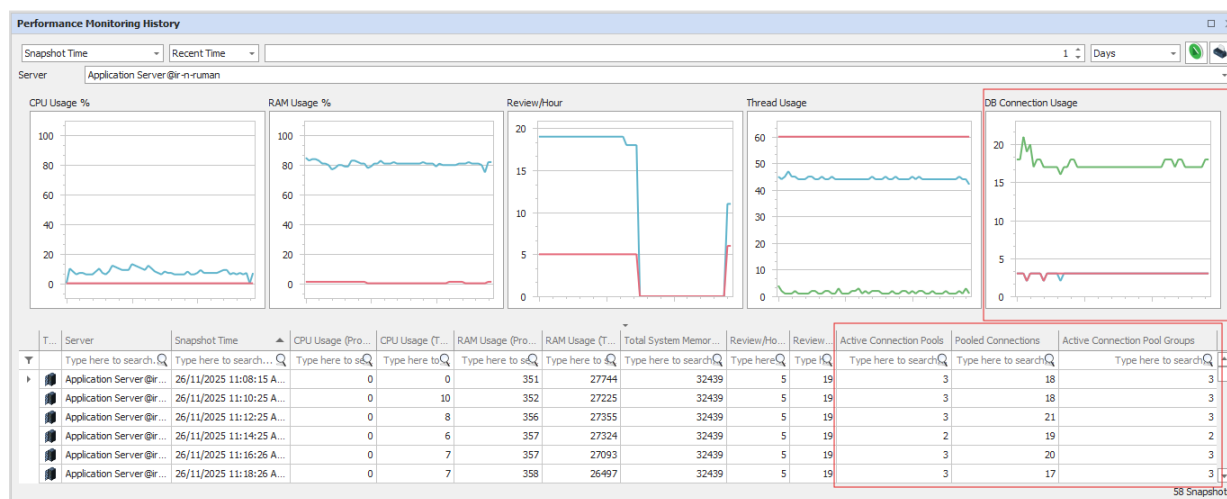
Improvements

- **Sync Performance:** General optimisations to entity synchronisation from the software to the controller on sites with a large number of entities.
- **Integrations:** General optimisations of loading associated Entities in the Associated Devices tab for Integrations.
- **Rest API V2:** Added support for Deleting Users to the User Management Module. Users can now be deleted by making a request to the DELETE Entity API Endpoint. See the REST API v2 web documentation for full details.



Note: The DELETE Entity API endpoint must be enabled from the Communication Handler settings to allow it to be used. This can be achieved by selecting 'Enable Entity Deletion'.

- **Integriti Installer:** Updated the default packaged version of SQL Server Express from 2017 to 2022.
- **REST API v1 & v2:** Added TotalPages and ResultSize properties to the PagedQueryResult when querying data via REST API v2. This provides summarised information about the results of the query that was executed, simplifying processing of the resulting data.
- **Performance Monitoring History:** Added support for monitoring Database Connection Usage which includes number of:
 - Active Connection Pools
 - Pooled Connections
 - Active Connection Pool Groups



Version 25.2.0

- **Stepped Controller Firmware Update:** Starting from Integrity v25.2.0, to update the Controller firmware to v25.2.0 or greater, requires the Controller to be first updated to v25.1.0 if the currently installed firmware is earlier than v25.1.0. To facilitate this process, Integrity now ships with Controller Firmware v25.1.0, in addition to the new version.
- **Web Client:** General performance improvements have been made in how Reviews and Entity State changes are updated in the Web Client.
- **KONE ACCESS 1000:** Updated Access Session Messages so that they now convey more meaningful information to the end users.

Issues Resolved

- **Schematic Maps:** Resolved issue resulting in the 'Elements' dropdown in the Schematic Map viewer incorrectly showing no elements. This dropdown will now show all available elements on the current Schematic Map.
- **Schematic Maps:** Resolved issue that could result in a memory leak when leaving large maps with a large number of frequently changing elements open for long periods of time.
- **XML Import:**
 - **Alert Definitions:** Fixed error preventing importing Alert Definitions with incorrectly configured Alert Groups.
 - **Holidays:** Resolved "start date must occur before end date" error when importing new Holidays.
 - **Integrated Devices:** Resolved issue that could prevent Integrated Devices from successfully importing into a system that doesn't contain all of the Entities referenced in the 'Associated Entities' of the imported Integrated Devices.
- **CSV/DUIM Import:**
 - **User Import:** Resolved issue that could result in Credential state not correctly updating to the value provided in the import in some circumstances when importing Credentials alongside Users.
 - **Import Configuration:** Fixed error that could prevent files with missing Column names from being imported.
 - **Blank Entities:** Cancelled/failed CSV imports no longer result in 'Blank' entities remaining in the system afterwards.
- **Controller Deletion:** Controllers can now be deleted without needing to first delete configuration referencing entities in that controller first (e.g. permissions, etc).
- **Web Client:**
 - **User Editor:** Resolved issue that could result in the 'Auto-Complete Password' feature of certain browsers incorrectly updating the 'PIN' field in the User editor to the password of the logged in Operator when changing the User currently open in the editor.
 - **Combo-Box Custom Fields:** Combo-Box Custom Fields no longer show a list of empty values when no Display Text is configured for the values to be shown in the combo box. Where no Display Text is configured, the dropdown will now show the Value instead.
 - **Biometric Credentials:** Resolved issue resulting in biometric credentials enrolled via the web client were incorrectly made inactive by default due to having an Expiry Date of 01/01/0001. Newly generated biometric credentials will now be active by default and have the correct Expiry Date configured.
Upgrading systems with existing biometric credentials experiencing this issue will need to manually fix the Expiry Date of these biometric credentials to re-activate them.
 - **Biometric Credentials:** Resolved issue that could result in additional cards being incorrectly generated for a User when viewing their existing biometric credentials from the web client.
- **Mobile Credentials:**
 - **Credential Revocation:** Resolved issue that could result in Mobile Credential licenses not being freed in some scenarios when revoking a mobile credential.

Version 25.2.0

INTEGRITI

- **Mobile Credential Pool Deletion:** Deleting a Mobile Credential Pool no longer automatically deletes all configured mobile credentials from the 3rd party system, allowing these credentials to continue to be used. When these credentials are no longer required, they can be manually revoked or deleted to de-activate them in both Integrity and the 3rd party system.
- **Guard Tour:**
 - **Guard Tour Step Configuration:** Improved error handling and UI feedback when configuring Guard Tour steps with CCTV elements. Placeholder images now display when no camera is available, and configuration fields are now dynamically enabled/disabled based on step ordering.
 - **Guard Tour Step Configuration:** Resolved potential errors that could be shown when attempting to add new Guard Tour steps.
 - **Action Configuration:** Resolved issue that could result in consecutive edits to Actions configured in nested dialogs not saving correctly without pressing the Save button multiple times.
 - **Format Strings:** Actions within Guard Tour steps using Format Strings now use Local Time instead of UTC Time for the Timeout and Completion values. This ensures the text used in the format string more closely aligns with expectations.
- **Visitor Management:**
 - **Add Visit:** Resolved issue that could prevent Visits from being added when the corresponding Visitor Management Configuration was configured with a 'Default Visitor Property' set to 'Inherit From Host'.
 - **Email Attachment on Check-In/Check-Out:** Fixed issue that would result in an error when configuring a Check-In or Check-Out Action that included a 'Send Communication Message via Email' action.
 - **Default Visitor Properties:** Fixed issue preventing removal or editing of 'Default Visitor Properties' withing a Visitor Management Configuration.
- **Commissioning Report:** Fixed issue resulting in the Point value calculated in the Integrity Commissioning Report was incorrect for both Standard and Access mapping for certain Input values.
- **Execute Report Task Actions:** Resolved issue resulting in it not being possible to configure an 'Hour' value in the Execute Report Task Action's 'Execution Timeout' field.
- **Door Schedules:** Resolved an issue where deleting a Door Schedule did not revert the door's state.
- **Report Designer:** Resolved issue that could result in the Report Designer freezing and becoming unresponsive when searching for properties in the Field List.
- **Review Synchronisation:** Resolved issue that could result in sporadic review records occasionally not being persisted to the software on systems with Review RLE enabled.
- **Challenge Definition:** Added missing options to Format Strings for Challenge Definitions.
- **Alerts:** Resolved a potential memory leak on systems with large numbers of Alert activations and associated Alert actions occurring.
- **Intelligent Reader:** Resolved issue resulting in the Battery Needs Replacement option in Intelligent Reader Modules never automatically being set to true.
- **Integrity CS:** Resolved issue that resulted in Unibus Door Expanders not being shown in the Navigation Tree within Integrity CS. These expanders are now correctly listed under the attached ILAM.
- **Operator Permission to Discover Controller:** Resolved an issue where trying to scan for Controllers would result in a permission error.
- **Communication Handlers:** Resolved issue resulting in a blank Communication Handler being generated after configuring, but not saving, a new Communication Handler of certain types.
- **Bulk Add Cards and Users:** Fixed error thrown when bulk adding cards and users on a system containing Card Templates without an associated Card Format.
- **Software Upgrade SQL Script:** Resolved issue that could result in the SQL update script hanging for a long period of time when updating the Integrity software on some systems.
- **GateKeeper Auto-Login:** Resolved issue where GateKeeper would not enter full screen where configured alongside auto-login.

