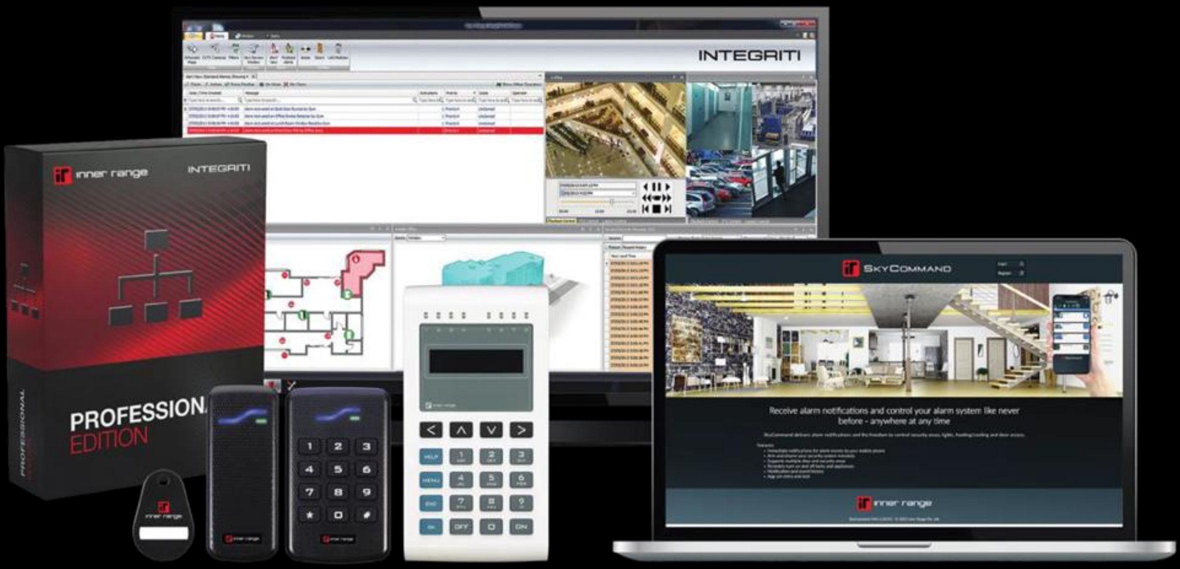
RELEASE NOTES

inner range

UNIFIED VIDEO, ACCESS & SECURITY SYSTEMS



INTEGRITI

Release Notes 25.1.0

July 2025

INNERRANGE.COM

Contents

Contents

Version 25.1.0

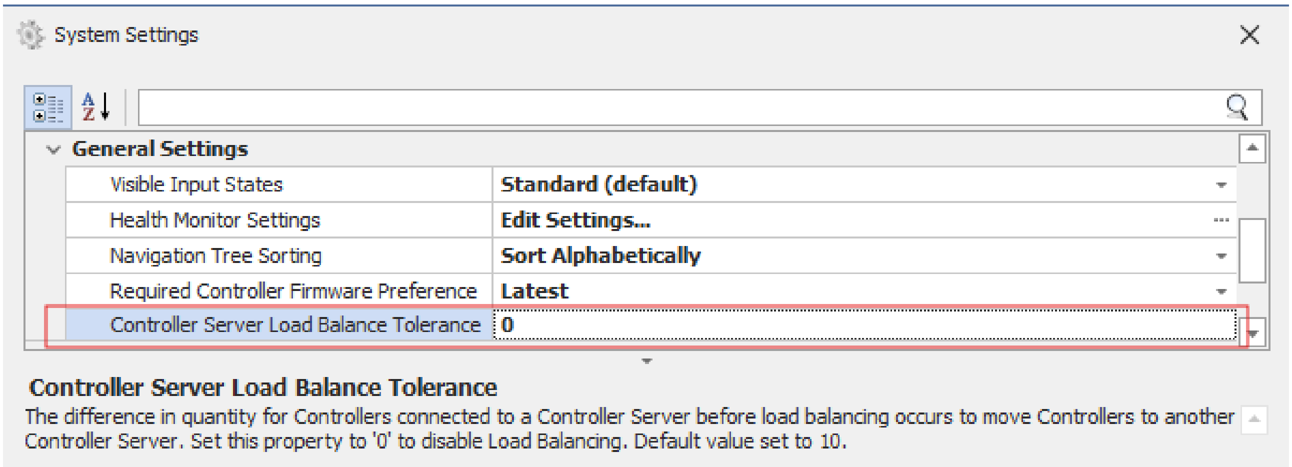
July 2025

Controller Load Balancing

For Integriti installations utilizing multiple Controller servers within its High Availability architecture, Integriti 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 Integriti's System Settings.



Visible Input States	Standard (default)
Health Monitor Settings	Edit Settings...
Navigation Tree Sorting	Sort Alphabetically
Required Controller Firmware Preference	Latest
Controller Server Load Balance Tolerance	0

Controller Server Load Balance Tolerance
The difference in quantity for Controllers connected to a Controller Server before load balancing occurs to move Controllers to another Controller Server. Set this property to '0' to disable Load Balancing. Default value set to 10.

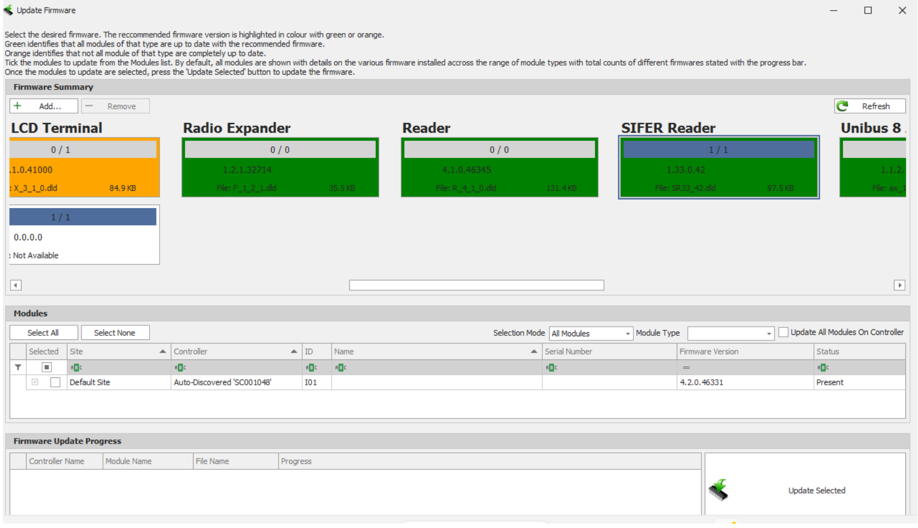
For new Integriti installations from version 25.1.0 onwards, Controller Load Balancing is enabled by default with no additional configuration needed. For systems upgrading from an earlier version, this feature will be disabled by default, maintaining existing connection configurations. It can be enabled 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: Integriti'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 Integriti's Controller Load Balancing, please refer to the Integriti Load Balancing guide.

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.



Update Firmware

Select the desired firmware. The reccommended firmware version is highlighted in colour with green or orange.
Green identifies that all modules of that type are up to date with the recommended firmware.
Orange identifies that not all module of that type are completely up to date.
Tick the modules to update from the Modules list. By default, all modules are shown with details on the various firmware installed accross the range of module types with total counts of different firmwares stated with the progress bar.
Once the modules to update are selected, press the 'Update Selected' button to update the firmware.

Firmware Summary

LCD Terminal	Radio Expander	Reader	SIFER Reader	Unibus 8
0 / 1 .1.0.41000 : X_3_1_0.dld 84.9 KB	0 / 0 1.2.1.32714 File: F_1_2_1.dld 35.5 KB	0 / 0 4.1.0.46345 File: R_4_1_0.dld 131.4 KB	1 / 1 1.33.0.42 File: SR33_42.dld 97.5 KB	1.1.2. File: ax_
1 / 1 0.0.0.0 : Not Available				

Modules

Selection Mode: All Modules
Module Type:
□ Update All Modules On Controller

Selected	Site	Controller	ID	Name	Serial Number	Firmware Version	Status
□	Default Site	Auto-Discovered 'SC001048'	I01			4.2.0.46331	Present

Firmware Update Progress

Controller Name	Module Name	File Name	Progress

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.

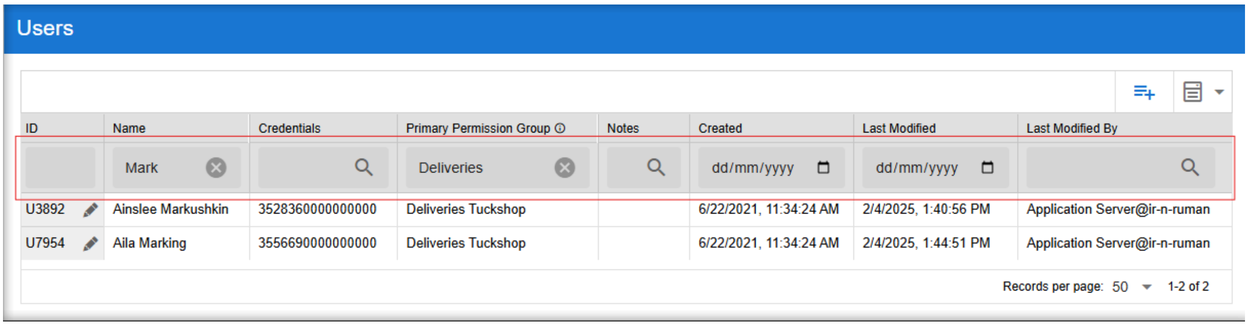
3. **Firmware Update Progress:** This section allows you to start and track the firmware update process. Pressing the 'Update Selected' button will apply the selected firmware to the chosen modules. Each module will show its progress in the progress list, allowing you to clearly track the update.

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.

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.

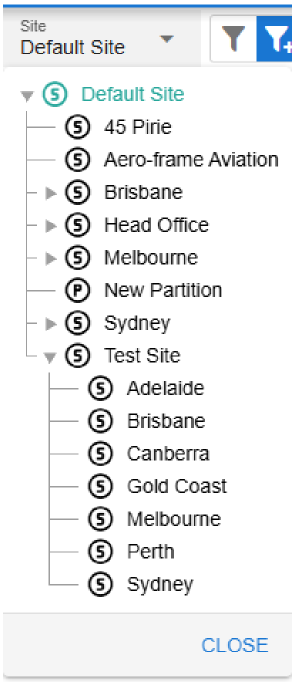


Users

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

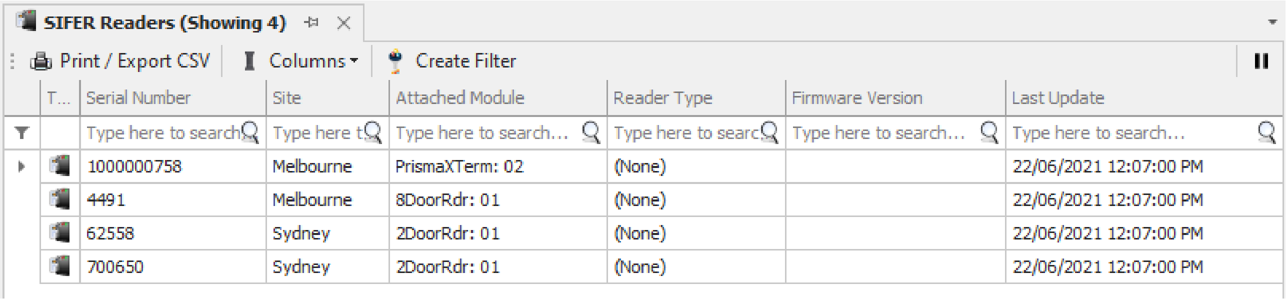
- **Web Client:** The Site Tree in the navigation panel is now sorted alphabetically, making it simpler to find Sites.



Site
Default Site

- Ⓢ Default Site
  - Ⓢ 45 Pirie
  - Ⓢ Aero-frame Aviation
  - Ⓢ Brisbane
  - Ⓢ Head Office
  - Ⓢ Melbourne
  - Ⓟ New Partition
  - Ⓢ Sydney
  - Ⓢ Test Site
    - Ⓢ Adelaide
    - Ⓢ Brisbane
    - Ⓢ Canberra
    - Ⓢ Gold Coast
    - Ⓢ Melbourne
    - Ⓢ Perth
    - Ⓢ Sydney

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



T...	Serial Number	Site	Attached Module	Reader Type	Firmware Version	Last Update
	Type here to search	Type here t	Type here to search...	Type here to searc	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 Integriti 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.

Documentations

- **Hardware and Software Prerequisites:** Updated the Platform (Operating System) and MS SQL versions supported by Integriti.
- **Guide – Integriti Load Balancing:** Added guide describing usage and configuration of Controller Load Balancing.
- **Integriti 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

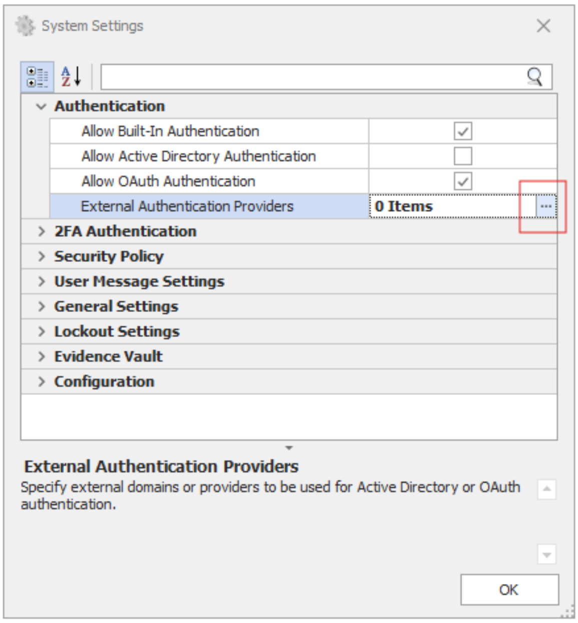
January 2025

OAuth Authentication

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

Integriti 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 Integriti SW. Where this flow is configured, Operators will instead be required to login via a separate web browser (opened automatically by the Integriti 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, Integriti 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')

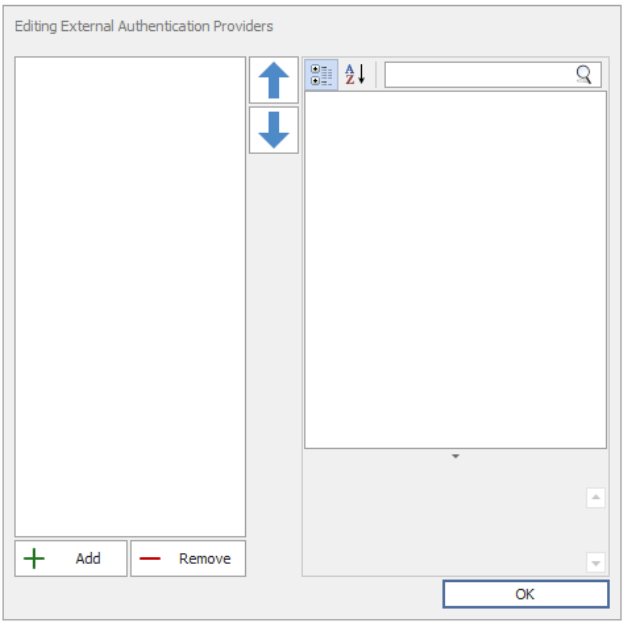


System Settings

Authentication
- Allow Built-In Authentication ☑
- Allow Active Directory Authentication □
- Allow OAuth Authentication ☑
- External Authentication Providers: 0 Items

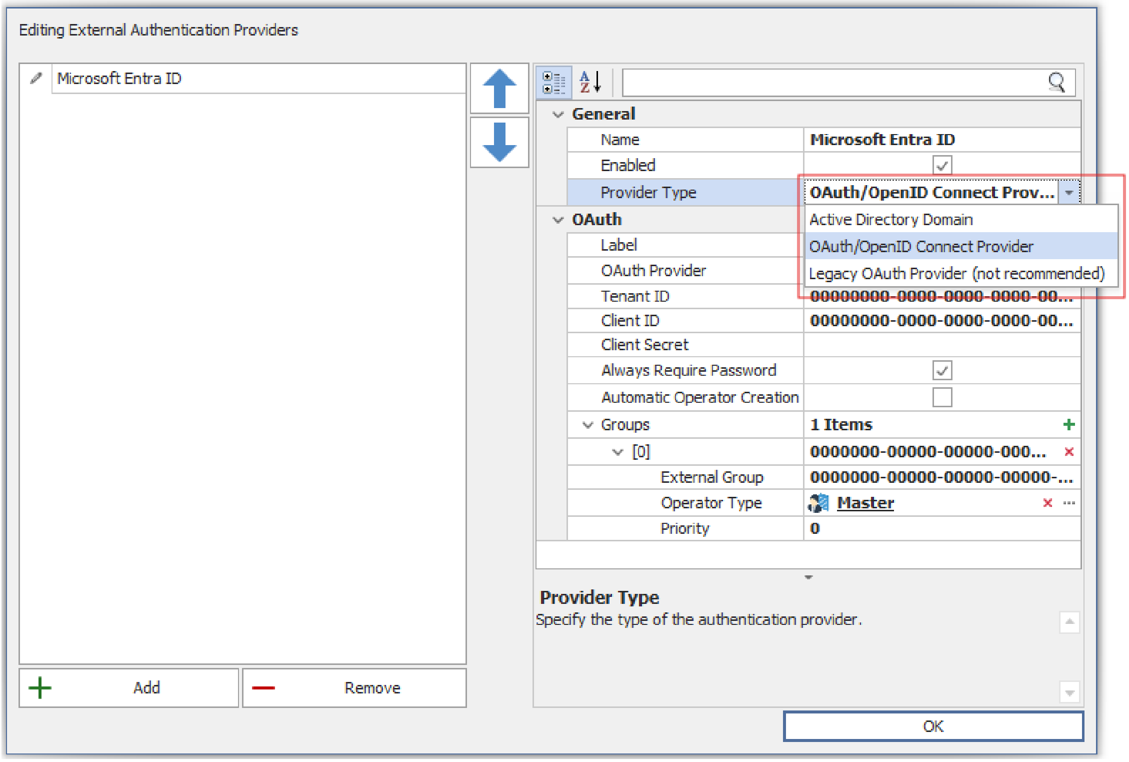
External Authentication Providers

Specify external domains or providers to be used for Active Directory or OAuth authentication.



