Integriti 23.1.1 Release Notes



Important Notes

Customers Upgrading From a version **prior to 18.0** should read about the changes to the “Review” event log in.

Click Here to find out more.

CONTENTS

Release Notes 1
Important Notes 1
Contents 2
Bug-Fix Release (v 23.1.1) 4
Version 23.1 6
Version 23.0 15
Version 22.2 23
Bug-Fix Release (v 22.1.2) 30
Bug-Fix Release (v 22.1.1) 31
Version 22.1 33
Bug-Fix Release (v 22.0.2) 39
Bug-Fix Release (v 22.0.1) 40
Version 22.0 41
Bug-Fix Release (v 21.1.2) 53
Bug-Fix Release (v 21.1.1) 55
Version 21.1 56
Bug-Fix Release (v 21.0.2) 67
Bug-Fix Release (v 21.0.1) 68
Version 21.0 70
Bug-Fix Release (v 20.1.4) 81
Bug-Fix Release (v 20.1.3) 83
Bug-Fix Release (v 20.1.2) 84
Bug-Fix Release (v 20.1.1) 85
Version 20.1 86
Bug-Fix Release (v 20.0.3) 90
Bug-Fix Release (v 20.0.2) 91
Bug-Fix Release (v 20.0.1) 92
Version 20 93
Bug-Fix Release (v 19.1.5) 97
Bug-Fix Release (v 19.1.4) 98
Bug-Fix Release (v 19.1.3) 99
Bug-Fix Release (v 19.1.2) 100
Bug-Fix Release (v 19.1.1) 101

Contents

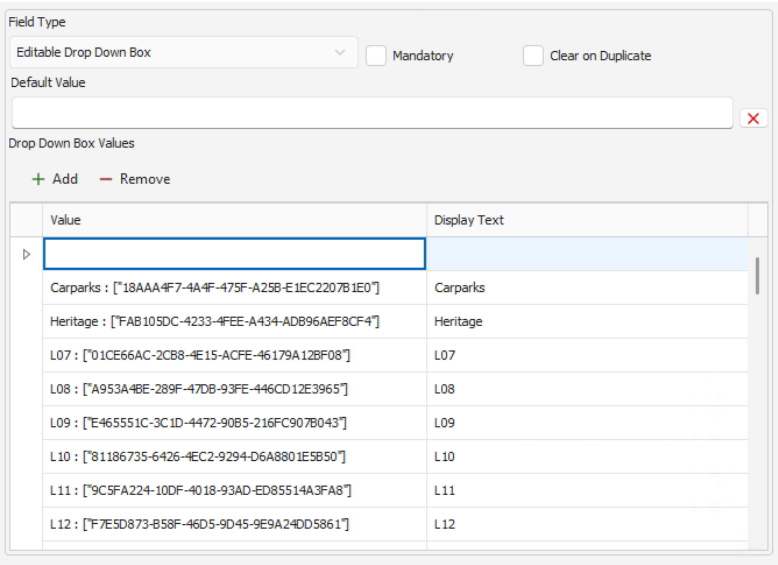
Version 19.1 102
Bug-Fix Release (v 19.0.1) 106
Version 19 107
Bug-Fix Release (v 18.2.3) 109
Bug-Fix Release (v 18.2.2) 110
Bug-Fix Release (v 18.2.1) 110
Version 18.2 111
Bug-Fix Release (v 18.1.2) 115
Bug-Fix Release (v 18.1.1) 116
New in Version 18.1 118
Bug-Fix Release (v 18.0.4) 121
Bug-Fix Release (v 18.0.3) 122
Bug-Fix Release (v 18.0.2) 122
Bug-Fix Release (v 18.0.1) 123
Version 18 124
Appendix 128
V18 Review Improvements 128

Bug-Fix Release (v 23.1.1)

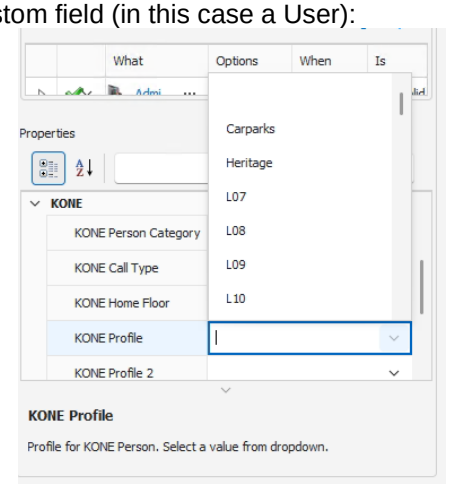
December 2023 - 23.1.1

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:



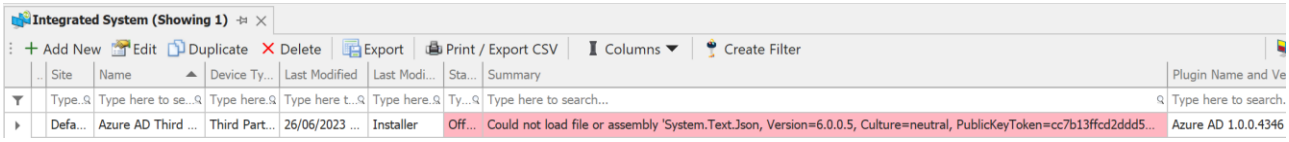
While editing an entity with the custom field (in this case a User):



- **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.

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':



- **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'.

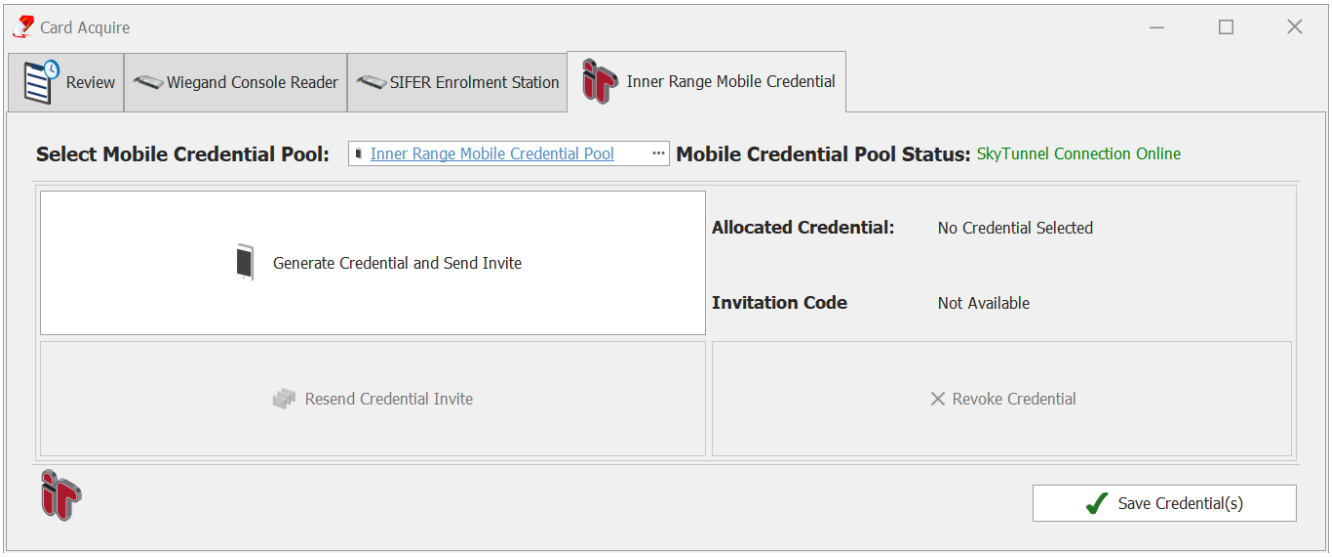
VERSION 23.1

November 2023 - 23.1

Inner Range Mobile Access

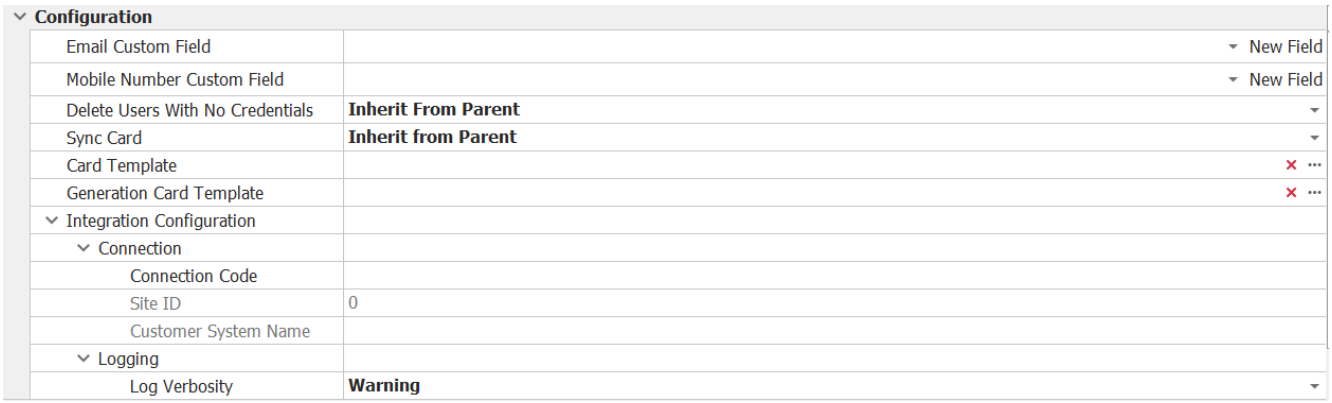
NOTE: Inner Range Mobile Access is only available in beta at the time of release, only systems that are part of the beta program will be able to create an Inner Range Mobile Access account and generate mobile credentials. Sites running Integriti v23.1 will be able to take full advantage of Inner Range 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.



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.



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.



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.

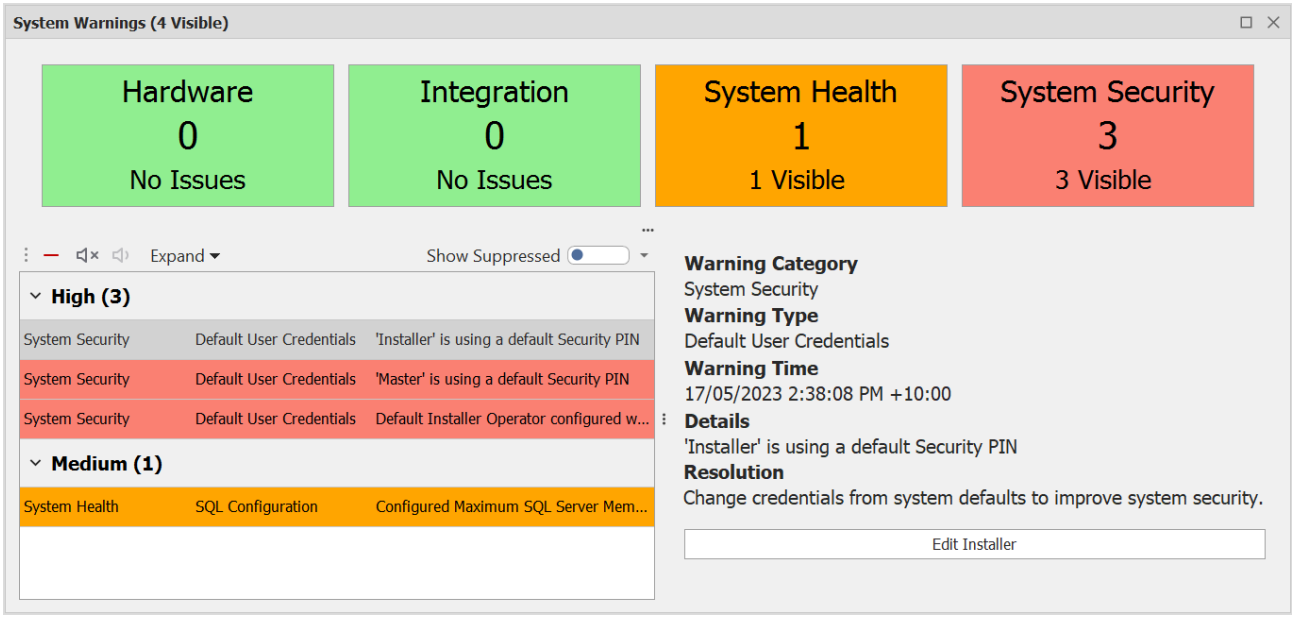
The Inner Range Mobile Access integration requires Integriti Pro edition or higher. Additionally, 1 Sifer Mobile Access Credential license (part number 994635) is required for each active credential in the system. If insufficient licenses are available, no further mobile credentials will be able to be 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 Credentia*ls 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

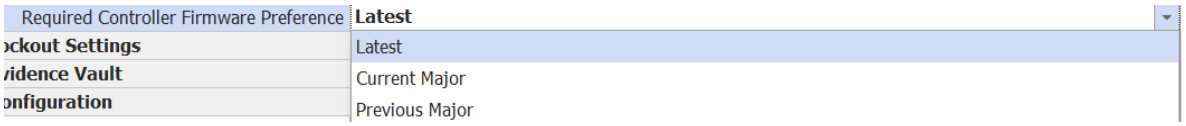
Integriti v23.1 further expands on the improvements to the System Warning architecture introduced with the release of Integriti v23.1 by adding a range of new System Warning Types. These new System Warnings further assist in identifying potential system issues as soon as possible, assisting in the prevention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



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.



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

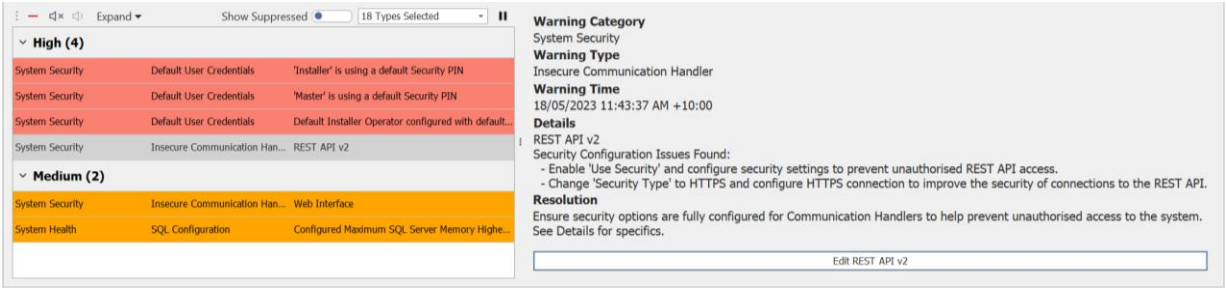
- **Offline Integration:** Integrated Devices and Communication Handlers that are enabled but offline will now generate Offline Integration warnings. These warnings will be generated whenever an Integrated Device or Communication Handler goes offline, including failing to start, connection lost while 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.

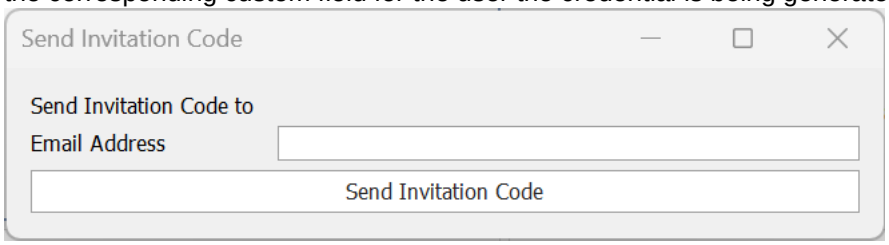


Improvements

- **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.



- **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.



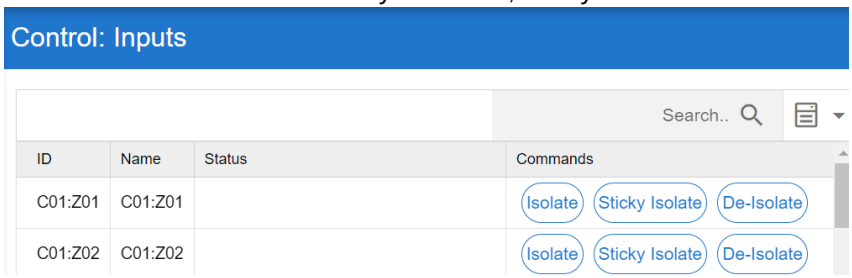
- **Web Client Licensing:** Added a new floating client license specifically for web client connections. The new web client licenses will be purchased and counted separately to the existing client licenses, allowing better management of client licenses on a system. Web client licenses will be the preferred 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.

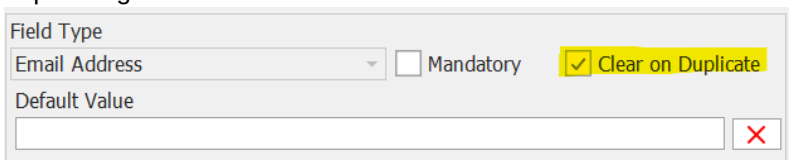


- **Execute Report Task Action:** Review is now logged whenever a report is executed through the Execute Report Task Action. In the case where the action is executed from 'Run Task Now' on a Scheduled Task, the name of the Operator who triggered the execution will be included in the logged Review.

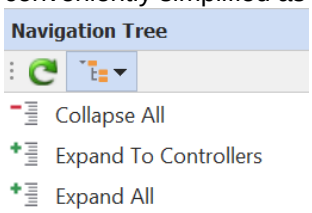


Review will be logged with the same Review Category (Report Run) as when a report is manually executed.

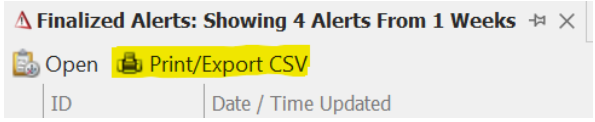
- **Custom Fields:** Added a 'Clear on Duplicate' option to Custom Field Definitions to allow specified Custom Fields to be cleared when duplicating Entities rather than being copied to the new Entity. This prevents the need to manually clear custom field values that should be unique between entities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



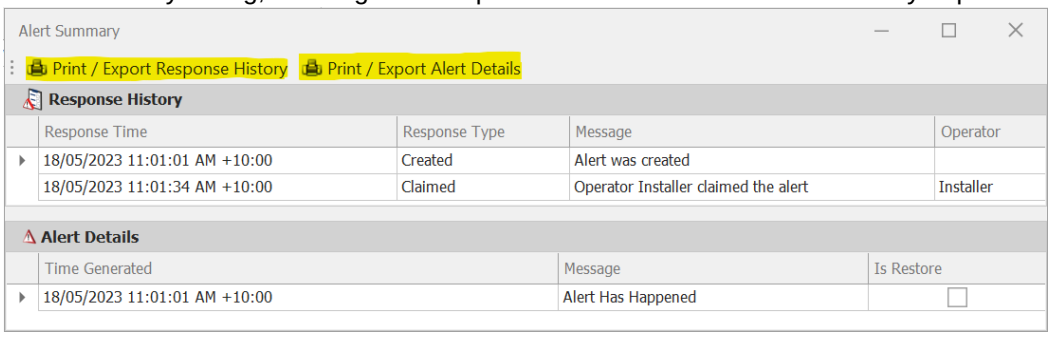
- **Navigation Tree:** Added the option to Expand/Collapse the Navigation Tree to collapse all nodes, expand all nodes or expand to the controller level. This allows the Navigation Tree's view to be conveniently simplified as required, regardless of which nodes are expanded.



- **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.



- **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

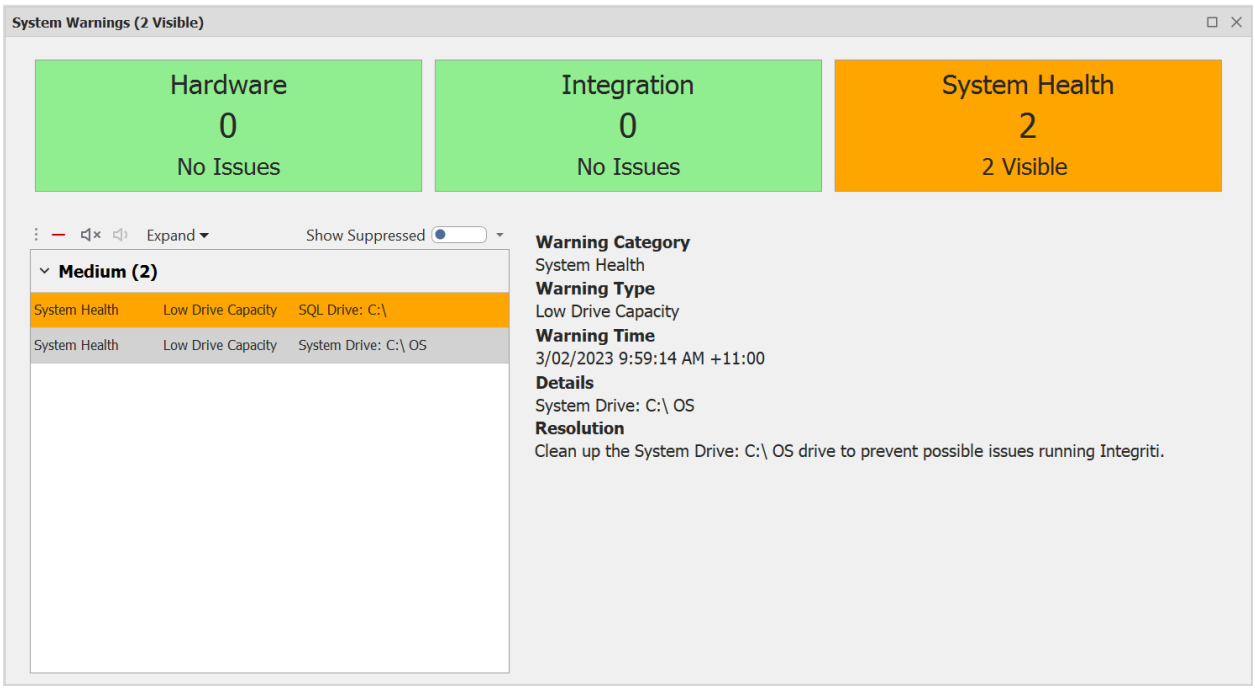
March 2023 - 23.0

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.

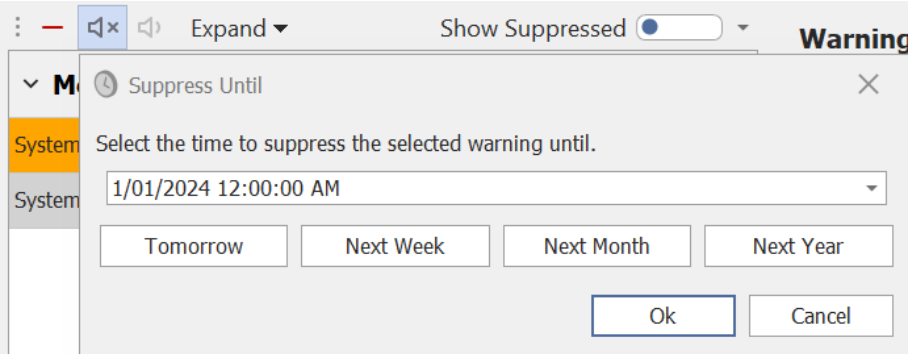


Below this, a list of all current System Warnings is shown, allowing each individual warnings to be analysed and processed. This list can be filtered down to show a subset of current System Warnings, either by the overarching warning category or by individual types of warnings. This further simplifies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



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.