Version 25.2.0

INTEGRITI

- **Operator Types:** Resolved issue preventing configuring an Editor Layout Set, a System Designer Layout, a GateKeeper Layout or a Security Policy against an Operator Type in the Operator Type editor.
- **Partitions:**
 - Resolved an issue that could result in Partition names not being persisted after being updated.
 - Resolved an issue where Controllers could be moved between Partitions without the relevant permissions.
- **Controller Entity List:** Resolved issue that could result in filter applied against State columns not being correctly applied in the Entity List of Controllers.
- **IR Connect Notifications:** Resolved issue that could result in notifications no longer being sent to the IR Connect application in some cases after a network outage on the Integriti Application Server.
- **Translations:** Added missing translations.
- **REST API v2:**
 - **Card Status:** Resolved issue resulting in it not being possible to set a card's status to 'Active' after having previously set the card to an inactive state.
 - **Add Entity:** Resolved issue that could result in Entities created via the AddOrUpdate endpoint missing Site information. This would cause errors attempting to interact with this Entity going forward.
 - **Get Cards:** Querying cards with the FullObject parameter set to true now supports retrieving Cards without a Card Number configured.
 - **Add User:** Adding a User with the IncludeObjectInResult parameter set to true will now correctly return the full object in the response. Previously, this could result in a 500 error being returned in some circumstances.
 - **Add Or Update User:** Resolved issue resulting in a duplicate credential being created instead of using the existing credential when attempting to add a Card to a User without specifying the site of the Card in the request.
 - **Paged Query Result:** Set the NextPageURL property from the PagedQueryResult to empty when querying entities to clearly indicate that there is no more data available.
- **REST API v1:**
 - **Paged Query Result:** Resolved issue that could result in the Count property in the PagedQueryResult displaying an incorrect value when querying entities. The Count now correctly displays the total number of items matching the specified query.
- **KONE Access 500:** Fixed an issue where in some circumstances, incorrect Card Data can be synced to KONE Access 500 server.
- **KONE Access 1000:** Fixed an issue where in some circumstances, incorrect Card Data can be synced to KONE Access 1000 server.

Documentation

- **REST API V2 Documentation:** Updated the REST API v2 web documentation with the latest changes made to the API.
- **Hardware and Software Prerequisites:** Updated the Platform (Operating System) versions supported by Integriti.

Version 25.2.0

Cyber Security Updates

1 issues have been resolved in this release.

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

Every release incorporates the latest security and vulnerability patches, helping to protect your systems 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 25.1.1 Bug-Fix

INTEGRITI

Version 25.1.1 Bug-Fix

October 2025

Issues Resolved

- **IR Mobile Access:** Fixed an issue where Downloading Cloud Credential using the IR SIFER Reader Config App would fail in certain circumstances for IR Mobile Access Integration.
- **Infiniti:** Resolved an issue where Infiniti could create and write to the wrong Review database in some scenarios.
- **DB Configuration tool:** Resolved an issue where in Infiniti changes made to the Connection String using the DB Configuration tool would not always be persisted.
- **Two-Factor Authentication (2FA):** Resolved an issue where Enrolling an Operator using Duo Push Authentication would not work.

Version 25.1.0

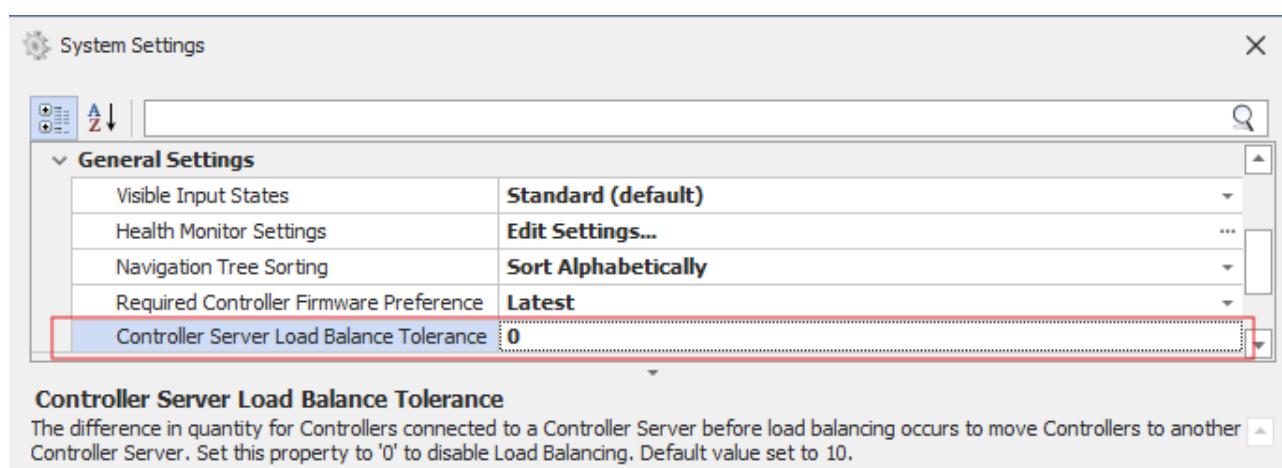
July 2025

Controller Load Balancing

For Integrati installations utilizing multiple Controller servers within its High Availability architecture, Integrati now offers automatic distribution of connected controllers across all servers. This feature ensures controllers connect to the server with the fewest connections, enhancing automatic load balancing in addition to any manual load balancing configured via the Primary Server.

This automatic load balancing functionality is enabled by default for all controllers running firmware version 25.1.0 or higher on systems with two or more Controller Servers. Single-server installations will continue to operate as in previous versions.

When Controller Load Balancing is active, controllers will initially connect to their configured Primary Server. However, if another Controller server has significantly fewer connections, the controller will be redirected to this alternative server. Among multiple alternative servers, the one with the fewest connections will be chosen. The threshold for triggering these redirections can be adjusted using the 'Controller Server Load Balance Tolerance' setting in Integrati's System Settings.



For new Integrati installations from version 25.1.0 onwards, Controller Load Balancing is enabled by default with no additional configuration needed. For systems upgrading from an earlier version, this feature will be disabled by default, maintaining existing connection configurations. It can be enabled by setting a non-zero value for the 'Controller Server Load Balance Tolerance' property in the System Settings, and disabled by setting this value to zero.

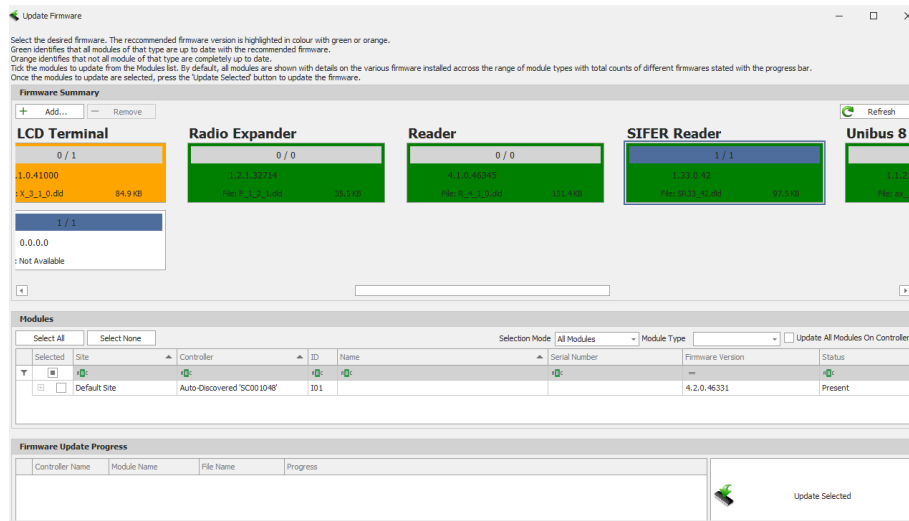
Note: Integrati's load balancing requires all controllers to run firmware version 25.1.0 or higher. Controllers with earlier firmware will continue to connect only to their specified server, as per previous versions. Controllers on version 25.1.0 or newer will still consider older firmware controllers when determining server connections.

For comprehensive details on configuring and using Integrati's Controller Load Balancing, please refer to the Integrati Load Balancing guide.

Version 25.1.0

Firmware Update

Integriti's Firmware Update dialog has been redesigned to streamline the process of updating firmware for Integriti Controllers and LAN Modules. The updated dialog clearly indicates the 'recommended' firmware version packaged with the current Integriti version and identifies the firmware distribution of connected devices.



The redesigned Firmware Update dialog is divided into three clear sections, designed to be used sequentially from top to bottom:

1. **Firmware Summary:** This section summarizes the currently installed firmware for all Controllers and LAN Modules configured in the system. It details the number of Controllers/Modules with each firmware version, providing a comprehensive system overview. Selecting a firmware version will automatically populate the Modules section with Controllers or LAN Modules that support the selected firmware. The recommended firmware packaged with the current Integriti version will be highlighted, but newer firmware versions can also be manually added and applied.
2. **Modules:** This section lists all Controllers or LAN Modules that support the selected firmware. It automatically includes only those modules that are online and running an older firmware version than the selected one, streamlining the update process. Additional modules can be displayed by selecting an alternative value from the 'Selection Mode' dropdown. Use the checkbox next to each module to select it for the firmware update.
3. **Firmware Update Progress:** This section allows you to start and track the firmware update process. Pressing the 'Update Selected' button will apply the selected firmware to the chosen modules. Each module will show its progress in the progress list, allowing you to clearly track the update.

For firmware updates to Unibus Modules and SIFER readers, selecting the relevant firmware will automatically display all modules with an applicable Unibus Module/SIFER Reader connected. The details of individual Unibus Modules and SIFER Readers will be shown under each parent module in the list. Selecting the parent module will apply the firmware update to all connected Unibus Modules or SIFER Readers.

Integriti's Firmware Update dialog has been redesigned to provide a more streamline experience for updating the firmware of Integriti Controllers and LAN Modules. The updated dialog clearly indicates the 'recommended' firmware version that was packaged with the current version of Integriti, as well as clearly identifying the firmware distribution of connected devices.

Version 25.1.0

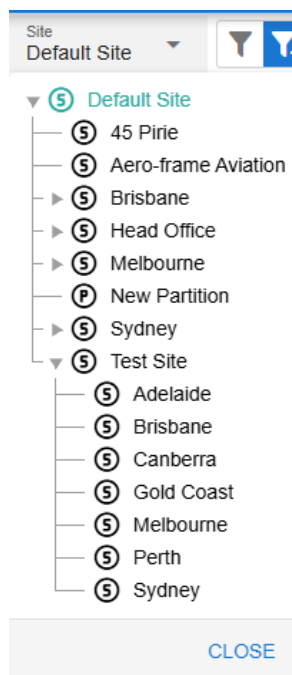
Improvements

- Web Client:** Integriti's Web Client now automatically remembers customisations made to the Visible Columns for all entity lists. This allows column selections to be retained when navigating to different pages or across sessions, saving the need to reselect the visible columns each time the entity list is opened.
 Customisations made to the Visible Columns for an entity list are associated with a specific User and browser, allowing multiple different Users to have separate column customisations both within the same browser and across different browsers.
 Note: Visible Columns are tied to the browser they were configured in, and will need to be re-applied on each additional browser/PC the web interface is accessed from.
- Web Client:** The search functionality within entity lists in Integriti's Web Client has been enhanced to allow per-column searching. This provides significantly increased granularity, allowing search criteria to only apply to a specific column. Separate searches can be applied to multiple columns to allow more granular search functionality.