Editing External Authentication Providers

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.



Editing External Authentication Providers

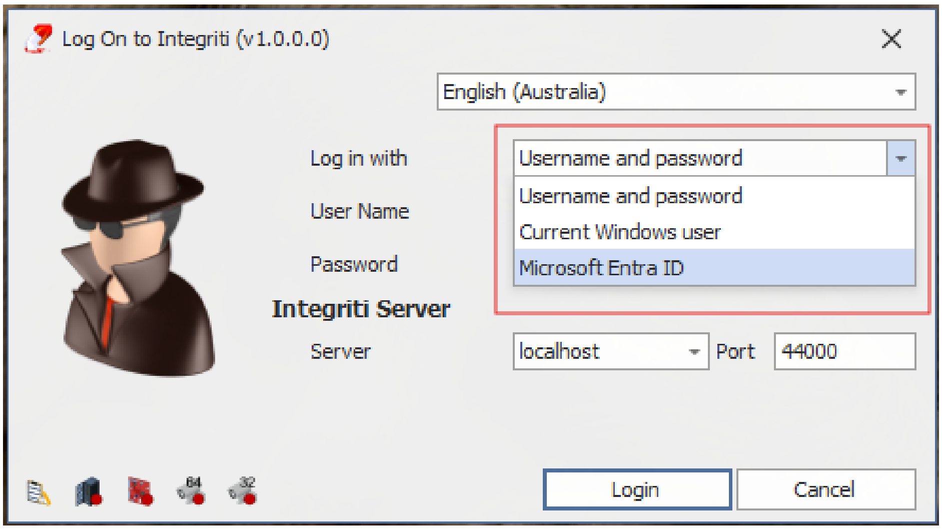
Microsoft Entra ID

General	
Name	**Microsoft Entra ID**
Enabled	☑
Provider Type	**OAuth/OpenID Connect Prov...**
OAuth	
Label	
OAuth Provider	
Tenant ID	**00000000-0000-0000-0000-00...**
Client ID	**00000000-0000-0000-0000-00...**
Client Secret	
Always Require Password	☑
Automatic Operator Creation	□
Groups	**1 Items**
[0]	**0000000-00000-00000-000...**
External Group	**0000000-00000-00000-00000-...**
Operator Type	**Master**
Priority	**0**

Active Directory Domain
OAuth/OpenID Connect Provider
Legacy OAuth Provider (not recommended)

Provider Type
Specify the type of the 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 Integriti 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 Integriti software.



Log On to Integriti (v1.0.0.0)

English (Australia)

Log in with: Username and password

User Name

Password

Integriti Server

Server: localhost Port: 44000

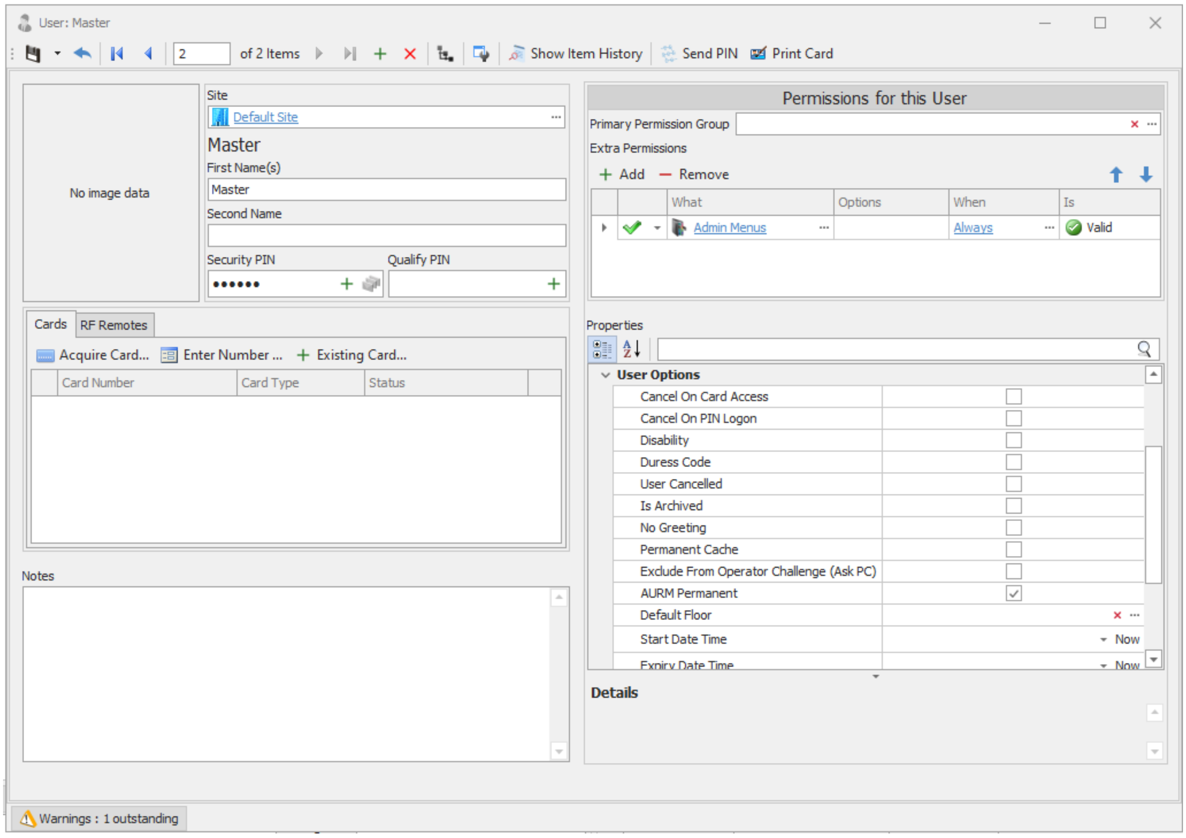
Upgrading Integriti systems will have their Active Directory and OAuth SSO configuration automatically migrated to the new 'External Authentication Provider' configuration, allowing them to continue using the system with no manual changes needing to be made. It is recommended to migrate legacy OAuth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

Archiving Users

With Integriti 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 Integriti 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.



Site: Default Site

Master

First Name(s): Master

Second Name:

Security PIN: ••••••

Qualify PIN:

Card Number	Card Type	Status

Permissions for this User

Primary Permission Group:

Extra Permissions

What	Options	When	Is
Admin Menus		Always	Valid

User Options

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	Now
Expiry Date Time	Now

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 Integriti CS will no longer be officially supported, as this can result in conflicting User IDs.

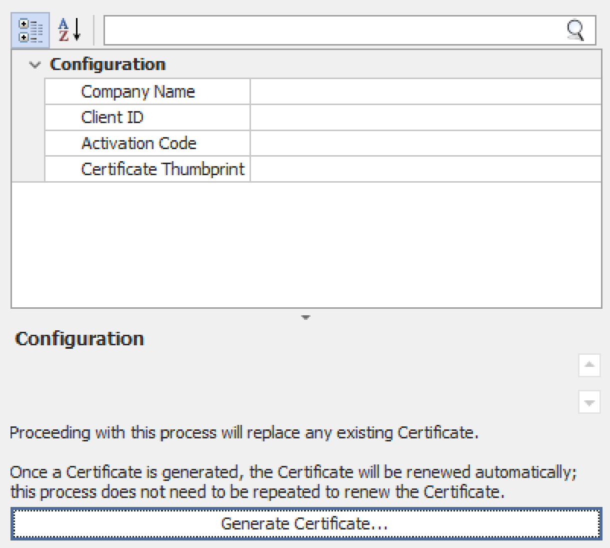
KONE Access 1000 Integration

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 Integriti, 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).

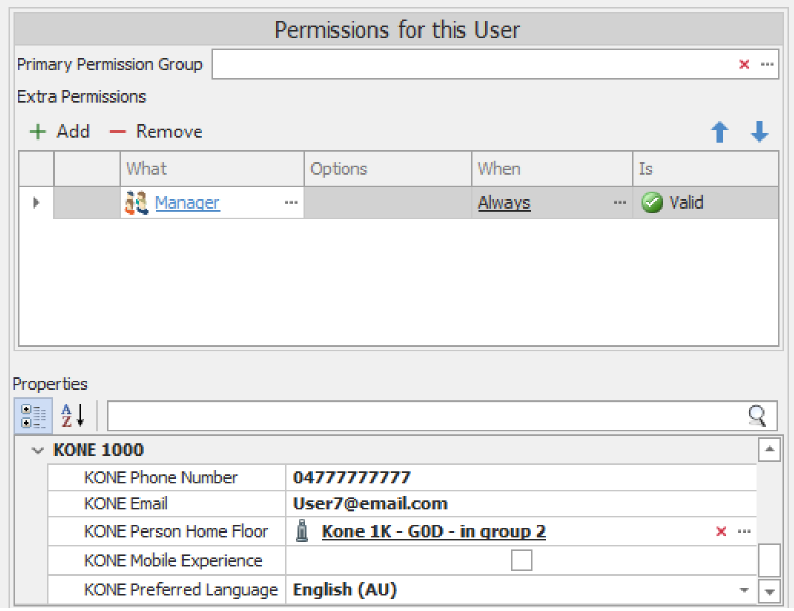


Proceeding with this process will replace any existing Certificate.

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

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 Integriti 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 Integriti. 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

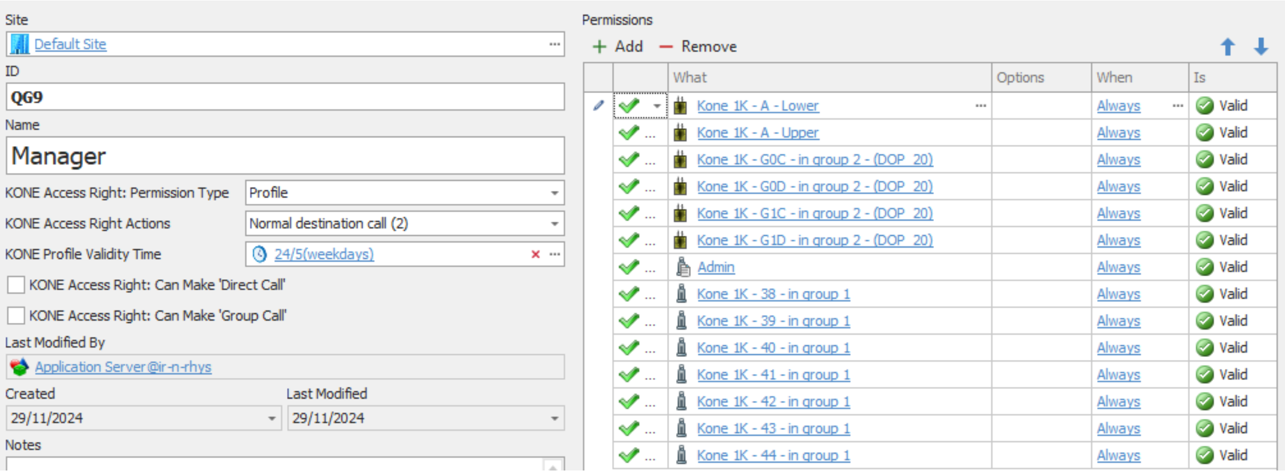
	What	Options	When	Is
	Manager		Always	Valid

Properties

KONE 1000

KONE Phone Number	04777777777
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

Default Site

ID

QG9

Name

Manager

KONE Access Right: Permission Type	Profile
KONE Access Right Actions	Normal destination call (2)
KONE Profile Validity Time	24/5(weekdays)

□ KONE Access Right: Can Make 'Direct Call'

□ KONE Access Right: Can Make 'Group Call'

Last Modified By

Application Server@ir-n-rhys

Created	Last Modified
29/11/2024	29/11/2024

Notes

Permissions

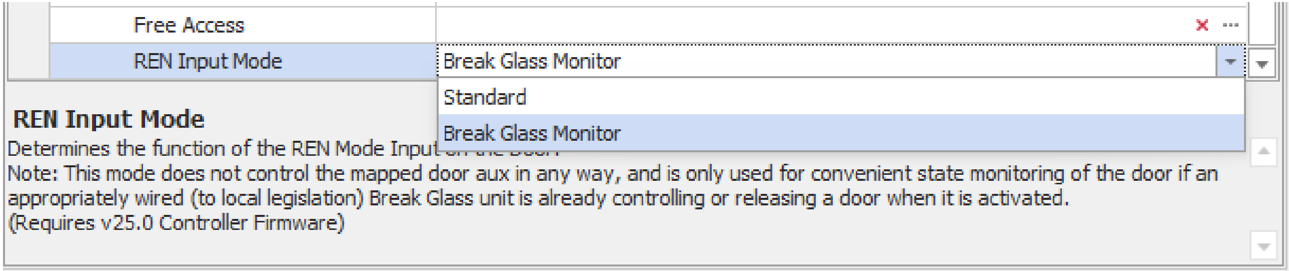
+ Add — Remove

	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.

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.

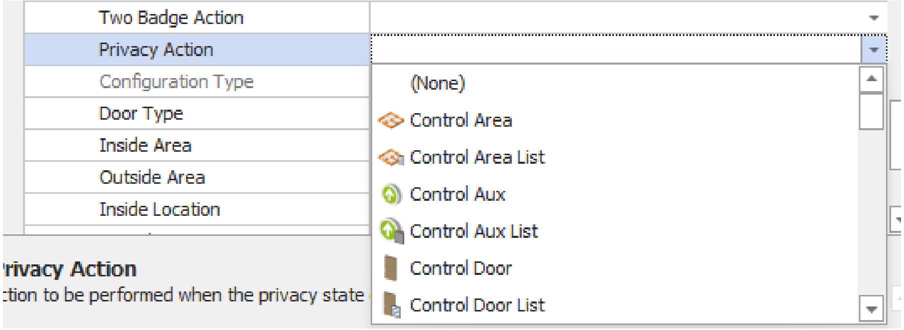


Free Access

REN Input Mode: Break Glass Monitor

REN Input Mode
Determines the function of the REN Mode Input
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.
(Requires v25.0 Controller Firmware)

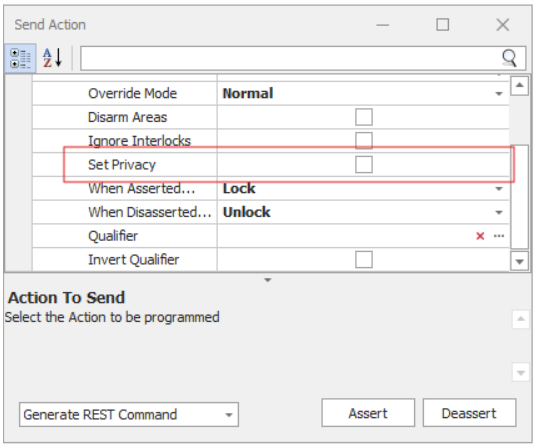
- **Door Privacy Mode Action:** Doors can now have a Privacy Action configured to trigger when the privacy state of the door is changed.



Two Badge Action
Privacy Action
Configuration Type
Door Type
Inside Area
Outside Area
Inside Location

rivacy Action
tion to be performed when the privacy state

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



Send Action

Override Mode	Normal
Disarm Areas	□
Ignore Interlocks	□
Set Privacy	□
When Asserted...	Lock
When Disasserted...	Unlock
Qualifier	
Invert Qualifier	□

Action To Send
Select the Action to be programmed

- **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

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

August 2024

Issues Resolved

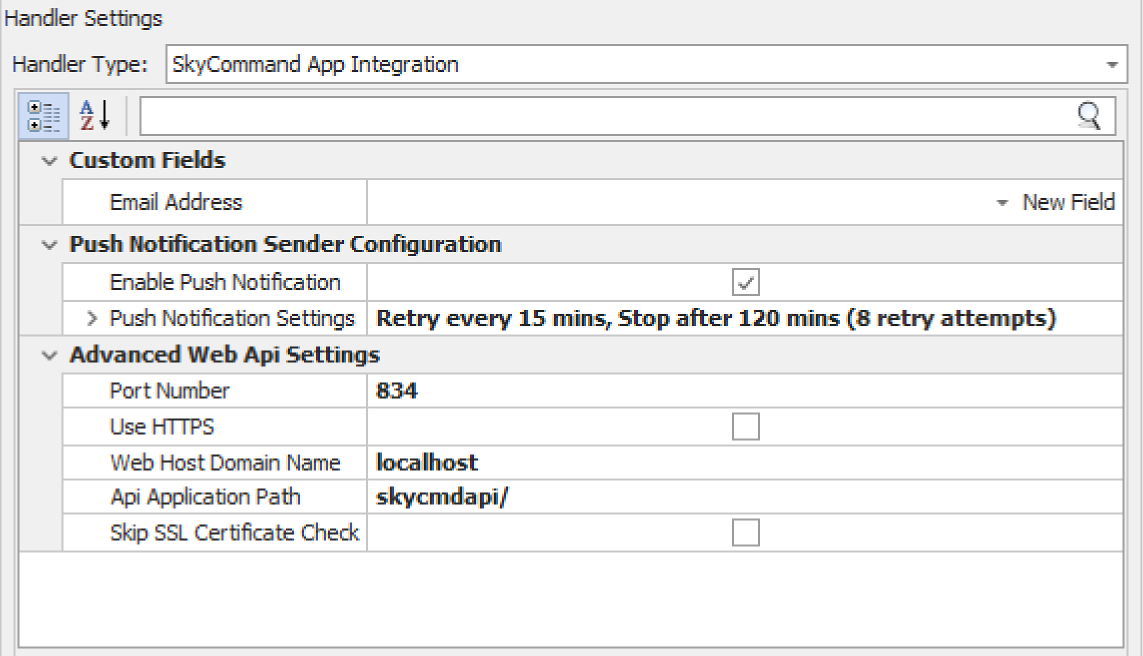
- **Custom Layouts:** Resolved an issue that could cause Custom Fields to not appear in a customised User Editor layout. The custom fields should once again be visible in the layout and in the 'Customisation' window when modifying the User Editor's layout.
- **System Warnings:** Resolved an issue where 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