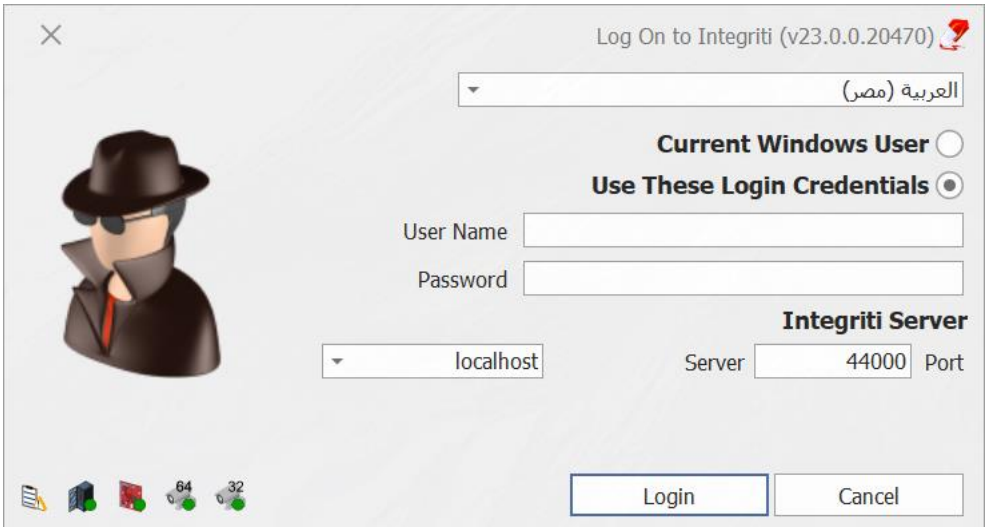
The translation language for each individual Integriti Server can be configured on a per-server basis directly from the Server Instance settings for the server. The server's language will be updated to the selected language on the next server restart, resulting in all messages and review generated by 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.



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.

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.

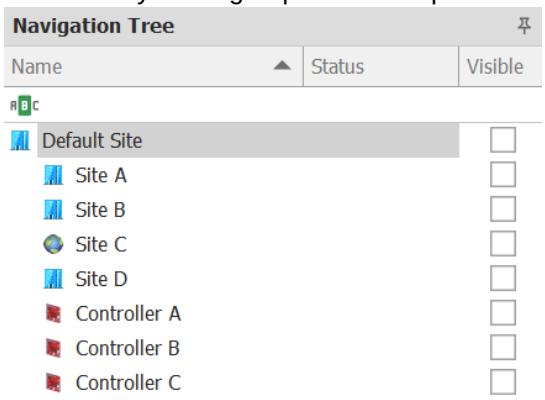
See 'Hardware and Software Prerequisites' for full details on currently supported operating systems.

Integration Compatibility

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

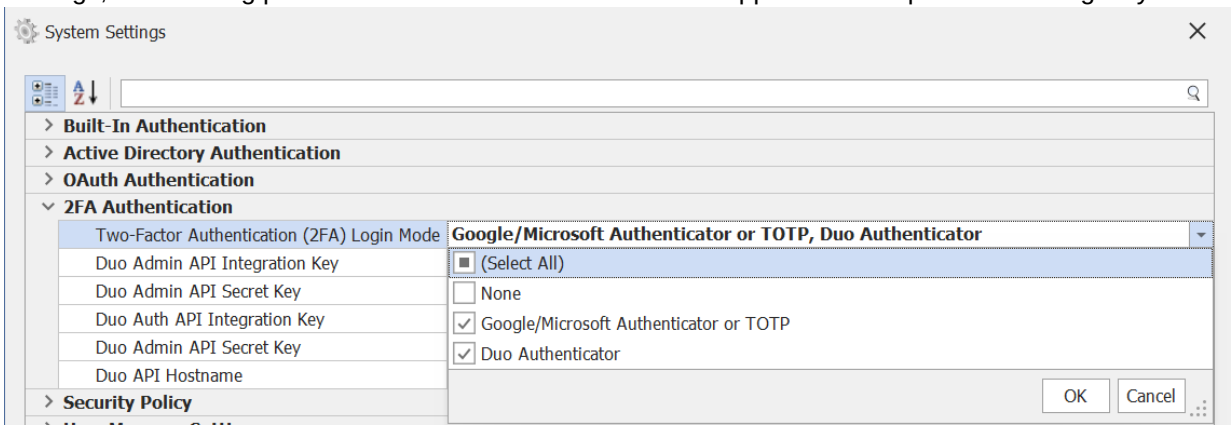
Improvements

- **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.



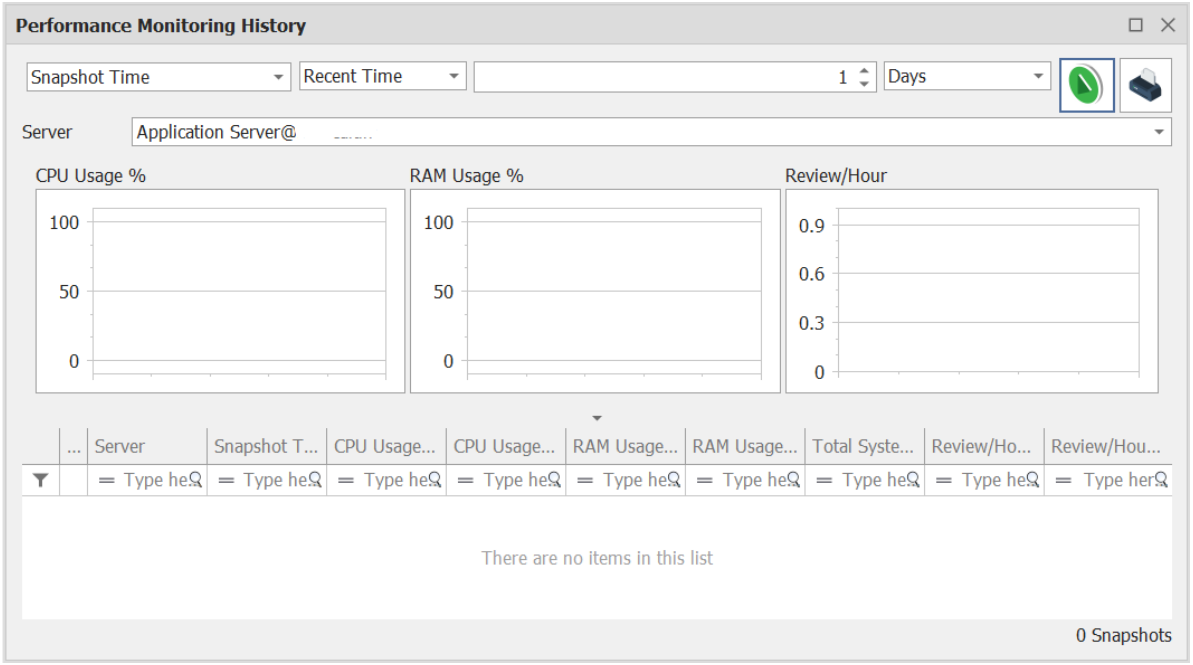
  Optionally, the default navigation tree sorting mode can be changed from the 'Navigation Tree Sorting' property in the System Settings. This can be set to one of:
  - Unsorted: No sorting will be explicitly applied by default. This will put items in the navigation tree in the same order as on previous 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.



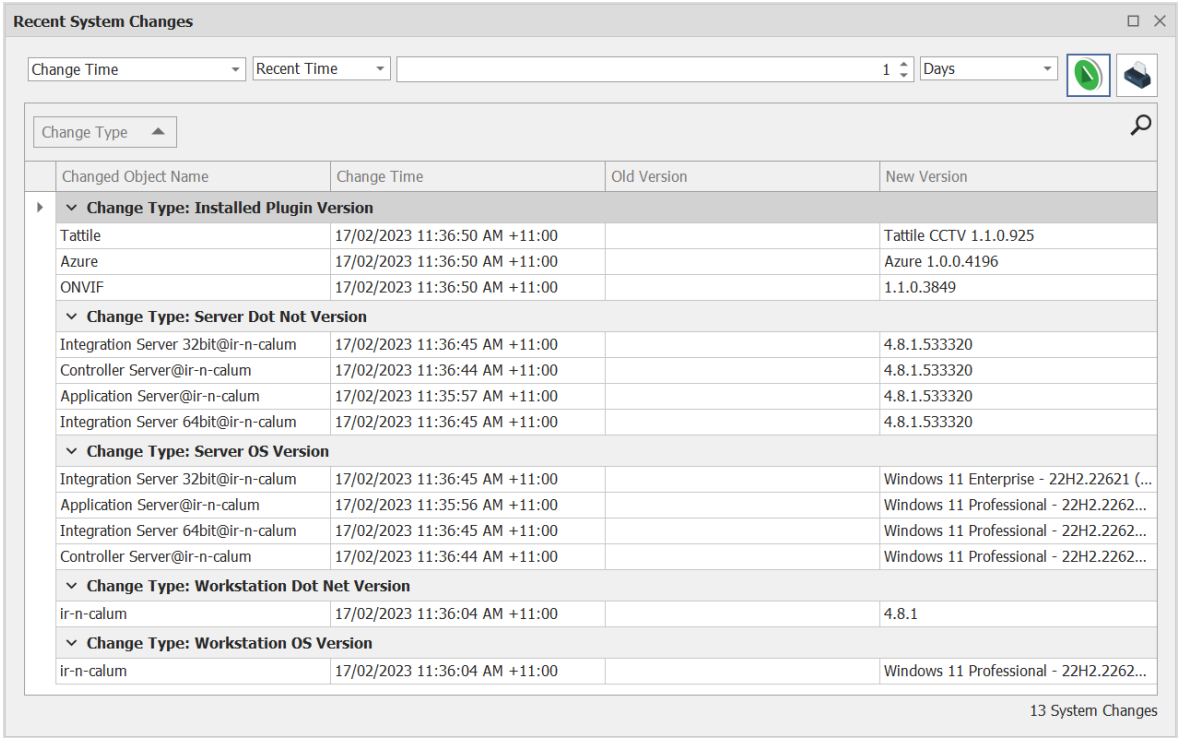
Once configured, 2FA can be configured for individual Operators from the Operator editor, allowing the Operator to be linked to the 2FA system for future logins.

- **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.



- **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.



- **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.



- **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

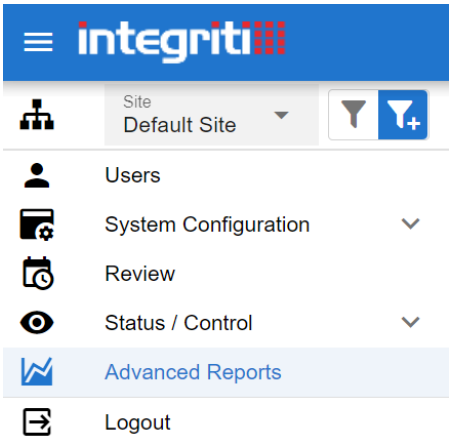
- **Hardware & Software Pre-Requisites:** Improved the Hardware & Software Pre-Requisites document to be clearer on OS and SQL Server requirements.
- **Integriti Translations:** Updated the Integriti Translations document to be up to date on the latest translation processes and include details on translating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

VERSION 22.2

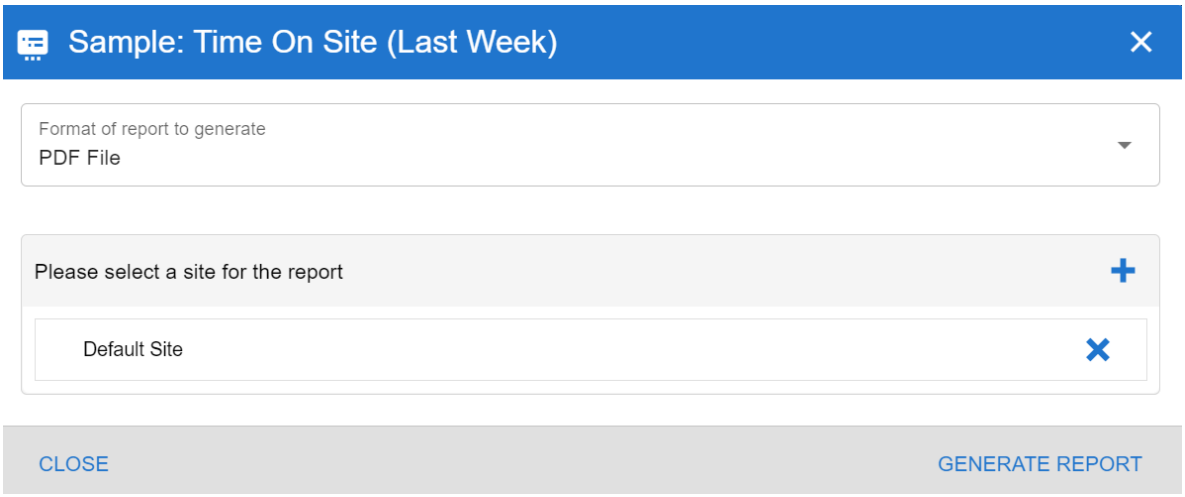
December 2022 - 22.2

Web Interface Report Generation

Integriti's web interface now supports generating and exporting Advanced Reports, saving the need to have a full System Designer or GateKeeper client installed to view reports. A new 'Advanced Reports' button has been added to the navigation pane of the web interface to show a list of all available reports configured in the system.



From the reports list, an Advanced Report can be exported to one of several different formats, including PDF and CSV. Reports will be exported with the default settings for the given export format. When exporting Advanced Reports with the 'Ask User When Report is Run' flag enabled for a report parameter, the user will be prompted for values for these parameters directly from the web interface prior to generating the report.



Once a report has been generated in the selected format it can be downloaded from the web interface and viewed on the client PC.

NOTE: Editing the configuration of Advanced Reports must be done from a full System Designer client. The web interface only supports exporting already configured reports.

Installation Packages

Simplified Integriti Installers

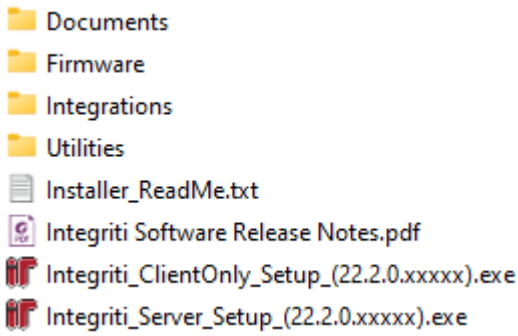
Integriti's installation packages have been simplified to streamline the installation process and provide specific installers for each type of installation. Integriti now provides the following 4 installation packages:

- **Integriti Server Setup:** Installs all the components required for an Integriti server installation. This includes all services, SQL Server (optional), and the System Designer and GateKeeper clients. The Controller and Integration (32 and 64 bit) Services can be optionally excluded from the installation when running this installer.
- **Integriti Client Only Setup:** Installs only the components required for an Integriti client installation. This will install both the System Designer and GateKeeper clients, but none of the Integriti Services or SQL packages included in the server installation package.
- **Integriti Mimic Viewer Feature Setup:** Installs all components required to use the Mimic Viewer feature of Integriti. The Mimic Viewer solution is a stand-alone installation and is intended to work independently of other Integriti software. The Mimic Viewer is limited to a read only connection to the controller, preventing any controller programming from being made. For more information, please refer to 'Integriti Mimic Viewer.pdf'.
- **Integriti Commissioning Software (CS):** Installs the Integriti CS package. Integriti CS is available to Integriti certified security installers free of charge and is to be used to commission Integriti controllers. It is not to be made available to end user customers under the terms of the license agreement. For more information, please refer to 'Integriti_CS-Quick_Start_Guide.pdf'.

ZIP Installation Package

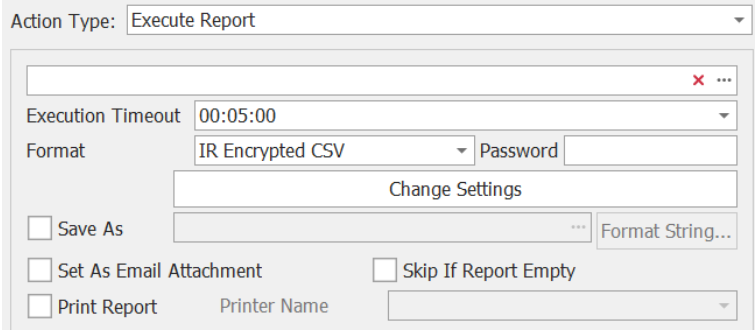
Integriti is now distributed in several convenient ZIP installation packages for Integriti, Mimic Viewer and Commissioning Software setups. Each zip contains several useful files for the relevant installation, including:

- The Integriti installer/s
- Latest Integriti Release Notes
- Integriti Documentation and Manuals
- Latest Controller and LAN Module Firmware
- Latest Software Integration Release Notes and Manuals
- Utility Tool Installation Packages

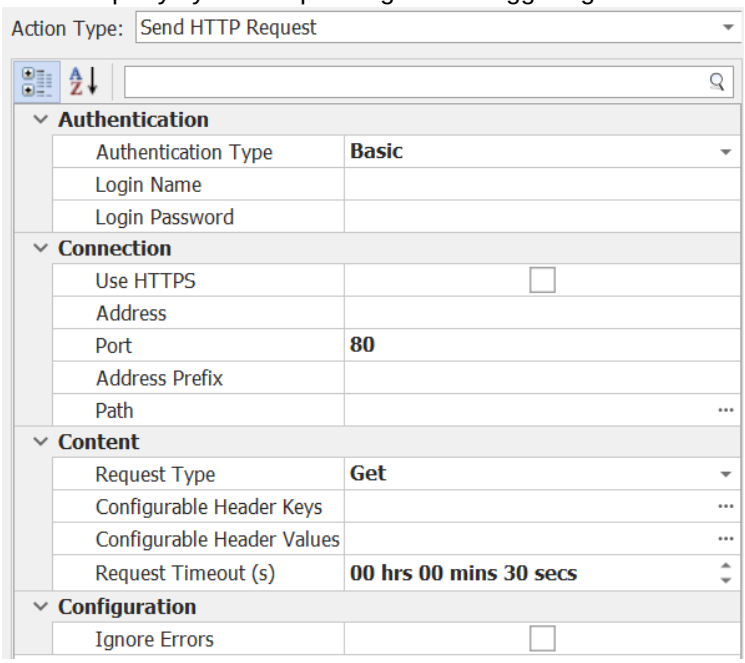


Improvements

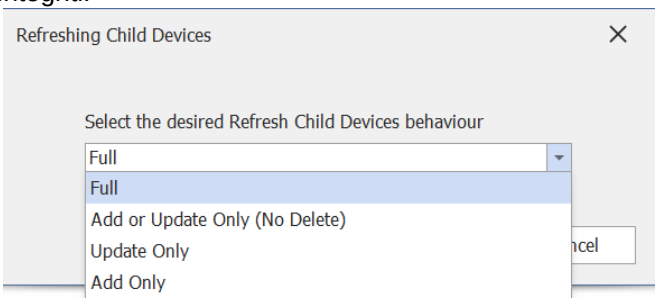
- **Packaged SQL Server Version:** The packaged version of SQL Server (Express edition) in the Integriti installation packages has been updated to SQL Server 2017. The new SQL Server version will only be installed for new installations or when installing in a new database. Existing installations will stay on the same version of SQL until manually updated.
- **Execute Report Task Action:** Added 'IR Encrypted CSV' export type to the Execute Report Task Action. This allows reports to be exported in an encrypted format, protected by a user-specified password. IR Encrypted CSV exports can then be imported into any Integriti system running v22.2 or higher via DUIM or the Import Data dialog after providing the correct password for the file.



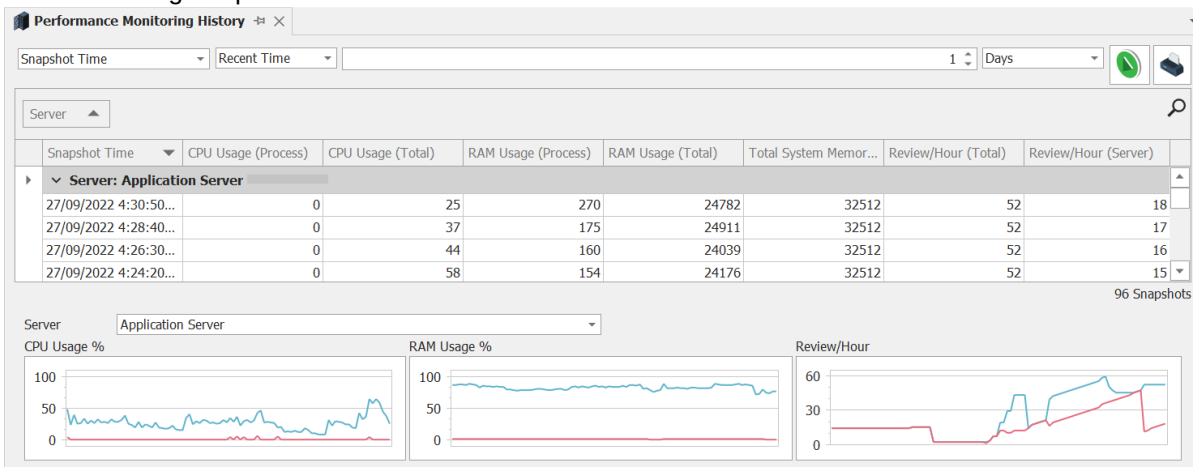
- **Send HTTP Request Task Action:** Added a new Task Action to allow a custom HTTP request to be automatically sent to a 3rd party system on a given trigger. This allows actions to be automatically triggered in external systems in response to events occurring in the Integriti system.
  The Send HTTP Request Task action allows HTTP requests to be sent with a configurable request type, headers and body to ensure compatibility with a wide range of different 3rd party APIs. The body and URL of the request can be configured as a format string, allowing them to be customised with options specific to the event triggering the action, allowing a single configuration to perform different commands in the 3rd party system depending on the triggering event.



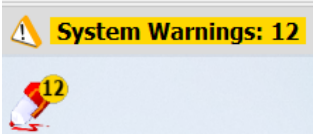
- **Integrations:** Added new options to customise the behaviour when Refreshing Child Devices for an Integrated System, including the option to prevent existing child device configuration from being deleted. The following options are now available when refreshing child devices for an Integrated System:
  - **Full:** Perform a full sync with the 3rd party system; adding, updating and deleting child devices in Integriti as required to match the configuration in the 3rd party system. This option is consistent with the behaviour from previous versions of Integriti.
  - **Add or Update Only (No Delete):** Update and add child devices to match the configuration of the 3rd party system. Existing child devices won't be deleted from Integriti regardless of whether they are present in the 3rd party system, ensuring no Integriti configuration is unintentionally lost.
  - **Update Only:** Only updates child devices that have already been pulled from the 3rd party system from a previous Refresh Child Devices. No new devices will be added and no child devices will be deleted.
  - **Add Only:** Only new child devices that exist in the 3rd party system but not in Integriti will be added. Existing child devices won't be updated, and no child devices will be deleted from Integriti.