Users							
ID	Name	Credentials	Primary Permission Group	Notes	Created	Last Modified	Last Modified By
	Mark		Deliveries		dd/mm/yyyy	dd/mm/yyyy	
U3892	Ainslee Markushkin	3528360000000000	Deliveries Tuckshop		6/22/2021, 11:34:24 AM	2/4/2025, 1:40:56 PM	Application Server@ir-n-ruman
U7954	Aila Marking	3556690000000000	Deliveries Tuckshop		6/22/2021, 11:34:24 AM	2/4/2025, 1:44:51 PM	Application Server@ir-n-ruman

Records per page: 50 1-2 of 2

- Web Client:** The Site Tree in the navigation panel is now sorted alphabetically, making it simpler to find Sites.



Version 25.1.0

- **SIFER Readers Entity List:** Added a new Entity List for viewing details of all SIFER Readers that have been connected to the system.

SIFER Readers (Showing 4)

Print / Export CSV

Columns

Create Filter

T...	Serial Number	Site	Attached Module	Reader Type	Firmware Version	Last Update
Type here to search	Type here to search	Type here to search	Type here to search	Type here to search	Type here to search	Type here to search
1000000758	Melbourne	PrismaXTerm: 02	(None)		22/06/2021 12:07:00 PM	
4491	Melbourne	8DoorRdr: 01	(None)		22/06/2021 12:07:00 PM	
62558	Sydney	2DoorRdr: 01	(None)		22/06/2021 12:07:00 PM	
700650	Sydney	2DoorRdr: 01	(None)		22/06/2021 12:07:00 PM	

Issues Resolved

- **IR Connect (SkyCommand):** General improvements to the stability and load times of the IR Connect (SkyCommand) app when connecting to an Integrity system.
- **IR Connect (SkyCommand):** Resolved issue resulting in entities from child sites being returned when selecting a Site filter in the IR Connect app.
- **IR Connect (SkyCommand):** Resolved issue resulting in Sites with no visible entities being shown in the SkyCommand app.
- **Schematic Maps:** Resolved issue that could result in Schematic Maps causing excessive memory usage for some configurations.
- **Schedule Overrides:** Resolved issue where Schedule Override Time Periods do not become active at midnight on the dates selected.
- **Schindler Lift HLI:** Resolved issue that could result in User Card State Synchronization not getting processed correctly.
- **Mobile Credential Integrations:** Resolved issue that could result in being unable to configure a Mobile Credential when a User already has a valid Mobile Credential.
- **Review Filter:** Resolved issue when using the 'Local Time' 'Today' Review filter that resulted in review from the selected time period being excluded. This issue is now resolved for Review DB Object Filters, as well as Advanced Reports such as the Time on Site and User Access reports.
- **Biometric Integrations:** Resolved issue that prevented Biometric Systems from being saved in some circumstances.
- **Performance History:** Fixed an issue where the Thread Usage Chart would cut off at 100 rather than showing the full thread usage.
- **User/Permission Group Permissions:** Resolved issue that could result in the Permission's When description changing to 'Sometimes' rather than 'Always' when clearing the Start and End Date for a Permissions When condition.
- **Review Syncing:** Resolved an issue that could result in individual Controller Review records occasionally not appearing in the Integrity Software in rare circumstances.

Version 25.1.0

INTEGRITI

Documentations

- **Hardware and Software Prerequisites:** Updated the Platform (Operating System) and MS SQL versions supported by Integrati.
- **Guide – Integrati Load Balancing:** Added guide describing usage and configuration of Controller Load Balancing.
- **Integrati Communication Handlers – IR Connect (SkyCommand) Integrations:** Added documentation describing the usage and configuration of IR Connect (SkyCommand) Integrations.

Cyber Security Updates

2 issues have been resolved in this release.

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

Every release incorporates the latest security and vulnerability patches, helping to protect your systems 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 25.0.0

INTEGRITI

Version 25.0.0

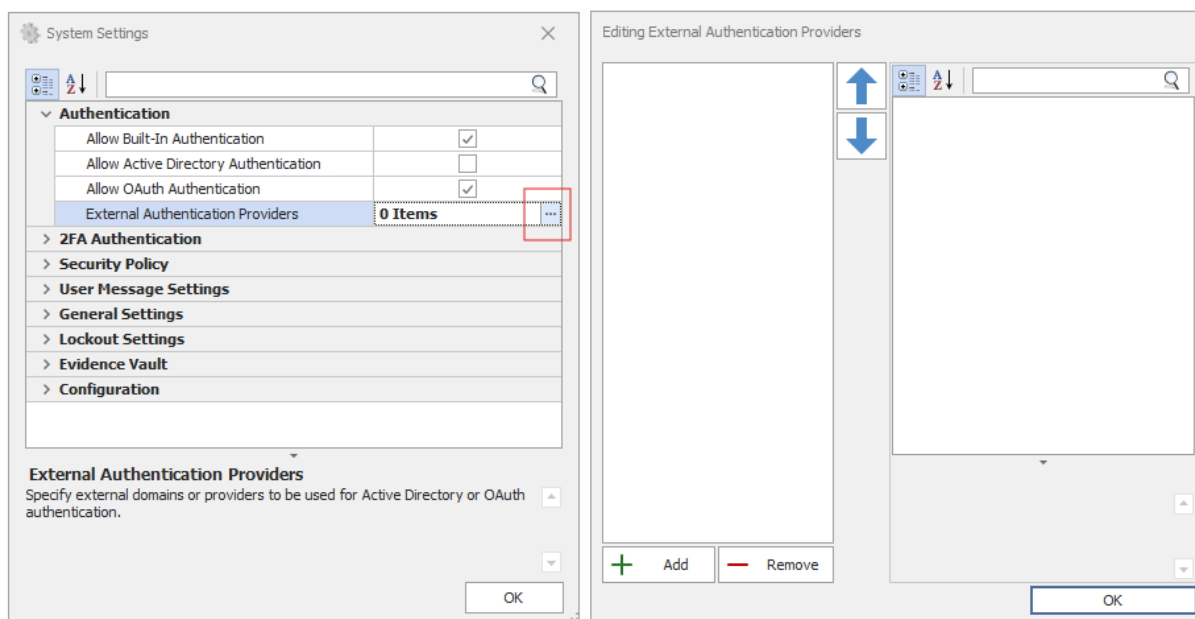
January 2025

OAuth Authentication

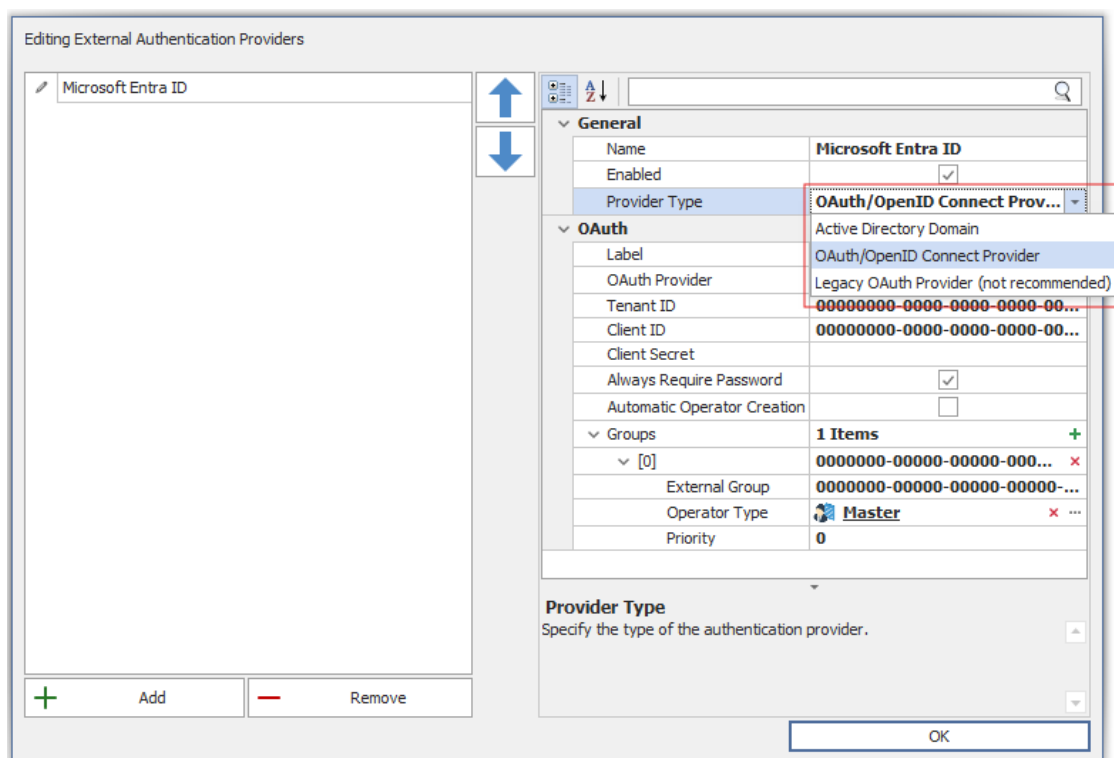
With Integrity v25.0.0, Integrity's existing OAuth SSO functionality has been significantly improved, both in terms of security and ease of configuration.

Integrity now supports configuring the OAuth SSO login to use the 'Authorization Code' grant type, which allows a login to be performed without user login data ever being provided to the Integrity SW. Where this flow is configured, Operators will instead be required to login via a separate web browser (opened automatically by the Integrity login dialog), providing their credentials directly to the OAuth provider. This additionally adds support for multi-factor authentication to be configured in the OAuth provider directly, allowing authentication to be fully achieved through the single authentication system.