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



Handler Settings

Handler Type: SkyCommand App Integration

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

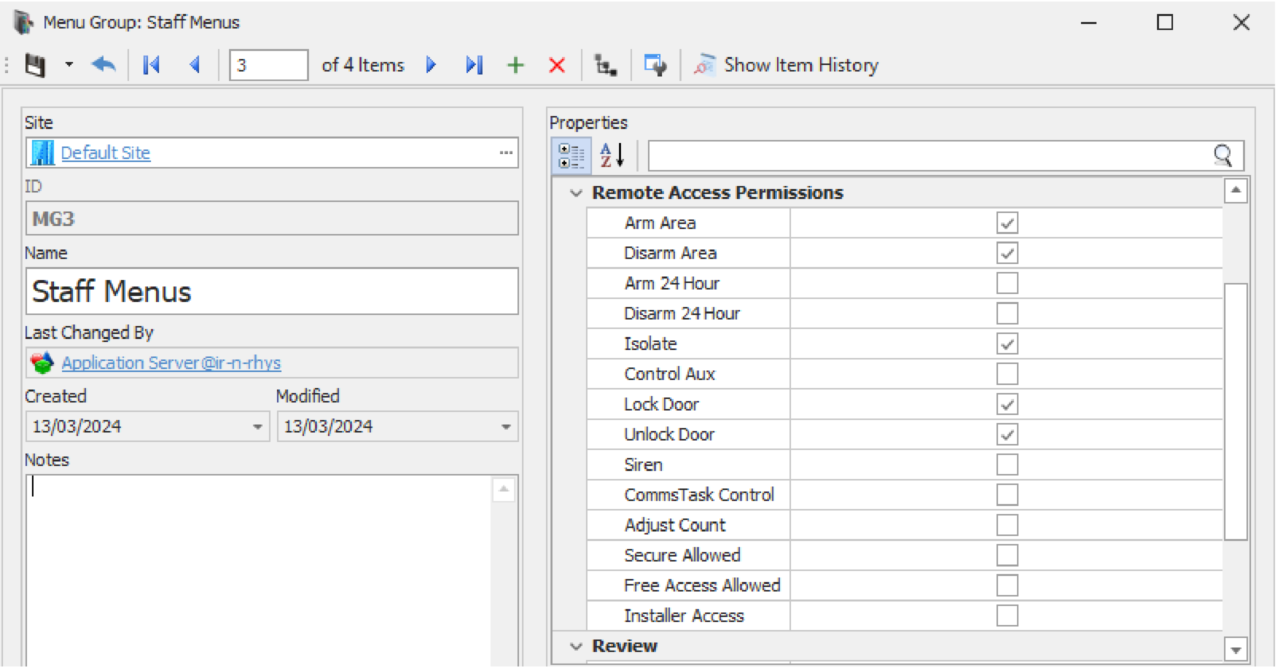
Port Number	834
Use HTTPS	□
Web Host Domain Name	localhost
Api Application Path	skycmdapi/
Skip SSL Certificate Check	□

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 Integriti 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.



Site: Default Site

ID: MG3

Name: Staff Menus

Last Changed By: Application Server@ir-n-rhys

Created: 13/03/2024

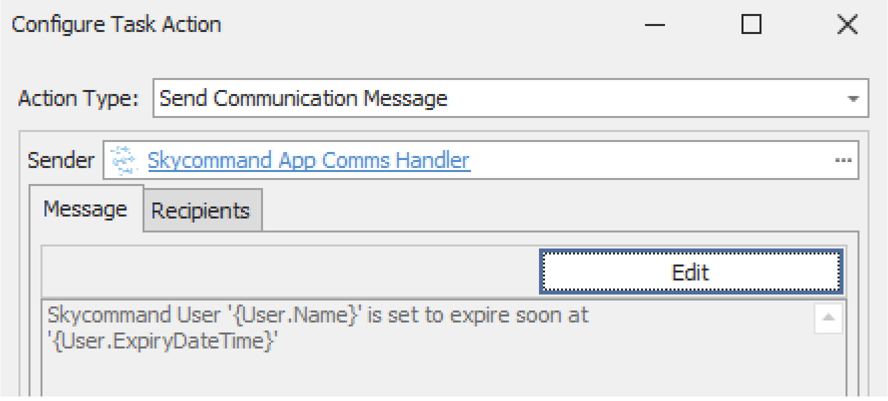
Modified: 13/03/2024

Notes

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	□

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.



Action Type: Send Communication Message

Sender: Skycommand App Comms Handler

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

Lift Integration Improvements

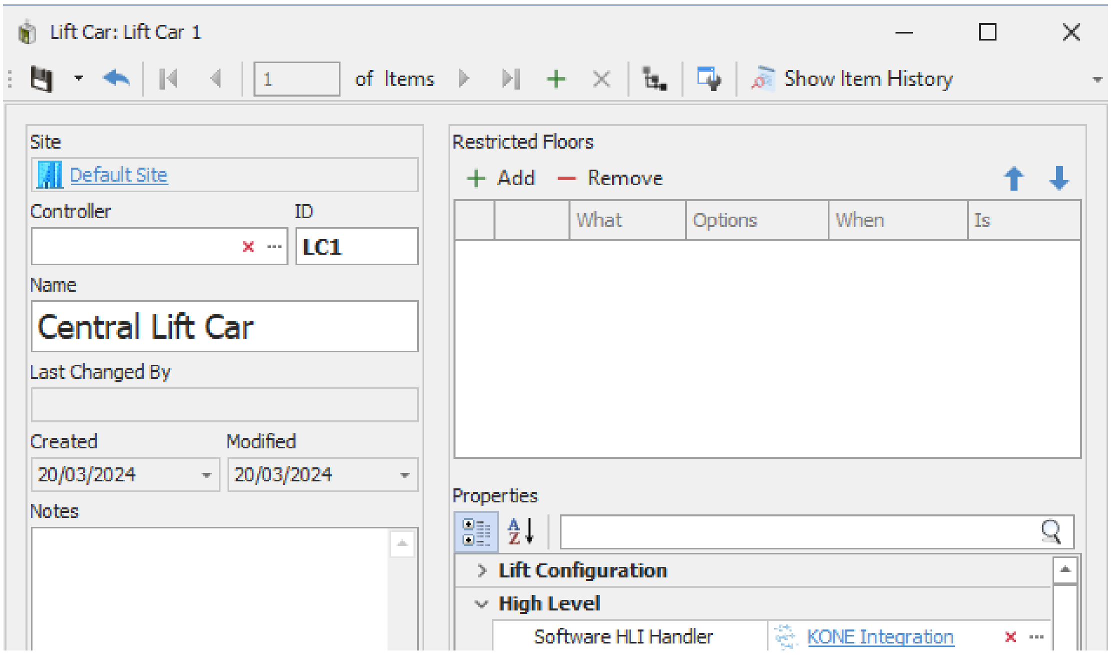
Several improvements have been made to the KONE and Schindler Lift Integrations, primarily streamlining the installation process by reducing the volume of custom fields that need to be created and configured, as well as leveraging the new 'Entity Link' custom field to more strongly connect the information 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'



Lift Car: Lift Car 1

Site: Default Site

Controller:

ID: LC1

Name: Central Lift Car

Last Changed By:

Created: 20/03/2024

Modified: 20/03/2024

Notes:

Restricted Floors

		What	Options	When	Is

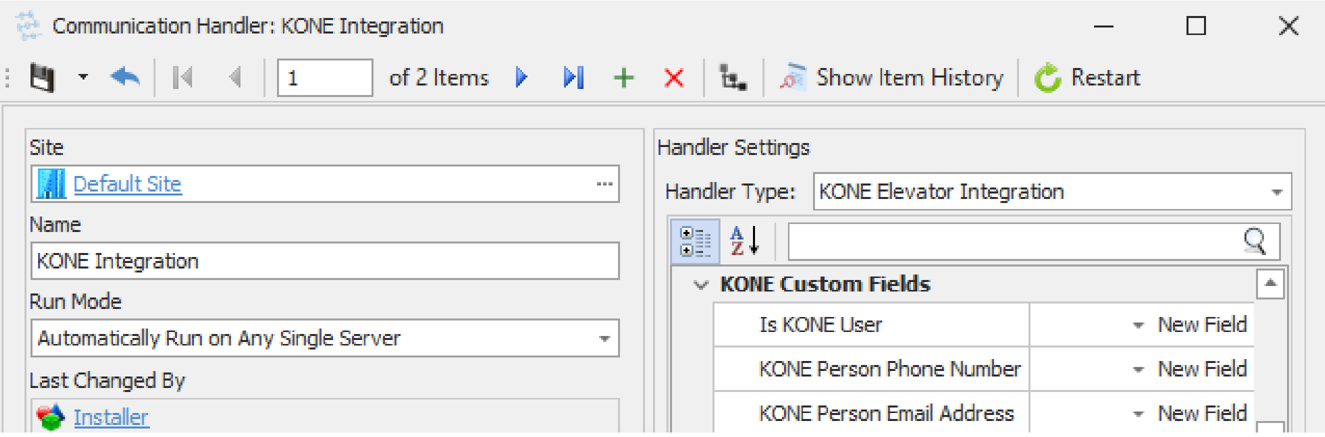
Properties

Lift Configuration

High Level

Software HLI Handler: KONE Integration

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.



Communication Handler: KONE Integration

Site: Default Site

Name: KONE Integration

Run Mode: Automatically Run on Any Single Server

Last Changed By: Installer

Handler Settings

Handler Type: KONE Elevator Integration

KONE Custom Fields

Is KONE User	New Field
KONE Person Phone Number	New Field
KONE Person Email Address	New Field

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 Integriti) 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.

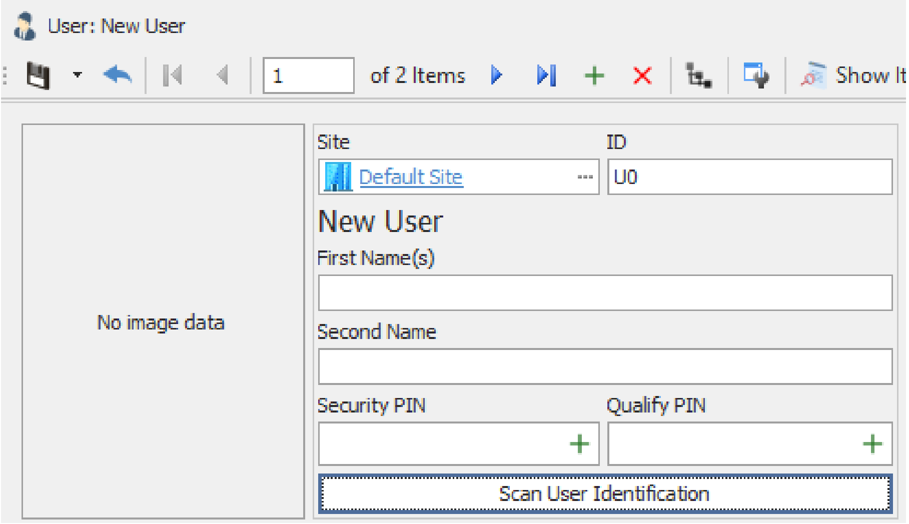
Scanner Integration Support

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

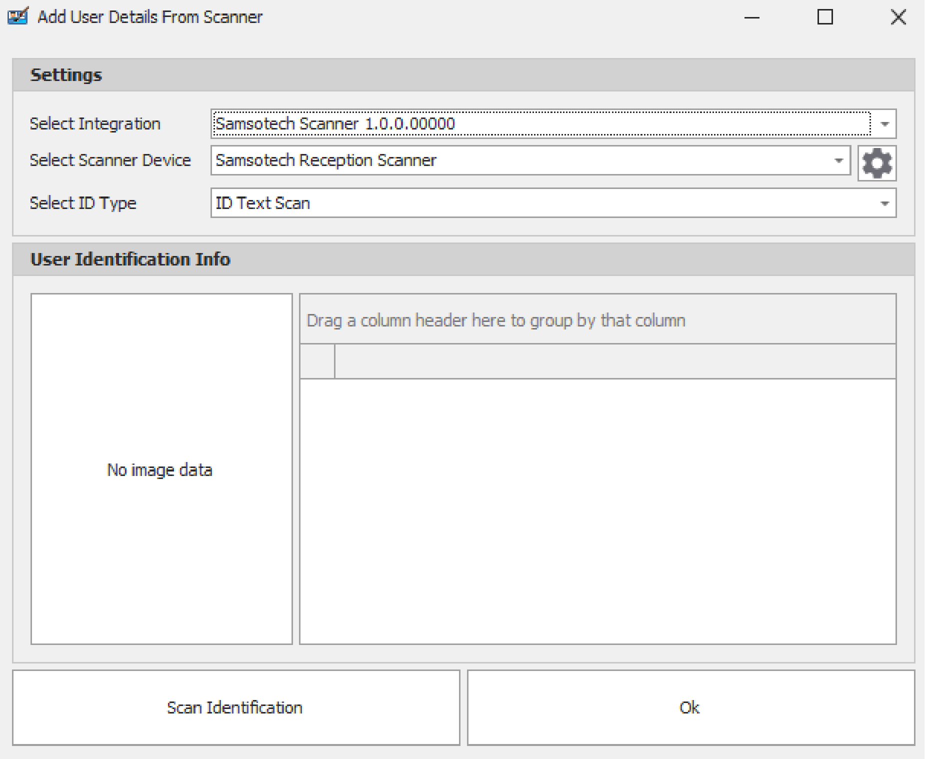
These integrations help streamline creating and/or updating new Users by importing information such as a User’s Name, Address, etc. from scanned documents, reducing the amount of manually entered information for Users created/updated in this way.

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.

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.



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

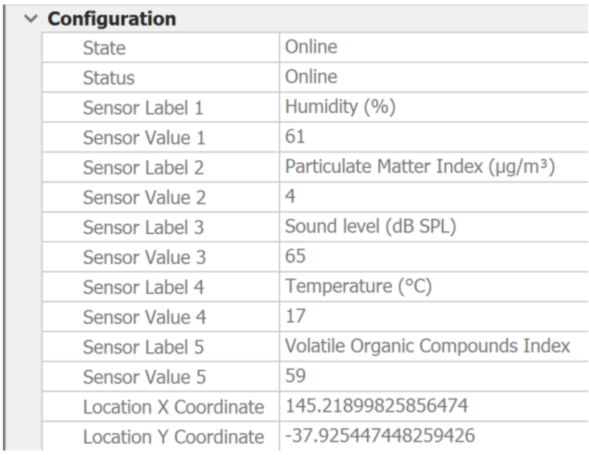
Select ID Type: ID Text Scan

Sensor Integration Support:

Support for Sensor Integrations has been added. Sensor Integrations update a Sensor's state in Integriti 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 Integriti, 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.

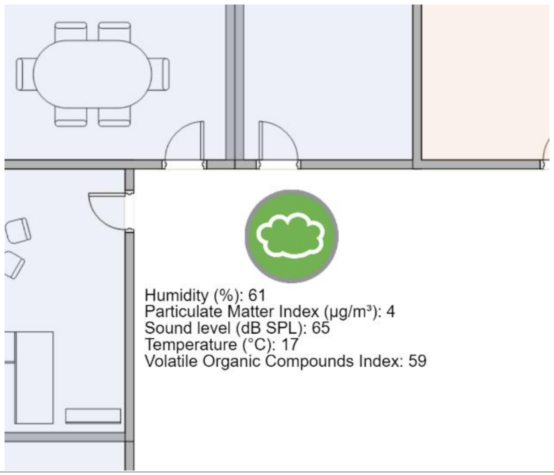
Sensor States are defined and maintained by Sensor Integrations, with a name and value for each field. These are automatically updated by the Integration while it is online and receiving updates from the Third Party System. An example of the state values and names:



Configuration

State	Online
Status	Online
Sensor Label 1	Humidity (%)
Sensor Value 1	61
Sensor Label 2	Particulate Matter Index (µg/m³)
Sensor Value 2	4
Sensor Label 3	Sound level (dB SPL)
Sensor Value 3	65
Sensor Label 4	Temperature (°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

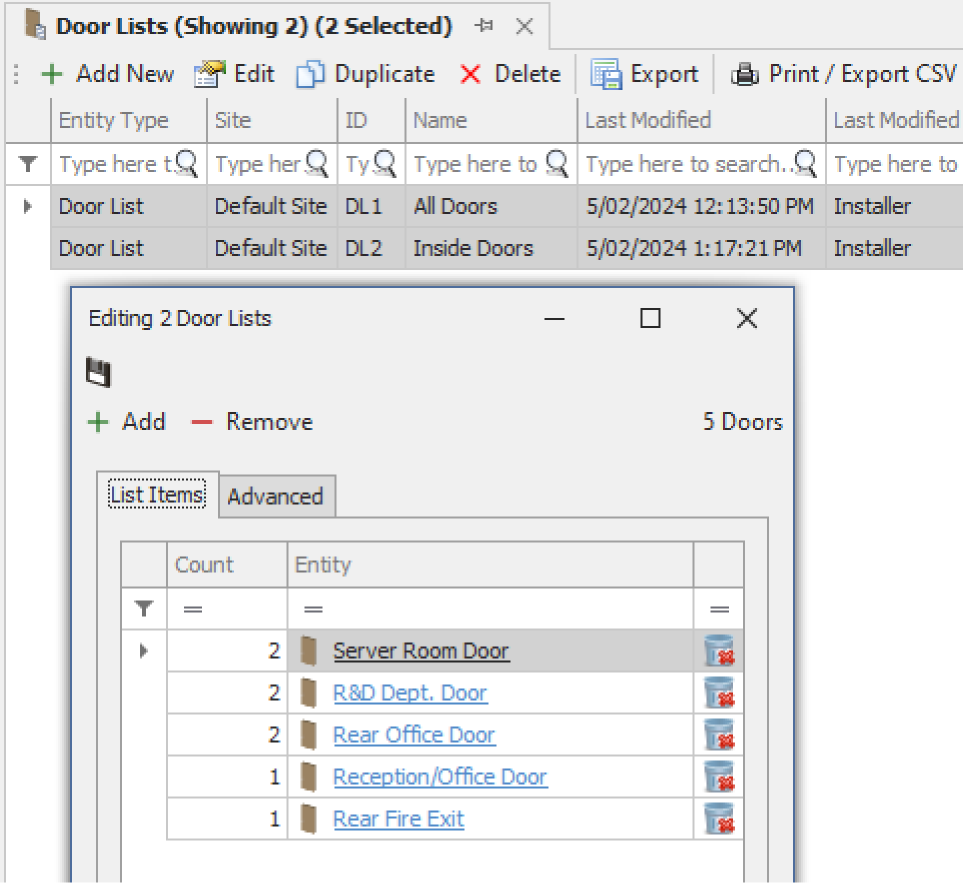
To display this information on Schematics Maps requires the configuration of an Element Presenter, which defines what information is displayed, as well as conditions to change the appearance of the presenter. For more information on how to configure Element Presenters, please refer to the 'Integriti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



Humidity (%): 61
Particulate Matter Index (µg/m³): 4
Sound level (dB SPL): 65
Temperature (°C): 17
Volatile Organic Compounds Index: 59

Improvements

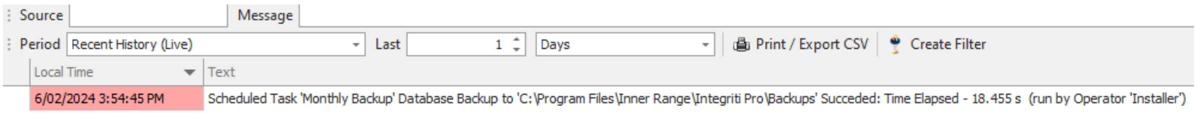
- **License Key Manager:** Licenses are now sorted by ‘Feature Name’ by default.
- **Review Sender:** Improved TLS support for the Review Sender.
- **Format Strings:**
  - Format String properties can now be cleared by a button in the property editor
  - Format Strings can now have a Format String configured 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.