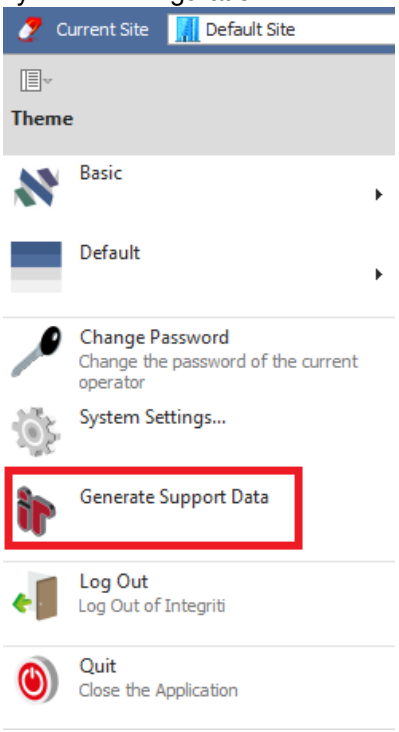
- **Integrations:** Added the ability to directly associate CCTV Cameras with non-Camera Integrated Device Endpoints. This allows for cameras to be directly associated with devices such as Intercom Points and Integrated Sensors to be used when showing CCTV footage from the device. This includes directly from the device (such as in the list and schematics) and from events generated by the device.
- **Performance Metrics:** Added new Server Performance Snapshots to assist in tracking the performance of a given server over time. Snapshots are taken every couple of minutes and automatically cleaned up over time, allowing the recent performance of a given server to be viewed. Snapshots contain details of the total (system-wide) and per-server CPU usage and RAM usage, as well as the total and per-server review rate (review/hour). The Performance History can be viewed from the Performance History button in the Administration tab of the System Designer ribbon, allowing both a list of snapshots and several charts detailing the performance over time to be viewed.



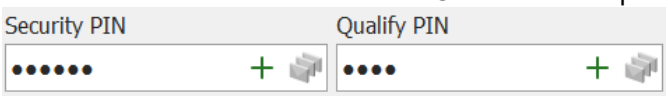
- **System Warnings:** Added a count of current System Warnings to the bottom right of the System Designer client and to the taskbar icon for open System Designer windows. This ensures outstanding System Warnings are clearly visible to Operators as they are generated and any current issues in the system are made known to Operators as they occur.



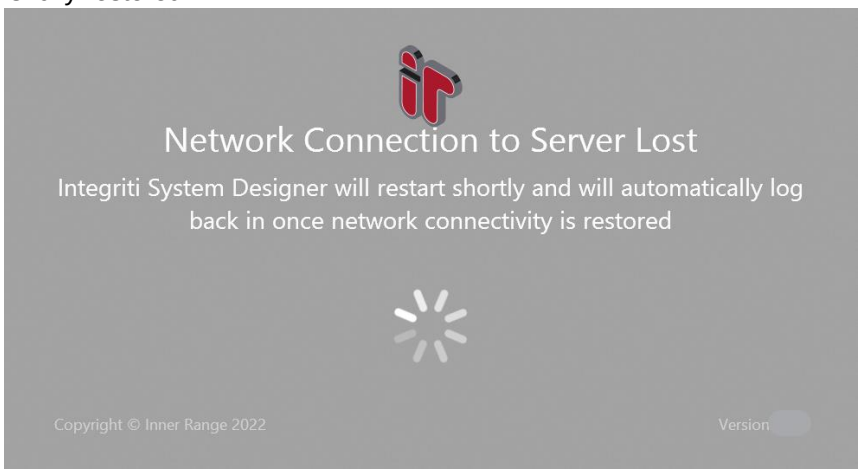
- **High Availability Scheduled Tasks:** Added the option to specify the priority of configured Scheduled Tasks. Server Instances can then be configured with a 'Minimum Priority to Process' and a 'Highest Priority to Process', allowing Scheduled Tasks of given priorities to only be run on specific servers in High Availability setups. This provides support for use cases such as running all long-running or low-priority tasks (such as executing reports) on a specific server to ensure they don't interfere with higher priority tasks running at the same time.
- **Generate Support Data Button:** A new button has been added to the System Designer menu that allows for the download of a support data file that can be used by Inner Range support to diagnose issues. The generated file contains information frequently requested by support when diagnosing issues, providing a simple way to collate the required information, and allowing for faster assistance. The generated support data file will include internal system logs as well as general information about the system's configuration.



- **User PIN:** Added Operator Type Feature Permission to prevent showing auto-generated User PINs to the user as they're generated. This allows an extra layer of security, ensuring only the User the PIN belongs to ever sees the auto-generated PIN.
- **User PIN:** Added a send pin button to the User editor's Security and Qualify PIN fields. This allows the PIN to be directly sent to the selected user using the default configuration in the same way the 'Send PIN' context menu command on the User sends the pin.



- **Firmware Update:** When updating firmware using the firmware update dialog, the progress column now shows progress downloading firmware from the controller to the specific LAN Module in addition to the progress initially downloading the firmware to the controller.
- **Client Connection Issues:** When network problems cause Integriti Clients to lose their connection to the server, a new window is briefly shown explaining that the Integriti client will be restarted and will automatically log back into the server once the connection is recovered, ensuring all client functionality is fully restored.



- **Visitor Management:** Added the option to print/export past visits from the Visit History list when viewing a Visitor Management Configuration. This allows both printing of the currently visible results, as well as exporting to one of several different formats, such as CSV and PDF.
- **Visitor Management:** Added a button to the lookup field property in the Visitor Management Visit editor to allow a matching User to be looked up based on the value entered. If a matching User is found, the Visit editor will be populated with the current configuration of the matching User.



- **Editor Layout Sets:** Added support for saving changes made to the editor layouts of several additional entity types that previously allowed the editor layout to be customised but not saved.
- **Advanced Reports – Permissions Report:** Added the option to include permissions to Permission Groups in the output of Permissions Advanced Reports.
- **License Plate Card Format:** Added support for entering Arabic characters into license plates when using the License Plate Card Format.
  NOTE: The original license plate may not always be fully recoverable from the generated Card Data.
- **Access Review:** Added the card number to Review Text for Review generated when access is attempted with an unknown card.
- **System Settings:** Changes to System Settings are now audited to allow tracking of any changes made.
- **Mimic Viewer:** Added support for using Review Trigger Scheduled Tasks in Mimic Viewer. This allows for configurations such as using the Control Workstation Task Action to automatically play a sound or show a specific Schematic on an event occurring in the Mimic Viewer system.
- **REST API v2:** Added support for updating User photos and image Custom Fields from the User Management Module of REST API v2.
- **REST API v1 & v2:** Added support for creating and updating global entities into partitions. This can be achieved by including the 'PartitionID' attribute in the entity XML, see below for required XML to create a User named John Smith into Partition 2. When updating an Entity, only entities in the Partition specified will be updated (where the identifier attribute matches).

```
<User PartitionID="2">
   <FirstName>John</FirstName>
   <SecondName>Smith</SecondName>
</User>
```

- **REST API v2:** Entities of the following types are now available for querying in the following modules:
  - **User Management:**
    - Custom Field Definition – Read
    - Site – Read
    - Partition – Read
    - Keyword – Read Summary
  - **Basic Status and Control:**
    - Custom Field Definition – Read
    - Site – Read
    - Partition – Read
    - Keyword – Read Summary
  - **Review IO:**
    - Custom Field Definition – Read
    - Site – Read
    - Partition – Read
    - Keyword – Read Summary
  - **Virtual Card Badge:**
    - Intelligent Reader Module – Read
    - User - Read
    - Site – Read
    - Partition – Read
    - Keyword – Read Summary

Issues Resolved

- **Site/Controller Export:** Resolved potential error the could be encountered when exporting Sites/Controllers from the Navigation Tree on large sites.
- **XML Import:** Resolved error that could be encountered when importing IREntities files containing large numbers of controllers.
- **CSV Import:** Resolved issue that could result in blank credentials being created when a credential clash is encountered while doing a CSV import and the credential clash behaviour is set to 'Skip Row'.
- **Advanced Reports – Time on Site Report:** Resolved issue resulting in the 'Break Time' or 'Off-Site Time' being zero for all report results when 'Daily Summary' is selected.
- **Advanced Reports – Time on Site Report:** Resolved issue that could result in the Time on Site values not being set correctly when using a Processing Mode of either 'By Area/Location (User Access)' or 'By Area/Location (Location Change)'.
- **Advanced Reports – Audit Report:** Start Date and End Date are now set to the correct values and can be used in the output of the report.
- **Controller Synchronisation:** Resolved issue that could result in the Controller's sync status in the navigation tree incorrectly indicating that there were remaining items to synchronise after controller synchronisation had completed.
- **Controller Detection:** Resolved issue that could result in auto-discovered controllers being added multiple times, resulting in duplicate controllers in the system.
- **3rd Party Door Integrations:** Resolved issue that could result in commands sent to doors being executed multiple times on each door with some configurations.
- **Biometric Reader Licensing:** Resolved issue that could result in some Biometric Readers incorrectly being marked as unlicensed.
- **Scheduled Task Door/Area Trigger:** Scheduled tasks configured with a Door/Area Trigger will now correctly trigger for users who have had their Primary Permission group changed to match the Door/Area Trigger's configuration after the Scheduled Task is configured.

Bug-Fix Release (v 22.1.2)

September 2022 - 22.1.2

Issues Resolved

- **Client Connections:** Resolved issue that could result in Client Connections not being correctly dropped when the connection between the Integriti client and server is lost in some circumstances.
- **Expiring User Qualifications:** Resolved issue that could result in Expiry and Warning actions for expiring User Qualifications only being executed once for each user. This would prevent the Expiry and Warning actions being executed additional times in the case where the Date specified in the associated custom field is moved forward from the original date after the qualification has already expired.
- **Advanced Reports:** Resolved issue resulting in the 'Ask User at Run Time' feature not working when specified against individual rows in one of the filters for a report.

Bug-Fix Release (v 22.1.1)

August 2022 - 22.1.1

Improvements

- **Integrated Sensors:** Added a new Integrated Sensor device type to represent sensor objects from integrated 3rd party systems. Integrated Sensors are able to be placed on Schematics and associated with Entities, allowing for Schematics and associated CCTV to be automatically shown from generated events and for controller action task actions to automatically control the entity associated with the Integrated Sensor triggering the action.
- **Integrations:** Supported integrations can now associate a location with generated Review records. This can be used to show where generated review occurred on a Schematic, as well as automatically showing relevant CCTV footage based on camera fields of view covering the location of the Review.
  Alerts generated from this review can be automatically shown at the correct location on a Schematic Map, with the position automatically updating as new Review records associated with the same object are generated at new locations.
- **CSV/AD Import:** Added support for using Name Match on columns mapped to Controller properties when configuring the String to Entity transformation.

Issues Resolved

- **Controller State:** Resolved issue that could result in Controllers incorrectly showing as Offline in the Navigation Tree and Controller List.
- **Operating System Version Detection:** Resolved issue that could result in Windows 11 systems being marked as Windows 10 in Server Instances and Client Connections.
- **Controller SkyTunnel Connection:** Resolved potential issue that could result in controller connections to SkyTunnel failing in some scenarios.
- **Database Restore:** Resolved issue that could result in Review databases not successfully restoring when restoring a Review database from the Integriti Database Configuration tool.
- **Integrated Device List:** Resolved issue resulting in filtering on the Status column not working.
- **Schematics:** Resolved issue resulting in configured Labels and Status/Hover Text for map elements (and Element Presenters) not correctly showing details of the associated object (such as name) for some Entity Types (such as Lift Cars and Lift Floors).
- **Advanced Reports:** Resolved issue resulting in filter rows configured with Ask User at Run Time not having changes made in the Report User Parameter Input dialog be applied to the resulting report.
- **Advanced Reports:** Resolved issue resulting in several properties not being available from the Advanced Report's report designer. This includes the User properties Cards, Permissions and Photo.
- **CSV Import:** Resolved issue where nested rows weren't imported when Skip Empty Fields is enabled.
- **CSV Import:** Resolved issue where nested imports failed for CSV files with nested rows in separate columns where values aren't entered for all rows. This is now supported with Skip Empty Fields enabled.
- **Active Directory User Sync:** Resolved issue that could result in Users failing to import when configured as a member of groups not visible to the Active Directory Communication Handler.
- **Modbus TCP Slave Communication Handler:** Resolved potential error resulting in state changes not being sent to the Modbus system, with an Invalid Cast exception being logged for each attempt.
- **Foreign Entity Controller Sync:** Resolved issue that could result in changes to Foreign Entities not being applied to Named Actions using them as triggers.
- **Door List:** Resolved issue resulting in the Door Type column in the Doors list not being sortable.

Documentation

- **Integriti Integrations - Core:** Added core integration manual to cover common integration configuration options where an integration isn't covered by a specific integration manual.

VERSION 22.1

June 2022 - 22.1

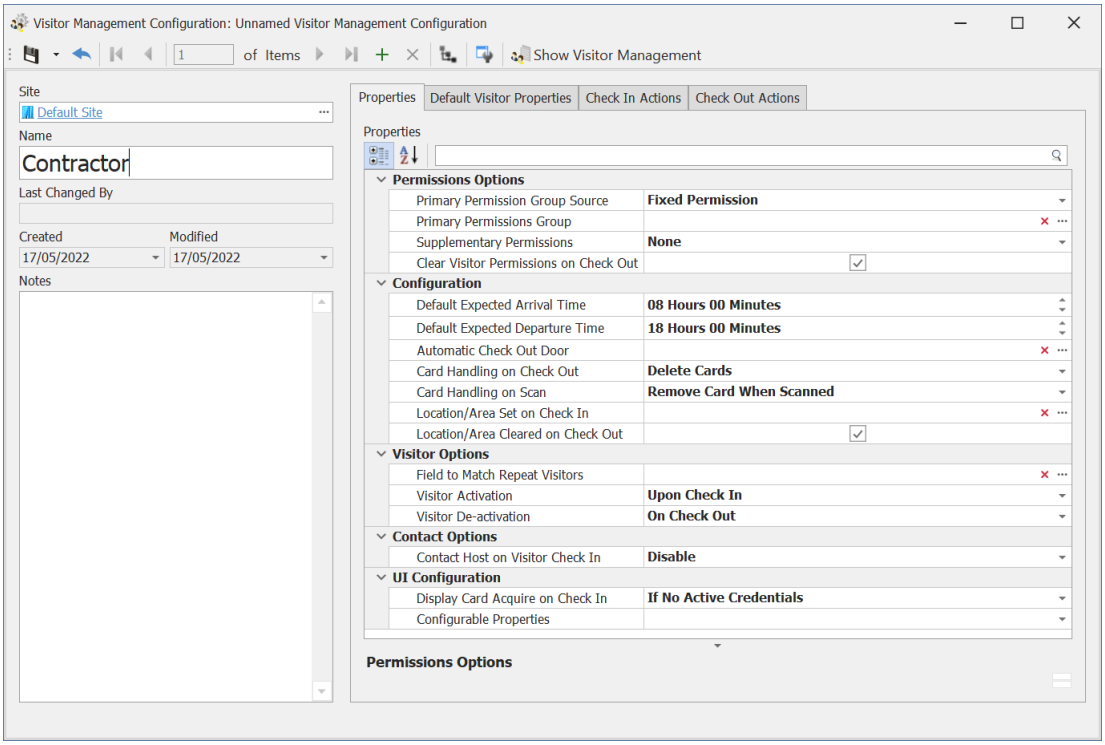
Visitor Management

Integriti v22.1 adds basic visitor management functionality as built in functionality for Integriti. This allows for a simpler workflow for visitors to a site, with a dedicated interface and automated management options for permissions and credentials. Visits for different types of visitors can be added directly from GateKeeper, associated with any configured Visitor Management Configuration. This allows different types of visitors to be treated differently, with different default properties and permissions, and different behaviour on a visit ending.

The new built-in visitor management functionality is included with installations of Integriti that are Business edition or higher. No additional licenses are required to use the new functionality.

Configuration

Any number of Visitor Management Configurations can be configured from System Designer, allowing for separate configurations to be used for different purposes, such as for different sites and different types of visitors (e.g. contractors and internal staff). Each configuration can be configured with different settings, allowing for each visitor's default properties, permissions and check-in/check-out behaviour to be customised depending on the configuration the Visit is created under.

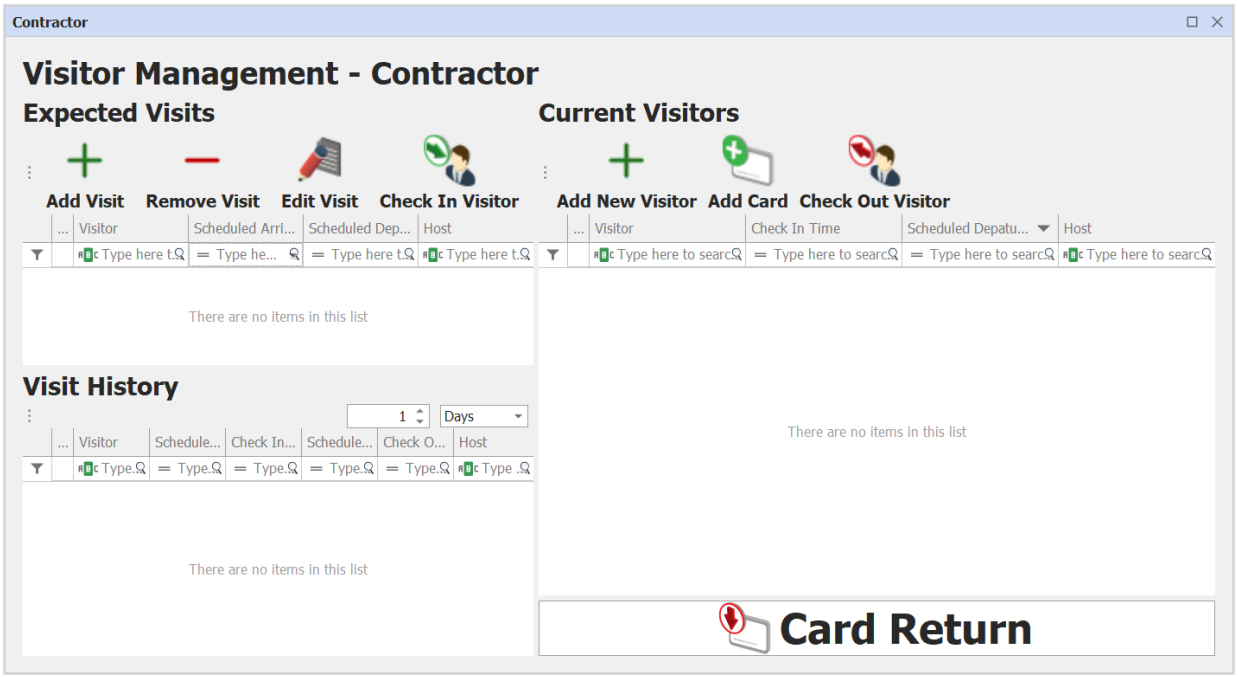


Managing Visits

Visits can be managed for a given Visitor Management Configuration by opening the configuration from the configuration list in GateKeeper. This will open the Visit Management Panel, which allows viewing and managing of all visits currently in the system for the selected configuration.

The visitor management panel is broken into 3 core modules – Expected Visits, Current Visitors and Visit History:

- **Expected Visits** shows visits that have been scheduled for the current day, showing who is expected to arrive that day. Future visits can be directly added, removed and edited from this module. Once a visitor arrives, they can be directly checked in and moved to the Current Visitors module.
- **Current Visitors** shows all visitors who are currently on site, allowing impromptu visits to be created as visitors arrive and visitors to be manually checked out as they leave.
- **Visit History** shows the previous visits for the selected configuration over the selected time period. This allows viewing of who visited a site over a given time period.



Visit Workflow

Visits can be created either ahead of time for known expected visitors from the Expected Visits module, or from the Current Visitors module for unplanned Visitors as they are checking in. Adding a Visit will create the Visit and associated User record with the visitor's details and configured options. For repeat visitors, the previous User record will be automatically re-used for the new visit, allowing for accurate reporting for repeat visitors. Depending on the specified Visitor Management Configuration, Visitors and their associated User record may automatically have default properties or relevant permissions automatically configured. These can be either hard-coded values or automatically extracted from the Host User.
Visitor Start and End times may be optionally configured on Visit creation depending on the configured Visitor Activation and Visitor De-Activation options. These properties provide the option for a Visitor to have early access to a Site prior to them checking in (with a pre-configured credential such as a license plate or a mobile credential), as well as allowing expected check-in/check-out times to be enforced, explicitly preventing a Visitor having access to a site a set amount of time before/after the expected arrival/departure time regardless of what time they check in or check out.

Visits can be manually checked in from the Visit Management Panel, at which point, after selecting an associated credential, they will be marked as checked in on the Visit Management Panel. On checking in, additional default properties can optionally be configured, as well as the Visitor's associated Area/Location. A custom Task Action action can also be configured to be executed on User check in.

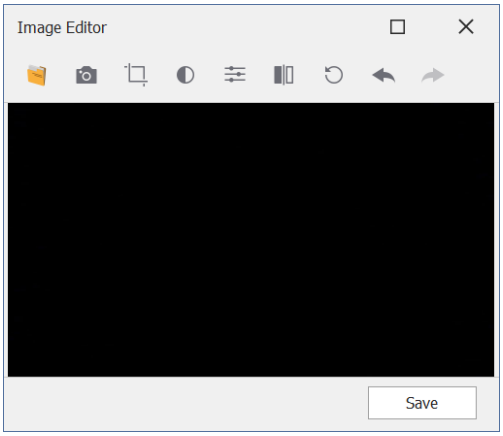
Checking out visitors can either be done manually on a per-visit basis from the Visit Management Panel, in bulk through the 'Card Return' option or automatically when a Visitor badges their card at the configured 'Auto-Checkout Door'. Checking out a Visitor will remove their access, optionally remove their configured permissions and credentials, and optionally set/reset configured property values to default values. Additionally, a task action can be automatically executed on check-out.

Visitor Credentials

Visitors can have credentials allocated to them as part of the check-in process. Physical cards can be assigned to a visitor through a pop-up box, badging the card at a reader for quick assignment. The card can be returned via the bulk return feature, while lost cards can show which visitor they were assigned to. Alternatively, Mobile credentials or QR Code credentials can be automatically generated for the visitor, either for all visitors or specific visitors only. This can occur on check-in or prior to their visit if credentials are required to access the site. On check out or end of day, the Mobile credential can be automatically revoked, freeing up the credential for future visitors.

User Photo Editor

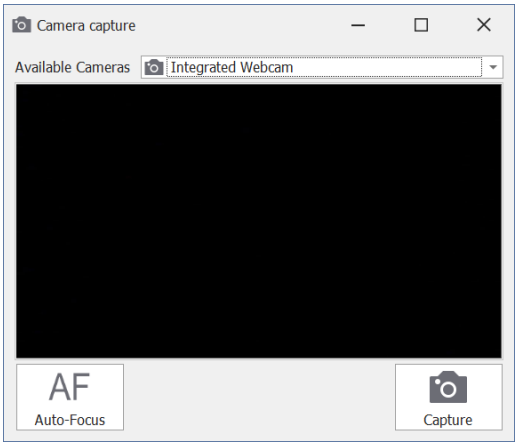
Integriti's user photo editor has been redesigned to simplify adding and editing of user photos, along with adding new sources for User Photos. The updated editor can be accessed in the same way as the previous User Photo editor by double clicking on the User Photo in the User editor or by selecting edit from the photo's context menu.



From the editor, the current User photo can be updated from file or from a camera, and different visual aspects of the current photo can be modified, including rotation and scaling, before saving the changes to the User.

User Photo From DSLR/CCTV Camera

In addition to the existing functionality allowing user photos to be sourced from file and webcam, the User photo editor has been expanded to allow user photos to also be sourced from supported DSLR and CCTV cameras, allowing significantly more flexibility in how user photos can be taken.