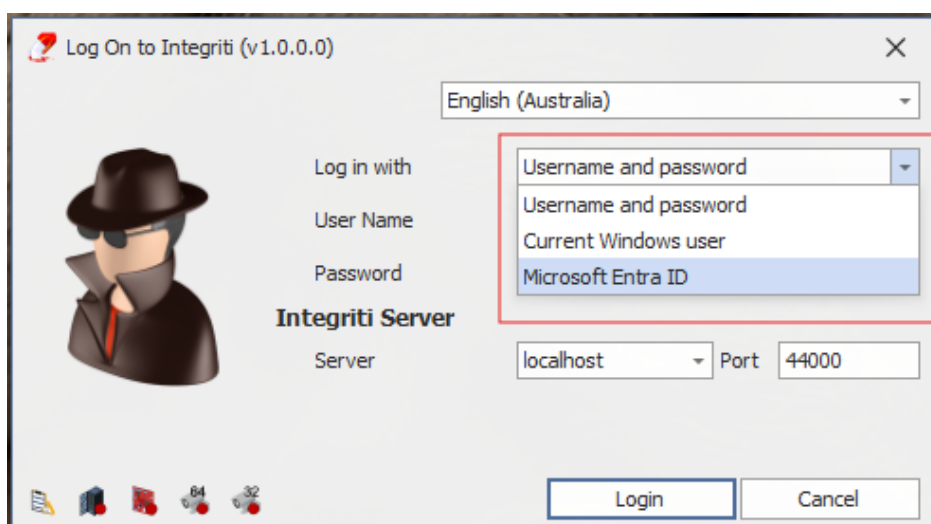
Additionally, Integrity now supports simple configuration of multiple 'External Authentication Providers', which includes both OAuth and Active Directory. External Authentication Providers can be configured from the System Settings by any Operator with the 'Can Administer Servers' permission via the 'External Authentication Providers' property. Expanding "External Authentication" property allows each separate authentication provider to be individually named and enabled/disabled, as well as providing previously global options (such as 'Automatic Operator Creation')



An External Authentication Provider can be configured as one of 'Active Directory Domain', 'OAuth/OpenID Connect Provider' or 'Legacy OAuth Provider'. Each Provider Type exposes the relevant configuration options for that provider type, allowing simple configuration of one or more External Authentication Providers. To simplify the configuration process, the 'OAuth/OpenID Connect Provider' provides several options pre-configured when using Microsoft Entra, Google or Okta as the OAuth Authentication Provider.



The process of SSO login for Active Directory and Legacy OAuth remains the same, with the user's external credentials being entered directly into the Integrity login dialog. Where one or more OAuth/OpenID Connect providers are configured, a new dropdown will be shown on the login dialog, allowing the user to select which system to log in through. After selecting the external authentication provider from the dropdown and pressing the login button, the Operator will be redirected to a login page for the external authentication provider in their web browser. Successfully logging in here (including completing any configured multi-factor authentication steps) will automatically complete the login to the Integrity software.



Upgrading Integrity systems will have their Active Directory and OAuth SSO configuration automatically migrated to the new 'External Authentication Provider' configuration, allowing them to continue using the system with no manual changes needing to be made. It is recommended to migrate legacy OAuth SSO configurations to the new configuration, however not required.

Version 25.0.0

Archiving Users

With Integrity v25.0.0, users can now be marked as 'Archived' when they no longer need to be active in the system. This will prevent these users from being synchronised to all Controllers and 3rd Party Systems (via integrations).

Previously in Integrity there was no way to prevent configured Users be synchronised to a Controller without deleting them. This included both active and inactive users in the system, which could result in Users who are no longer required to have access taking up some of the limited User slots in all controllers. For larger sites, this can result in Controllers running out of on-board space for Users and having to move to using a user expansion model (which prevent certain desired features).

An option has been added to the User's 'User Option' settings to allow them to be marked as 'Archived' in the system and be removed from controller synchronisation going forward. This can be configured in the same way as any other User property, including from the editor, CSV import or Active Directory import. Setting a User to be 'Archived' will have no effect on the user within the software, and will leave the User exactly as they are, retaining their history, audit, review linkage and all other details. Within the Controller however, setting a User to be 'Archived' will automatically delete them from all Controllers, and prevent synchronising them in the future, freeing up any User slots that they were using.

The screenshot displays the 'User Management' interface for a user named 'Master'. The interface is divided into several sections:

- User Information:** Includes fields for Site (Default Site), First Name(s) (Master), Second Name, Security PIN, and Qualify PIN.
- Permissions for this User:** A table showing the Primary Permission Group and Extra Permissions. The table has columns: What, Options, When, and Is. A single permission is listed: 'Admin Menu' with 'Always' when and 'Valid' status.
- User Options:** A list of checkboxes for various user settings:

User Option	Is
Cancel On Card Access	☐
Cancel On PIN Logon	☐
Disability	☐
Duress Code	☐
User Cancelled	☐
Is Archived	☐
No Greeting	☐
Permanent Cache	☐
Exclude From Operator Challenge (Ask PC)	☐
AURM Permanent	☒
Default Floor	☐
Start Date Time	☐
Expiry Date Time	☐
- Details:** A section for additional user information.
- Warnings:** A status bar at the bottom indicates 'Warnings : 1 outstanding'.

From the Controller's perspective, an 'Archived' User is equivalent to a User that has been deleted, so they will no longer have any access to any Controllers in the system.

NOTE: Once a system has 'Archived' Users in it, configuring Users directly through a controller or Integrity CS will no longer be officially supported, as this can result in conflicting User IDs.

Version 25.0.0

INTEGRITI

KONE Access 1000 Integration

Introduced in v25.0.0 is the KONE Access 1000 Integration. Like the KONE Access 500 Integration, it is a Communication Handler used to sync Lift objects into Integrati, for use with permissioning and programming, sending Users, their permissions and Card Data into KONE Access 1000 to allow synchronised Users access to Lifts in the KONE Access 1000 system.

Note: This new Communication Handler does not replace the KONE Access 500 Integration and existing Communication Handlers will continue to function without any action upon upgrading to v25.0.0. The KONE Access 1000 Integration is also not compatible with KONE Access 500 systems.

The major differences between the two includes an improved process to secure connections between the two systems, using an Activation Code provided by KONE to generate a certificate used to communicate with the KONE Access 1000 system, as well more comprehensive permission synchronising, using the Permissions belonging to a User and sending them directly to KONE Access 1000.

To start using this Communication Handler, a Certificate must be generated using it and KONE Access 1000. You should be provided an Activation Code from KONE, which can then be entered into the following form by pressing the 'Generate Certificate' button in the Communication Handlers editor (Details on sourcing the information for the request can be found in the KONE 1000 Guide).

Configuration	
Company Name	
Client ID	
Activation Code	
Certificate Thumbprint	

Configuration

Proceeding with this process will replace any existing Certificate.

Once a Certificate is generated, the Certificate will be renewed automatically;
this process does not need to be repeated to renew the Certificate.

Generate Certificate...

This certificate can be manually renewed during the time the certificate is active. Once the Certificate is generated and configuration in the editor is complete, the Communication Handler will import Lift objects from KONE Access 1000 to be used for User Permissions and other Integrati programming.

Users can then be synchronised to KONE Access 1000 by giving them permission to KONE Lift objects. A User's Permissions in KONE Access 1000 are derived from the Permission Groups that are assigned to the User in Integrati. Synchronising a User will also include any Card Data from Card's whose Templates are marked as being used in KONE, as well as information included in the Custom Fields the KONE Access 1000 uses.

Permissions for this User

Primary Permission Group

Extra Permissions

+ Add - Remove

	What	Options	When	Is
	Manager		Always	Valid

Properties

KONE 1000

KONE Phone Number	0477777777
KONE Email	User7@email.com
KONE Person Home Floor	Kone 1K - G0D - in group 2
KONE Mobile Experience	☐
KONE Preferred Language	English (AU)

Permission Groups can be 'Access Rights', containing a group of KONE Lift objects and the actions that can be taken using those objects, and 'Profiles', which can be assigned to Users and contain Access Rights and a Validity Time defining when the Access Rights apply. Permission Groups with permission to any KONE Access 1000 objects will be synchronised to KONE Access 1000.

Site

ID

Name

KONE Access Right: Permission Type

KONE Access Right Actions

KONE Profile Validity Time

☐ KONE Access Right: Can Make 'Direct Call'

☐ KONE Access Right: Can Make 'Group Call'

Last Modified By

Created Last Modified

Notes

Permissions

+ Add - Remove

	What	Options	When	Is
	Kone 1K - A - Lower		Always	Valid
	Kone 1K - A - Upper		Always	Valid
	Kone 1K - G0C - in group 2 - (DOP_20)		Always	Valid
	Kone 1K - G0D - in group 2 - (DOP_20)		Always	Valid
	Kone 1K - G1C - in group 2 - (DOP_20)		Always	Valid
	Kone 1K - G1D - in group 2 - (DOP_20)		Always	Valid
	Admin		Always	Valid
	Kone 1K - 38 - in group 1		Always	Valid
	Kone 1K - 39 - in group 1		Always	Valid
	Kone 1K - 40 - in group 1		Always	Valid
	Kone 1K - 41 - in group 1		Always	Valid
	Kone 1K - 42 - in group 1		Always	Valid
	Kone 1K - 43 - in group 1		Always	Valid
	Kone 1K - 44 - in group 1		Always	Valid

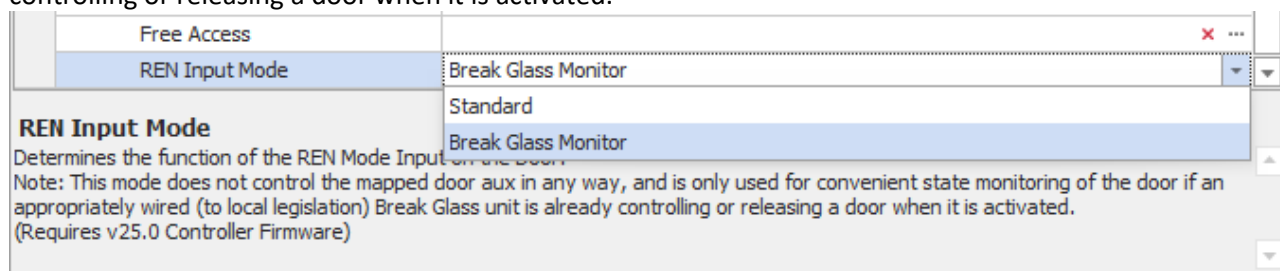
For more information on the configuration and use of the Integration, please refer to the 'Guide - KONE 1000 Elevator Integration' documentation.