Entity Type	Site	ID	Name	Last Modified	Last Modified
Door List	Default Site	DL1	All Doors	5/02/2024 12:13:50 PM	Installer
Door List	Default Site	DL2	Inside Doors	5/02/2024 1:17:21 PM	Installer

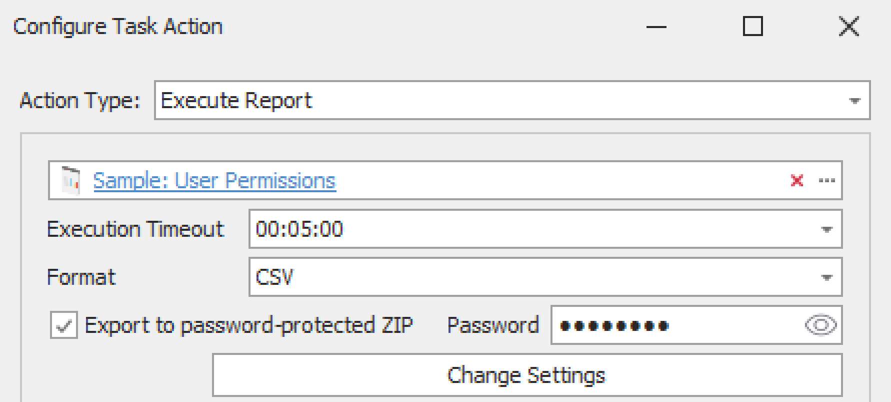
Count	Entity
2	Server Room Door
2	R&D Dept. Door
2	Rear Office Door
1	Reception/Office Door
1	Rear Fire Exit

- **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.



Local Time	Text
6/02/2024 3:54:45 PM	Scheduled Task 'Monthly Backup' Database Backup to 'C:\Program Files\Inner Range\Integriti Pro\Backups' Succeded: Time Elapsed - 18.455 s (run by Operator 'Installer')

- **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:



Configure Task Action

Action Type: Execute Report

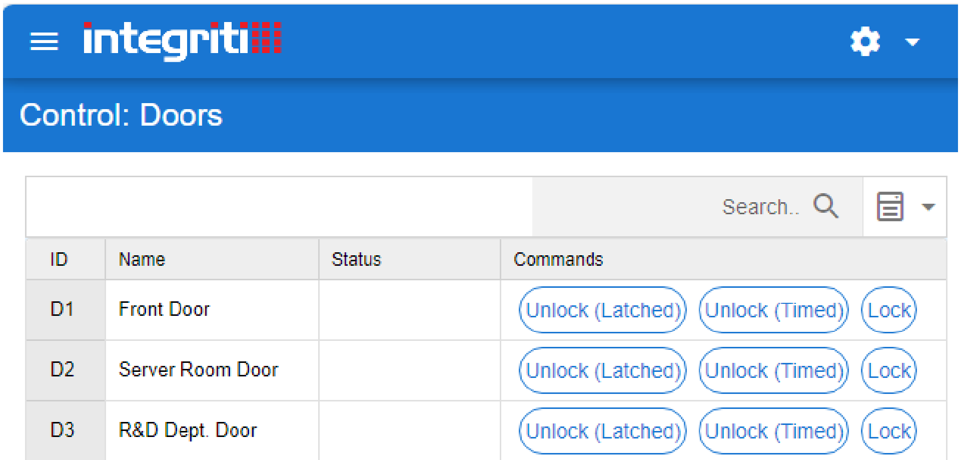
Sample: User Permissions

Execution Timeout: 00:05:00

Format: CSV

☑ Export to password-protected ZIP Password: ●●●●●●●●●

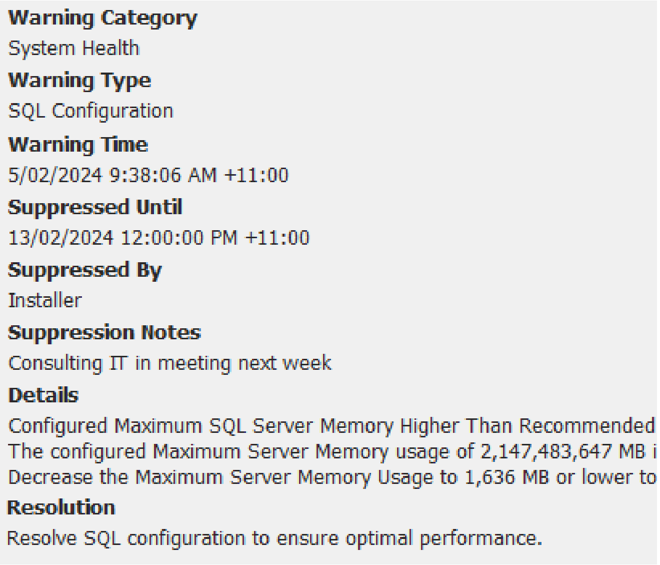
- **Web Interface:**
  - An 'Unlock (Timed)' command has been added to the Web Interface under the 'Control: Doors' page.



ID	Name	Status	Commands
D1	Front Door		Unlock (Latched) Unlock (Timed) Lock
D2	Server Room Door		Unlock (Latched) Unlock (Timed) Lock
D3	R&D Dept. Door		Unlock (Latched) Unlock (Timed) Lock

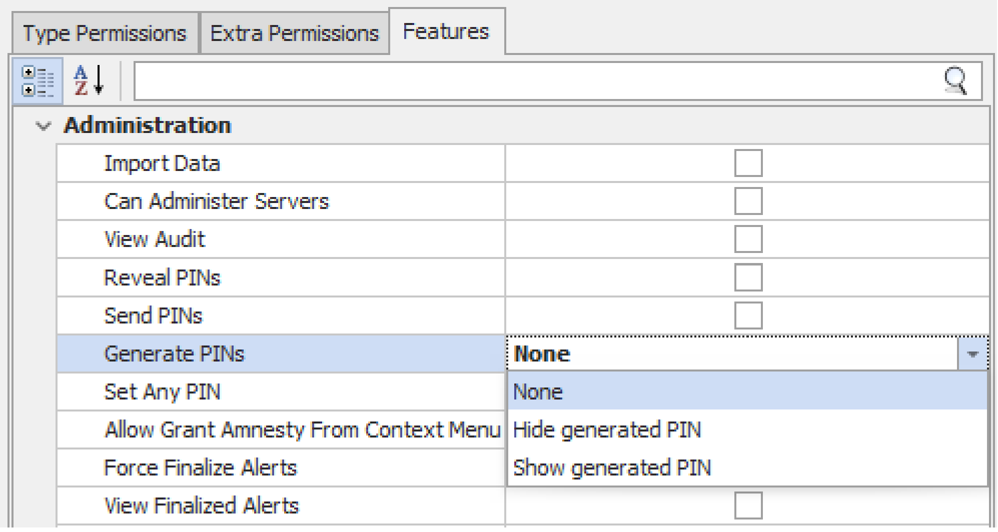
  - Operator Types can now be assigned a 'Web Client Timeout', defining the amount of time before an Operator is timed out when using the Web Interface without loading a new page. When upgrading to v24.0 and newer, this property will be set to the Operator Type's 'Inactivty Timeout Time' if one is definied, 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.

- **Integrated Device States:** The states ‘Enabled’, ‘Disabled’ and ‘Unmonitored’ have been added as states for Devices without persisted connections.
    - **Enabled:** Displayed for an Integration that has a persisted connection set to run, but before the connection has started up to confirm that the Integration has been set to run but not in an error state.
    - **Disabled:** Displayed for an Integration that has a persisted connection set to ‘Disabled’, which is different from ‘Offline’ which indicates the connection has failed and stopped.
    - **Unmonitored:** Displayed for Integrations that do not have a persisted connection, this state indicates that an Integration with no persisted connection is not in an error state simply for not having a persisted connection.
- **System Warnings:** Now display extra information for Warnings that were suppressed, including the suppressing Operator and notes.



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 i
Decrease the Maximum Server Memory Usage to 1,636 MB or lower to
Resolution
Resolve SQL configuration to ensure optimal performance.

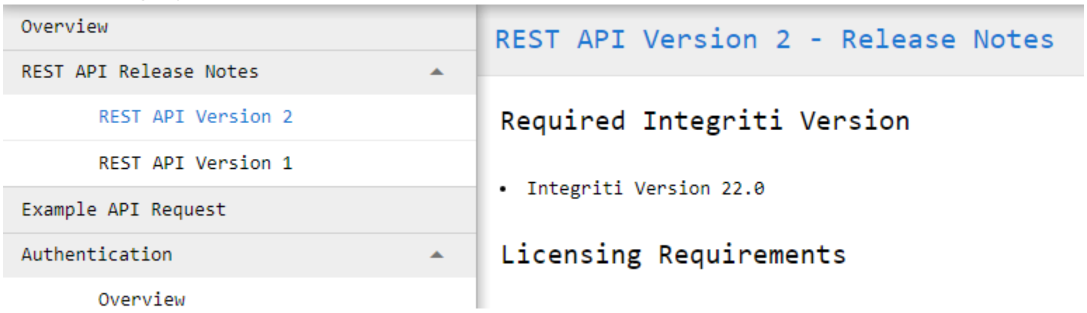
- **Operator PIN Permissions:** Operator options for viewing/setting PINs have been moved to Operator Types, including new options to deny setting auto-generated PINs and controlling manually entering or removing a User’s PIN.



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	□

- **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 Integriti 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



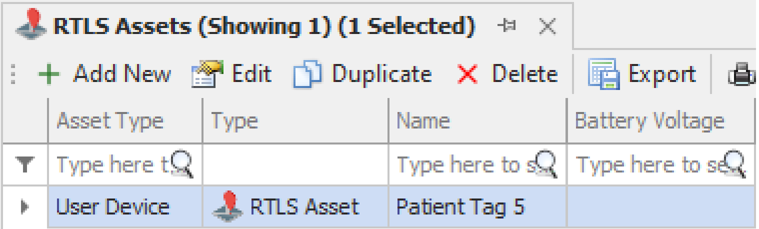
REST API Version 2 - Release Notes

Required Integriti Version

- Integriti Version 22.0

Licensing Requirements

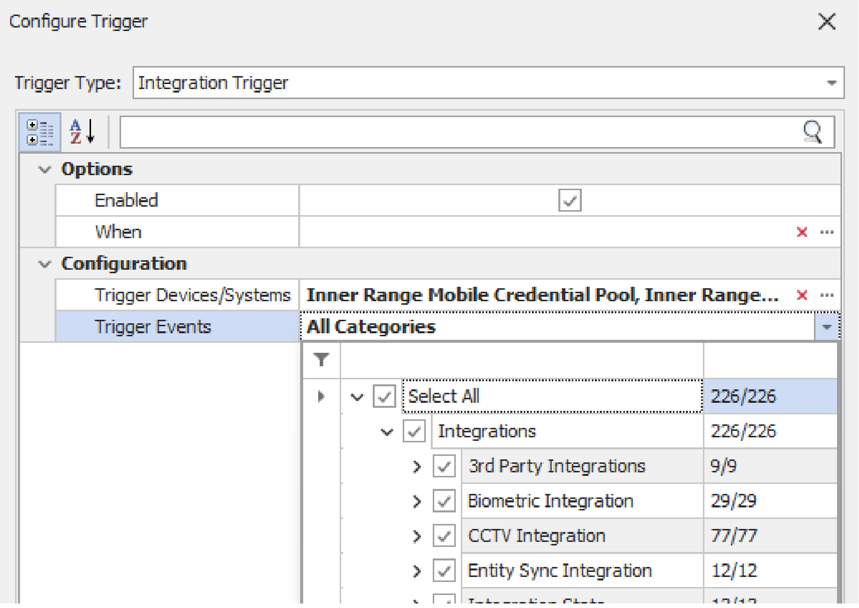
  - Username and Password fields in Authorisation Headers will now display errors when empty.
  - The ‘Request Body’ tab is no longer displayed for Requests that do not require a body in the REST API Doc.
- **Users:** Added a new reportable property to Users’ State, ‘User Last Accessed’, which contains 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.



Asset Type	Type	Name	Battery Voltage
Type here t		Type here to s	Type here to s
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.

  - **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 (Integriti 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.



Configure Trigger

Trigger Type: Integration Trigger

Options
Enabled ☑
When

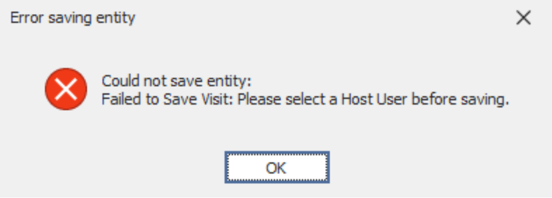
Configuration
Trigger Devices/Systems: **Inner Range Mobile Credential Pool, Inner Range...**
Trigger Events: **All Categories**

☑ Select All	226/226
☑ Integrations	226/226
☑ 3rd Party Integrations	9/9
☑ Biometric Integration	29/29
☑ CCTV Integration	77/77
☑ Entity Sync Integration	12/12

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.

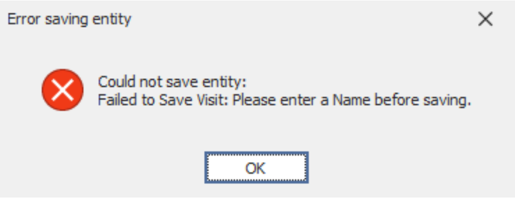
- **Control Modules:** The 'AC Holdoff Review' property has been added, preventing AC Failure from being logged to Review if set.

- **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.



Error saving entity

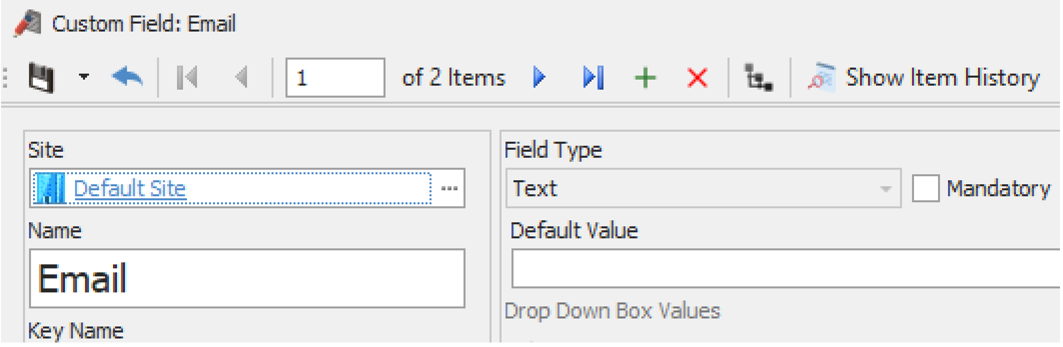
Could not save entity:
Failed to Save Visit: Please select a Host User before saving.



Error saving entity

Could not save entity:
Failed to Save Visit: Please enter a Name before saving.

- **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:



Custom Field: Email

Site: Default Site

Name: Email

Key Name

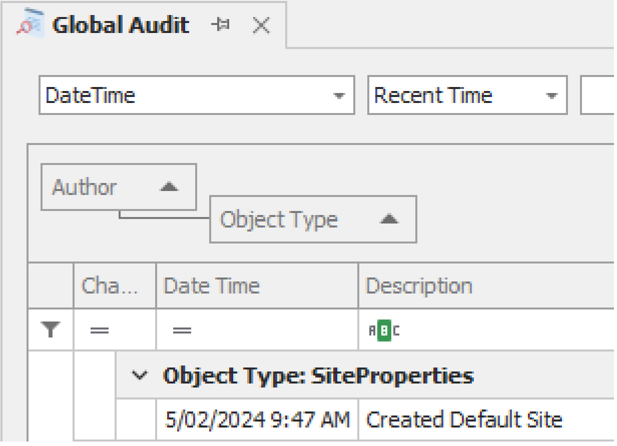
Field Type: Text

☐ Mandatory

Default Value

Drop Down Box Values

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:



Global Audit

Cha...	Date Time	Description
Object Type: SiteProperties		
	5/02/2024 9:47 AM	Created Default Site

- **.Net Version Warnings:** Pop-up messages generated when logging in to a Server with the Integriti 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 Inteface 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’ shorcut 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 occurrs 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.