The new Camera Capture dialog allows DSLR Cameras connected via USB to the client PC to be selected from the dropdown and used in the same way as webcams to take User photos, showing a live feed directly from the connected camera before capturing the photo.

In addition to DSLR Cameras, the updated Camera Capture dialog also supports capturing user photos from CCTV Cameras supporting the 'Export Current Frame' functionality. CCTV Cameras can be selected from the 'Select CCTV Camera…' option in the Available Cameras dropdown. Once selected, a live feed will be shown from the camera and the User photo can be captured.

NOTE: Only supported DSLR cameras can be used to take User photos. Selected Canon (Canon PowerShot SX70 (HSPC2357), Canon EOS200DII (DS126761)) and Nikon DSLR cameras have been tested.

Important Notes

The following operating systems are no longer formally supported from Integriti v22.1 onwards.

- Windows 7
- Windows Server 2008

It is recommended to update to a supported operating system prior to installing Integriti v22.1.

The following Microsoft SQL Server version is no longer formally supported by Integriti v22.1 onwards.

- Microsoft SQL Server 2008

It is recommended to update to a supported Microsoft SQL Server version prior to installing Integriti v22.1.

See 'Hardware and Software Prerequisites' for full details on supported operating systems and Microsoft SQL Server versions.

Improvements

- **Active Directory User Sync:** Added Existing User Lookup Mode option to Import Settings. This allows Users imported from Active Directory to be found in Integriti regardless of the site they are located in, rather than only the specified site. This allows for Users to be moved between groups in Active Directory and be automatically picked up by multiple Active Directory Communication Handlers storing Users in different sites in Integriti.
  NOTE: When an existing User is found in a site different to the 'Default Navigation Group' for the Active Directory communication handler, they will remain in their current site and not be moved to the default site for the Communication Handler. To achieve this functionality, it is necessary to specify the Site in the import mappings.
- **Security Policy:** Blacklisted words configured in a Security Policy's Blacklist are now case insensitive. This means regardless of the case used for a selected password, if it matches a password from the Blacklist it will not be permitted.
- **Photo ID Design:** Added support for rotating label elements through the 'Rotate Angle' property.
  NOTE: Rotate Angle must be set to a multiple of 90 degrees for the text auto-sizing feature to work.
- **Integrated Systems:** Refreshing Child Devices on an Integrated System will now automatically call Refresh Device on all supported child devices. This allows individual device configurations of multiple devices to be simply updated from a single click on the parent device.
- **REST API v2:** Added support for reading Time Periods to the User Management integration module. This allows Time Periods to be simply used for the When of User Permissions.
- **REST API v2:** Added support for updating User Photos and Image Custom Fields through API requests. See the REST API web documentation for full details on using the REST API to configure User Photos and Image Custom Fields.
- **QR Code Credentials:** Added support for the QR Code Credential integration. This allows both manually and automatically generated QR Code credentials for Users in the system and sending the QR Code image via email to the associated User.
  NOTE: The QR Code Credential integration is installed as a separate integration installer that can be downloaded from the Inner Range website.

Issues Resolved

- **Active Directory User Sync:** Resolved issue resulting in Time fields being imported from Active Directory in the wrong timezone.
- **Active Directory User Sync:** Added support for importing users from Active Directory into a Partition. This allows the Default Navigation Group of the Active Directory Communication Handler's Import Settings to be configured to a Partition rather than only working when a non-Partitioned Site is selected.
- **Active Directory User Export:** Resolved issue resulting in Users with blank properties not correctly exporting to Active Directory. Blank properties now honour the 'Skip Blank Values' option in the Active Directory Communication Handler's Export Settings.
- **CSV Import/Active Directory User Sync:** Resolved issue in Name Lookup Transformation resulting in it not being possible to set the 'Site' to a Partition when the 'Action If Not Found' is set to 'Add'.
- **CSV Import/Active Directory User Sync:** The Name Lookup Transformation can now be used to set the value for the Site of imported Entities.
- **DB Object Filters:** Resolved issue that could result in the specified filter not being applied for Filter windows stored in a layout after the layout is restored.
- **System/Personal Layout:** Resolved issue that could result in layouts being loaded with the wrong tab selected.
- **Schematics:** Resolved issue resulting in map elements created from dragging and dropping Entities onto Schematic Maps not having an associated Element Presenter.

Documentation

- **Guide - Visitor Management:** Added guide documenting use and configuration of Integriti's built in Visitor Management functionality.

Bug-Fix Release (v 22.0.2)

May 2022 - 22.0.2

Issues Resolved

- **Controller Sync:** Resolved issue that could result in some programming for already configured entities being lost after re-connecting to a Controller that has been defaulted.
- **Mobile/Biometric Credentials:** Resolved issue that could result in generated credential being created with the wrong Card Type where an existing credential already exists in the system with the same card number.

Documentation

- **Report Designer:** Added documentation on the usage of the Report Designer used for advanced reports.

Bug-Fix Release (v 22.0.1)

April 2022 - 22.0.1

Issues Resolved

- **Challenge Definitions:** Resolved issue resulting in associated CCTV footage not correctly showing in Challenge Definitions.
- **Challenge Definitions:** Resolved potential issue resulting in some Challenge Definitions having a blank Response Layout after updating from previous versions of Integriti.
- **Partitions:** Entities configured in a Partition that doesn't match their assigned Site will now be automatically placed in a separate '__Invalid_Partition_Px' Site in the correct Partition. This resolves potential errors loading Entity Lists and interacting with the client where Entities are incorrectly configured.
  If Entities are found in the '__Invalid_Partition_Px' Site, speak to Inner Range Technical Support for assistance resolving any Partition errors that were found.
- **Expiring Permissions:** Resolved issue resulting in not being able to configure a Permission row to have a Delayed Start but no Expiry.
- **Firmware Update Dialog:** Resolved issue resulting in filtering not working on the firmware update dialog's Module list in some circumstances.

VERSION 22.0

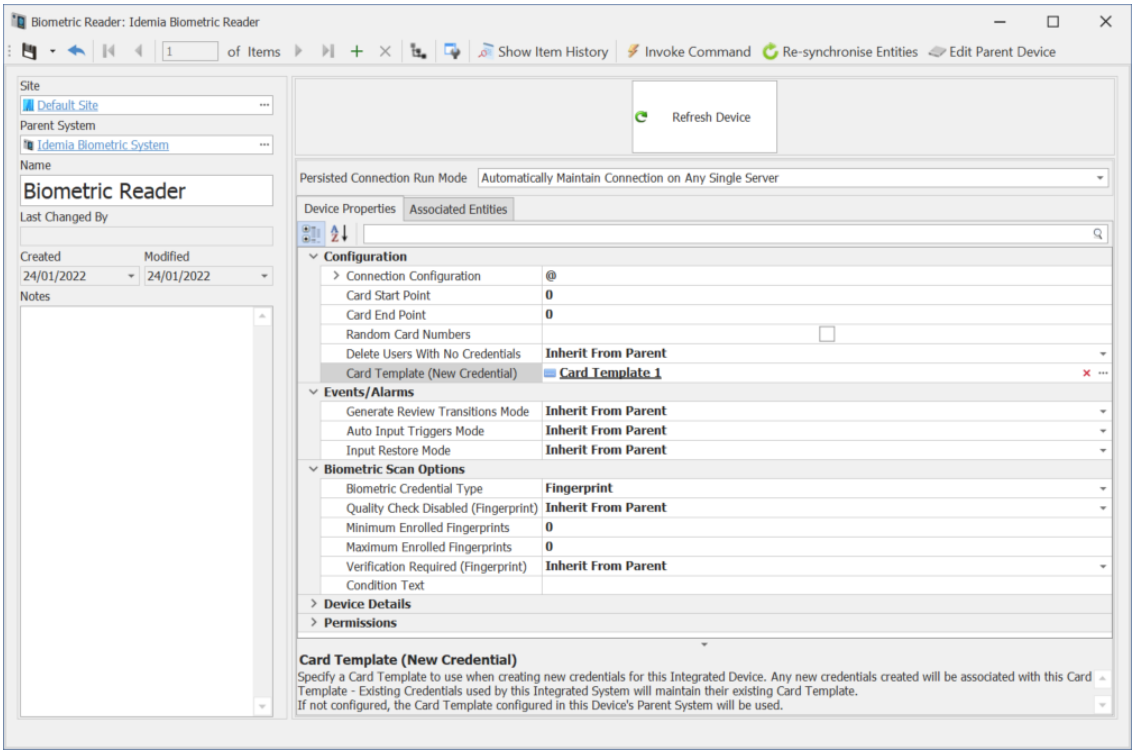
February 2022 - 22.0

Biometric Integrations

Integriti's Biometric Integration architecture has been improved to add support for connecting directly to individual biometric readers. When syncing directly to biometric readers Users will only be synchronised to relevant readers, as determined by which readers a User has permission to access. This ensures the reader's internal user database only contains the necessary users for the reader to function, preventing the internal databases on biometric readers from filling up and increasing the speed of biometric lookups on the devices.

NOTE: Biometric Readers with their persisted connection set to Disabled will not be available for biometric credential management and user sync.

NOTE: Existing biometric integrations do not currently support connecting directly to biometric readers. For future biometric integration releases, see each integration's manual for details on supported connection modes.

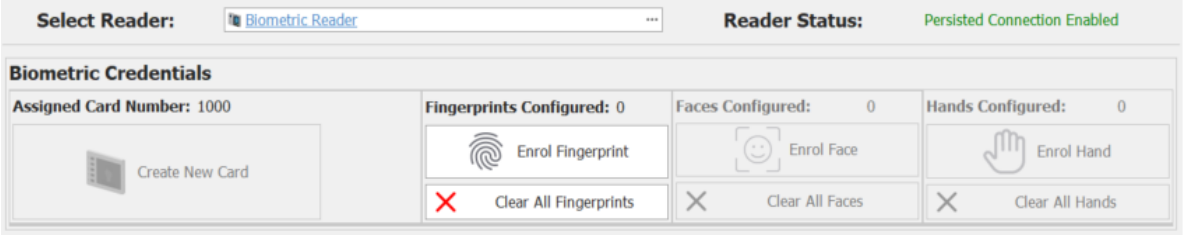


Licensing

All Biometric Integrations require the 'Integriti Integration - Biometric Management' (PN: 996969) license to be used. For integrations connecting directly to biometric readers, the 'Integriti Managed Biometric Reader' (996970) license is required in addition to the 'Integriti Integration - Biometric Management' (PN: 996969) license. Systems will require one 'Integriti Managed Biometric Reader' (996970) license for each reader that will be configured in the system. Unlicensed readers will not be able to enrol biometrics or synchronise users data from Integriti.

Biometric Credential Generation/Management – System Designer/GateKeeper

Biometric credentials can be generated and managed directly from a user's 'Acquire Card' dialog regardless of the connection mode, allowing for a simple and consistent UI for all biometric integrations. Once biometrics for a user are updated and the corresponding User is saved, the updated credentials will be automatically synchronised to the configured biometric system or biometric readers as required.

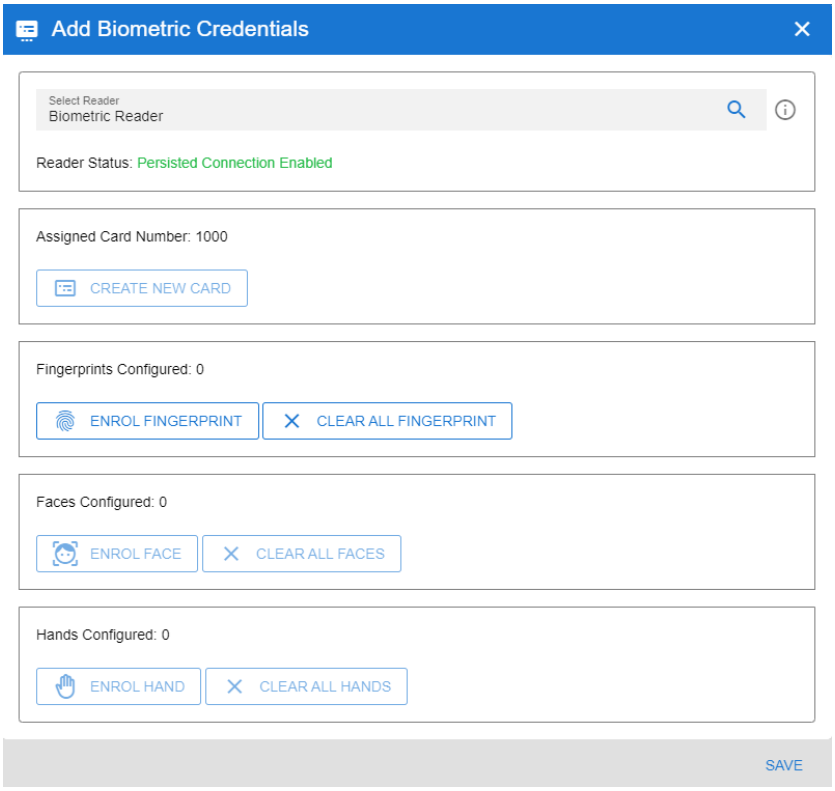


Biometric Credential Generation/Management – Web Interface

Biometric credentials for users are now able to be generated and managed directly from Integriti's web interface for supported biometric integrations. This allows the credentials to be configured for a user without the need to have an Integriti System Designer/GateKeeper client or the biometric plugin installed.

Biometric credentials can be managed for a user in the cards tab of the user editor. Selecting the 'Biometric' button above the cards list will open the biometrics dialog to allow management of the user's biometrics. Once updated, changes can be saved by pressing the save button on the biometrics dialog and saving the user. Once saved, changes will be automatically synchronised to the configured biometric system or biometric readers as required.

NOTE: Only supported biometric integrations support configuring biometrics from Integriti's web interface. Compatibility for a given biometric integration can be confirmed from the integration's release notes.



Biometric Reader User Sync

For biometric integrations configured to connect directly to individual biometric readers, Integriti is able to automatically determine which readers each user should be synchronised to. Users with biometric credentials configured will be automatically synchronised to all configured biometric readers they have been given permission to, as determined by them having permission to access the 'Associated Door' of the Biometric Reader in Integriti. Changes to a User's permissions and biometrics will result in them being automatically added to and removed from associated readers as the change is made. This allows for modifying a user's permissions at any point after their biometrics have been configured, and having that reflected on all configured readers.

The associated door of a biometric reader can be configured by either configuring the 'Associated Door' property of the biometric reader or adding the door to the 'Associated Entities' of the reader. Users will not be synchronised to readers without an associated door configured.

Biometric Reader Configuration

Integriti's biometric integrations allow limited configuration of biometric reader options directly from Integriti when connecting directly to the biometric reader. This allows frequently modified settings to be conveniently updated from a central point, saving opening the biometric reader's configuration tool. Supported configuration options differ on a per-integration basis, see the relevant integration manuals for further details.

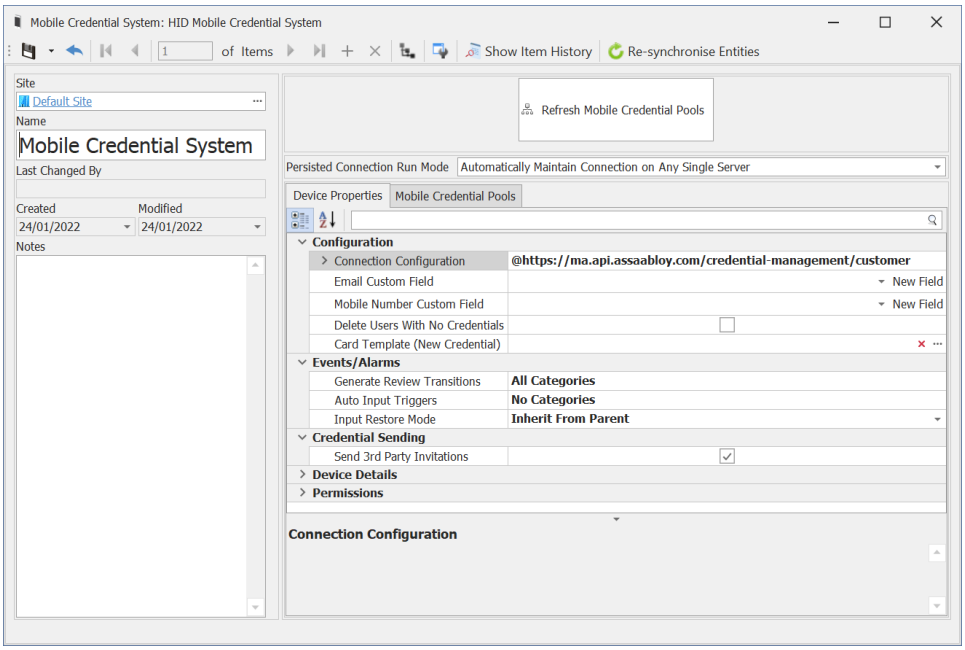
NOTE: Once configured, a Refresh Device must be performed on the device to send the updated reader configuration to each biometric reader.

Documentation

For more information, see the 'Integriti Integrations – Biometric' manual distributed with the Integriti installer.

Mobile Credential Integrations

Integriti's mobile credential integration architecture has been updated to simplify configuration of integrations to mobile credential systems. Mobile credential systems integrations are now installed as separately packaged plugins, rather than being built-in Communication Handlers. This allows for mobile credential integrations to take advantage of Integriti's existing plugin architecture, allowing finer control of the connection to the mobile credential system. On top of this, Mobile Credential Pools for a given Mobile Credential System are now represented as separate objects in Integriti, allowing for convenient per-pool configuration.



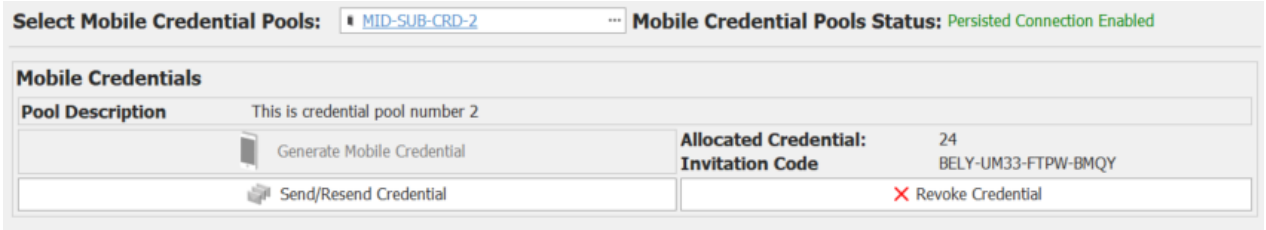
Licensing

Mobile Credential Integrations require the 'Mobile Credential Management Integration' license to be used. This allows an unlimited number of mobile credentials to be configured in a system.

Mobile Credential Generation

Mobile credentials can be generated and managed directly from a user's 'Acquire Card' dialog. Selecting the tab for the integration to use allows for generation of a new credential for the user, or for an existing credential to be revoked or have an invitation to be re-sent (where supported by the integration).

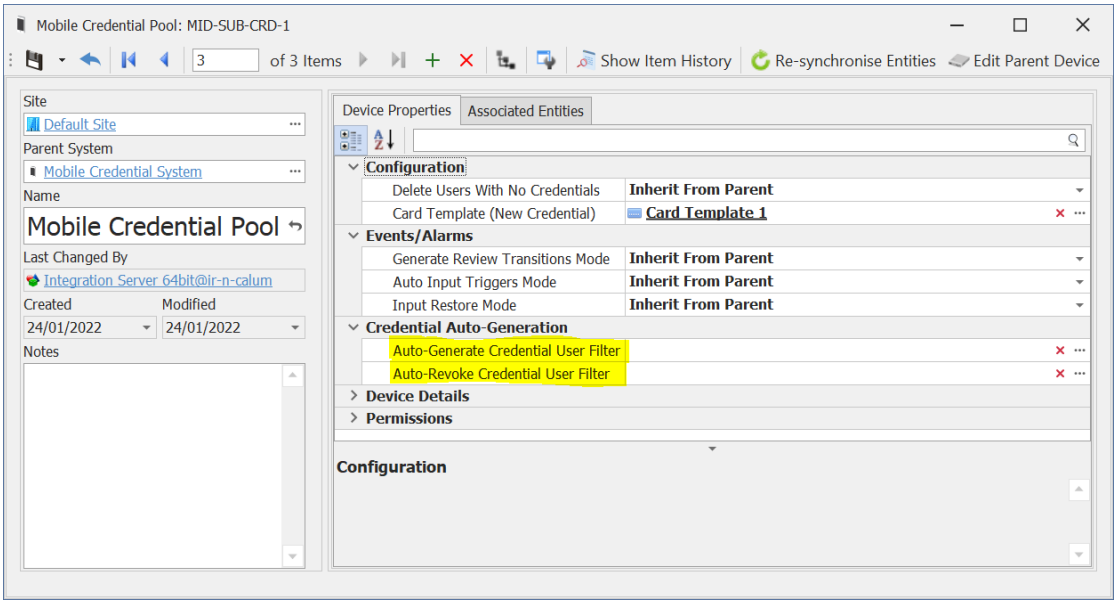
Integriti's mobile credential integrations support generating a single mobile credential for each user per mobile credential pool. For mobile credential systems with multiple credential pools, one credential can be generated per pool for a given user. Where a mobile credential is already configured in the mobile credential system, that credential will be automatically retrieved by the 'Acquire Card' dialog.



Automatic Mobile Credential Generation

Integriti's mobile credential integrations add support for automatic generation of mobile credentials for any user in the system based on custom criteria, on a per-mobile credential pool basis. Automatic credential generation is configured through a mobile credential pool's 'Auto-Generate Credential Filter' property, allowing automatic credential generation to be triggered based on any of a user's properties or custom fields, supporting different criteria being specified for each pool. This could allow automatically generated credentials to use one credential pool for staff and another for visitors, allowing for simple credential pool management.

Once configured, mobile credentials will be automatically generated in each mobile credential pool for all users in the system who match the configured filter, regardless of how they are added to the system or updated. Matching users already in the system will have their credentials automatically generated as the integration starts its persisted connection, while newly added users will have their credential automatically generated shortly after they are added. Users whose properties are changed to match the filter after they are created will have a credential automatically generated for them shortly after the change is saved. This allows for a User to be created or updated from an external source and have a Mobile credential assigned and issued without any human interaction.



Automatic Mobile Credential Revocation

Similar to the Automatic Mobile Credential Generation filter, an Automatic Mobile Credential Revoke filter can be configured for each Mobile Credential Pool to automatically revoke mobile credentials from a given mobile credential pool for users matching a specified filter. This can be used both separately to or in parallel with the Automatic Mobile Credential Generation filter, depending on the specific needs of the site. Revoked credentials will be both marked as revoked in Integriti and revoked from the 3rd party system, preventing it being used in the future. Users matching both the Automatic Mobile Credential Generation filter and the Automatic Mobile Credential revoke filter will have the revoke take priority and no credential will be generated.

Automatic Mobile Credential Revocation allows for mobile credentials to be automatically freed up within the Mobile Credential system for future use when no longer required. This can include when a visitor or contractor concludes their time on site, or when staff leave the company.



Mobile Credential Management

Once a mobile credential is generated (either automatically or manually), Integriti will ensure that the 3rd party system is kept up to date with changes to the credential and its associated user as they are made. This includes both changes to a User's properties (that are synchronised by the integration) and changes made to the mobile credential.