Version 25.0.0

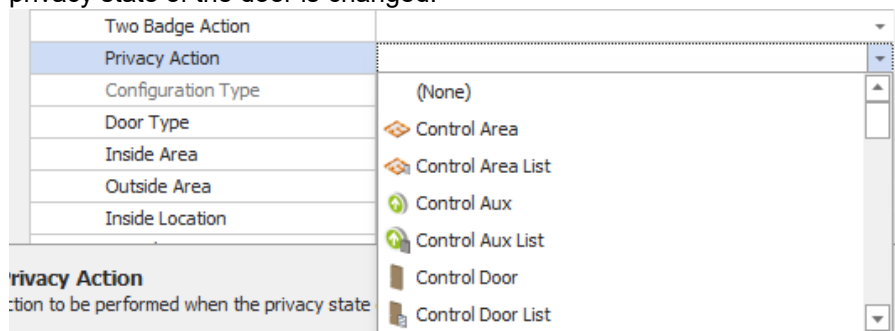
Improvements

- Door Configuration – REN Mode:** Added support for configuring REN mode, which can now be configured as Standard or Break Glass Monitor. The REN mode can be configured by going to the advanced section in the Door settings. Configuring as Break Glass allows for an emergency break glass switch to be connected to the REN input. Currently it only supports Break Glass, however more are coming soon.

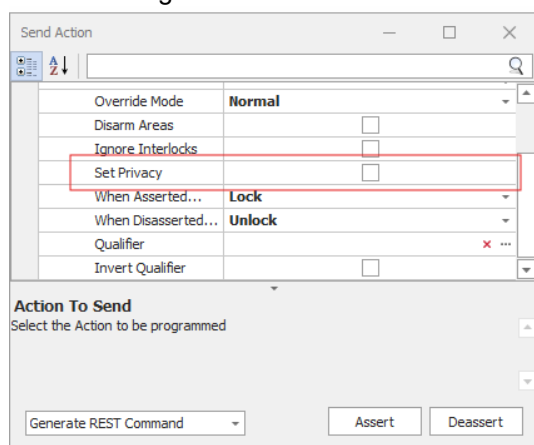
NOTE: This mode does **not** control the mapped door aux in any way, and is only used for convenient state monitoring of the door if an appropriately wired (to local legislation) Break Glass unit is already controlling or releasing a door when it is activated.



- Door Privacy Mode Action:** Doors can now have a Privacy Action configured to trigger when the privacy state of the door is changed.



- Door 'Set Privacy' Controller Action:** Added a new 'Door' Action that allows Privacy to be 'Set' or 'Unset' for a given Door.



- Controller 'Return to Path':** The Controller has gained the ability to fall back to the highest priority ethernet connection after a network outage. To enable this feature, select "Enable Return to Path" in the Connectivity Paths section of the Comms Task Setup. Additionally, one can setup the time to wait after

Version 25.0.0

INTEGRITI

connecting before trying to establish a new connection again and the duration spent waiting between connection attempts.

NOTE: This requires Integriti Controller firmware v25.0.0 or higher.

Issues Resolved

- **Controller Synchronisation:** Resolved issue that could result in all Permission Groups being resynchronised on a regular basis. On large systems, this could present itself as Controllers constantly resynchronising.
- **Schindler Lift HLI - User Synchronization issue:** Resolved issue that could result in User Synchronization not getting processed correctly.
- **Mobile Credential Integrations:** Resolved issue that could result in generated mobile credentials being automatically revoked, or have multiple invitations sent out in some scenarios. This issue could apply to both manually and automatically generated mobile credentials.
- **Entity Sync Integrations:** Resolved an issue where Entity List objects synchronised to Third Party Systems would have their contents assigned to a User or Permission Group in the Third Party System instead of the list object itself. For example, Synchronising a Permission Group to SALTO SHIP with a Door List previously resulted in the Doors being assigned to the Permission Group, instead of the Door List object.

Version 24.0.1 Bug-Fix

Version 24.0.1 Bug-Fix

August 2024

Issues Resolved

- **Custom Layouts:** Resolved an issue that could cause Custom Fields to not appear in a customised User Editor layout. The custom fields should once again be visible in the layout and in the 'Customisation' window when modifying the User Editor's layout.
- **System Warnings:** Resolved an issue where System Warnings reporting a Controller is offline would not get cleared when the connection was restored. Existing warnings of this type will be cleared upon the upgrading system starting up and reconnecting to its Controllers.
- **Integrated System/Device Editor:** Resolved an issue causing Licensing error messages to appear when saving an Integrated System or Device that were correctly licensed.

Version 24.0.0

June 2024

Skycommand App Integration

Integrati v24.0 adds support for the Skycommand App, allowing it to control and view Entities within Integrati via the app, as well as facilitate receiving push notifications from Actions and Scheduled Tasks in Integrati. This is available through a new Communication Handler added to Integrati.

Handler Settings

Handler Type: SkyCommand App Integration

A Z ↓

Custom Fields

Email Address	New Field
---------------	-----------

Push Notification Sender Configuration

Enable Push Notification	☒
> Push Notification Settings	Retry every 15 mins, Stop after 120 mins (8 retry attempts)

Advanced Web Api Settings

Port Number	834
Use HTTPS	☐
Web Host Domain Name	localhost
Api Application Path	skycmdapi/
Skip SSL Certificate Check	☐

The Skycommand App Communication Handler is configured with an email address, used to connect Skycommand accounts to a User in Integriti, determining the permissions that account will have for viewing/controlling Entities in Integriti. Push Notifications are enabled by default and their retry period and attempts can be configured, defaulting to every 15 minutes, retrying 8 times.

Additionally, the endpoint on which the Communication Handler receives commands from Skycommand can also be configured. This is useful when the Handler is configured on a public machine that needs to specify a specific host name, or when the default port or application paths need to be customised.

Once the Communication Handler is set up, logging into Skycommand with an account whose email belongs to an Integirti User should show the Integirti instance. Selecting this instance will display a list of Entities (Doors, Areas, Inputs, etc.) the User is able to see and, where permitted, the commands that can be called on each Entity.

These are determined by Menu Groups assigned to the User, where the Menu Group's 'Remote Access Permissions' flags determine the potential commands that can be executed on the entities that are viewable.

Menu Group: Staff Menus

Site: [Default Site](#)

ID: M63

Name: Staff Menus

Last Changed By: [Application Server@ir-n-rhys](#)

Created: 13/03/2024 Modified: 13/03/2024

Notes:

Properties

Remote Access Permissions

Arm Area	☒
Disarm Area	☒
Arm 24 Hour	☐
Disarm 24 Hour	☐
Isolate	☒
Control Aux	☐
Lock Door	☒
Unlock Door	☒
Siren	☐
CommsTask Control	☐
Adjust Count	☐
Secure Allowed	☐
Free Access Allowed	☐
Installer Access	☐

Review

Push Notifications can be pushed to Skycommand simply by using the Skycommand App Communication Handler as the 'Sender' of a 'Send Communication Message' Task Action. As such, notifications can be sent to Skycommand whenever such Task Actions are triggered, for example as the result of a Scheduled Task, during a Guard Tour, etc.

Configure Task Action

Action Type: Send Communication Message

Sender: [Skycommand App Comms Handler](#)

Message Recipients

Message: Skycommand User '{User.Name}' is set to expire soon at '{User.ExpiryDateTime}'

Edit

Version 24.0.0

INTEGRITI

Lift Integration Improvements

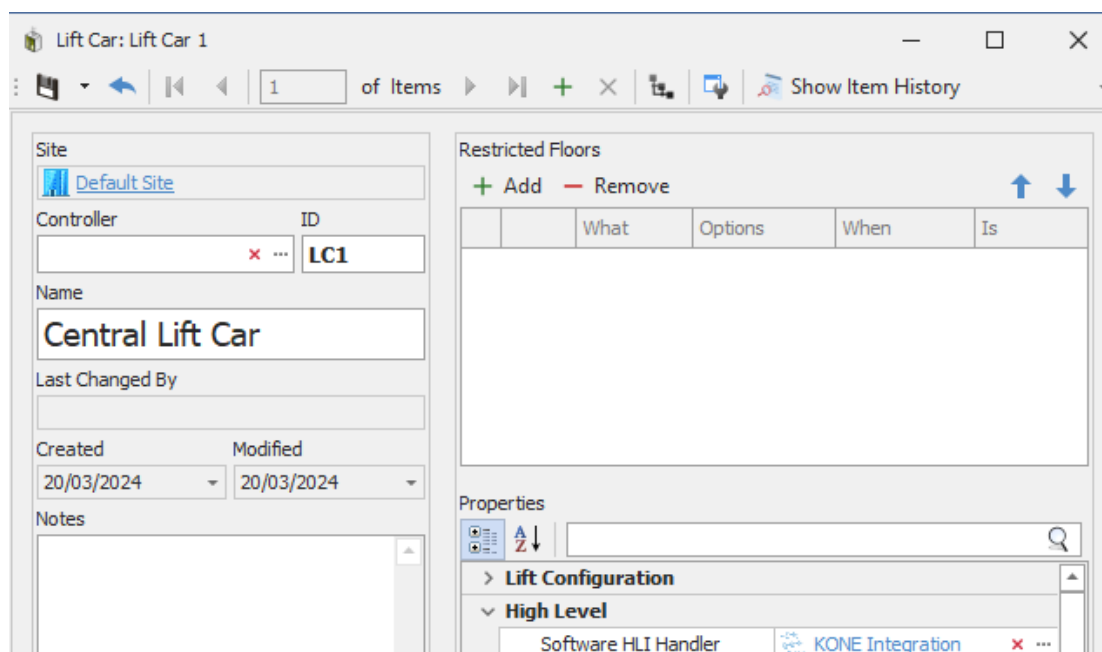
Several improvements have been made to the KONE and Schindler Lift Integrations, primarily streamlining the installation process by reducing the volume of custom fields that need to be created and configured, as well as leveraging the new 'Entity Link' custom field to more strongly connect the information configured in Custom Fields rather than relying on names or IDs.