- **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 Integriti 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

- **Integriti 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.

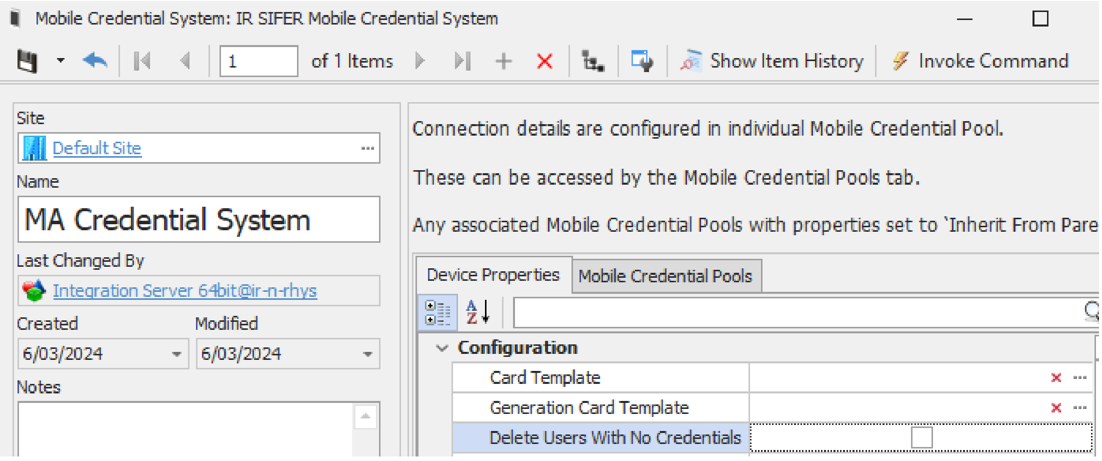
Version 23.1.2 Bug-Fix

March 2024

Issues Resolved

Mobile Access

- Resolved an issue preventing the ‘Delete Users With No Credentials’ property from appearing in a Mobile Access Integrated System’s configuration. Configuring this option will remove Users from Mobile Access when they have credentials removed from them in Integriti.



Mobile Credential System: IR SIFER Mobile Credential System

Site: Default Site

Name: MA Credential System

Last Changed By: Integration Server 64bit@ir-n-rhys

Created: 6/03/2024

Modified: 6/03/2024

Notes

Connection details are configured in individual Mobile Credential Pool.

These can be accessed by the Mobile Credential Pools tab.

Any associated Mobile Credential Pools with properties set to 'Inherit From Pare

Configuration

Card Template

Generation Card Template

Delete Users With No Credentials ☐

- Resolved an issue where Users that had Mobile Access credentials revoked could not be assigned a Mobile Access credential afterward.
    - If a User was in this state on upgrade, using the ‘Delete Users With No Credentials’ property and removing any revoked Mobile Access credentials from the User should remove the User from Mobile Access, allowing the User to be re-added and assigned a credential.
- Resolved an issue where a credential generated by the Mobile Access Integration could be instantly revoked after generation.

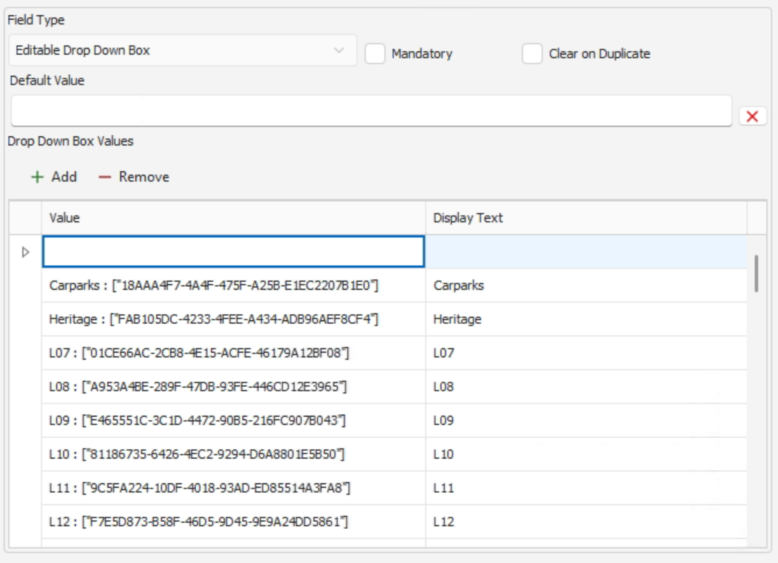
Integrated Devices: Resolved an issue preventing the ‘Associations’ tab in Integrated Device editors from being displayed after updating to v23.1

Version 23.1.1 Bug-Fix

December 2023

Improvements

- **Custom Fields:** Dropdown Custom Fields now have configurable display text for each value in its dropdown list. These are configurable in the UI when creating custom fields. This allows installers to create readable text for custom fields that were traditionally used for selecting unique identifiers when configuring entities like Users. Below is an example using KONE HLI custom fields.
  In the editor:



Field Type: Editable Drop Down Box

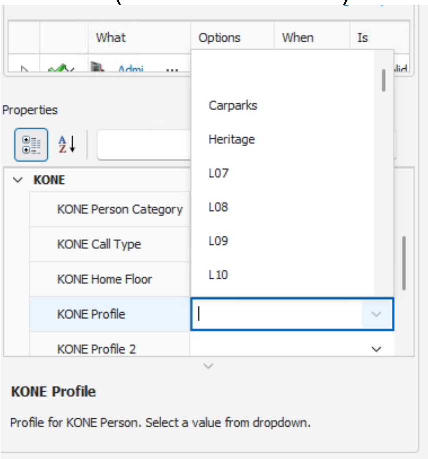
☐ Mandatory ☐ Clear on Duplicate

Default Value

Drop Down Box Values

Value	Display Text
Carparks : ["18AAA4F7-4A4F-475F-A25B-E1EC2207B1E0"]	Carparks
Heritage : ["FAB105DC-4233-4FEE-A434-ADB96AEF8CF4"]	Heritage
L07 : ["01CE66AC-2CB8-4E15-ACFE-46179A12BF08"]	L07
L08 : ["A953A4BE-289F-47DB-93FE-446CD12E3965"]	L08
L09 : ["E465551C-3C1D-4472-90B5-216FC907B043"]	L09
L10 : ["81186735-6426-4EC2-9294-D6A8801E5B50"]	L10
L11 : ["9C5FA224-10DF-4018-93AD-ED85514A3FA8"]	L11
L12 : ["F7E5D873-B58F-46D5-9D45-9E9A24DD5861"]	L12

While editing an entity with the custom field (in this case a User):



KONE Profile

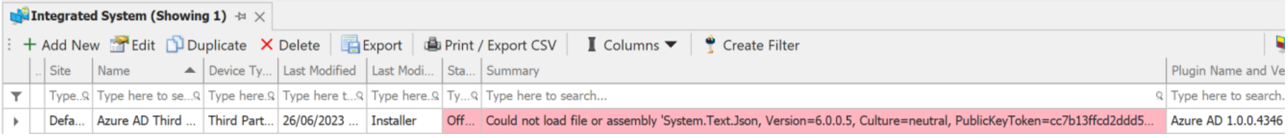
Profile for KONE Person. Select a value from dropdown.

- **KONE HLI:** KONE Custom Fields now take advantage of the new Display Text feature described above. Display Text is generated by the HLI when custom fields are populated, which is performed by stopping the Comms Handler, clicking ‘Show/Hide Service Data’, checking the ‘Populate Custom Fields’ check box, then starting the Comms Handler once again.

Version 23.1.1 Bug-Fix

Issues Resolved

- **Azure AD/Entra ID:** Resolved issue that prevented the Azure AD/Entra ID Integration from running on v23.1.0. This issue would be encountered on the integration starting up where the following message would be displayed in the device’s ‘Summary’:



..	Site	Name	Device Ty...	Last Modified	Last Modi...	Sta...	Summary	Plugin Name and Ve
	Type..	Type here to se...	Type here.	Type here t...	Type here.	Ty...	Type here to search...	Type here to search.
	Defa...	Azure AD Third ...	Third Part...	26/06/2023 ...	Installer	Off...	Could not load file or assembly 'System.Text.Json, Version=6.0.0.5, Culture=neutral, PublicKeyToken=cc7b13ffcd2ddd5...	Azure AD 1.0.0.4346

- **Cleanup Database Task Action:** Resolved issue that prevented ‘Review Export Location’ from selecting a destination folder instead of an existing file.
- **KONE HLI:** Resolved issue that prevented access messages via the Push Api Interface from generating Review and often requiring the Comms Handler to be restarted to continue receiving other Review messages and sync Users.
- **Permission Qualifiers:** Resolved issue that caused Delayed Start qualifiers to always be expired when no Expiry date was also defined.
- **Alerts:** Resolved an issue that prevented Alerts from triggering in cases where multiple app servers where started for the first time in quick succession.
- **REST Interface:** Resolved issue resulting in changes to most Card properties not being persisted when sent as part of a User. This includes changes to properties such as ‘Start Date/Time’ and ‘Expiry Date/Time’.

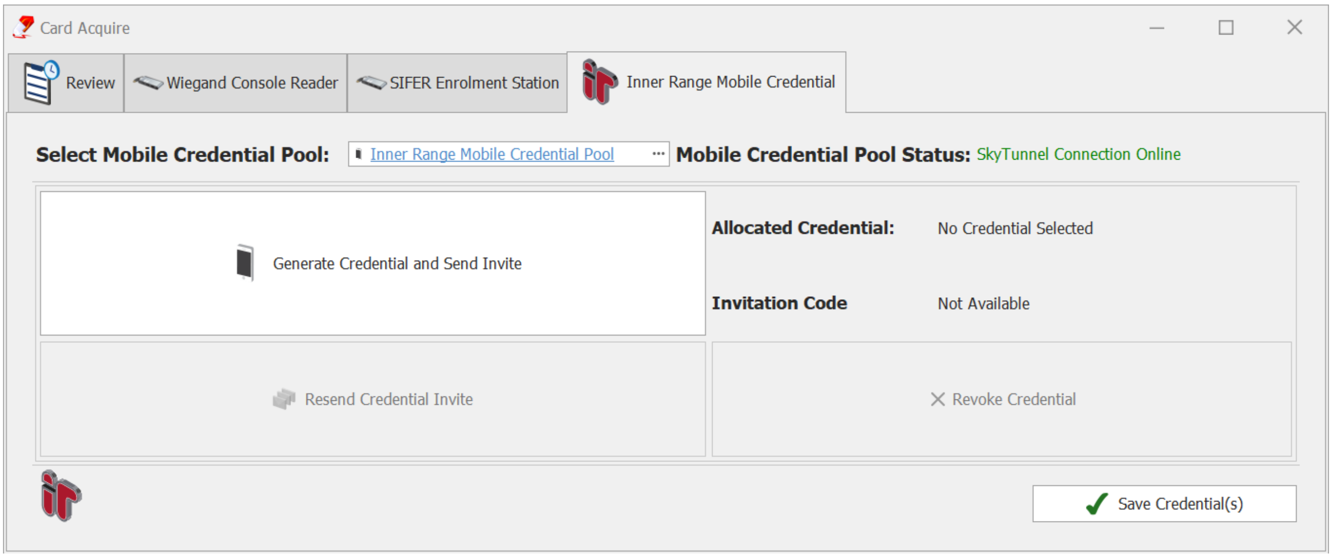
Version 23.1.0

November 2023

Inner Range Mobile Access

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 and generate mobile credentials. Sites running Integriti v23.1 will be able to take full advantage of Inner Range Mobile Access functionality when the Inner Range Mobile Access platform is launched, expected for release in Q2 2024**.**

Integriti v23.1 adds a full integration to Integriti's 'Inner Range Mobile Access' mobile credential architecture. This integration will come pre-installed with Integriti, with no need for a separate installer to get started using the integration.



Select Mobile Credential Pool: Inner Range Mobile Credential Pool

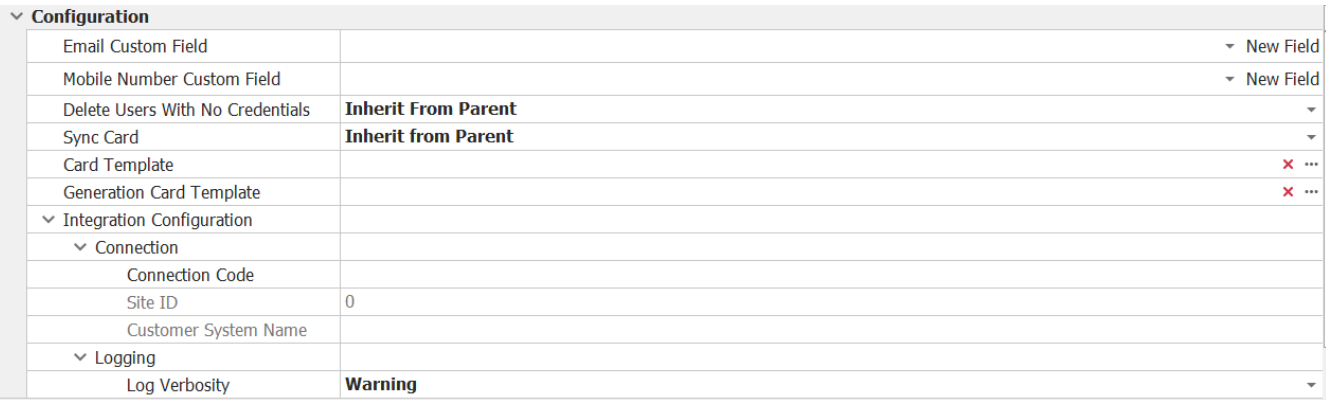
Mobile Credential Pool Status: SkyTunnel Connection Online

Allocated Credential: No Credential Selected

Invitation Code: Not Available

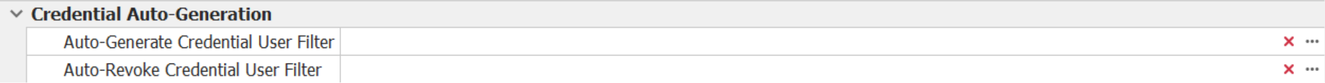
The Inner Range Mobile Access integration can be configured by adding a new Mobile Credential Pool. Once added, the *Email Custom* Field, *Generation Card Template* and *Connection Code* must be configured, before pressing Refresh Device to complete the linking process. The *Connection Code* can be retrieved from the *Integration* tab of the System on the Inner Range Mobile Access portal by selecting *Link Access Control System* and copying the *Link Code*.

Once the linking is successful, the Mobile Credential Pool is ready to start generating credentials.



Configuration	
Email Custom Field	New Field
Mobile Number Custom Field	New Field
Delete Users With No Credentials	Inherit From Parent
Sync Card	Inherit from Parent
Card Template	
Generation Card Template	
Integration Configuration	
Connection	
Connection Code	
Site ID	0
Customer System Name	
Logging	
Log Verbosity	Warning

Mobile Credentials can be added either manually through the *Inner Range Mobile Credential* tab in the Acquire Card Dialog for a given user, or automatically through the *Auto-Generate Credential User Filter* option in the Mobile Credential Pool. Once generated, the credential will be associated with the User in Integriti ready for use, and an invitation will be sent directly to the user's configured email address the Inner Range Mobile Access Portal. Once received by a user, the credential can then be activated directly from the Inner Range Mobile Access Application and used on compatible Inner Range SIFER readers.



Credential Auto-Generation	
Auto-Generate Credential User Filter	
Auto-Revoke Credential User Filter	

Revoking of generated mobile credentials can be achieved by simply setting the state of the credential in Integriti to an inactive state. This will prevent future access from the selected credential and remove the credential from the user's phone. Alternatively, an *Auto-Revoke Credential User Filter* can be configured in the Mobile Credential Pool to automatically revoke credentials when specified criteria is met.

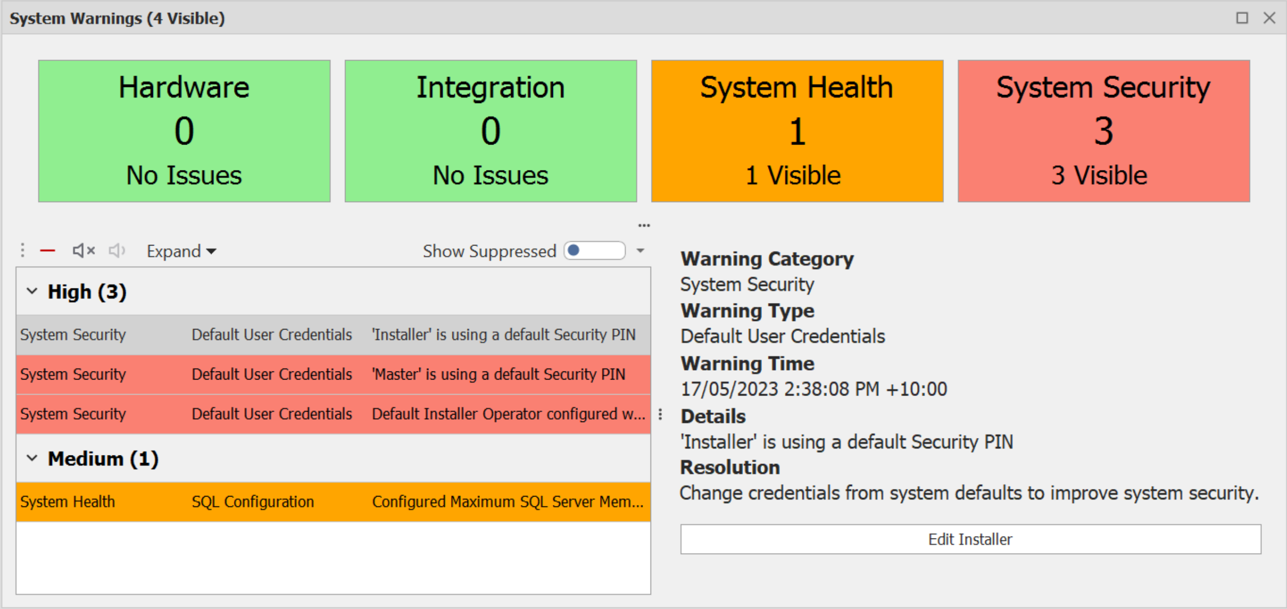
The Inner Range Mobile Access integration requires Integriti Pro edition or higher. Additionally, 1 Sifer Mobile Access Credential license (part number 994635) is required for each active credential in the system. If insufficient licenses are available, no further mobile credentials will be able to be generated until sufficient licenses are made available (either by adding more licenses or reducing the number of credentials in use). Only active credentials that are assigned to a user are use up a license, revoking a credential or settings its status to inactive will make the license used by that credential available again.