Once generated, mobile credentials can be revoked from the mobile credential system in a number of ways:

- **Acquire Card Dialog:** As with the previous Mobile Credential Communication handler, Mobile Credentials can be manually revoked directly from the Acquire Card dialog by simply selecting the relevant Mobile Credential Pool and pressing the '<REVOKE CREDENTIAL>' button.
- **Automatic Mobile Credential Revoke:** As detailed above, a filter can be configured in the Mobile Credential Pool settings to automatically revoke mobile credentials for Users matching a filter.
- **Card Status:** Credentials will be automatically revoked from the mobile credential system if the state of the credential in Integriti is changed to a permanent inactive state. This allows for mobile credentials to be managed in a way similar to physical credentials, without the need to explicitly revoke the credential. Mobile credentials will be automatically revoked regardless of how the state of the card is updated. Setting the state of a mobile credential to a temporarily inactive state in Integriti will leave the credential active in the mobile credential system, ready for the credential to be re-enabled in Integriti. This allows for features such as temporary credential replacement and card start times to function without the credential being incorrectly revoked from the mobile credential system.

HID Cloud Credential Communication Handler Migration

Sites using the existing HID Cloud Credential communication handler will have the option to migrate to the new HID Mobile Credential integration in their own time. The legacy communication handler will continue to function for existing configurations, with no changes to how it is used or configured for v22. It is, however, recommended to plan the migration to the new HID Mobile Credential integration in the near future, as the legacy communication handler will be disabled in a future update.

Migrating from the legacy HID Cloud Credential communication handler to the new HID Mobile Credential integration is a simple process, managed largely by the integration itself. The integration should be configured in parallel to the legacy communication handler/s, leaving the communication handler enabled. Upon refreshing child devices and starting the persisted connection of the Mobile Credential System, existing cloud credentials and user data created using the communication handler will be automatically migrated to the new format. Once completed, the legacy communication handler will be automatically disabled, and the newly configured integration can be used going forward, with all existing mobile credentials remaining configured for management with the new integration. After the legacy communication handler has been automatically disabled, it is safe to delete if required.

Documentation

For more information, see the 'Integriti Integrations – Mobile Credentials' manual distributed with the Integriti installer.

REST API v2

Integriti's REST API has been redesigned from the ground up to simplify developing integrations to Integriti. The updated API expands on the functionality supported by the current API, providing a number of new options and request endpoints to better support a number of integration use cases. API endpoints are now grouped by use case, providing more targeted functionality based on the type of integration being developed.

Getting Started

Integrators can start using Integriti's updated REST API by reaching out to Inner Range Sales and applying for an API Key. Each API key is tied to a unique Integriti license that must be present on the product keys of all Integriti systems using the integration. The necessary 'Unlock API Key' license will be generated as part of the API key application process, and can be added to any number of product keys from KeyPoint. Once an API key is generated, it must be included as part of the authentication with the Integriti server.

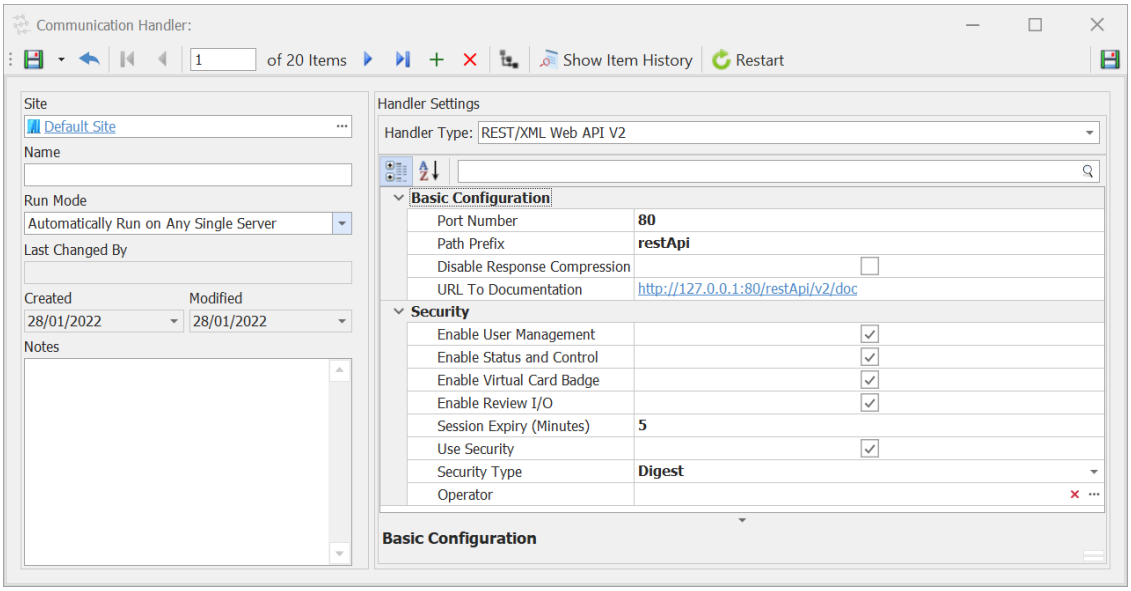
Licensing

Integriti's REST API v2 is now included for free with Integriti Professional and above. The previous REST API's Read, Write and Control Licenses are now only required when using integrations written against the REST API v1. The only requirement for a site running Integriti Pro or higher to use REST API v2 integrations is the addition of the 'Unlock API Key' license for each REST API v2 integration being used by the system.

Configuration

Once the necessary API key has been added to a system's product key, Integriti's updated REST API v2 is configured by creating a Communication Handler with a type of 'REST API v2'. From here, configuration options such as the port, URL prefix and security options can be configured.

To secure access to a system, individual components/use cases of the REST API can be optionally disabled from the REST API's configuration. This allows the endpoints exposed by the configured REST API to be limited to only those required for the integration/s being used, disabling additional functionality and access to the system. To assist with running multiple services on the same port, Integriti's REST API v2 requires a 'Path Prefix' to be configured. This allows multiple services to run on the same port (Integriti Web Interface, etc), where each is given a unique prefix – simplifying configuration and reducing the ports required to be opened in the firewall.



API Integration Modules

The following integration modules are supported by Integriti's REST API v2:

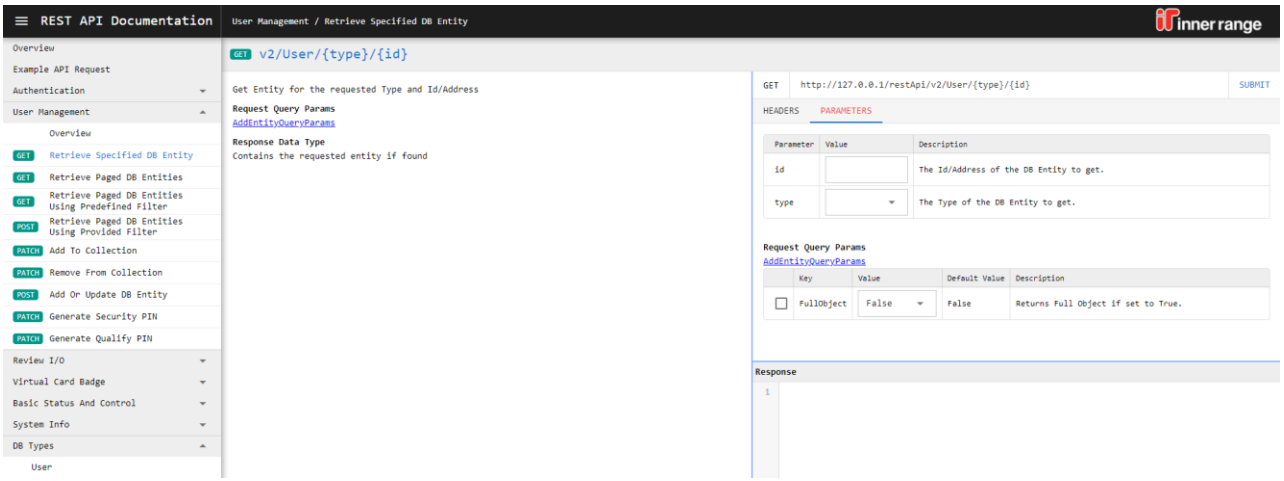
- **User Management:** The User management module allows for an integration to both manage Integriti users based on the configuration of a 3rd party system and to keep a 3rd party system's configuration up to date with changes made to users through Integriti. This module allows full user details, including permissions and credentials to be queried and/or updated through the API.
- **Review I/O:** The Review I/O module allows for systems to integrate to Integriti's review architecture. This allows for systems to either generate review in Integriti based on triggers from a 3rd party system, or to trigger actions in the 3rd party system based on Review being generated in Integriti. This module supports querying Review and basic details of associated Entities from Integriti, as well as saving Review to Integriti (along with associations to Integriti Entities).
- **Virtual Card Badge:** The Virtual Card Badge module allows an integration to trigger a card badge to occur on an Integriti reader based on a trigger from a 3rd party system. Instead of just unlocking the specified door, the virtual card badge allows full access control logic to occur, as though the user had physically presented their credential at the specified reader. This includes checking the permissions of the user associated with the credential prior to granting access, updating the user's associated area/location, logging access review and allowing for multi-credential access on doors requiring multiple types of credentials. This module supports receiving basic details of Integriti's access modules, as well as the ability to trigger a 'Virtual Card Badge' (either with card data/number or a license plate).
- **Status and Control:** The Status and Control module allows for an integration to monitor the status of Integriti entities and trigger controller actions in the Integriti system. This module supports retrieving basic details and status of Entities and triggering a number of actions on Integriti controllers (such as granting access to doors or moving a User to a different Area).

Documentation

The web-based documentation for Integriti's REST API has been completely re-written to fully describe all possible endpoints supported by the updated API. The documentation is conveniently grouped by integration module, ensuring all necessary endpoints for a given type of integration are close together.

The documentation contains details on all supported endpoints, including sample request and response data, and a built-in tool for trying out each endpoint. This tool provides details of all possible parameters for each request, as well as providing possible options for a number of endpoints where possible. On top of this, each endpoint provides detailed documentation for all types that can be interacted with by that endpoint, along with all properties that can be retrieved and modified through the API.

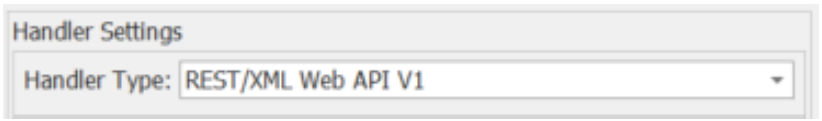
Along with the web-based documentation and endpoint testing tool, a Postman configuration is available to download from the web-based documentation. This provides the configuration for all supported REST API endpoints to be loaded into Postman to assist with testing endpoints and possible configurations.



Legacy API Integrations

Existing integrations to Integriti's REST API v1 will continue to function as expected on existing systems, no changes need to be made. Integrations written against REST API v1 can be used on new versions of Integriti by creating a 'REST API v1' Communication Handler. Configuration for this Communication Handler has not changed from previous versions of Integriti.

API Integrations must fully migrate to the new API, using the new endpoints, to take advantage of the new functionality added in REST API v2. Systems using the updated integration must create a new REST API v2 Communication Handler for the updated integration to communicate with.
NOTE: To migrate an integration to using the new API, it is necessary to first apply for an API key. See above for details.



Muster Point (Mobile Reader) App

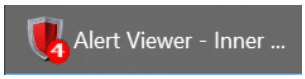
Systems using the Muster Point app should continue to use the REST API v1 Communication Handler. Existing Muster Point configuration will continue to work after updating, with no changes being made.

Integration Compatibility

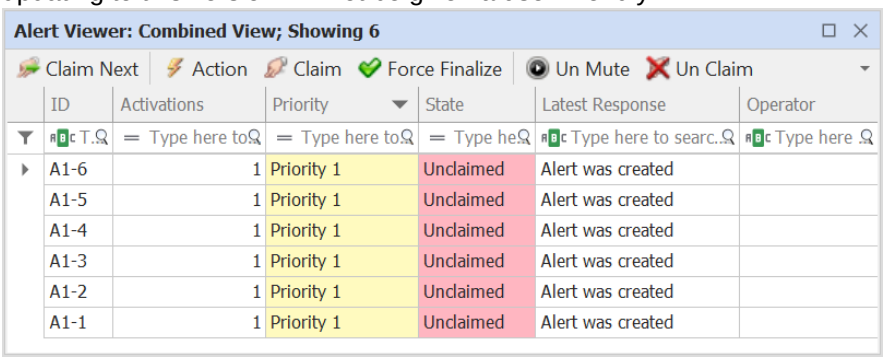
- Visionline (VingCard) Visitor Management v2.3 or higher is required for Integriti v22.0 onwards

Improvements

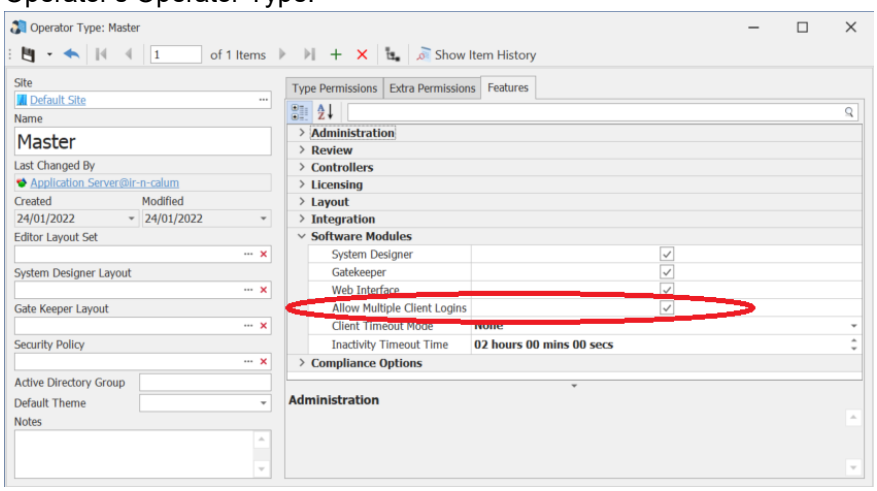
- **Alerts:** Added current unclaimed Alert count to the taskbar icon for GateKeeper. This will automatically be shown upon logging into GateKeeper, and will show the number of unclaimed Alerts visible to the currently logged in Operator.
  As new Alerts are received, the GateKeeper taskbar icon will flash to indicate the new Alert, and the unclaimed Alert count will be updated.



- **Alert User Friendly IDs:** Added an additional 'user-friendly' ID to Alerts. This gives each Alert an easy to read identifier that is simple to read aloud and remember. Each Alert's user-friendly id is comprised of an identifier for the server that generated the Alert and a numeric identifier for the alert (e.g. A1-13).
  All newly created alerts will be given a user-friendly ID, Alerts already present in the system prior to updating to this version will not be given a user-friendly ID.



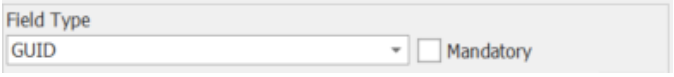
- **Controller Sync:** Improved performance and CPU usage of communications with Integriti controllers on systems with large numbers of controllers.
- **Operator Login:** Added new feature permission to restrict Operators from logging into multiple clients at the same time. This ensures that a given Operator is only able to use a single client connection, preventing them from logging in on additional clients and using multiple client seats.
  An operator attempting to login to an additional client with the 'Allow Multiple Logins' Feature Permission disabled will be given the option to either logout of the client they're already logged into, or cancel their login on the new client.
  This feature can be enabled by configuring the 'Allow Multiple Logins' Feature Permission for an Operator's Operator Type.



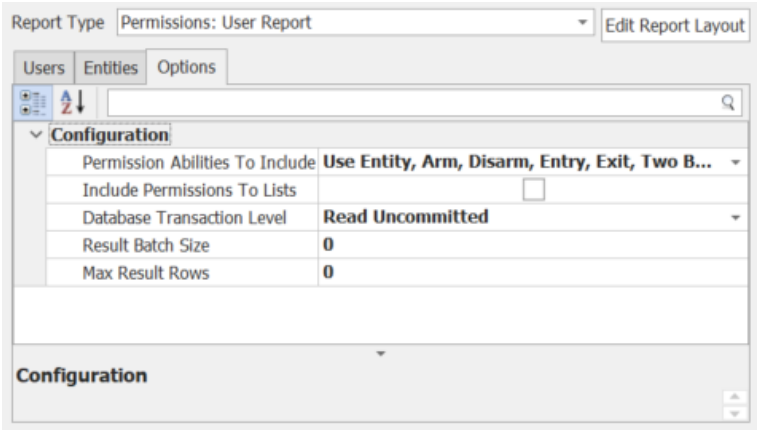
- **Indexed Custom Fields:** Added support for indexing string, numeric and boolean custom field values. This allows for better performance in queries when looking up entities based on custom field values. All numeric and boolean custom fields will be automatically indexed after updating. To index string Custom Fields, it will be necessary to create a new Custom Field of type 'String (Indexed)' and migrate current values from the existing custom field to the newly created custom field. Values in the new custom field will be indexed.
  Indexed string custom field values are limited to a maximum of 250 characters. If custom field values are to be larger than this, the 'String (Indexed)' custom field type is not supported, and the 'String' custom field type must be used.
  Custom Fields created after updating will be automatically indexed where they are given a numeric, boolean, 'String (Indexed)' or 'Unique Identifier' custom field type. Custom Fields created with any other custom field type will not be indexed.



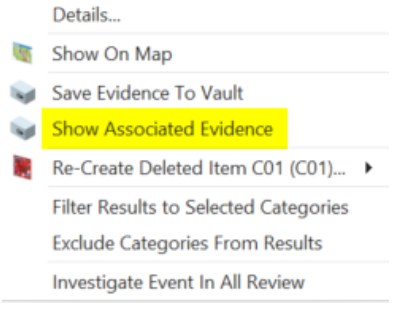
- **GUID Custom Fields:** Added a 'GUID' Custom Field type to allow storing custom data as a Guid in the database. Unique Identifier custom fields are automatically indexed in the database.



- **Permissions Report:** Improved the execution time and memory usage of the Permissions report. Existing Permissions reports will automatically take advantage of these improvements, and will not need to be modified.
- **Permissions Report:** Added property to optionally specify which Permission Abilities are shown in the results of Permissions Report.



- **Evidence Vault:** Added 'Show Associated Evidence' button to the context menu of Review. This allows evidence generated from a given review record to be easily accessed directly from the Review record. If multiple evidence items are associated with the selected Review record, a list of Evidence Items will be shown to allow easy selection of the correct Evidence Item from the vault to show.
  Showing Associated Evidence will load the file associated with the Evidence using the default program for that file type on the client machine that executed the command.



- **Send User Message:** Sending a message from the context menu of a User will now remember the last Communication Handler used for that client to save having to select the Communication Handler to use to send the message every time a message is sent.
- **KONE Lift Integration:** Added support for up to 5 KONE User Profiles for each User. These are configured through additional 'KONE User Profile' custom fields in Integriti Users.
- **KONE Lift Integration:** Added support for more formats of KONE Entity IDs in the Custom Fields linking Integriti Entities to KONE entities.
  Newly supported formats include "Text : 123" and "123".
- **Operating System Support:** Added support for Windows 11 and Windows Server 2022.
  NOTE: The packaged SQL Server (2014 SP2) is not officially supported on Windows 11 or Windows Server 2022 by Microsoft. On these operating systems we recommend downloading & installing SQL Server Express 2019 prior to installing Integriti.

Issues Resolved

- **Server Instance Deletion:** Prevented potential Foreign Key Exceptions when deleting Server Instances.
- **Editor Layout Sets – Door Editor:** Resolved issue where Door Configuration properties were not able to be included in the layout for a Door editor. Door Configuration properties will now show in the property list when editing layout of the Door editor, similar to previous versions of Integriti.
- **Editor Layout Sets – Door Editor:** Resolved issue resulting in the stored Editor Layout Set for the Door editor being lost after updating Integriti.
- **Audit:** Resolved issue that could result in not being able to view or revert to audited changes made on a previous version of Integriti for some entity types.Documentation
- **Integriti Integrations – Mobile Credentials:** Added manual describing configuration of Integriti's 3rd party door integrations. This manual contains details on configuration that is common across all integrations, see the integration specific manual for specific details on configuring that integration.
- **Integriti Integrations – Biometric Credentials:** Added manual describing configuration of Integriti's 3rd party door integrations. This manual contains details on configuration that is common across all integrations, see the integration specific manual for specific details on configuring that integration.
- **Integriti Integrations – 3rd Party Doors:** Updated manual describing configuration of Integriti's 3rd party door integrations. This manual contains details on configuration that is common across all integrations, see the integration specific manual for specific details on configuring that integration.

Bug-Fix Release (v 21.1.2)

December 2021 - 21.1.2

Issues Resolved

- **User Expiry:** Resolved potential issue preventing processing of user expiry for Users with special characters in their Name, Notes or an associated Custom Field.
- **Display Themes:** Resolved potential issue resulting in it not being possible to select a value for a Display Theme Rule in the editor after changing the Property Name.
- **Display Themes:** Resolved potential issue resulting in duplicating Display Theme Rules in the editor not working for some properties.
- **Mimic Viewer:** Resolved issue resulting in Schematics not being able to open using the Mimic Viewer client on some installations.
- **Security Policy:** The default global Security Policy (configured in the System Settings) is now used when logging in as an Operator without a Security Policy associated with their Operator Type when determining whether to the Enforce 2FA check.
- **Make Xmit For Area Controller Action:** Resolved issue resulting in the 'Make Xmit For Area' Controller Action not working correctly when executed from a Controller Action Task Action or the Send Action dialog.
- **Lockers:** Opening the Lockers list now correctly shows all lockers configured in the system.
- **Locker Bank:** Resolved issue resulting in an error being given when using the 'Bulk Create Lockers' command without the 'Assign Readers' option be selected.
- **Schematics:** Removed the potential for the Integriti client to crash when failing to load a Schematic Map in some circumstances.
- **Partitions:** Resolved potential error could result in it not being possible to add entities to newly created Partitions.
- **Filtered Data Report:** More types now support the Start Time and End Time properties in the report editor.
- **CCTV Integration:** Default PTZ speed options can now be configured directly from the CCTV System for all child cameras of that system.
- **Third Party Door Integration:** Increased the maximum number of 3rd Party Doors associated with a single 3rd Party Controller from 255 to 65,535.
- **Integrations:** Refreshing Child Devices on an Integrated System will now no longer add duplicate child devices (with the same 3rd Party ID) where the same child device is retrieved from the 3rd party system by the integration multiple times.
- **RTLS Assets:** Resolved issue that could result in RTLS Assets being duplicated when refreshed or reloaded by the RTLS integration managing them.
- **Reports:** Resolved issue resulting in reports continuing their execution on the server to completion even after the report has been cancelled. Reports will now stop execution shortly after the report has been cancelled from the client, after the step currently being processed has been completed.
  NOTE: There may still be a delay between cancelling a report and the execution of the report stopping for reports processing large amounts of data. Execution of the report will be stopped once the currently executing step of the report has concluded, which may vary in completion time depending on the complexity of the report.
- **Entity Deletion:** Resolved potential 'Object Reference not set to an instance of an object' error when deleting Entities with associations to Doors.
- **Dot NET Detection Logic:** Updated Dot Net Detection logic to detect Dot NET 4.8 installed on Windows 11 and Windows Server 2022.