Note: Existing KONE and Schindler Integrations will continue to function based on their previous behaviour once upgraded to v24.0, no action is needed to allow the Integrations to function once the upgrade is performed. However, in some instances, new functionality may not be available until new associations or Custom Fields are created and configured, which will be noted as each improvement/change is described.

KONE Lift Integration

Review generated by the KONE Integration will now include Users in their entity entries, as well as Controllers, Lift Cars and Floors once additional configuration is made, allowing for actions driven by the presence of these entities to be triggered by KONE review (eg. View CCTV device for linked floor). For Controllers, Lift Cars and Floors to be included in the Review, the Lift Car property 'Software HLI Handler' needs to be configured and set to the KONE Integration being used.

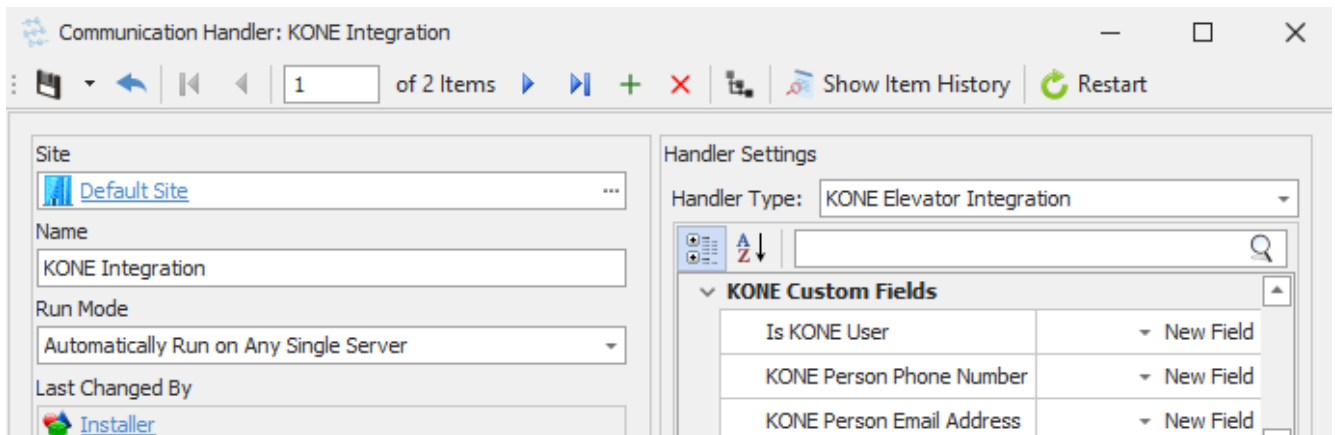
Additionally, associating a Lift Car with a KONE Integration will now also automatically generate Lift Floors when the Integration starts up. This is achieved by setting the 'Software HLI Handler'



User configuration has several new additions requiring new custom fields. Firstly, User Email and Mobile Number fields can now be synchronised to KONE, utilising new custom fields to be configured in the Communication Handler.

Version 24.0.0

INTEGRITI



Additionally, Personal Lift Floor can now be directly selected in a User via the new 'Entity Link' custom field instead of the two that were required previously. Creating the new custom field for the Integration requires the Integration to first be stopped, the previous Custom Fields to be deleted, then the Integration started up. Once this is complete, the Lift Floor can be selected in the User to be used as the Personal Lift Floor.

A smaller change has also been included to send the 'Card Badge Names' (which were the Card Numbers in Integrati) in decimal format instead of hexadecimal.

Schindler Lift Integration

The new 'Default Auto-Destination Boarding Lift Floor' property has been added to the Schindler Integration's Communication Handler, allowing for a single Lift Floor to be configured for this purpose and not configured in every User used with the Integration.

The 'Zone ID' custom field is now configured in Lift Cars instead of Users, reducing the amount of configuration required to set up the Integration and reduces further maintenance required.

Scanner Integration Support

Support for Scanner Integrations has been added. Scanner Integrations allow User details to be entered into Integrati by scanning documents (such as a Driver's License or Passport) and mapping the details of the Document to properties on an Integrati User.

These integrations help streamline creating and/or updating new Users by importing information such as a User's Name, Address, etc. from scanned documents, reducing the amount of manually entered information for Users created/updated in this way.

Configuring a Scanner Integration will include creating a set of import mappings from properties of scanned documents to User's properties, defining how a scanned document's information populates a given User.

Version 24.0.0

INTEGRITI

Once a Scanner Integration has been installed in Integriti, the option to scan a document using the Integration will appear in the User editor, as shown below.

User: New User

1 of 2 Items

Site: Default Site ID: U0

New User

First Name(s)

Second Name

Security PIN Qualify PIN

Scan User Identification

From here, any configured scanner can be chosen to scan in information for the User being edited.

Add User Details From Scanner

Settings

Select Integration: Samsotech Scanner 1.0.0.00000

Select Scanner Device: Samsotech Reception Scanner

Select ID Type: ID Text Scan

User Identification Info

No image data

Drag a column header here to group by that column

Scan Identification Ok

Version 24.0.0

INTEGRITI

Sensor Integration Support:

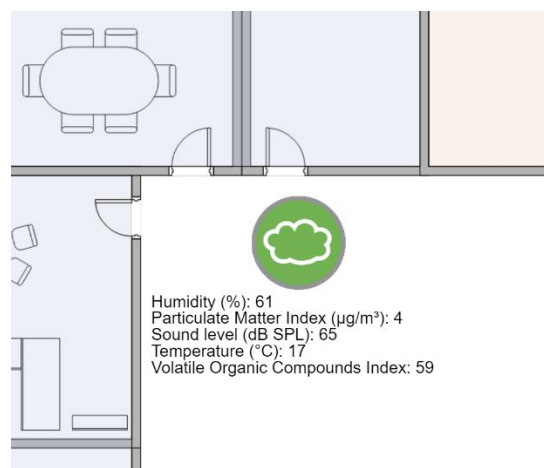
Support for Sensor Integrations has been added. Sensor Integrations update a Sensor's state in Integrati to be displayed on Schematics Maps as well as generating Review on update events to drive Scheduled Tasks and other features on sensor state changes.

These Integrations help monitor changes in sensors on a site by reflecting them in Integrati, allowing Schematics Maps to communicate the current state to those monitoring the maps. The Review generated by these Integrations also help drive Alerts and Tasks to ensure high priority changes in sensor states are reported and alert Operators of potential issues on a site, as well as keeping record of major changes to be reviewed when needed.

Sensor States are defined and maintained by Sensor Integrations, with a name and value for each field. These are automatically updated by the Integration while it is online and receiving updates from the Third Party System. An example of the state values and names:

Configuration	
State	Online
Status	Online
Sensor Label 1	Humidity (%)
Sensor Value 1	61
Sensor Label 2	Particulate Matter Index ($\mu\text{g}/\text{m}^3$)
Sensor Value 2	4
Sensor Label 3	Sound level (dB SPL)
Sensor Value 3	65
Sensor Label 4	Temperature ($^{\circ}\text{C}$)
Sensor Value 4	17
Sensor Label 5	Volatile Organic Compounds Index
Sensor Value 5	59
Location X Coordinate	145.21899825856474
Location Y Coordinate	-37.925447448259426

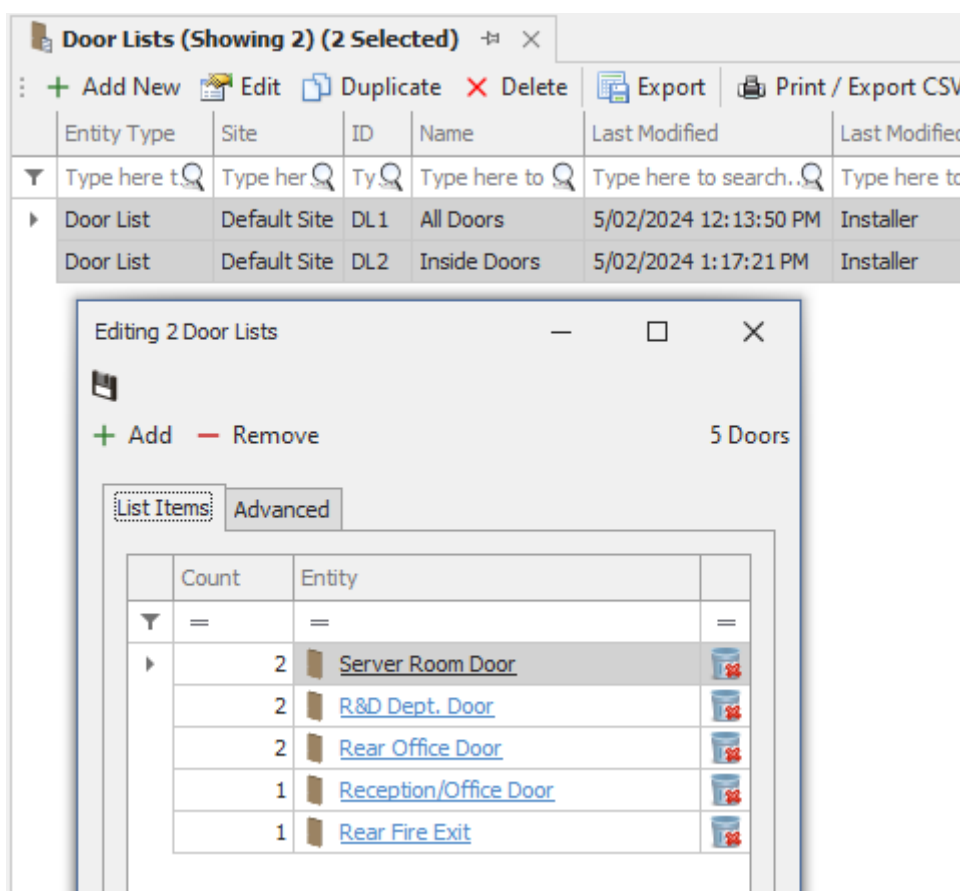
To display this information on Schematics Maps requires the configuration of an Element Presenter, which defines what information is displayed, as well as conditions to change the appearance of the presenter. For more information on how to configure Element Presenters, please refer to the 'Integrati Schematics – Editor' manual provided with Integrati.