See the *InnerRangeMobileCredential_Integration_Manual* and *Integriti Integrations - Mobile Credential*s manuals for full details on both configuring the Inner Range Mobile Access integration and using the core mobile access functionality available in Integriti.

System Warnings

Integriti v23.1 further expands on the improvements to the System Warning architecture introduced with the release of Integriti v23.1 by adding a range of new System Warning Types. These new System Warnings further assist in identifying potential system issues as soon as possible, assisting in the prevention of long-term issues.

Additionally, a new System Warning category has been added to encompass warnings around System Security. The new System Security category will contain warnings that pertain to potential security issues in the system, providing suggestions to increase the security of the configuration of the system.


System Warnings (4 Visible)

Hardware 0 No Issues | Integration 0 No Issues | System Health 1 1 Visible | System Security 3 3 Visible

High (3)

System Security	Default User Credentials	'Installer' is using a default Security PIN
System Security	Default User Credentials	'Master' is using a default Security PIN
System Security	Default User Credentials	Default Installer Operator configured w...

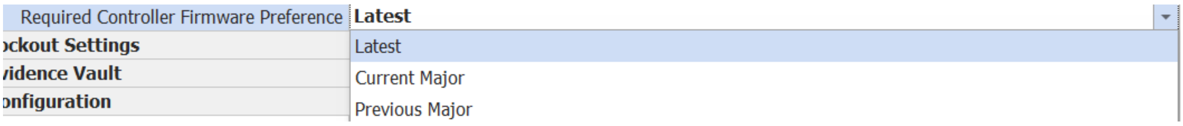
Medium (1)

System Health	SQL Configuration	Configured Maximum SQL Server Mem...

Warning Category
System Security
Warning Type
Default User Credentials
Warning Time
17/05/2023 2:38:08 PM +10:00
Details
'Installer' is using a default Security PIN
Resolution
Change credentials from system defaults to improve system security.

Hardware

- **Offline Controller:** Controllers configured with a *Connection Mode* of *Auto* that are unable to make a connection to the Controller will now generate an Offline Controller warning. This warning will be automatically generated as soon as the Controller goes offline or if an initial connection is unable to be made on startup. This includes where no Controller Server is available to connect to the Controller. Warnings will be automatically cleared when the offline Controller comes online.
- **Old Controller Firmware:** Connecting to a Controller that is running firmware that is determined to be 'too old' will automatically generate a warning indicating that the firmware needs to be updated. The required firmware version used to determine whether Controller's firmware is 'too old' can be configured on a per-system basis through the *Required Controller Firmware Preference* property in the System Settings. This can be configured to one of:
  - **Latest:** Controller Firmware that is older than the firmware packaged with the Integriti release will generate a warning. Use this option for systems where the most up to date controller firmware should always be used.
  - **Current Major:** Controller firmware that is from before the current major release will generate a warning. For the Integriti v23.1 release, this will generate a warning for any controllers on v22.x firmware or older.
  - **Previous Major:** Controller firmware that is from before the previous major release will generate a warning. For the Integriti v23.1 release, this will generate a warning for any controllers on v21.x firmware or older.



Required Controller Firmware Preference	Latest
ockout Settings	Latest
idence Vault	Current Major
onfiguration	Previous Major

Old Controller Firmware warnings will be automatically cleared after updating the firmware installed on a controller to a valid version.

- **Controller Firmware Too New:** Connecting to a Controller running firmware that is newer than the installed Integriti version will automatically generate a warning. It is recommended to downgrade the firmware to be no higher than the installed Integriti version to avoid potential compatibility issues. Warnings will be automatically cleared after downgrading the controller’s firmware.

Integrations

- **Offline Integration:** Integrated Devices and Communication Handlers that are enabled but offline will now generate Offline Integration warnings. These warnings will be generated whenever an Integrated Device or Communication Handler goes offline, including failing to start, connection lost while running or when there is no server available for it to run on. This helps ensure problems with Integrated Devices and Communication Handlers are quickly raised, allowing them to be addressed. Warnings will be automatically cleared as soon as an offline Integrated Device or Communication Handler comes back online.
- **Integration Licensing:** Unlicensed Integrated Devices and Communication Handlers will now generate Integration Licensing warnings detailing the required licenses to run the Integrated Device/Communication Handler. Generated warnings will be automatically cleared once the necessary licenses have been loaded into the system.

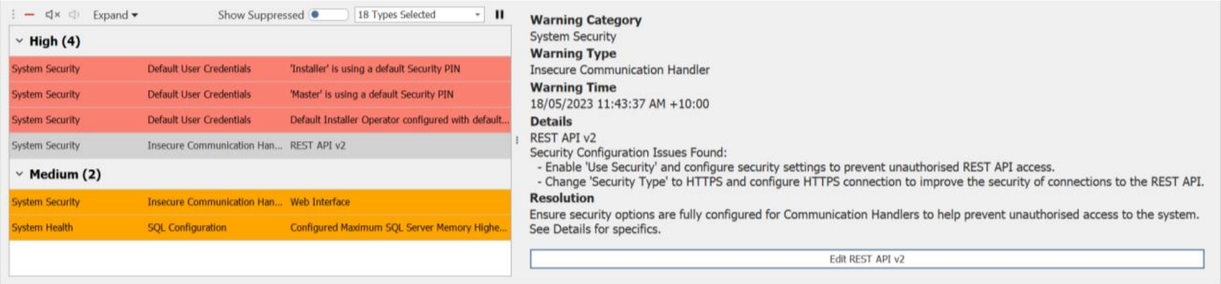
System Health

- **Version Compatibility:** Warnings will be generated on Application Server startup when the server’s operating system or the connected SQL Server is not a version that is supported by the installed Integriti. This ensures that the installed version of Integriti has been fully tested against these core components of the system, helping avoid potential issues that can be found when running against unsupported versions. Warnings will be automatically cleared on the next Application Server startup once the versions of these components have been updated to a supported version. Minimum system requirements for a given Integriti version can be found in the packaged ‘Hardware and Software Prerequisites’ document.
  Version Compatibility warnings will be additionally generated when connecting to an Integriti Application Server from a client with a different Dot Net version to the server. This has been known to cause compatibility issues, and it is recommended to ensure the installed Dot Net versions of all servers and clients match.
- **SQL Configuration:** Warnings will now be automatically generated as common SQL configuration issues are identified. This includes using an inappropriate SQL Edition for the size of the system and having the Maximum Server Memory Configuration in SQL configured to higher than the recommended value. The required SQL Edition for a given system size and the recommended value to configure the Maximum Server Memory Configuration to can both be found in the packaged ‘Hardware and Software Prerequisites’ document.

- **Low Drive Capacity:** The existing Low Drive Capacity warning has been improved to provide dynamic warning priority based on the percentage of disk space that is available. Warnings will now escalate from low priority when < 10% of disk space is available, to medium priority when <5% of disk space is available, to high priority when < 2.5% of disk space is available. Warning priority will automatically escalate/de-escalate as available disk space increases/decreases, with warnings being cleared when more than 10% of disk space is available.

System Security

- **Default User Credentials:** Warnings will be automatically generated for systems configured with Users or Operators using any of the built-in login credentials. This includes both Users configured with one of the default Security Pins or an Operator configured with the default Username and Password.
  Warnings will be generated automatically on server startup, as well as if a User or Operator is changed to use one of the default credentials at a later point.
  Warnings generated for User's with a default Security Pin will be automatically cleared either when the Security Pin of the User is changed, or when the User is Cancelled.
  Warnings Generated for an Operator with the default Username and Password will be automatically cleared either when the Password of the Operator is changed, or when the Operator is Disabled.
- **Insecure Communication Handler:** Warnings will now be automatically generated when Communication Handlers are configured and enabled without the recommended security options configured. This includes cases where security is disabled for the communication handler or HTTPS is not being used, potentially allowing less secure connections to the system. Warnings will be automatically cleared as the recommended security options are enabled.



High (4)

System Security	Default User Credentials	'Installer' is using a default Security PIN
System Security	Default User Credentials	'Master' is using a default Security PIN
System Security	Default User Credentials	Default Installer Operator configured with default...
System Security	Insecure Communication Han...	REST API v2

Medium (2)

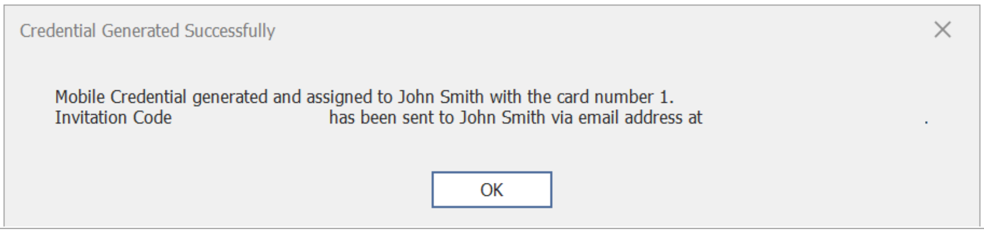
System Security	Insecure Communication Han...	Web Interface
System Health	SQL Configuration	Configured Maximum SQL Server Memory Highe...

Warning Category
System Security
Warning Type
Insecure Communication Handler
Warning Time
18/05/2023 11:43:37 AM +10:00
Details
REST API v2
Security Configuration Issues Found:
- Enable 'Use Security' and configure security settings to prevent unauthorised REST API access.
- Change 'Security Type' to HTTPS and configure HTTPS connection to improve the security of connections to the REST API.

Resolution
Ensure security options are fully configured for Communication Handlers to help prevent unauthorised access to the system. See Details for specifics.

Improvements

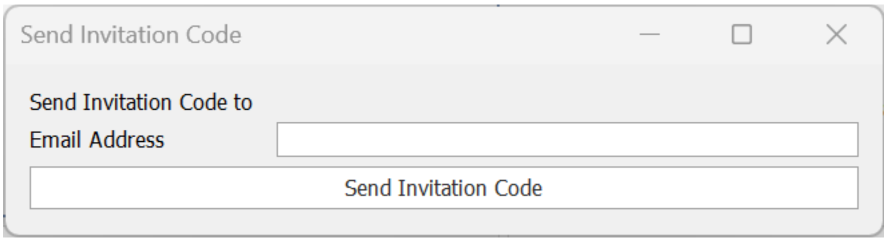
- **Mobile Credentials:** Generating a mobile credential from the acquire card dialog will now automatically send the invitation and close the dialog on successful generation of a mobile credential. This simplifies the process of generating mobile credentials, removing the need to explicitly close the dialog on successfully generating a credential. On successful credential generation, a message box will be shown containing the generated card number and invitation code prior to the dialog closing, allowing this information to be conveniently viewed as required.



Credential Generated Successfully

Mobile Credential generated and assigned to John Smith with the card number 1.
Invitation Code has been sent to John Smith via email address at .

- **Mobile Credentials:** Added the option to allow the email address and mobile number to use when generating a mobile credential to be viewed and modified when generating a mobile credential from the credential acquire dialog. This can be configured through the *Require Communication Verification* property of the Mobile Credential System/Pool to either show for every generated credential, or only when required and not already configured (such as the email address for the Inner Range Mobile Access integration). Updating the displayed email address or mobile number will automatically update the corresponding custom field for the user the credential is being generated for.

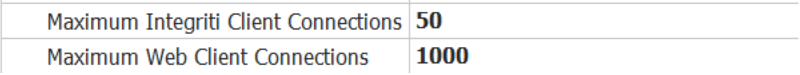

Send Invitation Code

Send Invitation Code to

Email Address

- **Web Client Licensing:** Added a new floating client license specifically for web client connections. The new web client licenses will be purchased and counted separately to the existing client licenses, allowing better management of client licenses on a system. Web client licenses will be the preferred licenses for web client connections, being used before the current client licenses are used.. This can reduce the likelihood of floating client licenses being used up by web clients, preventing Operators logging in to System Designer and GateKeeper.

  Where no web client licenses are available, the web client will fall back to using the existing client licenses.
- **Client Connection Limits:** Application Servers can now be configured to limit the number of concurrent client connections that can be made to the server. This allows maximum limits to be specified, preventing a server from being overloaded by an excessive number of concurrent client connections.
  Client connection limits can be configured individually for Integriti clients (e.g. System Designer and GateKeeper) and web clients, allowing individual limits for each type of client connection to be configured. These limits can be configured from the Server Instance associated with Application server through the *Maximum Integriti Client Connections* and *Maximum Web Client Connections* properties. By default these are set to 50 and 1000 respectively.

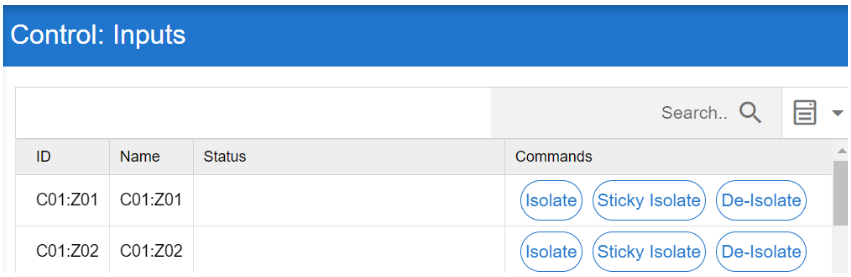


Maximum Integriti Client Connections	**50**
Maximum Web Client Connections	**1000**

A maximum of 50 Integriti client connections and 2000 web client connections are supported.

- **Integrations:** The state of Integrated Devices will now automatically go ‘Offline’ when there are no integration servers available for the Integrated Device’s persisted connection to run on. This allows a clearer view of whether Integrated Devices are currently running from the Integrated System list.
- **Web Interface:** When attempting to go directly to a given page of the web interface while logged out, the browser will now automatically redirect to the original page after logging on. This allows navigating directly to different aspects of the web interface (such as through bookmarks) without being redirected to the home page when the web interface isn’t already logged in.
- **Web Interface:** When viewing lists of Entities from the Web Interface, the provided search box is now able to search for the specified text in each Entity’s state, as well as in the Name and Notes columns.

- **Web Interface:** Added the ability to Isolate, Sticky Isolate and De-Isolate Inputs from the web interface.

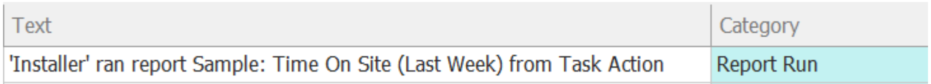


Control: Inputs

Search..

ID	Name	Status	Commands
C01:Z01	C01:Z01		Isolate Sticky Isolate De-Isolate
C01:Z02	C01:Z02		Isolate Sticky Isolate De-Isolate

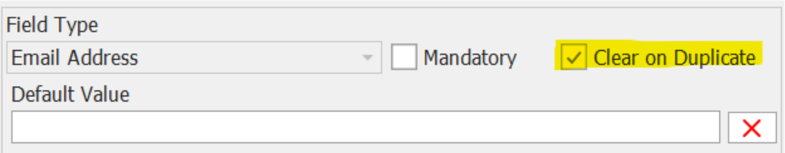
- **Execute Report Task Action:** Review is now logged whenever a report is executed through the Execute Report Task Action. In the case where the action is executed from 'Run Task Now' on a Scheduled Task, the name of the Operator who triggered the execution will be included in the logged Review.



Text	Category
'Installer' ran report Sample: Time On Site (Last Week) from Task Action	Report Run

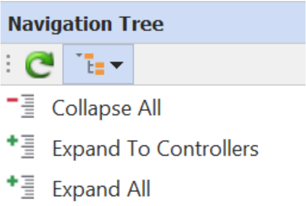
Review will be logged with the same Review Category (Report Run) as when a report is manually executed.

- **Custom Fields:** Added a 'Clear on Duplicate' option to Custom Field Definitions to allow specified Custom Fields to be cleared when duplicating Entities rather than being copied to the new Entity. This prevents the need to manually clear custom field values that should be unique between entities when duplicating entities.



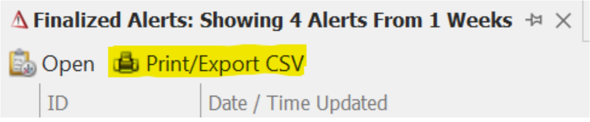
Field Type
Email Address ☐ Mandatory ☑ Clear on Duplicate
Default Value

- **Navigation Tree:** Added the option to Expand/Collapse the Navigation Tree to collapse all nodes, expand all nodes or expand to the controller level. This allows the Navigation Tree's view to be conveniently simplified as required, regardless of which nodes are expanded.