- **User List:** Added support for using the 'Is Not Blank' and 'Is Blank' filters on the Credentials column to filter down to only users that either have or don't have Credentials.
- **Operator Type List:** Improved load times of the Operator Type list on large systems.

Bug-Fix Release (v 21.1.1)

October 2021 - 21.1.1

Issues Resolved

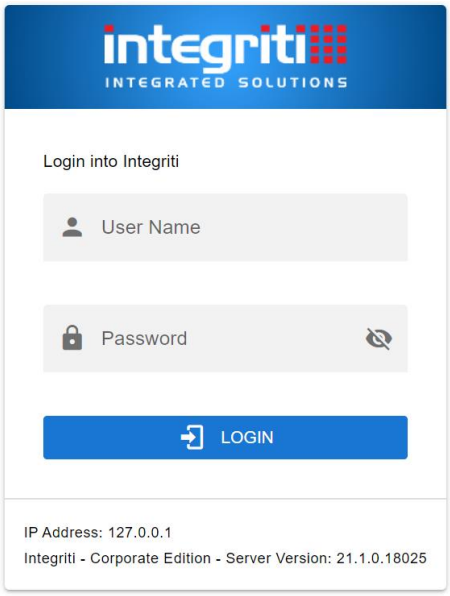
- **Schindler Lift HLI:** Resolved issue preventing the Schindler Lift Integration from working on older versions of the Schindler software (v1.2 or earlier). When integrating to Schindler v1.2, set the 'Schindler Version' property of the Schindler Communication Handler to 'v1.2 or older'.
- **Controller Creation:** Resolved issue that could result in not being able to create Controllers when logged in as an Operator using the default Operator Type.
- **Item History:** Resolved issue that could prevent closing the item history dialog without selecting an audit row first for some item types.
- **Operator Type Editor:** Resolved issue resulting in several properties of Operator Types not being editable.
- **Lift Access Granted Review:** Lift Access Granted Review Records are now correctly associated with the Lift Car the access was granted at rather than a potentially incorrect Lift Floor.
- **Entity List:** Removed duplicate columns from several entity lists
- **User List:** Filtering on a User's Primary Permission Group in the auto-filter row now works with partial matches using a string contains, rather than requiring an exact match.

VERSION 21.1

July 2021 - 21.1

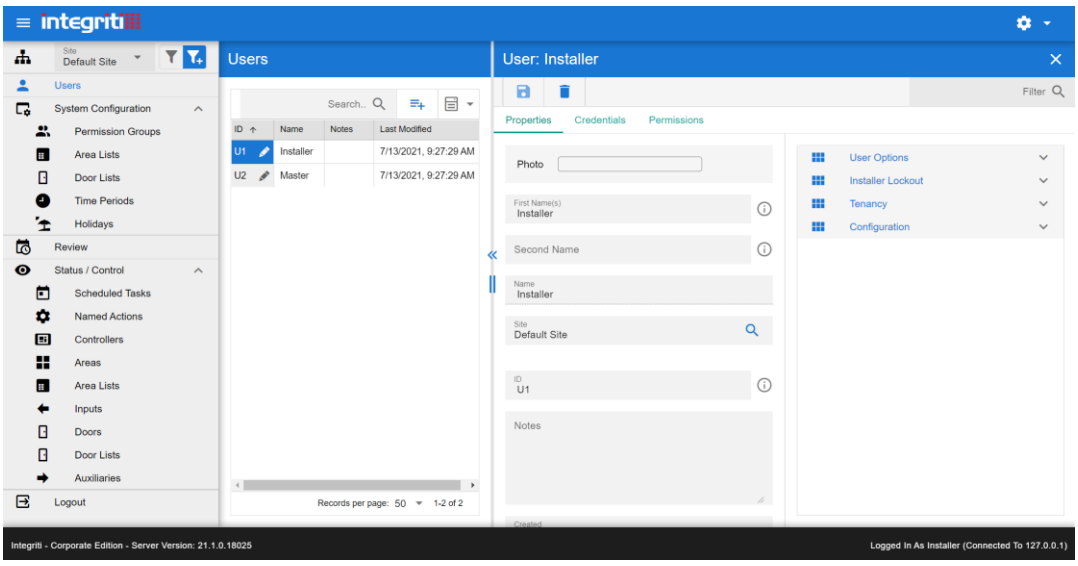
Improved Web Interface

Integriti's web interface has been redesigned from the ground up, providing a more usable and modern interface. The improved web interface retains the existing functionality from the previous web interface, with a number of general improvements and a completely redesigned interface.

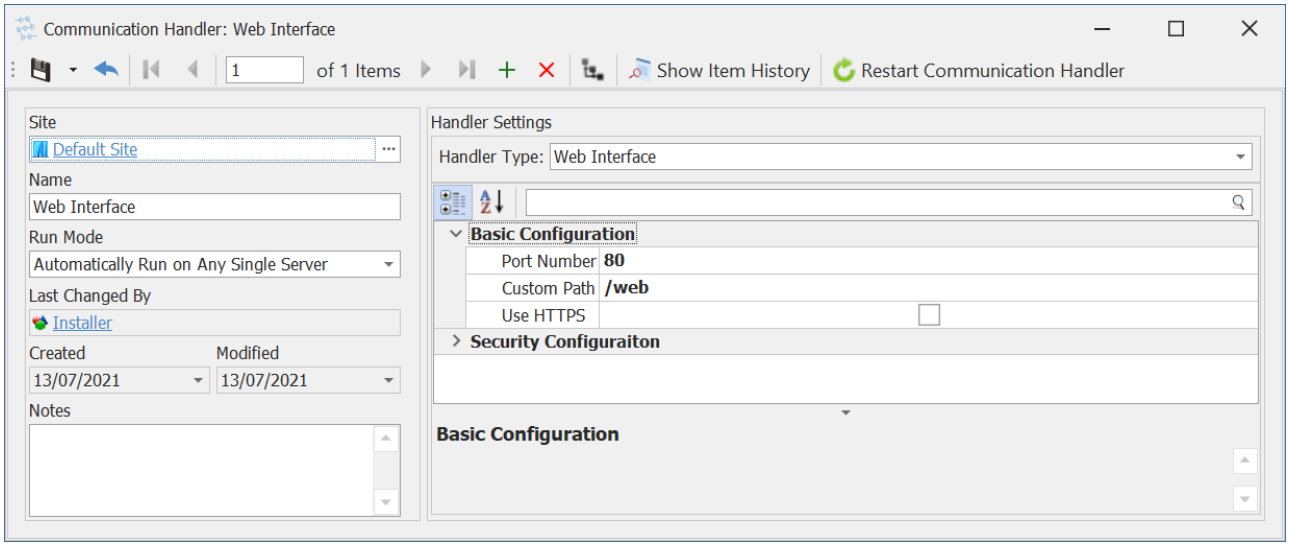


©2021 Integriti by Inner Range

Upgrading systems with existing web interface configurations will automatically be migrated to the improved web interface with no additional configuration being required. Clients will be able to access the new web interface from the same URL and with the same login details as those used for the old web interface.



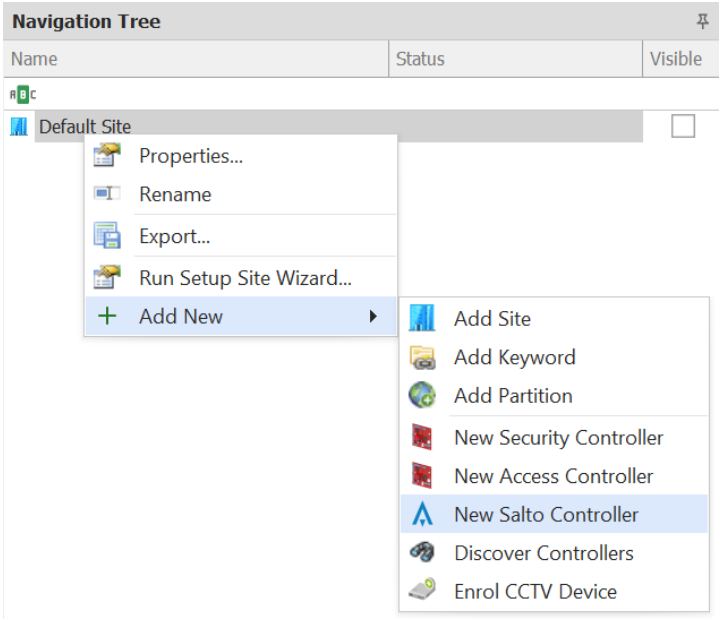
All previous configuration options are still available for configuring the improved web interface. In addition to existing configuration options, it is now possible to optionally configure a prefix for the web interface. This allows the URL used to navigate to the web interface to be configured, allowing multiple services to run on the same port (with different prefixes).



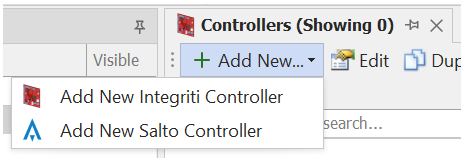
Licensing requirements for the improved web interface haven't changed from the existing web interface, still requiring Integriti Business or Corporate edition and at least one available client seat per web interface connection.

Third Party Doors

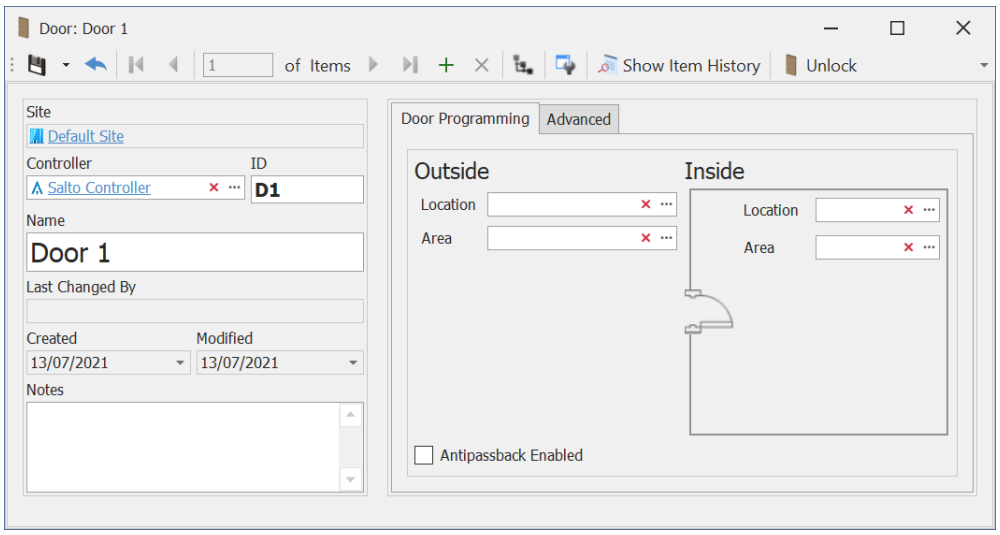
Integriti's architecture for integrating to 3rd party door systems has been completely redesigned to make doors from external systems fully built into the Integriti software. This makes configuration of all doors in the Integriti system follow the same flow, regardless of whether they are using Integriti or 3rd party hardware.



As with Integriti Doors, 3rd Party Doors can be created by adding a 3rd Party Controller (each individual integration has its own controller type), associating that 3rd Party Controller with an Integrated System tied to a 3rd party door system, then creating doors in that controller. All Doors created in a 3rd party controller will automatically be created as 3rd Party Doors for the system the 3rd Party Controller is referencing. This will create a Door in Integriti with properties directly mapped to the properties in the external system. This ensures that all properties shown will always be relevant to the 3rd party door system being used. With a 3rd party door integration correctly configured, doors will be automatically synchronised to the linked 3rd party door system as soon as they are added or changed in Integriti.



The updated 3rd Party Doors interface allows significant simplification of synchronising doors to 3rd party systems, with the only requirement being to create a door in a 3rd Party Controller. There is no longer a need to explicitly mark doors, door lists or any other Integriti objects as external doors by specifying a value in a custom field as on previous versions of Integriti. Integriti will now automatically determine which objects are relevant to the external system based on their association with a 3rd Party Door tied to the system (e.g. putting a 3rd Party Door in a Door List will result in that Door List being automatically synchronised to the 3rd party system containing all 3rd Party Doors in the Door List).

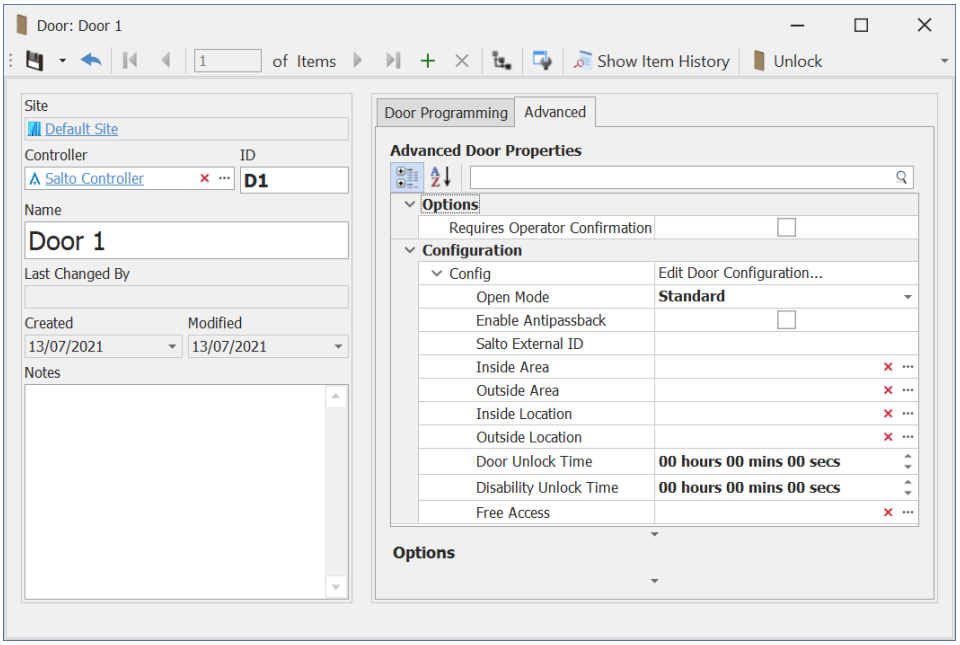


Each 3rd Party Controller type will automatically show up in the list of Controller types that can be created (both in the Navigation Tree and in the Controller List) based on the 3rd party door plugins currently installed on the Integriti system (must be installed on both the server and on the client). Systems with no 3rd party door integrations installed will only have the option to create Integriti Controllers, while systems using 3rd party door integrations will have the associated Controller type for the integration appear as an option to create.

Configuration of Integriti Doors has not been changed in this update, with the same process being in place for creating and editing Integriti Doors. That being said, the configuration properties of all Doors are now stored in a separate table in the database. This means configuration of objects such as Filters, Display Themes, etc will now require specifying door configuration properties via the Configuration property of the door. All existing configurations will continue to function as expected, however new configurations must use the new Configuration property to reference door configuration properties.

Licensing of 3rd party doors has not changed with the upgraded 3rd party doors interface. A system must have a 3rd Party Door license for each 3rd party door configured in the system. Unlicensed doors will not be synchronised to the 3rd party system. Integriti doors are still licensed separately through the Integriti Door license.

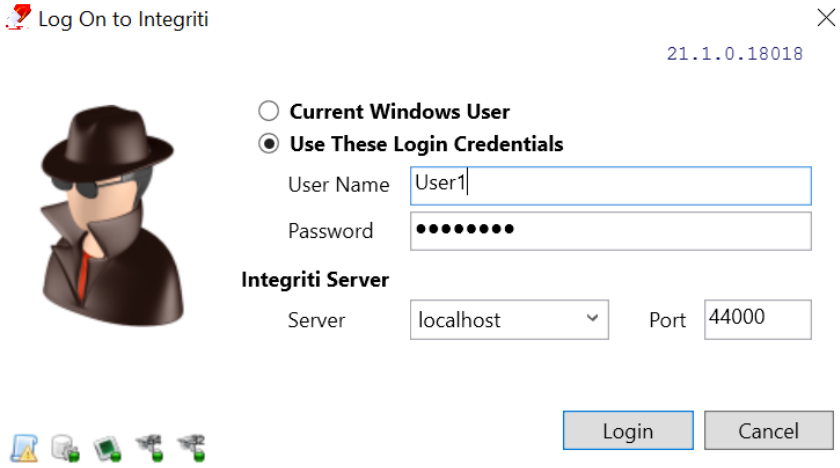
Currently the only 3rd party door integration that is supported is Salto. Note that the Salto v2.0 integration is required in order to use the new 3rd party door interface. Older versions of the Salto integration will continue to work on the new versions of Integriti, however Doors must be configured as on previous versions of Integriti until the integration is updated. As described above, Salto doors can be created by configuring a Salto Controller and creating Doors in that Controller. Once configured, Salto Entities will automatically be synchronised to the configured Salto server. See the Salto integration manual for more details on configuring the Salto integration.



Upgrading Integriti systems using the existing Salto integration can continue using the previous version of the Salto integration (<v2.0) on new versions of Integriti, however the integration will continue to function the same as on previous versions of Integriti and will not use the upgraded 3rd party doors interface. After upgrading the Salto integration to v2.0 or higher, the configuration of the integration can stay the same, however it will be necessary to manually import the Salto configuration back into Integriti in the new format. This can be achieved by performing an 'Import Doors', then an 'Import Users' command on the Integrated System through the Invoke Command mechanism. This will automatically pull door and user configuration from Salto into Integriti and create the relevant Salto Controller and Salto Doors, and ensure permissions are correct for all Users in the Salto system.

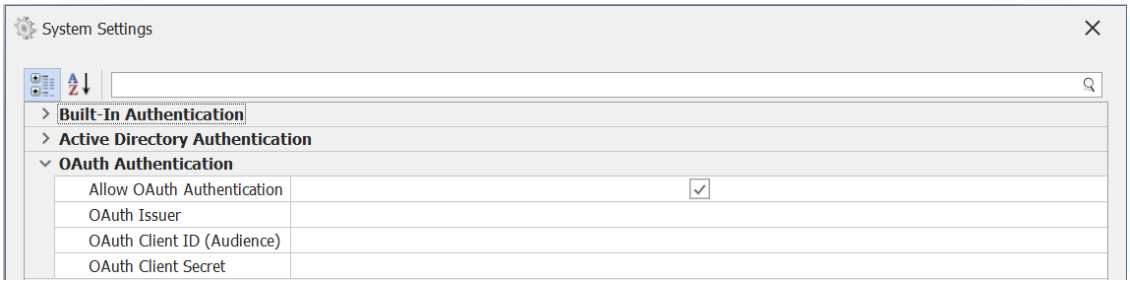
OAuth Authentication Module

Integriti's new Operator authentication module provides an additional mechanism for authenticating Operators logging into the Integriti system, in addition to the existing built-in and Active Directory authentication modules. Similar to the Active Directory authentication module, the OAuth authentication module allows authentication of Operators through a central external system, allowing credential management to be centralised across multiple separate systems. This both reduces ongoing Integriti configurations, and simplifies the login process for Operators, allowing them to use the same password for all systems authenticating against the OAuth system. Operator credentials are both stored and managed in the external OAuth system, with changes made to Operator passwords in the OAuth system being automatically applied for Integriti logins.

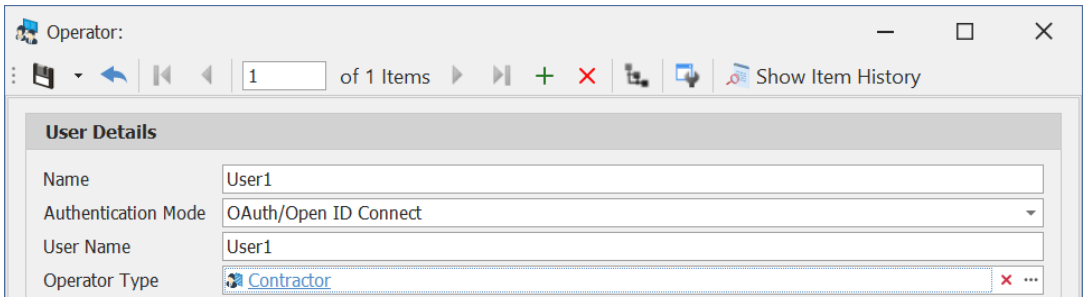


The OAuth authentication module adds support for authenticating against any OAuth comapatible authentication system that supports the 'Password' grant type. The authentication module has been explicitly tested against both Microsoft Azure Enterprise and Okta, however any OAuth system that supports the OAuth Password grant type should be supported.

OAuth authentication can be configured by Allowing OAuth Authentication and entering the configuration of the OAuth system into the Integriti system's System Settings.



Once enabled, Operators must be created and configured for each OAuth user to log into the system. OAuth operators should have their Authentication Mode set to OAuth, and their Username set to the Operator's username from the OAuth system. Once configured, the Operator is able to log into Integriti through the Integriti login dialog using the current username and password from the OAuth system.

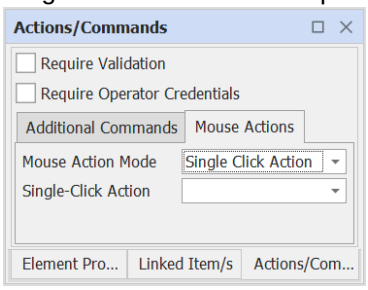


Integration Compatibility

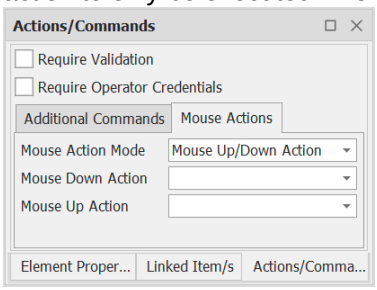
- Geutebruck GCore CCTV v3.1 or higher is required for Integriti v21.1 onwards
- Panasonic Video Insight CCTV v1.1 or higher is required for Integriti v21.1 onwards
- Tattile CCTV v1.2 or higher is required for Integriti v21.1 onwards

Improvements

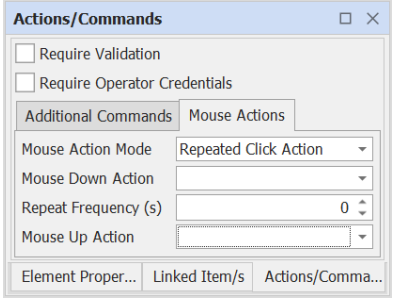
- **Schematics:** Improved mouse action functionality on Schematic elements to support mouse up/mouse down and repeated mouse actions as well as the existing single-click actions.
  - Single-Click Actions: The specified action is executed after clicking on the element.



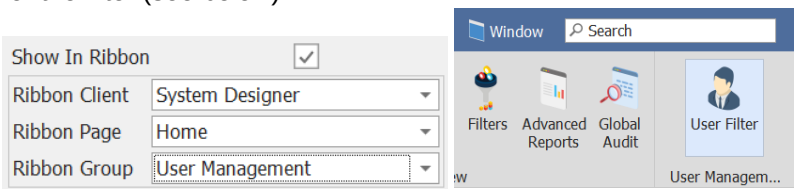
  - Mouse Up/Mouse Down Actions: Separate actions can be configured for when the mouse is pressed and when it is released. The mouse down action will be executed when the mouse is pressed on the element, and the mouse up action will be executed when the mouse is released. This allows for 2 separate actions to be configured for a single click on an element, with it being possible to hold the mouse down to delay execution of the mouse up action.
    It is also possible to only configure one of the mouse up/mouse down actions, allowing for an action to only be executed when the mouse is either pressed or released.