Version 24.0.0

Improvements

- **License Key Manager:** Licenses are now sorted by 'Feature Name' by default.
- **Review Sender:** Improved TLS support for the Review Sender.
- **Format Strings:**
 - Format String properties can now be cleared by a button in the property editor
 - Format Strings can now have a Format String configured per Language available in the client editing it. This allows Format Strings to change their output based on the language required by whatever is processing it (eg. A Server configured to use a specific language).
- **Multi Select Edit:** Selecting multiple Entity Lists of the same type allow for their List contents to be edited. After selecting multiple Entity Lists and clicking 'Edit', the editor will now display the combined contents of the selected lists, with a count representing the number of lists referencing a specific Entity. Below is an example using Doors and Door Lists.



- **Database Backup Task Action:** Review can now be generated when these Tasks are performed, including the file path the backup is saved to, the time taken to execute and whether the task succeeded. Additionally, when run using the 'Run Task Now' button in the Schedule Task editor the Review will include the Operator that initiated the task.

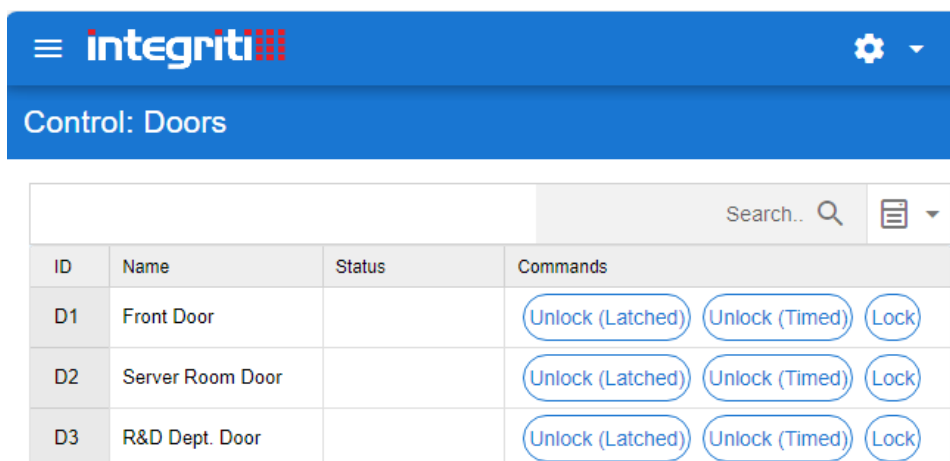
Source	Message
Period	Recent History (Live)
Last	1 Days
Print / Export CSV	Create Filter
Local Time	Text
6/02/2024 3:54:45 PM	Scheduled Task 'Monthly Backup' Database Backup to 'C:\Program Files\Inner Range\Integrity Pro\Backups' Succeeded: Time Elapsed - 18.455 s (run by Operator 'Installer')

Version 24.0.0

INTEGRITI

- **Execute Report Task Action:** Now has the option to place exported files into password-protected ZIP Archive. This option can be found when configuring a given 'Execute Report' Task Action, as seen below:

- **Web Interface:**
 - An 'Unlock (Timed)' command has been added to the Web Interface under the 'Control: Doors' page.



- Operator Types can now be assigned a 'Web Client Timeout', defining the amount of time before an Operator is timed out when using the Web Interface without loading a new page. When upgrading to v24.0 and newer, this property will be set to the Operator Type's 'Inactivity Timeout Time' if one is defined, otherwise it will default to a 2 hour timeout.
- Primary Permission Groups for Users are now highlighted when editing Users.
- Reduced the volume of browser logs generated when running the Web Interface.
- Search Field contents no longer persist when loading a different page (ie. Moving from Area entity list to Door entity list).
- **CSV Imports:**
 - Review generated now includes the number of entities deleted by Navigation Group Resynchronisation and the number deleted by Import Mapping Transforms.
 - Added new 'Collection Update Mode' property to Import Settings to allow the collection import behaviour to add to a collection instead of replacing. For example, this allows for new credentials to be created via the Import without removing existing credentials from any User that is changed by the Import.
- **REST API:** List properties, such as a User's 'Cards' and 'Permissions', can now be returned by the REST API using the Additional Properties parameter.

Version 24.0.0

- Warning Category**
System Health

Warning Type
SQL Configuration

Warning Time
5/02/2024 9:38:06 AM +11:00

Suppressed Until
13/02/2024 12:00:00 PM +11:00

Suppressed By
Installer

Suppression Notes
Consulting IT in meeting next week

Details
Configured Maximum SQL Server Memory Higher Than Recommended
The configured Maximum Server Memory usage of 2,147,483,647 MB is higher than the recommended value of 1,636 MB.
Decrease the Maximum Server Memory Usage to 1,636 MB or lower to ensure optimal performance.

Resolution
Resolve SQL configuration to ensure optimal performance.

- Type Permissions
Extra Permissions
Features

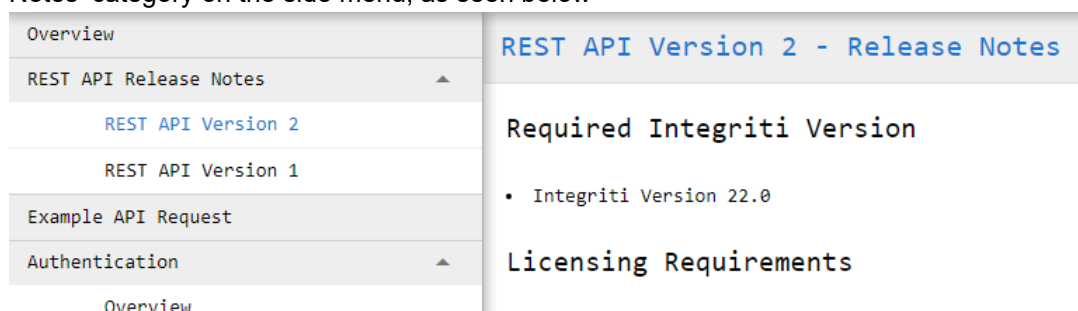
Administration

Import Data	☐
Can Administer Servers	☐
View Audit	☐
Reveal PINs	☐
Send PINs	☐
Generate PINs	None
Set Any PIN	None
Allow Grant Amnesty From Context Menu	Hide generated PIN
Force Finalize Alerts	Show generated PIN
View Finalized Alerts	☐

Version 24.0.0

INTEGRITI

- **Performance Monitor:** Logs generated from denied access to the 'Global' Registry Key can now only be produced once a day. This should reduce the volume of logs generated by this issue, which could flood the Integrati log if not addressed when first encountered.
- **Reader Module Editor:** Clarified that the 'Offline Function' options only apply to Concept 3000 Two Door Readers (C3K 2DAMs).
- **Credential Acquire:** When assigning credentials via a Biometric Integration, a pop-up message is now displayed before the dialogue session times out, allowing the Operator to refresh the session without losing the newly enrolled credentials. This timeout is now 1 hour, and the pop-up will appear 2 minutes prior to expiry.
- **REST API Doc:**
 - Release Notes have been added to the REST API Documentation, detailing the changes that have been made to each version of the API. This can be found under the 'REST API Release Notes' category on the side menu, as seen below



- Username and Password fields in Authorisation Headers will now display errors when empty.
 - The 'Request Body' tab is no longer displayed for Requests that do not require a body in the REST API Doc.
- **Users:** Added a new reportable property to Users' State, 'User Last Accessed', which contains the time the User was last granted access to a Door via Card or PIN.
- **RTLS Assets:** Battery Voltage will be blank for Assets that have not had their Battery State set, ie. By an Integration.

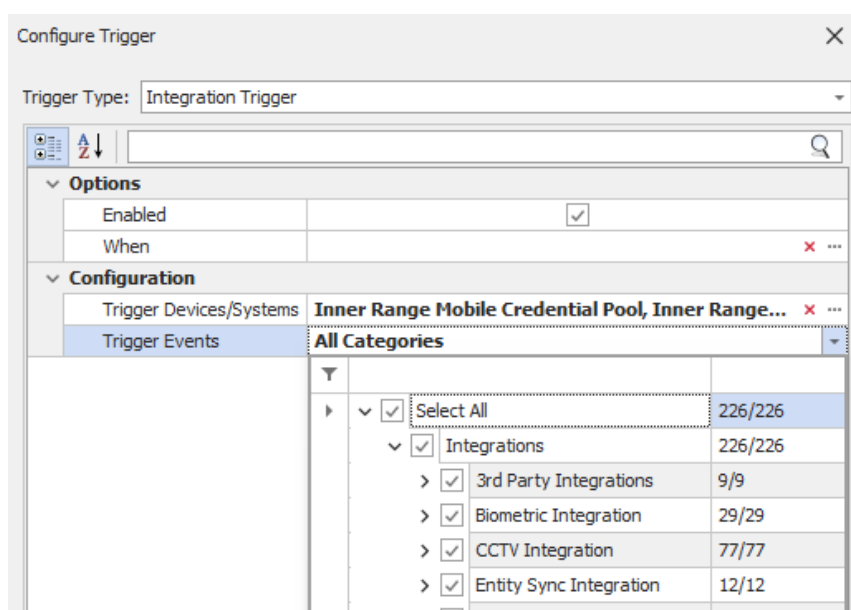
RTLS Assets (Showing 1) (1 Selected)			
+ Add New Edit Duplicate Delete Export			
Asset Type	Type	Name	Battery Voltage
Type here to search		Type here to search	Type here to search
User Device	RTLS Asset	Patient Tag 5	

- **Time Periods:**
 - Schedule Overrides can now be sorted.
 - Schedule Overrides can no longer have dates configured before the current Date and Time.
- **Control AUX/AUX List:** Expanded and clarified options in the 'Control Type' property description.
- **KONE IP Comms Task:**
 - Added the 'Kone Source Control' property, which allows separate source & destination control for this Comms Task.
 - Added options for a 'Quinary Ethernet Connection' for specification of a fifth set of connection/server settings.
- **Graphic Terminal:** Added the 'Area Arming Mode' property, which has options to filter which Areas can be seen in addition to Operator Permissions:
 - **Control:** Show all area lists where user has permissions to Arm and Disarm all area's contained in the area list.