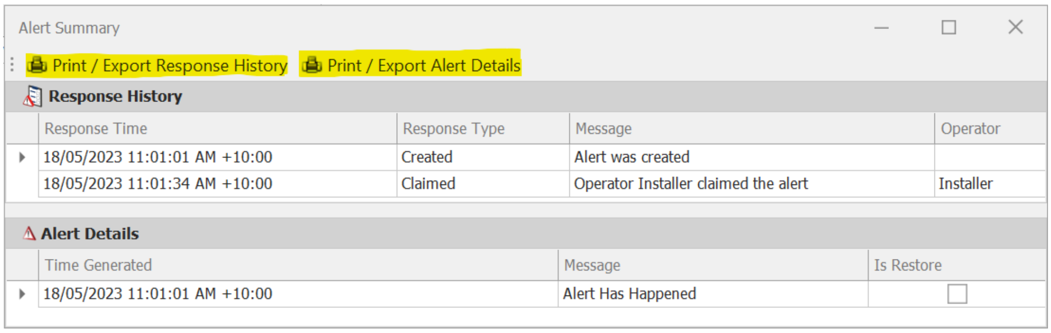


- **Navigation Tree:** The Navigation Tree now has a Refresh button to allow contents of the list to be manually reloaded from the server.
- **Review List:** The 'Copy Card Number' context menu command now copies the card number (rather than the card data) for direct entry card badges. This allows for uses such as copying the license plate directly out of an LPR card badge review record.
  Additionally, a new 'Copy Card Data' context menu command has been added for direct entry card badges to allow the card data to be copied directly from the Review record.

- **Alerts:** Added the option to 'Print/Export CSV' to the Finalized Alerts list. This allows details of finalized alerts to be conveniently exported from the system or printed directly from the Finalized Alerts list.



- **Alerts:** Added the option to 'Print/Export CSV' the Alert Response History and the Alert Details to the Alert Summary dialog, allowing Alert responses and details to be conveniently exported and printed.



Response History

Response Time	Response Type	Message	Operator
18/05/2023 11:01:01 AM +10:00	Created	Alert was created	
18/05/2023 11:01:34 AM +10:00	Claimed	Operator Installer claimed the alert	Installer

Alert Details

Time Generated	Message	Is Restore
18/05/2023 11:01:01 AM +10:00	Alert Has Happened	□

- **Audit:** Audit from creation and deletion of entities now contain details on the name and ID of the created/deleted entity in the Audit's description.
- **Audit:** Audit from modifying a complex property (such as the report layout of an Advanced Report) now has a simplified description, summarising the change rather than displaying the raw XML from the change. This makes the description simple to read when viewing a summary of changes that have been made.
- **License Plate Recognition:** Further improved support for Arabic license plates, now supporting an additional range of Arabic characters in license plates.

Issues Resolved

- **Send Communication Message Task Action:** Resolved issue that could occasionally result in not all attachments being sent to some recipients when sending multiple attachments to multiple recipients in the same task action.
- **Filters:** Resolved issue resulting in the 'NOT (and)' and 'NOT (or)' filters not providing the expected results when only a single filter row is configured.
- **Filters:** Resolved issue resulting in filters containing a 'Today' operator on a Custom Field failing to execute.
- **Filters:** Resolved issue resulting in the Recent/Previous Time filters showing results covering the wrong period of time when used on Custom Fields.
- **Duplicate Entity:** Resolved issue resulting in an Entity's underlying GID being duplicated to the new Entity when duplicating an Entity. This would result in duplicate Entity GIDs being present in the system, preventing them being used as a key through the REST API. Entity GIDs is now guaranteed to be unique and can be used as a unique identifier through the REST API if required.
- **Door Editor:** Resolved issue resulting in an error occurring when attempting to configure a door's *Two Badge Action* through the multi-select editor. The *Two Badge* Action can now be fully configured through the multi-select editor.
- **Entity Item History:** Resolved potential error saving Entities when using the Show Item History option to Revert to a Previous version of the Entity in some circumstances.

- **Module Editor Dashboard:** Resolved issue preventing editing the *Day of Week* property of a LAN Module through the Module Editor Dashboard.
- **CCTV Viewer:** Resolved issue that could allow viewing of CCTV footage from a camera an Operator doesn't have permissions to view when viewing CCTV from an associated Entity or Integrated Device.
- **Server Instance:** Resolved potential issue that could prevent deletion of Server Instances in some circumstances.
- **Performance History:** Resolved issue that could result in an error being encountered when changing the selected server on the Performance History panel.
- **User Qualifications:** Resolved issue that could result in the configured warning and expiry actions not being executed on some systems.
- **Review List:** Resolved issue resulting in the 'Copy Card Number' context menu command giving an error when executed on Review generated from a simulated card badge.
- **RTLS Alerts:** Resolved issue resulting in Alerts not showing at the correct location on a Schematic map when generated directly from RTLS Asset events.
- **3rd Party Doors:** Resolved issue resulting in filtering by 3rd party Controllers from the Navigation Tree not correctly filtering lists to only entities present in the selected Controller.
- **3rd Party Doors:** Resolved issue resulting in the Area selection dialog showing no Areas by default when setting the Area/Location of a 3rd party door.

REST API v2 Improvements

- **XML Format:** Ref nodes in the XML sent via the REST API will now include Name of the referenced object for the *Site* and *ModifiedBy* properties. This allows the names of these properties to accessed directly without performing an additional API query.
- **Grant Door Access Command:** The *Grant Door Access* endpoint of the *Basic Status and Control* module now supports setting the *UnlockSeconds* property to 0 to unlock the specified door for the default unlock time. The *Grant Door Access* command additionally supports the option to *ForceEvenIfOverridden*, allowing the door access command to ignore the override state of the door.
- **User Qualifications:** Added Read Summary of User Qualifications to the User Management module of the REST API.
- **Card Templates:** Added Read Summary of Card Templates to the User Management module of the REST API.
- **Cards:** Added Read Summary of Cards to the Virtual Card Badge module of the REST API.

Documentation

- **Inner Range Mobile Credential Integration Manual:** New manual describing the use and configuration of the new Inner Range Mobile Credential integration.
- **Integriti Communications Handlers - REST XML Web API V1:** Added notes on required manual port registration requirements for application servers not running with administrator privileges.
- **Integriti Communications Handlers - REST XML Web API V2:** Added notes on required manual port registration requirements for application servers not running with administrator privileges.
- **Integriti Communications Handlers - Web Interface:** Added notes on required manual port registration requirements for application servers not running with administrator privileges.

Version 23.0.0

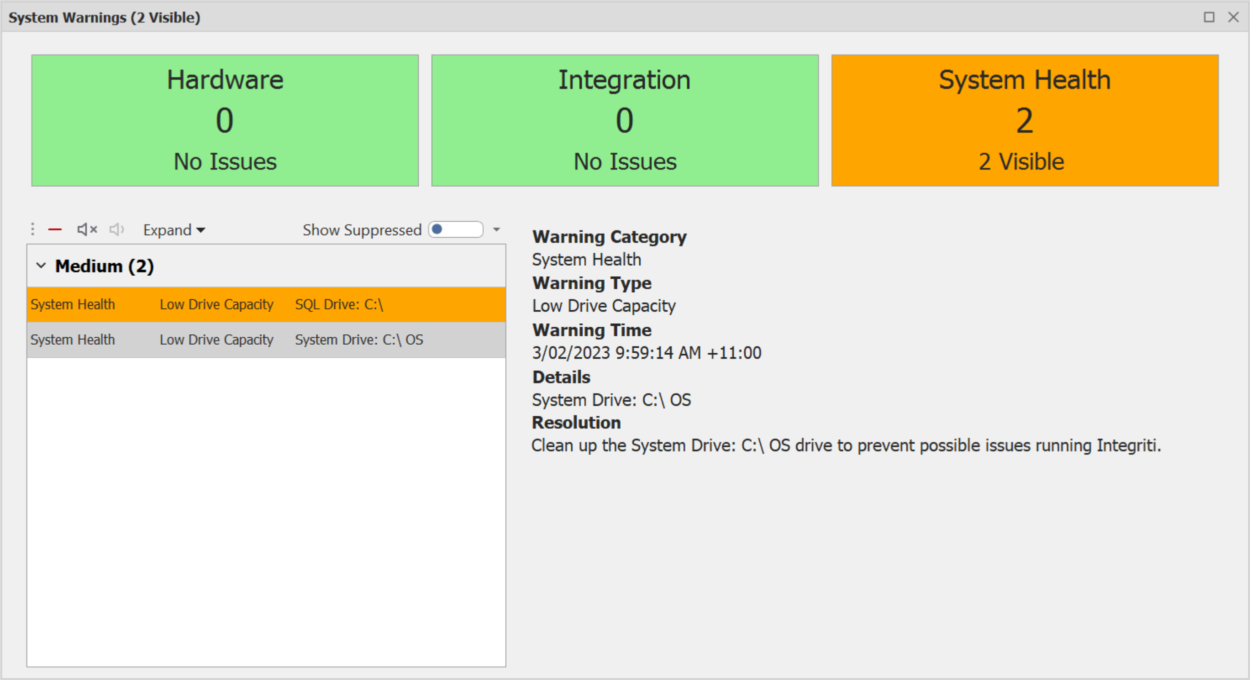
March 2023

System Warnings

With Integriti v23.0 the user interface for viewing and interacting with outstanding System Warnings has been redesigned in order to increase the visibility of problems in the system and increase the ease with which they can be resolved. This allows for potential problems in the system to be quickly noticeable, allowing them to be actioned as soon as possible, preventing long term issues.

User Interface

The System Warnings dialog shown when clicking on the 'System Warnings' button in the System Designer ribbon has been redesigned to simplify the process of monitoring System Warnings. All System Warnings are now grouped into one of 3 top-level categories: Hardware, System Health and Integration. A summary of the current System Warnings for each of these warning categories is now conveniently displayed at the top of the System Warning dialog, making it simple to identify which areas of the software problems are currently present in.


System Warnings (2 Visible)

Hardware	Integration	System Health
0	0	2
No Issues	No Issues	2 Visible

Medium (2)

System Health	Low Drive Capacity	SQL Drive: C:\
System Health	Low Drive Capacity	System Drive: C:\ OS

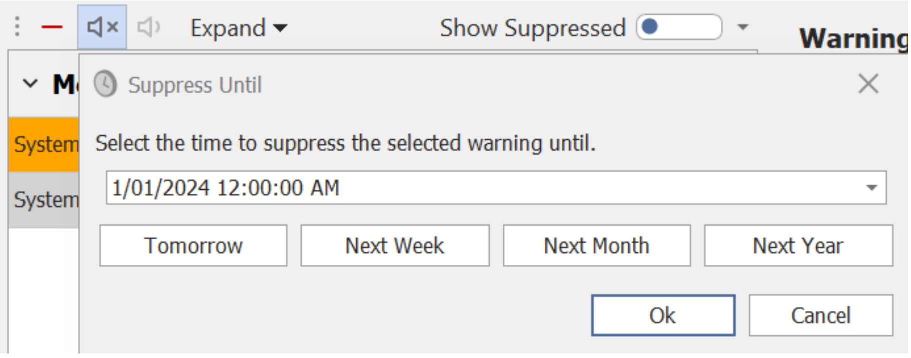
Warning Category
System Health
Warning Type
Low Drive Capacity
Warning Time
3/02/2023 9:59:14 AM +11:00
Details
System Drive: C:\ OS
Resolution
Clean up the System Drive: C:\ OS drive to prevent possible issues running Integriti.

Below this, a list of all current System Warnings is shown, allowing each individual warnings to be analysed and processed. This list can be filtered down to show a subset of current System Warnings, either by the overarching warning category or by individual types of warnings. This further simplifies the process of resolving System Warnings, allowing them to be viewed and processed by type or category.

Selecting a single System Warning from the list will show the full details of that warning to the right, allowing an in-depth investigation into the selected System Warning to be performed. Additionally, a recommendation for resolving the System Warning will be shown for most types of warnings, detailing the recommended steps to take to resolve the warning. For applicable warning types, a button may be shown with a link to the where in the software the issue can be best resolved from.

Warning Suppression

From the new System Warning dialog, System Warnings can now be suppressed for a configurable amount of time. This allows warnings caused by known factors to be removed from the dialog until they are ready to address, ensuring only currently applicable warnings are shown in the System Warning dialog at any one time.



Select the time to suppress the selected warning until.

1/01/2024 12:00:00 AM

Suppressed System Warnings will additionally be excluded from the System Warning count in System Designer, with the number shown only including currently active System Warnings.

Existing System Warnings (Upgrading Systems)

NOTE: For upgrading systems, all existing System Warnings will be deleted on upgrading to v23.0. System Warnings that are still applicable will be automatically re-generated over time after starting Integriti services and re-connecting to Controllers.

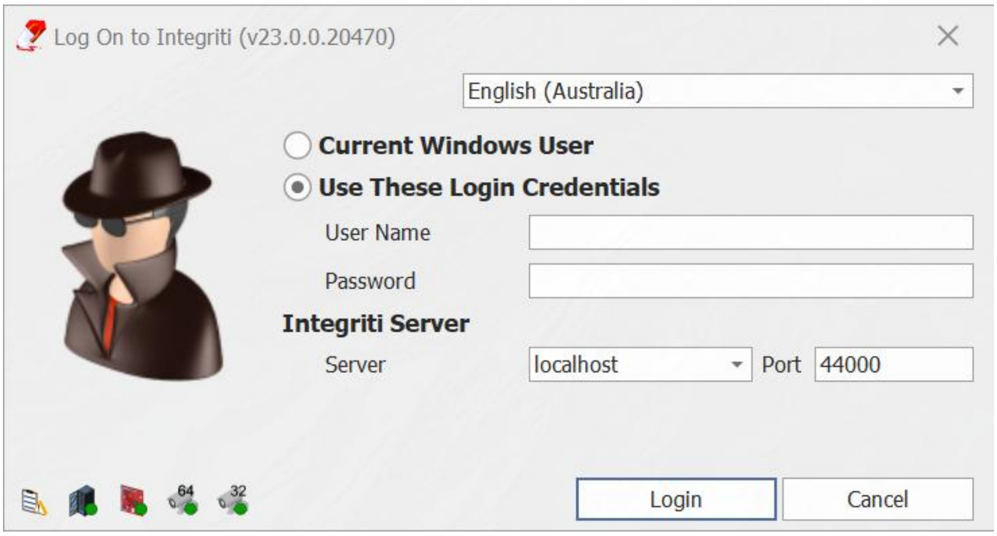
Translations

Integriti's translation architecture has received several improvements to assist in translating the Integriti software for use in different cultures. This includes simplifying selection of the translation language for the software, right-to-left support and support for translating Integriti software integrations.

Manual Language Selection

The language used for Integriti's translations can now be manually specified, allowing the Integriti language to differ from the system language. Integriti's translation language can be separately specified for both individual clients and the Integriti services themselves, allowing a great deal more flexibility, especially on multi-lingual sites.

Integriti's client language can be specified from the client's login dialog by selecting the desired language from the language dropdown. Changing language will automatically reload the login dialog in the selected language and, upon logging in, the selected language will be used for that client. The selected language will be saved based on the Windows User, storing the selected language for use each time the same User opens the Integriti client, while allowing different windows users on the same PC to translate the Integriti client into different languages.



Log On to Integriti (v23.0.0.20470)

English (Australia)

○ Current Windows User

● Use These Login Credentials

User Name

Password

Integriti Server

Server: localhost Port: 44000

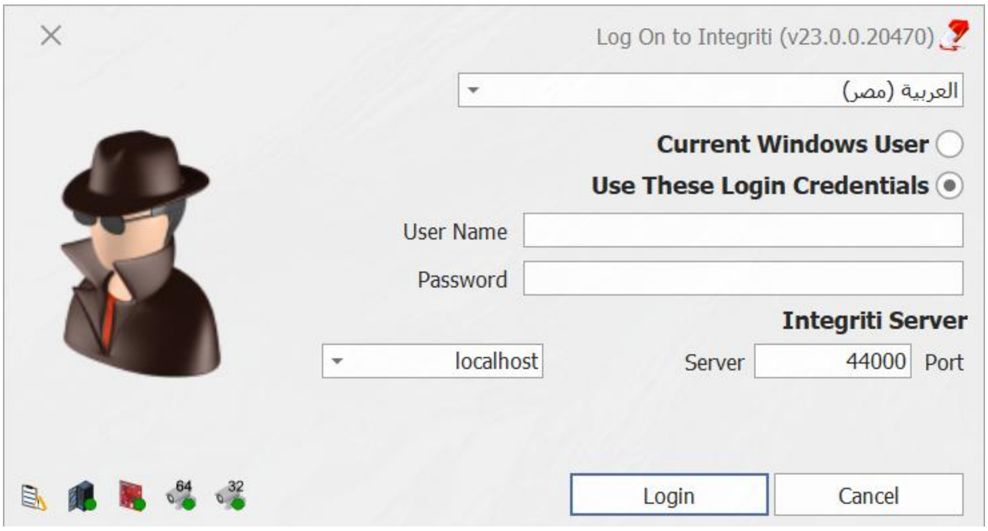
The translation language for each individual Integriti Server can be configured on a per-server basis directly from the Server Instance settings for the server. The server's language will be updated to the selected language on the next server restart, resulting in all messages and review generated by that server being in the selected language. Note that review and messages generated externally to the server (such as Controller review) will need to be translated separately.

Upgrading systems will continue to have their clients and servers translated to the Windows system language until a different translation language is specified (if required).

NOTE: Only languages that are installed on the client/server can be selected as the translation language. The necessary language files must be copied to all applicable clients and servers before they can be used. Removing the language files for a given language will result in any clients or servers using that language reverting to the system language until either a new language is selected or the language files are re-added.

Right-to-Left Support

Translating Integriti to a language that is natively displayed right-to-left will now display the Integriti clients in right-to-left format. Integriti clients will automatically change to the new right-to-left format as required based on the selected translation language for the Integriti client being used.



Log On to Integriti (v23.0.0.20470)

العربية (مصر)

Current Windows User ○

Use These Login Credentials ●

User Name

Password

Integriti Server

Server: localhost Port: 44000

Integriti Software Integration Translations

Integriti software integrations now support being translated to alternative languages. Translation files can be generated and loaded in the same way as the Integriti software, with individual integration template files being made available with all new integration releases. Once translated, the resulting translation file must be copied into the same directory as the Integriti software translations on the Integriti server and all Integriti clients that will be using the translation.