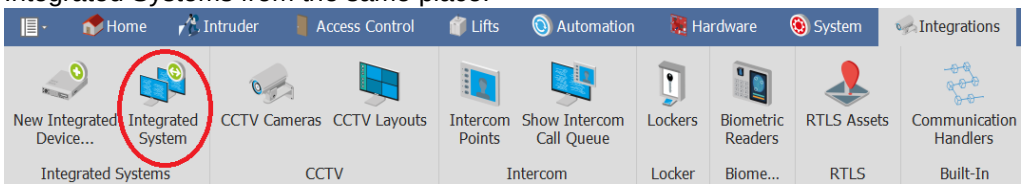
  - Repeated Mouse Actions: Repeated mouse actions function the same as Mouse Up/Mouse Down actions, with the key difference being that the mouse down action will be repeated at the frequency specified in 'Repeat Frequency' until the mouse is released (and the mouse up action is optionally executed).
    This allows for an action to be executed for the duration of the mouse being down, with the action stopping once the mouse is released. This can be configured as a timed controller action that will be retriggered (extending the action end time) until the mouse is released. If the connection to the server is lost while executing the action, this configuration will allow for the action to automatically stop after the configured time in the controller action.



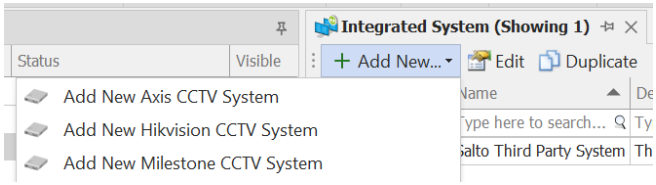
- **DB Filters:** Filters can now be configured to be shown in the System Designer or GateKeeper ribbon. This allows for pre-defined filters to be made more accessible to users, with direct access to the filtered list being available from the ribbon. This is supported by all types of filters and is enabled from the editor for the filter (see below).



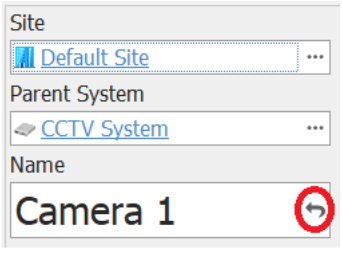
- **Integrated Devices:** Integrated Systems (CCTV Systems, Intercom Systems, etc) are now all accessed from the same ribbon button from System Designer and GateKeeper to allow configuration of all Integrated Systems from the same place.



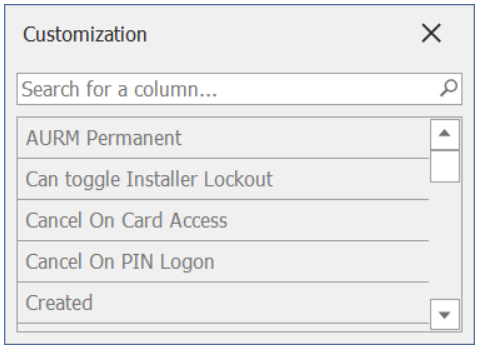
- **Integrated Devices:** Integrated Devices can now be added directly from the Integrated Device List using the Add New button. For systems with only one integration of that type installed an Integrated Device will be automatically created for that integration. For systems with multiple integrations for a type installed, the desired integration can be selected from the dropdown that appears after selecting the Add New button.
  Integrated Devices can still be added through the New Integrated Device button on the ribbon for all integration types, allowing adding of Integrated Devices by integration rather than by Integrated Device.
  NOTE: Integrations will only show up in the list of Add New options if installed on both the client and the server.



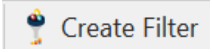
- **Integrated Devices:** Added support for duplicating Integrated Devices from the Integrated Device lists. This allows an existing Integrated Device's configuration to be used as a base point when configuring new Integrated Devices.
- **Integrated Device:** The Unlock Door command will now work on all Integrated Device Endpoints (Cameras, KeyLockers, etc) as well as Intercom Points. This allows all Doors associated with an Integrated Device to be unlocked directly from the device's context menu.
- **Integrated Device:** Added support for customizing the name of Integrated Devices in Integriti without the overridden names being trampled when refreshing the device from the external system. Refreshing the device will keep track of the name from the external system, but will only update the name of the device if a custom name isn't being used. This allows full customization of the name of devices in Integriti, while providing the option to reset the name to the default value from the 3rd party system from the integrated device editor if required.



- **Integrated Devices:** When creating Integrated Devices with connections directly to the endpoint (Cameras, Intercom Points, etc) a parent Integrated System will be automatically created for the new device. This allows common settings, such as the event monitoring options, to be configured from a central point, rather than individually for all endpoints.
- **Integrated Devices:** Newly created Integrated Devices will now be placed into the currently selected site in the Navigation Tree rather than the top-level site, simplifying configuration of Integrated Devices to ensure they are created in the most relevant site.
- **Integrated Devices:** Simplified configuration of which Integration server (32 or 64 bit) the Integrated Device will run on. This is now specified by simply selecting the Associated Server of the Integrated Device. For HA systems, devices will only fall back to servers of the same type as the one specified.
- **CCTV Viewer:** Viewing CCTV footage for devices that don't support playing back archived footage will now result in the playback controls being disabled to make it clear that playback is not supported. If any of the devices being viewed support playback of archived footage, the playback controls will be enabled to allow control of that device.
- **Custom Items:** Added 'Show On Map' command to context menu of Custom Item Instances. This allows Custom Items to be shown on a map either where they are placed on a Schematic Map or via the positions of the Custom Items.
- **Application Theme:** Customisations made to the application's theme no longer require the logged in Operator to have permission to edit Operators for the changes to be persisted between logins. The application theme will be saved on closing the application and reloaded the next time the Operator logs in.
- **Application Theme:** Added the option to specify the default Application Theme for a given Operator Type. This is the application theme that will be used for all Operators of this Type logging into Integriti when they don't have an Application Theme already saved or when customization of the Application Theme is disabled in their Operator Type.
- **Application Theme:** Added support for disabling customization of the Application Theme to Operator Types. Operators of this type will always use the default Application Theme specified in their Operator Type.
- **Entity List:** The column chooser for entity lists now has a search bar to assist in finding columns to show in the list.

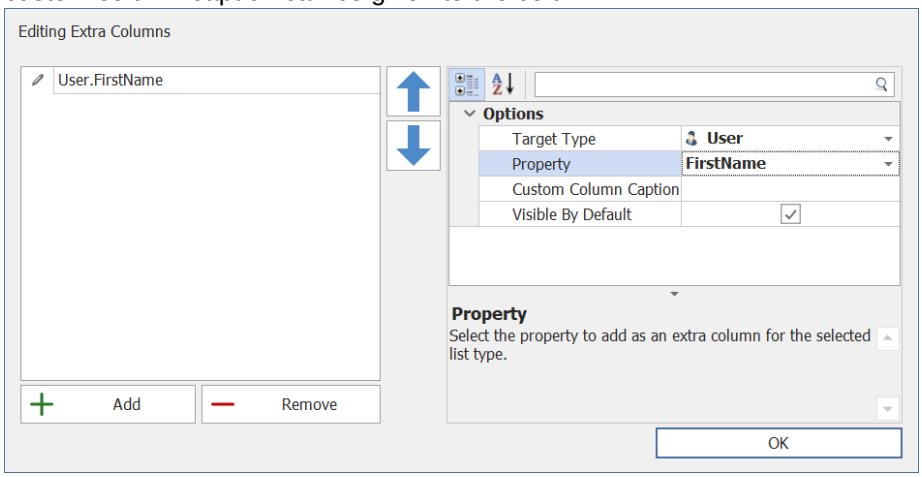


- **Entity List:** Filters can now be created directly from Entity Lists, pulling the currently applied column filter on the list into a Filter that can be accessed at any point.

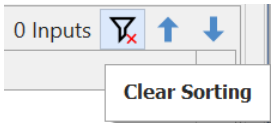


- **Entity Lists:** Additional columns can now be configured for complex columns in entity lists, allowing additional information that isn't visible from the list by default to be conveniently viewed. Additional columns can be configured system-wide from the 'Extra Columns' property of the System Settings. Extra columns can be added for any type in the system by specifying th Type and Property Name of the property to add. Optionally, the column can be configured as visible by default for new systems, and a

custom column caption can be given to the column.



- **Area Input List:** Added sorting of Area's Inputs list to allow associated Inputs to be sorted by the desired column. Sorting will disable changing the underlying order of the list until the sorting is cleared. This can be achieved by either clicking the 'Clear Sorting' button or using the column's context menu.



- **Entity Positions:** Added a 'Clear Positions' command to the Entity, Integrated Device, RTLS Asset and Custom Item Instance context menus. This allows positions added to entities (either from Schematics or an RTLS system) to be manually cleared when the position is no longer relevant. This prevents the associated position being used to show the object on schematic maps or for finding associated CCTV Cameras from camera FOVs.
- **Property Selector:** The property selector used for Filters, DBObjects and anywhere else that allows selection of properties has been upgraded to provide a tree of available properties. This allows complex properties that are multiple levels deep to be selected rather than only top-level properties, allowing more complex filters and display themes to be configured.
  NOTE: Creating more complex filters may have an impact on system performance. This should be kept in mind when configuring complex filters and display themes.
- **Controller Action Task Action:** Added support for the 'Use Entities From Context' option in Controller Action Task Actions for Lift Actions. This allows Lift Actions to be automatically executed on the Lift or Lift Floor that triggered the action.
- **Reports:** Added progress updates to loading screen when executing reports.
- **Web Browser:** Updated the web browser used for showing web pages in Integriti (through Control Workstation Task Actions, Response Plans and Challenge Responses) to use a Chromium based browser rather than an Internet Explorer based browser. This will provide a more modern and reliable browsing experience, as well as providing support for more modern webpages that weren't supported on the previous browser.
- **Web Browser:** Viewing web pages that require authentication will now show a pop-up allowing credentials to be entered for the page as they are required.
- **DevExpress Localisation:** Added the ability to log all DevExpress strings that require translation to a text file. This allows the strings that are translated as part of the DevExpress localisation process to be limited to only those that are being used by the specific system. This can be enabled by setting the 'CollectDevExpressLocalisationStrings' registry key to true prior to logging into System Designer or GateKeeper.
  NOTE: Strings will only be added to the localisation file as they are accessed by Integriti. If using the output of the DevExpress localisation process to determine which strings need to be translated, any strings that are not explicitly viewed in the software while generating the file will not be included in the

list of strings to localise. To ensure all DevExpress strings are translated, it is recommended to use a full DevExpress translation rather than relying on the output of this feature.

- **HID Cloud Credential:** Updated the default Invitation URL for new HID Cloud Credential Communication Handlers to the default invitation URL for the HID Origo portal. This will only be applied for new Communication Handlers, and can optionally be manually modified as required.
- **Schindler Lift HLI:** Added support for synchronizing the Phone Number/Email and Automatic Destination fields from an Integriti custom field to Schindler. This must be configured in the Schindler HLI settings by specifying the Custom Fields containing this data. Once configured, these fields will be automatically synchronized to the Schindler system.

Issues Resolved

- **Control Workstation Task Action:** Resolved issue resulting in Control Workstation Task Actions with the load layout option configured not correctly executing other aspects of the task action. This could result in actions with this configured not showing the specified cctv cameras and schematics when the action is executing.
- **Mimic Viewer:** Resolved issue that could result in an insufficient client licenses error being shown when connecting from a remote client.
- **CCTV Viewer:** Resolved issue that could result in duplicate video streams being shown in the resultant CCTV viewer when showing associated footage from an Entity or an Alert. This includes the context menu on these items, video shown using the control workstation task action and Alert Response Plans.
- **Response Plans:** Resolved issue that could result in settings from one element on a Response Plan being copied to the newly selected when changing the current selection to an item of the same type.
- **Review List:** Resolved issue that could result in the All Review list not opening when a Review Filter was already open in the layout.
- **Control Workstation Task Action:** No longer require the 'View' permission on Sounds for the 'Play Sound' option in the Control Workstation Task Action to be able to play a sound for an Operator.
- **Control Workstation Task Action:** Resolved issue that could result in the Control Workstation action being executed on all logged in workstations, rather than only for the Operators/Operator Types selected in the action configuration.
- **Entity Permissions Report:** Resolved potential error resulting in Entity Permissions Reports not successfully executing when a User filter was configured.
- **Partitioned Controller Connection:** Resolved potential error attempting to connect to partitioned Controllers on large systems.
- **Show Surrounding Cameras:** Fixed potential error shown when attempting to view surrounding cameras for a given camera.
- **Door Controller Syncing:** Resolved potential issue resulting in Doors being synchronising to Controllers without a Door type on systems using a 3rd Party Door Integration.
- **Alerts:** Resolved issue that could result in Alerts configured with a Hardware Offline Alert Source not honouring the specified site and module filters. This would cause the Alert to be triggered for all Hardware Offline events on the system, rather than only those it was configured to trigger on.
- **Control Workstation Task Action:** Resolved potential issue resulting in the action failing to execute when configured to automatically select the client to show on.

Documentation

- **Guide - Operator Authentication Modules:** Added manual describing configuration of Integriti's Operator Authentication Modules. This includes instructions on the use of the built-in and Active Directory authentication modules, as well as the newly added OAuth authentication module.
- **Integriti Integrations – 3rd Party Doors:** Added manual describing configuration of Integriti's 3rd party door integrations. This manual contains details on configuration that is common across all integrations, see the integration specific manual for specific details on configuring that integration.

Auto-Update Requirements

Integriti v21.1 has the following new pre-requisites that must be installed for parts of the software to function correctly. These will be automatically installed by all Integriti v21.1 installers, however will need to be installed manually on each client (if not already present on the system) for systems using the auto-update mechanism to automatically update Integriti client installations. The installers for these pre-requisites can be found in the Integriti installation directory of any PC that has run an Integriti v21.1 installer, or at the links below.

- Microsoft Visual C++ 2019 Redistributable (x86) (vcredist_x86_2019.exe): https://aka.ms/vs/16/release/vc_redist.x86.exe
- Microsoft Visual C++ 2019 Redistributable (x64) (vcredist_x64_2019.exe): https://aka.ms/vs/16/release/vc_redist.x64.exe

Rest/XML Interface

- **Door Queries** – The configuration options for Doors are now contained in a separate class under the Configuration property of the Door. Queries made on doors should reference configuration properties as Door.Configuration.<Property>. Doors returned from Integriti will also be returned in the new format, with Door configuration properties no longer accessible from the root level of the door in the XML. Existing queries using XML filters will continue to function as previously, however it is recommended to update the format of these queries to reference the new properties.

Bug-Fix Release (v 21.0.2)

June 2021 - 21.0.2

Improvements

- **Kone Access lift HLI:** Added support for custom card formats.

Issues Resolved

- **Integrations:** Resolved issue that could result in Refreshing Child Devices for an Integrated Devices failing in some circumstances.
- **Alert Definitions:** Resolved issue that could result in the Claim Timeout and Finalise Timeouts not being configurable.
- **Send Camera To PTZ Preset Task Action:** Resolved issue that could result in the selected Camera being lost after re-opening the Task Action editor.
- **Schematics:** The 'Show on Map' context menu command now works for Alerts and Review generated from an Integration.
- **Muster Point Mobile App:** Resolved potential error connecting new Mobile Devices to Integriti using the Inner Range Muster Point mobile application.
- **Schematics:** Resolved issue that could result in Commands on elements not successfully executing on Schematics using Fields of View in some circumstances. This includes both context menu commands and single-click actions.

Bug-Fix Release (v 21.0.1)

May 2021 - 21.0.1

Improvements

- **Alerts:** Added 'Clear Affected Entities' option to Alert Definitions. Alerts generated by Alert Definitions with this option enabled will only be associated with Entities retrieved from the Alert's latest trigger.
  Alerts with this configuration will only show the most up to date information from their associations, with the Alert no longer being associated with Entities not in the latest trigger. Showing associated CCTV will only show CCTV related to the latest triggering of the event, and only the latest entity/ies to trigger the Alert will show as having Alerts on a Schematic Map.
  Alerts with this option disabled will maintain the existing functionality of keeping the Alert associated with all of the Entities that have triggered it, allowing for all entities associated with the alert from when it was first created to maintain that association. Showing associated CCTV will show footage for all Entities that have triggered the Alert, and all Entities that have previously triggered the Alert will show as having Alerts on Schematic Maps until the Alert is finalized.
- **EkoTek RTLS Integration:** The EkoTek integration will now automatically ensure a User's associated Area/Location is up to date whenever an Alarm is received for that User. This ensures that even when a Location Changed message is missed from EkoTek, any Users with an active alarm will always be marked as being in the correct Area/Location.
- **Schematics:** Improved the time taken to load complex Schematic maps with large numbers of elements placed on them in both the Schematics Viewer and Schematics Editor.
- **Infiniti Mimic Viewer:** Added support for Infiniti Mimic Viewer.
- **Credential Management:** Attempting to re-activate a previously expired credential through the User editor will now show a notification that the selected credential already has an expiry, with the option to automatically remove the expiry from the credential.
- **Credential Management:** Attempting to set an expiry on a credential through the User editor will now prevent entering a start date that is later than the expiry date.
- **Mimic Viewer:** Added support for automatically playing a sound on a Mimic Viewer client through the use of the Control Workstation Task Action. This can be configured to automatically play a custom sound either at specified times or on an event being received.
- **Mobile Reader:** Activation and de-activation of Mobile Devices in System Designer is now achieved through the context menu of the Mobile Device. This removes the need to open the editor to change the state to the desired value, simplifying the Mobile Device enrolment process.
- **License Manager:** Added details on the license usage for Mobile Reader Device and 3rd Party Door licenses. This allows the number of available licenses for these licenses to be easily viewed directly from the License Manager.
- **Evidence Vault:** Evidence Items can now be accessed from GateKeeper. This allows a list of current Evidence Items' configuration and associations to be viewed, and the associated evidence to be opened directly from GateKeeper.
- **Control Workstation Task Action:** Showing video in the default viewer using a Control Workstation Task Action will now always result in only video streams from the cameras specified by the Control Workstation Task Action being shown in the viewer. This ensures that only relevant footage is shown, rather than including extra video streams from additional cameras that were already showing in the CCTV viewer.

Issues Resolved

- **Filters:** Resolved issue resulting in changes made to the columns of entity lists shown when viewing a filter not being saved. Changes made to these columns will now be saved for the specific filter being viewed, allowing individual customisation of columns on a per-filter basis.
- **RTLS:** Review generated for Location Changes from RTLS systems now shows the associated Area/Location's name rather than address in the Review's text.
- **Controller Action Task Action:** The Set User Area Controller Action now supports automatically selecting the User or Area/Location to use for the action based on the context of the trigger through the 'Get Entities From Context' option. This allows for much more flexible actions to be configured, automatically selecting the relevant Entity rather than requiring manual configuration of each Entity in the action.
- **Custom Item Changed Trigger:** Resolved issue resulting in the Custom Item Changed trigger's filter not showing the correct properties for the configured Custom Items.
- **Intercom Integrations:** Resolved issue resulting in the 'Unlock Associated Door' and 'Lock Associated Door' context menu commands for Intercom Points not working.
- **Integration Persisted Connection:** Selecting a Persisted Connection Run Mode of 'Simultaneously Maintain Connection on All Servers' will now only run the persisted connection on one of the 32 or 64 bit servers rather than on both. This ensures the persisted connection is not unnecessarily running on multiple servers on the same PC, and instead will only run an all HA servers of the configured processor type (32 or 64 bit).
- **Integration Persisted Connection (HA):** Refreshing Child Devices or Refreshing Device on an Integrated Device with a Persisted Connection Run Mode of 'Simultaneously Maintain Connection on All Servers' will now restart the persisted connection on all servers the persisted connection is running on, rather than only the server the Refresh Child Devices/Refresh Device command is executed on.
- **License Manager:** Integriti Door license usage no longer includes configured 3rd Party Doors. This ensures that the license usage now correctly shows the total number of remaining Integriti Door licenses for systems using 3rd Party Doors.
- **REST XML Interface:** Resolved issue that could result in the results of Review queries not being sorted correctly.

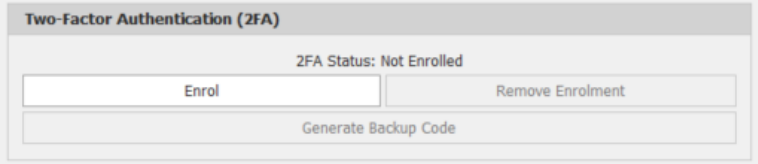
VERSION 21.0

March 2021 - 21.0

Two-Factor Authentication (2FA) Login

Integriti now supports 2FA for additional security on operator login, requiring the operator to enter an additional time-based six-digit code from their smartphone or personal device. Operators can also generate an emergency backup code to login with in the event that they have lost access to their personal device.

- 2FA login is supported for System Designer, Gatekeeper, and the Integriti web interface, and is compatible with Active Directory Integration & SSO.
- To enable 2FA login, tick the "Configuration -> Enable Two-Factor Authentication Login" checkbox in System Settings. Operators can be enrolled for 2FA individually from the Operator Edit dialog.
- 2FA can be enforced for certain operators by enabling the "Enforce Two-Factor Authentication" option in their Security Policy. Affected operators will be prompted to register for 2FA the next time they log into Integriti if they are not already registered.

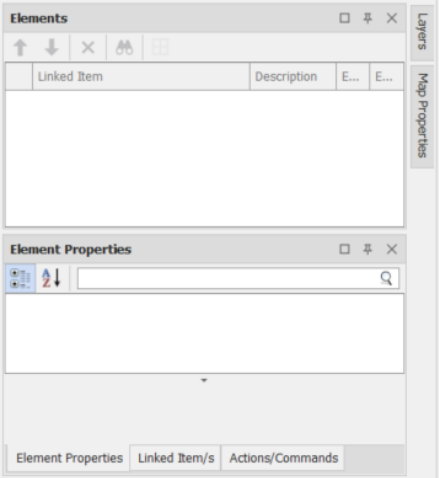


For more detailed information on how to configure 2FA operator login, see the ‘Guide - Two Factor Authentication’ configuration guide.

Schematics

Dockable Property Windows

The Schematics editor’s property windows are now able to be docked in any position on the screen. This allows full customisation of the key aspects of the Schematics editor UI, including which panels are visible, tabbed or auto-hiding. Panels can either be docked to any side of the Schematics editor or as floating panels, able to be placed anywhere on the screen.



The layout of the editor's property windows will automatically be saved upon closing the Schematics editor, and will be restored automatically when the Schematics editor is opened.

The following property windows now support docking in the Schematic editor:

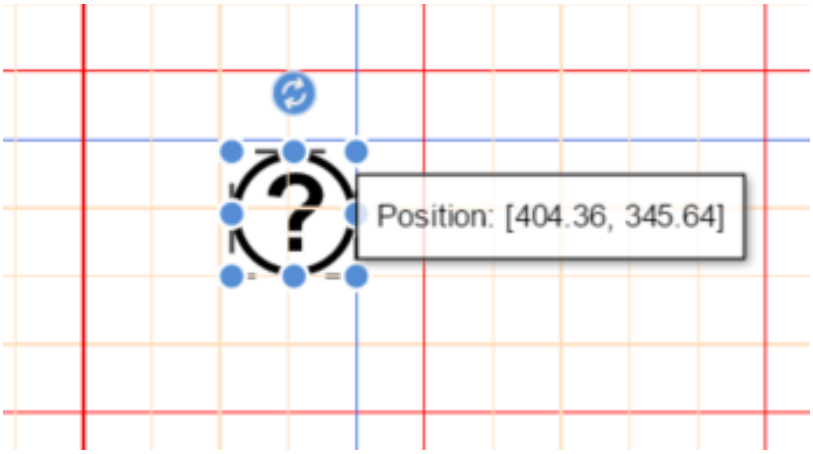
- Element List
- Element Properties
- Element Linked Items
- Element Actions and Commands
- Map Properties
- Layers List

Grid Overlay

The Schematics editor's Grid Overlay now supports customisation of the lines on the grid, including Major Grid Lines, Minor Grid Lines and the Snap/Selection Line. Existing functionality, including customising the Width and Height of each Grid Block remains the same.