Version 24.0.0

INTEGRITI

- **Arm:** Show all area lists where user has permissions to Arm all area's contained in the area list.
 - **Disarm:** Show all area lists where user has permissions to Disarm all area's contained in the area list.
 - **None:** Don't apply filtering to the area list menu. Users can see all area lists where user has permissions to Arm/Disarm one or more areas in the area list.
- **Integration Entity Import:** Review generated on Import now indicates whether the Import was a Full or Partial Import.
- **Integrated Device Editor:** Warnings will now be displayed when an editing an Integrated Device whose Integration does not meet licensing requirements (Integrati Software Version or missing Feature License). This can help identify licensing issues on a per Integration or Device basis without having to compare licenses in the License Manager to Integration documentation:
- **IR Mobile Access:** A Warning is now displayed when editing or saving a Mobile Credential Pool for Mobile Access that changes could delete the Sifer Reader's encryption key.
- **Alerts Sources/Triggers:** There is now an 'Integration Trigger' for Alert Sources and Triggers used by Scheduled Tasks, which will trigger when specified Event Categories would be selected Integrated Devices or Systems. This can be selected from the 'Trigger Type' dropdown when adding or editing a Trigger.



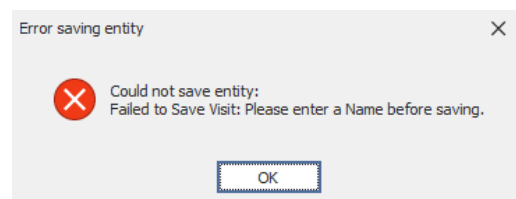
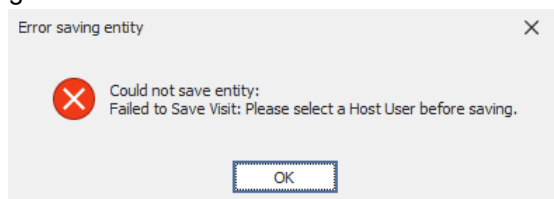
Integration Triggers can be assigned multiple Devices or Systems to monitor for events, with Systems triggering this condition whenever it or any child devices would generate events configured.

Additionally, Trigger Events can be configured to define which events from the Devices or Systems should trigger the Scheduled Task or Alert Source. Note that the events configured here do not need to be configured to generate Review in any of the Devices or Systems selected to cause the Trigger conditions to be met.

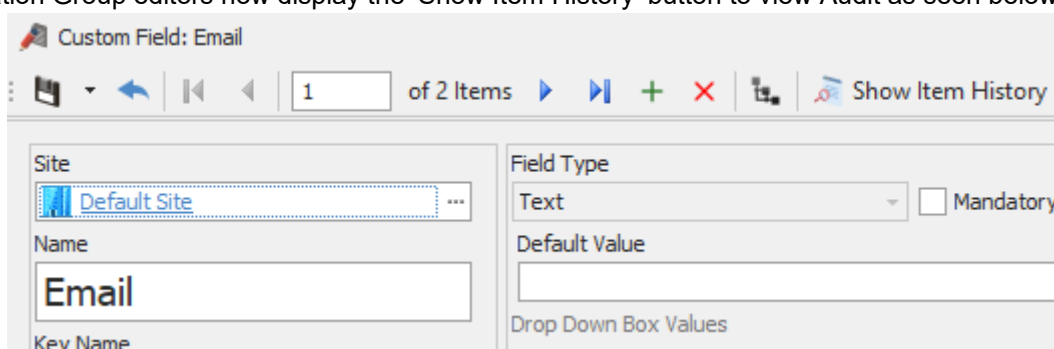
- **Control Modules:** The 'AC Holdoff Review' property has been added, preventing AC Failure from being logged to Review if set.

Version 24.0.0

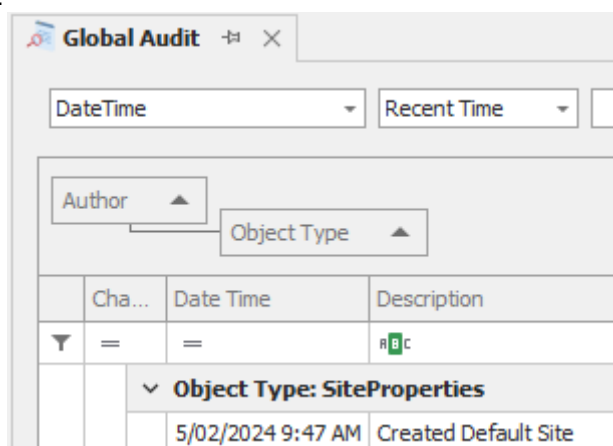
- **Visitor Management:** An error is now displayed when a Visitor is not given a name or when no Host is specified when creating a Visit, ensuring that visits cannot be created without both information being configured.



- **Audit Trail:** Custom Field, Navigation Group and Site Properties are now audited. Custom Field and Navigation Group editors now display the 'Show Item History' button to view Audit as seen below:



A Site Property's Audit can only be viewed in Global Audit. The Global Audit can be grouped by 'Object Type' to view changes specific to Site Properties, by dragging the 'Object Type' column next to the 'Author' text above the Audit list:



- **.Net Version Warnings:** Pop-up messages generated when logging in to a Server with the Integrati Client where the .Net Version differs no longer shows on every log in; it will appear once, then re-appear if there are changes to either Version. System Warnings for this are still generated regardless.

Issues Resolved

- **Entity List:**
 - Resolved an issue where 'Is Blank' filters were not correctly applying, for example when used to filter Users that have no credentials.
 - Resolved an issue where attempting to sort by the 'Time Since Update' column (where applicable) would throw an exception.
 - Resolved an issue preventing an entity list from being created if there was an entity of the given type with no Controller assigned (ie. Doors/Door Lists).
- **Response Plan:** Resolved an issue where Escalate Alert Task Actions could not be executed from a Plan's Action Button.
- **Scheduled Task:** Resolved an issue where it was possible for a Scheduled Tasks' trigger to not start correctly on save.
- **Web Interface:**
 - Resolved an issue where it was possible to configure a Holiday to have an End Date before its Start Date.
 - Resolved an issue preventing horizontal scrolling and causing text to overlap on thin mobile devices, in particular for entity lists and Advanced Reports.
 - Resolved an issue allowing Operators with no permission to Custom Fields to edit Custom Field values in entities.
 - Resolved an issue showing Biometric Readers to Operators without the necessary permissions.
 - Resolved an issue where Web Interface logins were not updating Operator 'Last Successful Login Date'.
 - Resolved a type in the Advance Report 'Format Option' dropdown.
- **Multi Select Editor:**
 - Resolved an issue where configured properties for selected items could not be viewed in the editor.
 - Resolved issue that could result in Actions not being configurable from the multi-select editor.
 - Resolved an issue preventing the 'CTRL+S' shortcut from saving changes.
- **.Net Version Warnings:** Resolved an issue where .Net warnings could be shown more often than intended.
- **Find Entity Form:** Resolved an issue switching between Third Party Doors and Integriti Doors when searching for Doors via a Find Entity Form.
- **Credentials:** Resolved issue that could result in changes to a Credential's state not being correctly synchronized to controllers.
- **Schematics Maps:**
 - Crash logs are now generated when a crash occurs in Schematics Maps; these logs are placed into the following file path: 'C:\Users\[CurrentUser]\AppData\Local\[AppName]\User Data'
 - Resolved an issue where moving a map and RTLS Assets in the map after an Alert was raised could result in exceptions being thrown.
- **Firmware Update:**
 - Resolved an issue where the percentage download during an update was misleading regarding its progress.
 - Resolved an issue causing a Controller Firmware System Warning when successfully updating a Peripheral's Firmware.

Version 24.0.0

INTEGRITI

- **Users:**
 - Resolved an issue preventing 'User Expired' from being cleared after manually clearing the User's Expiry Date.
 - Resolved an issue that could occur when manually typing a Date/Time field with no Offset set.
- **Integration Configuration:**
 - Properties where a Server address is selected via a drop down, eg. 'Alarm Listening Address' in the Hikvision CCTV Integration, can now be set to '(None)', allowing the property to be cleared once set
 - Resolved an issue where 'Send 3rd Party Invitations' property was displayed in Integrated Devices/Systems that do not use it.
- **Display Themes:** Resolved an issue preventing Display Theme settings from being applied to a Door's Inside/Outside Area columns.
- **Navigation Tree:** Resolved an issue preventing Sites and Controllers being sorted according to Controller States.
- **Review Sender:**
 - Resolved an issue loading TLS Certificates from a Client connection using the Review Sender.
 - Resolved an issue preventing heartbeats from being sent on busy systems.
- **Controller Sync:** Resolved an issue preventing Users with RF Remotes without a Template from being synchronised to the Controller.
- **Active Directory Import:** Resolved an issue where Users were placed in the wrong site during an AD Import.
- **Doors:** Resolved an issue changing the Reader Module from an Intelligent to Standard module when saving or opening the Hardware Options dialog.
- **Controller Enrolling:** Resolved an issue preventing Controllers from being enrolled via the Set Site Wizard if permission to view Server Instances was not available in Integrati CS.
- **Time Trigger Scheduled Task:** Resolved an issue where UI elements were not appearing correctly when using high resolution monitors.
- **Alerts:**
 - Resolved an issue where Operators were able to see all finalised Alerts regardless of the Operator's Permissions.
 - Resolved an issue allowing Operators to Finalise Alerts via 'Claim Next' regardless of the Operator's Permissions.
- **System Warnings:** Resolved an issue where Warnings generated from Integration Sync errors were not cleared if the entity in question was then re-configured to not be synchronised (eg. If a User failed to sync, re-configuring the User to not be synchronised by remove permissions did not clear the System Warning).
- **External Credentials:** Resolved an issue preventing certain external Credentials from being synchronised. This issue was noted when used with the Idemia Integration.
- **IREntities Import:** Resolved potential issue importing IREntities files into large systems.

Documentation

- **Integrati Intercom Integration Manual:** Updated the Enrolment instructions to include the Tab that the 'New Integrated Device' button can be found.
- **Mimic Viewer Documentation:** Added clarification on how the 'Prefer Controller Changes' works in the Mimic Viewer.



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

May 2026

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.

Copyright ©2026 Inner Range Pty. Ltd., Australia