Integrations will automatically use the same translation language as the Integriti software, with the Integriti Integration server's translation language being used for server-based text (such as review), and the Integriti client's translation language being used for client-based text (such as editors and video viewers).

NOTE: Text generated by the 3rd party system being integrated to will not be translated by Integriti, and must be translated by the 3rd party system where supported. This includes text such as Review generated directly from events from the 3rd party system.

See the 'Integriti Translations.pdf' document for further details on translating Integriti software and integrations.

Version 23.0.0

Important Notes

The following operating systems are no longer formally supported from Integriti v23.0 onwards.

- Windows 8.1

It is recommended to update to a supported operating system prior to installing Integriti v23.0.

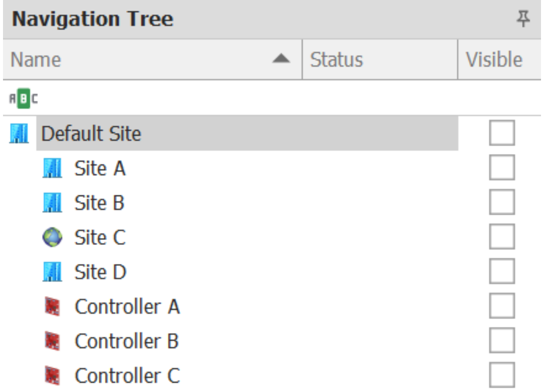
See ‘Hardware and Software Prerequisites’ for full details on currently supported operating systems.

Integration Compatibility

- Salto 3rd Party Door v2.4 or higher is required for Integriti v23.0 onwards.

Improvements

- **Navigation Tree:** Integriti System Designer’s navigation tree now supports being automatically sorted on opening the System Designer Client. The navigation tree will be sorted alphabetically by default, with all Sites/Keywords grouped at the top and all hardware grouped at the bottom.



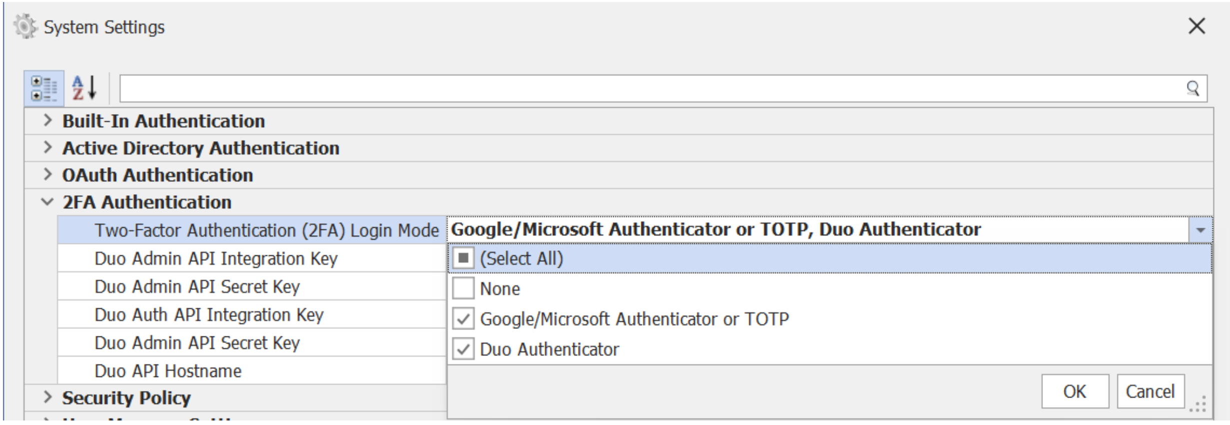
Navigation Tree

Name	Status	Visible
Default Site		□
Site A		□
Site B		□
Site C		□
Site D		□
Controller A		□
Controller B		□
Controller C		□

  Optionally, the default navigation tree sorting mode can be changed from the ‘Navigation Tree Sorting’ property in the System Settings. This can be set to one of:
  - Unsorted: No sorting will be explicitly applied by default. This will put items in the navigation tree in the same order as on previous versions of Integriti.
  - Sort Alphabetically: The navigation tree will be sorted alphabetically, with Sites/Keywords grouped together at the top and hardware grouped together at the bottom.
  - Sort By State: The navigation tree will be sorted similarly to ‘Sort Alphabetically’, with hardware items further grouped by their current online/offline state.
- **Firmware Update:** The latest Controller and hardware module firmware is now automatically loaded into Integriti’s firmware update dialog, simplifying the process of keeping firmware up to date. Available firmware will be automatically kept up to date with the latest available firmware versions as new versions of Integriti are installed.
  Alternate firmware versions may still be used where required, and firmware updates must still be manually applied.
- **Control Workstation Task Action:** The Control Workstation Task Action now supports selecting Challenge Definitions as an item to show. This allows the Challenge Response dialog to be automatically shown on an event occurring, allowing configurations such as explicitly showing the challenge dialog to a specified Operator as Challenges occur.
- **Installation Packages:** Added a command line option to the Integriti client installer to allow the default app server IP address and port for the client being installed to be specified.
  The default App Server IP Address can be specified by setting the /AppServerAddress parameter,

and the default App Server Port can be specified by setting the /AppServerPort parameter. e.g. Integriti_ClientOnly_Setup.exe /AppServerAddress=192.168.123.123 /AppServerPort=12345

- **Two Factor Authentication:** Added support for Duo 2FA and formal support for Microsot Authenticator to authenticate Operators logging in to Integriti clients. 2FA options can be configured from the System Settings, with it being possible to enable one or more of the supported 2FA options on a single system.



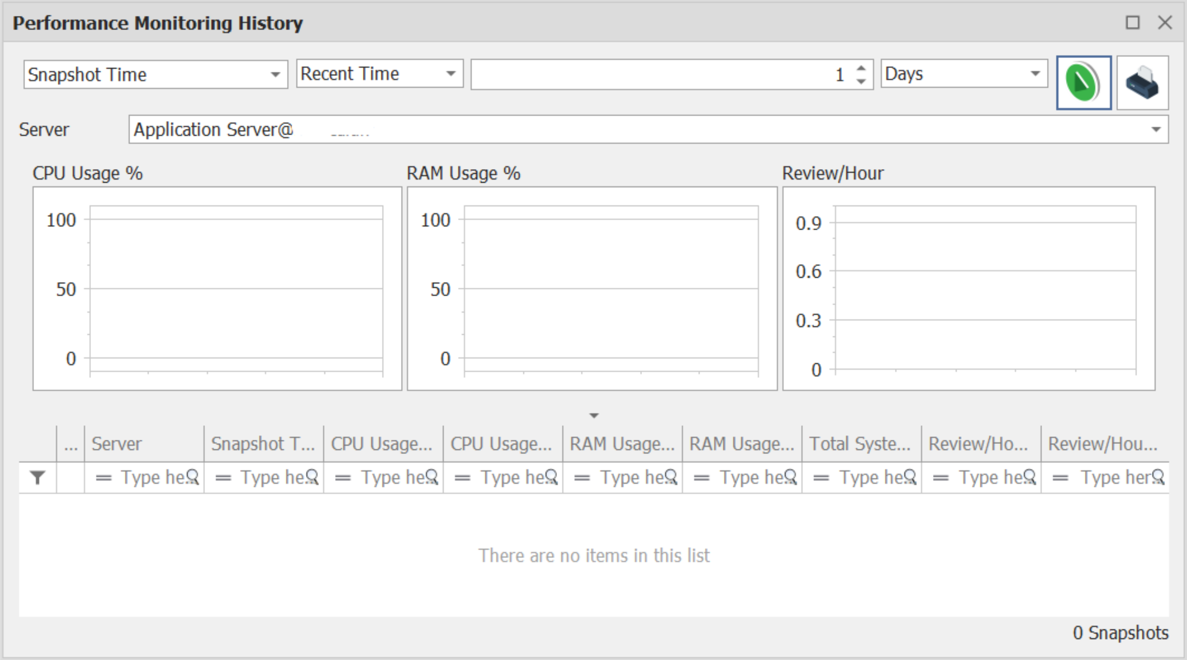
System Settings

- Built-In Authentication
- Active Directory Authentication
- OAuth Authentication
- 2FA Authentication
  - Two-Factor Authentication (2FA) Login Mode: Google/Microsoft Authenticator or TOTP, Duo Authenticator
  - Duo Admin API Integration Key
  - Duo Admin API Secret Key
  - Duo Auth API Integration Key
  - Duo Admin API Secret Key
  - Duo API Hostname
- Security Policy

■ (Select All)
☐ None
☑ Google/Microsoft Authenticator or TOTP
☑ Duo Authenticator

Once configured, 2FA can be configured for individual Operators from the Operator editor, allowing the Operator to be linked to the 2FA system for future logins.

- **Visitor Management:** Added the option to automatically delete Visitors (and their associated Users) after they have checked out. This can be configured through the Visitor Management Configuration's 'Keep Visitor' property with one of the following options:
  - Persist Forever – Keep visitors and their associated User's in the system forever (current behaviour).
  - Persist For Time – Delete unused visitors a configurable amount of time after they were last checked out.
  - Don't Persist – Immediately delete Visitors and their associated Users on check out.
- **Performance Monitoring History:** Improved the Performance Monitoring History panel to provide more focus on the charts displaying the performance history of the selected server. Additionally, snapshots will now be added to the Performance Monitoring History as they are taken from each server, providing a closer to live view of system performance.



Performance Monitoring History

Snapshot Time | Recent Time | 1 | Days

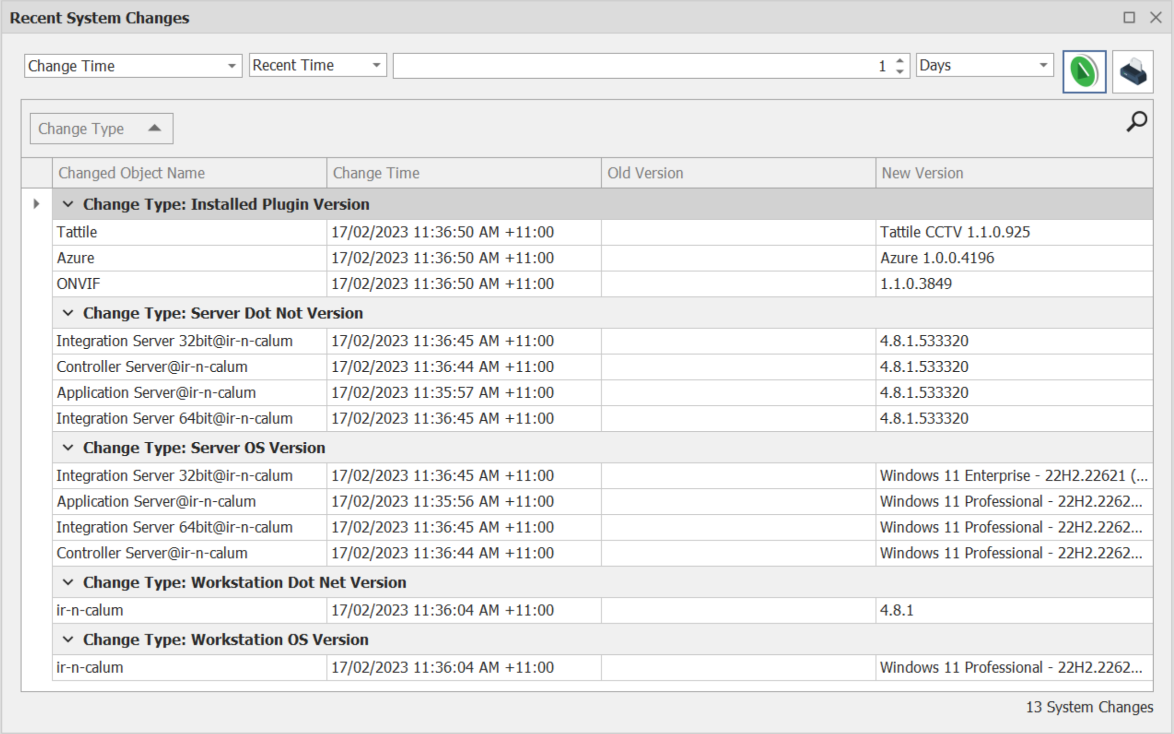
Server: Application Server@

...	Server	Snapshot T...	CPU Usage...	CPU Usage...	RAM Usage...	RAM Usage...	Total Syste...	Review/Ho...	Review/Hou...
	= Type he	= Type he	= Type he	= Type he	= Type he	= Type he	= Type he	= Type he	= Type her

There are no items in this list

0 Snapshots

- **SQL Server 2022**: Added formal support for using SQL Server 2022 to host the Integriti database.
- **System Changes:** Integriti now stores a log of changes made to the system. This includes changes such as updated OS and Dot Net versions, along with all plugin updates. This provides history of higher level changes made on the Integriti system architecture for future analysis.
  This information can help with diagnosing issues by seeing version differences between machines, or seeing what has changed recently on client or server machines.
  NOTE: Current versions will have a change added to the log as the initial version once the Integriti services start for the first time after updating Integriti.



Recent System Changes

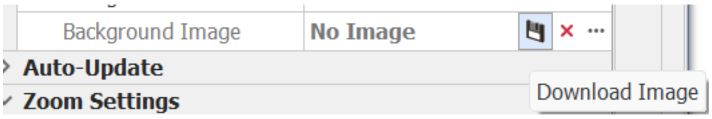
Change Time | Recent Time | 1 | Days

Change Type

Changed Object Name	Change Time	Old Version	New Version
Change Type: Installed Plugin Version			
Tattile	17/02/2023 11:36:50 AM +11:00		Tattile CCTV 1.1.0.925
Azure	17/02/2023 11:36:50 AM +11:00		Azure 1.0.0.4196
ONVIF	17/02/2023 11:36:50 AM +11:00		1.1.0.3849
Change Type: Server Dot Not Version			
Integration Server 32bit@ir-n-calum	17/02/2023 11:36:45 AM +11:00		4.8.1.533320
Controller Server@ir-n-calum	17/02/2023 11:36:44 AM +11:00		4.8.1.533320
Application Server@ir-n-calum	17/02/2023 11:35:57 AM +11:00		4.8.1.533320
Integration Server 64bit@ir-n-calum	17/02/2023 11:36:45 AM +11:00		4.8.1.533320
Change Type: Server OS Version			
Integration Server 32bit@ir-n-calum	17/02/2023 11:36:45 AM +11:00		Windows 11 Enterprise - 22H2.22621 (...
Application Server@ir-n-calum	17/02/2023 11:35:56 AM +11:00		Windows 11 Professional - 22H2.2262...
Integration Server 64bit@ir-n-calum	17/02/2023 11:36:45 AM +11:00		Windows 11 Professional - 22H2.2262...
Controller Server@ir-n-calum	17/02/2023 11:36:44 AM +11:00		Windows 11 Professional - 22H2.2262...
Change Type: Workstation Dot Net Version			
ir-n-calum	17/02/2023 11:36:04 AM +11:00		4.8.1
Change Type: Workstation OS Version			
ir-n-calum	17/02/2023 11:36:04 AM +11:00		Windows 11 Professional - 22H2.2262...

13 System Changes

- **Schematics:** Added the option to export the background image of a schematic map to file. This can be done by selecting the Download Image button on the Background Image property of the Schematic. This allows the background image of an already configured schematic to be easily retrieved and modified.



Background Image No Image

- **Operator Permissions:** Added new Operator Type Feature Permission ‘Can Duplicate Entities’ to optionally prevent selected Operators from duplicating Entities where Entities must be explicitly added from new as part of the Entity creation process.

Issues Resolved

- **Partitions:** Resolved issue that could result in global entities with IDs above the maximum supported ID for partitioned Controllers clashing with partitioned entities.
- **CSV Import:** Resolved issue resulting in User Photos not correctly importing.
- **IREntities Import:** Resolved issue that could result in blank Server Instances being added after importing an IREntities file.
- **IREntities Import:** Resolved issue that could result in blank entities sometimes being created in addition to the imported entities when importing global entities into a partition and using the ‘Create New’ import behaviour.
- **Filters:** Resolved issue resulting in Review Filters not correctly showing in the ribbon when ‘Show In Ribbon’ was selected for the Filter.
- **Navigation Tree:** Resolved issue that could result in the sync count in the navigation tree not clearing in some circumstances.
- **Mobile Credentials:** Resolved issue that could result in auto-generating and auto-revoking mobile credentials not occurring immediately after a user is created/modified to match the specified filter, with the credential generation/revocation instead happening at a later point.
- **3rd Party Door Integration:** Resolved issue that could result in Review generated by a 3rd party door integration not being visible to some Operators.
- **Visitor Management:** Printing the card of a Visitor now correctly shows the User’s photo when configured.
- **Operator Type Show Item History:** Resolved issue that could result in an error being shown when attempting to Show Item History for an Operator Type, preventing the item history from being shown.
- **User Editor:** Credential Acquire Options are now disabled for Operators without sufficient permission to add or edit Cards in the User’s Site.
- **List Contents Report:** Resolved issue that could result in an error when attempting to save newly created reports.
- **CCTV Viewer:** Resolved issue that could result in showing associated CCTV footage for an entity showing footage for associated cameras that the Operator doesn’t have permission to view.
- **HTTP Request Task Action:** Resolved issue where JSON used for the body of the HTTP Request to be sent wasn’t being formatted correctly, resulting in invalid JSON being sent.
  NOTE: When using the Send HTTP Request to send a JSON body, all curly braces should be escaped as ‘{{‘ and ‘}}’.
- **REST API v2:** The Add To Collection endpoint now supports adding credentials to Users. This resolves an issue where using this endpoint to add a credential to a User would create a ‘blank’ credential where the credential didn’t already exist in the system.
  Entities with IDs above the maximum supported ID for partitioned systems will now only be synchronised to global controllers and will not be synchronised to partitioned controllers.

Documentation

- **Hardware & Software Pre-Requisites:** Improved the Hardware & Software Pre-Requisites document to be clearer on OS and SQL Server requirements.
- **Integriti Translations:** Updated the Integriti Translations document to be up to date on the latest translation processes and include details on translating Integriti software integrations.

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

July 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.