To assist with positioning elements, Snap to Grid can now be enabled along with the grid overlay. This allows for elements to automatically snap to the nearest grid line whenever they are being added or edited. This includes when moving, resizing and rotating elements, as well as modifying control points for line and polygon-based elements.

Along with the above improvements, enabling the grid overlay for a Schematic will now only enable it in the editor, with the viewer no longer showing the grid overlay. This allows the grid overlay to be permanently left on for Schematics that should be edited with a grid overlay, no longer requiring the option to be disabled after finishing editing the Schematic to prevent it appearing in the viewer.



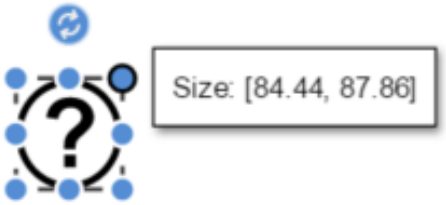
Undo/Redo Functionality

The undo and redo functionality in the Schematics editor has been expanded to cover all changes made in the editor. This includes any changes made to Element, Map or Layer properties in the Schematics editor, as well as any physical changes made to elements (adding, removing, moving, resizing, etc).

Inserting/Editing Schematic Elements

A number of improvements have been made to the Schematics editor's interface for adding and editing elements on a Schematic. These include, but are not limited to:

- **Editor Tooltips**: When moving, resizing and rotating elements, a tooltip is now shown providing details on the current size, position or rotation of the element, allowing for easier fine-tuned editing.



- **Freeform Shapes**: New points can now be added to freeform shape elements by simply clicking and dragging the corresponding green control point to the desired location of the new point, it is no longer necessary to hold additional keys or use a context menu to achieve this functionality.



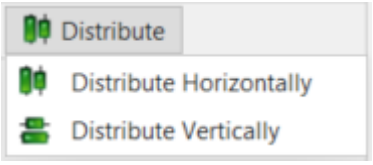
- **Freeform Shapes**: Double clicking when drawing a freeform shape element now adds a final point at the double-click position before completing editing of the shape. The previous behaviour of completing editing at the most recently added point can be achieved by pressing the escape key.
- **Rounded Rectangle Elements**: Rectangle elements can now configured to have rounded corners. This can be configured by setting the 'Rounded Corner' property of a rectangle element to specify the radius of the curve.



- **Element Rotation**: Elements are now rotated 15 degress at a time by default to assist in keeping element rotation consistent across elements. For more fine-tuned rotation control, the shift key can be held while rotating an element to rotate 1 degree at a time.

Element Distribution

New element distribution options have been added to automatically distribute all selected elements either vertically or horizontally. This will automatically evenly distribute all of the (2 or more) selected elements, ensuring even spacing between each element is even across the specified direction, ignoring grid snapping.



Element Tooltips

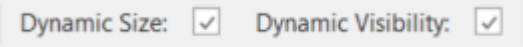
Element tooltips in both the editor and viewer have been improved to increase usability, and ensure they don't get in the way of other elements. Tooltips no longer show up immediately, instead waiting until the mouse has hovered over an element for a reasonable amount of time, and will remain at the position they were originally shown rather than following the mouse cursor. Tooltips will automatically disappear once the cursor moves away from the tooltip.

To allow for finer control of tooltips in both the editor and viewer, a new option has been added to allow tooltip visibility to be customised. This provides options for tooltips to be shown for all elements, only the selected element or to not be shown at all.



Dynamic Size/Visibility

To assist in editing Schematics containing elements with dynamic visibility or dynamic sizing, it is now possible to temporarily disable this functionality in the editor while configuring these elements. This can assist in editing elements where the dynamic sizing or visibility is resulting in an element being obscured or difficult to access.



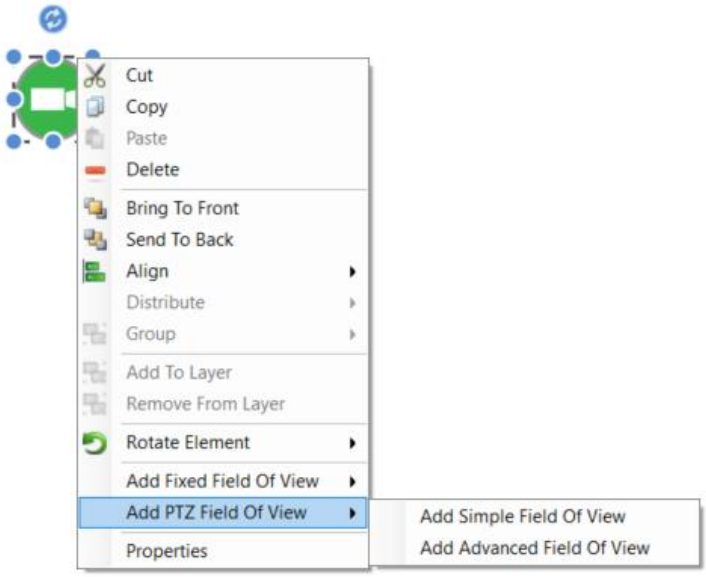
Entity Positions

Entity positions for all elements on a Schematic are now automatically added/updated whenever that Schematic is saved. The 'Auto-Allocate Positions' button has been removed, with the auto-allocate positions functionality being applied without requiring any specific user input. This ensures Entity positions are always kept up to date with changes made in a Schematic, removing the need to manually trigger an update.

Camera Fields of View

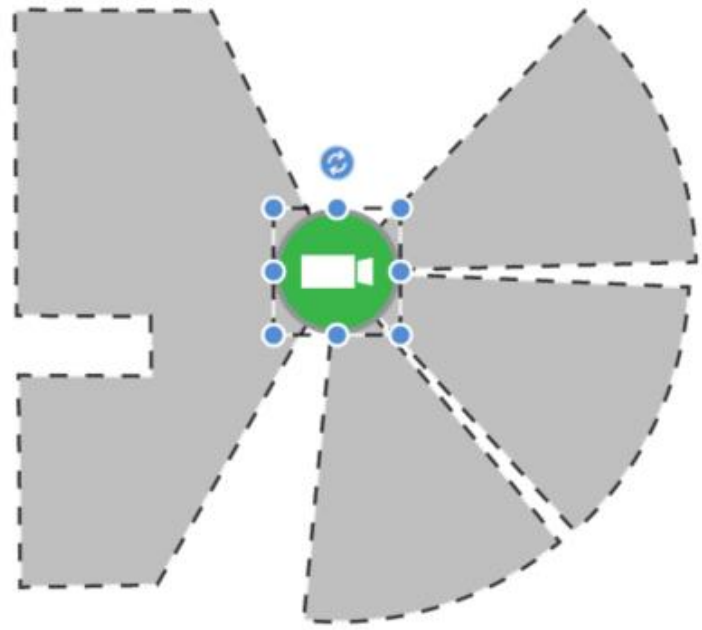
The fields of view (FOV) for Integrated Devices placed on Schematics can now be configured directly from the Schematics editor. This allows for the viewport of all cameras placed on Schematics to be visualised directly from the Schematic. FOVs can be viewed from both the Schematics editor and viewer, with FOVs for any currently selected Integrated Device being shown. Optionally, all FOVs can be shown at the same time to allow viewing of the full CCTV coverage for a Schematic, or all FOVs can be manually hidden to ensure all important information remains visible.

FOVs can be added for any element on a Schematic representing an Integrated Device by simply right-clicking on the element and selecting 'Add Fixed FOV' or 'Add PTZ FOV', then choosing from 'Simple FOV' or 'Advanced FOV'.
A **Fixed FOV** represents a single static view for a camera, intended for non-PTZ cameras that only have a single possible FOV. Only a single Fixed FOV is able to be configured per Integrated Device.
A **PTZ FOV** allows the viewport of a specific PTZ Preset on a PTZ enabled Integrated Device to be visualised. Configuring a PTZ Field of View allows for a PTZ Preset ID to be configured for the FOV, which can then be used to automatically send a camera to the specified PTZ Preset when viewing video associated with the PTZ FOV. PTZ FOVs are not limited in the number that can be configured.
Simple FOVs allow for a FOV to be configured as a sector of a circle around the Integrated Device element. The radius and depth of a simple FOV can be configured, however the shape is always the same.
Advanced FOVS allows an FOV to be configured as a freeform shape, allowing full customisation of the area covered by a FOV, including blindspots, walls and any other factors that effect the FOV.



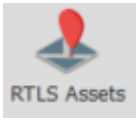
Once FOVs are configured for an Integrated Device on a Schematic they will be automatically used to calculate Entities associated with that Integrated Device (See '**Integrated Device Entity Associations-Entity Association Programming**' for more details), as well as allow associated Integrated Devices and PTZ Presets to be retrieved for a given point on a Schematic.

FOVs will also be used when showing video from a Schematic. Showing video from the context menu of an Integrated Device's PTZ FOV will automatically send the selected Integrated Device to the PTZ Preset configured in the PTZ FOV, ensuring the Integrated Device is pointing in the correct direction when the video stream is shown.
On top of this, a new option has been added to the context menu when right clicking anywhere on a Schematic to 'Show CCTV at Point'. This option will automatically retrieve all Integrated Devices with a FOV covering the point the context menu was shown at, and show video for all Integrated Devices with a view of that point. For PTZ FOVs covering the selected point, all cameras will also be sent to the PTZ Preset configured in the PTZ FOV.



RTLS Assets

RTLS integrations are now able to create 'RTLS Assets' associated with an RTLS Tag in the RTLS System. RTLS Assets hold the corresponding position data for the RTLS tag, as well as details of the Asset they represent, getting updated by the integration as it receives position changes from the 3rd party system.



RTLS Assets can either be standalone objects representing physical objects (such as equipment trolleys or other physical assets) or associated with a User to represent the position of that User in the RTLS system. When associated with a User, position changes on the RTLS Asset will be passed on to the associated User, ensuring the User always has the correct position based on their associated tag in the RTLS system.
RTLS Assets can also be assigned an Asset Type to assist in sorting and filtering Assets. This can either be one of several pre-defined values or a manually entered value.

Position changes on an RTLS Asset will automatically update the associated Area/Location of the RTLS Asset (and the Associated User if there is one) based on the Area/Location the RTLS Asset is physically in, allowing reports, associated CCTV and other features using the associated Area/Location to be used.

Where Fields of View are configured, retrieving associated integrated devices for an RTLS Asset will also retrieve all Integrated Devices with a Field of View covering the current position of the RTLS Asset. This allows Integrated Devices from other Areas/Locations that have a view of the RTLS Asset's current position to be included, and will restrict Integrated Devices retrieved through the Asset/User's Area/Location to only include the Integrated Devices that can physically see the current position of the RTLS Asset, ensuring only the most relevant CCTV streams are shown.

When an Alert is active on an RTLS Asset (triggered from an event from an RTLS integration) or a User associated with an RTLS Asset, the current position of an RTLS Asset can be used to show the current position of the Alert on a corresponding Schematic Map. This allows Users and RTLS Assets to be tracked live in the system whenever there is an Alert associated with them, until the Alert is successfully finalised.

Integrated Device Entity Associations

Entity Association Programming

Programming of Integrated Devices Associated Entities has been simplified to allow associations to be automatically calculated directly from the elements on a Schematic. This uses the physical location of the Integrated Device on the Schematic to automatically associate all of the Areas and Locations a device is within the bounds of with that device. For systems with FOVs configured in their Schematics all Entities located inside of a device's FOVs will be also be recognised as associations for that device. Integrated Device Entity Associations will automatically be added, removed and have their associated PTZ Preset ID updated for all Integrated Devices on a Schematic whenever that Schematic is saved, ensuring associations are always kept up to date.

If finer control of Entity associations is required, associations can be configured from the Entity Associations tab of the Integrated Device editor. Associations configured prior to updating and associations manually added through the Integrated Device editor will not be updated or removed by Schematics, and can only be modified from the Integrated Device Editor.

Associated PTZ Preset

Integrated Device Entity Associations now have the option to specify an associated PTZ Preset ID for that association. This will be used to automatically send the camera to the specified PTZ Preset when showing video from that associated Entity. This allows a system to be configured to automatically move a camera to be facing the Entity triggering an event when showing live CCTV for that event.

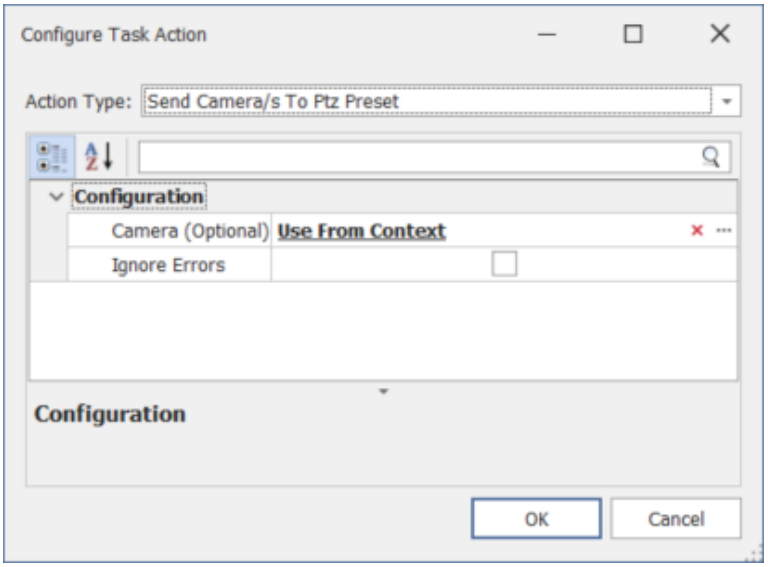
For manually configured associations, the associated PTZ Preset ID can be manually entered in the Integrated Device editor's Associated Entities tab. For associations added automatically through Schematics, the associated PTZ Preset IDs will be automatically set to match the PTZ Preset ID of the PTZ FOV the entity is inside of for that Device. Where the Entity association is added due to the Integrated Device being within the bounds of an Area/Location or the associated Entity is inside a fixed FOV for an Integrated Device, no PTZ Preset will be set on the association.

Cameras will be automatically sent to the associated PTZ Preset (where programmed) when viewing live CCTV footage from an association. This includes showing video directly from an Entity, from Review, from Alerts and through the Control Workstation Task Action, as well as anywhere else that shows video from an Integrated Device's associated entities.

Send Camera To PTZ Preset Task Action

For situations where a camera should be automatically sent to a PTZ Preset without showing a live video feed in Integriti, the Send Camera to PTZ Preset Task Action has been added. This can be configured in one of two ways:

- Manual Configuration: Manually specify a Camera and the ID of a PTZ Preset in order to send the selected camera to the specified PTZ Preset when the Task Action is triggered.
- Select From Context: Leave the 'Camera' property blank to automatically select the Camera/s and associated PTZ Preset/s from the context of the triggering event/alert. This option will automatically sends all cameras associated with the Entities that triggered the event/alert to the PTZ Presets configured in the corresponding association/s.



RTLS

For systems using position-based RTLS integrations (that update the x, y, z coordinates of a User or RTLS Asset), finding Integrated Devices associated with the User/RTLS Asset has been significantly improved for systems with FOVs configured in their Schematics, using the FOVs to determine exactly which Integrated Devices have a view of the exact position of the User/RTLS Asset.

On systems with FOVs configured for Integrated Devices retrieving associated Integrated Devices for a User or RTLS Asset will now automatically retrieve all Integrated Devices which have a FOV covering the x, y, z position of the User/RTLS Asset, allowing only relevant Devices to retrieved.
For systems without FOVs configured, or for systems not using Schematics at all, the existing behaviour of using all Integrated Devices associated with the User/RTLS Asset's associated Area/Location will be used.
For systems with FOVs only configured on some of their Integrated Devices, the resulting associated Integrated Devices for a User/RTLS Asset will be a combination of all Integrated Devices with a FOV covering the x, y, z position of the User/RTLS Asset, as well as all Integrated Devices inside of the User/RTLS Asset's associated Area/Location without a FOV configured.

This improved functionality will automatically be applied when retrieving associated devices for a User or RTLS Asset, both for showing associated CCTV Footage (e.g. from Review, Alerts, Entity Lists or the Control Workstation Task Action) and when determing associated devices from the context of the triggering event (such as Invoke Integrated Device Command Task Action and Send Camera To PTZ Preset Task Action).

Review Categories

The following Review Categories have been added or modified in this release:

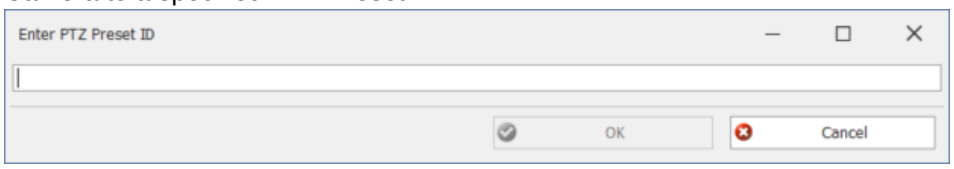
- (Area) Partially Armed
- Xmit Partially Armed
- RTLS Area/Location Change
- RTLS Button Input Change
- RTLS Battery Voltage Change
- RTLS Low Battery Alarm
- RTLS Low Battery Alarm Restore
- RTLS Tag Online
- RTLS Tag Offline
- RTLS Asset Start Movement
- RTLS Asset Stop Movement

Anywhere using a filter on Review Category should be reviewed to ensure these changes won't effect existing filters. Places Review Category filters can be found include:

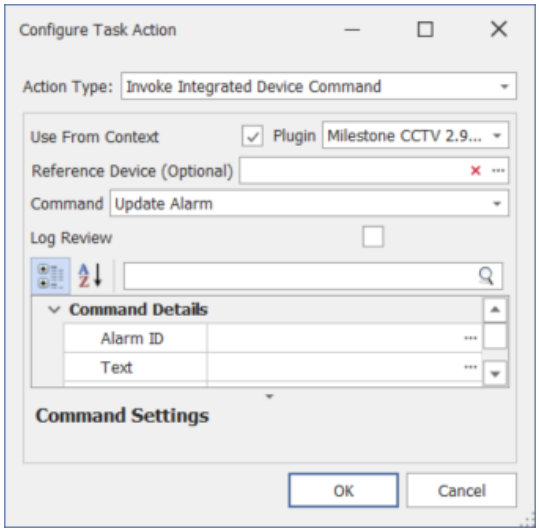
- Review Filters
- Operator Type Filters
- Scheduled Task Triggers
- Reports
- Saved Layouts

Improvements

- **Clickatell SMS Sender:** Added support for Clickatell's One API. Newly created Clickatell SMS Communication Handlers will be automatically created referencing Clickatell's One API. See the 'Integriti Communications Handlers – Clickatell SMS Sender' manual for details on configuring both Clickatell and Integriti to send SMS' via Clickatell's One API.
  Upgrading systems will continue using the previous Clickatell API, and will not require any configuration changes to continue working.
- **Integrations:** Added new Integrated Device types to better categorise new integrations. New integrations will automatically be given the correct Integrated Device type, while newly released integrations will be moved to the correct Integrated Device type (where applicable) after a plugin update.
- **Send Camera To PTZ Preset:** Added new Context Menu command to CCTV Camera to send the Camera to a specified PTZ Preset.

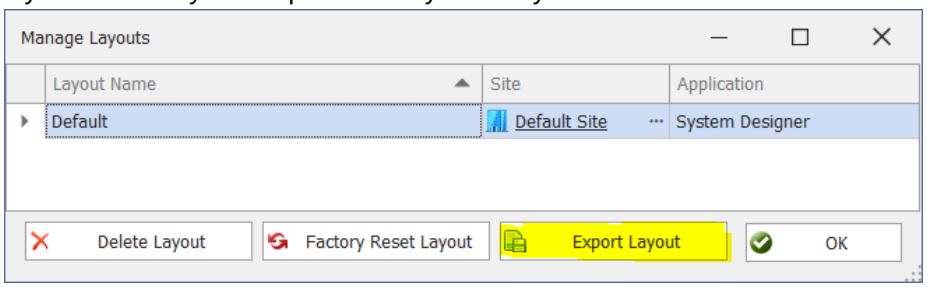


- **System Designer/GateKeeper Ribbon:** Moved buttons for all Integration types into a new Integrations tab in the System Designer and GateKeeper ribbon. In GateKeeper, only Buttons to show lists for each Integrated Device type will be shown in this tab where an integration of that type is currently installed. If no integrations of a specific Integrated Device type are installed, no button will be shown for that type in the Integrations tab on the ribbon.
- **Integrated Devices:** Integrated Devices can now be duplicated from an Integrated Device list to save having to enter similar configurations multiple times for each Integrated Device to be added.
- **Invoke Integrated Device Command Task Action:** Simplified configuration of the Invoke Integrated Device Command Task Action when using Integrated Devices from context by removing the need to specify a 'Reference Device' for most command types. When configured to load devices from context, for most commands, it is now only necessary to select which plugin should be used to execute the commands, before selecting and configuring the command itself.
  Some commands still require a 'Reference Device' to be specified in order to allow specific command details loaded from the 3rd party system to be shown. Selecting a command that requires a Reference Device to be selected will provide a notification indicating this requirement.

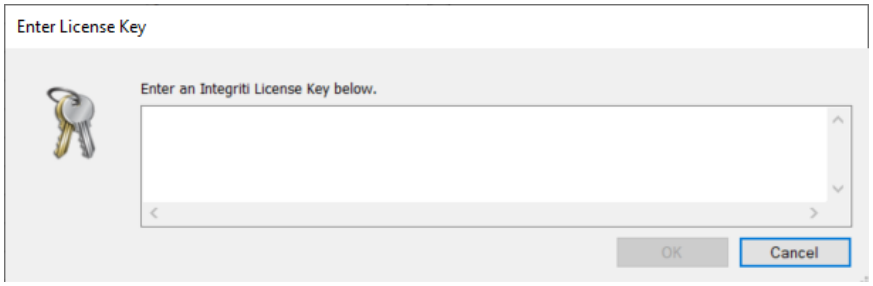


- **Task Actions:** Some Actions (configured in Scheduled Tasks, Alerts, etc.) now have the option to ignore errors occurring while executing the Action. If this option is enabled, the remaining configured Actions will continue to be executed, regardless of whether the Action fails to execute successfully.

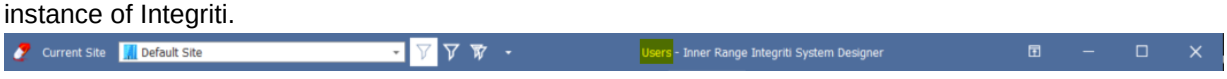
- **Log Review Task Action:** Added the ability to customise the Category of review generated by the Log Review Task Action. This can be one of 6 categories, allowing for simpler reporting and filtering of generated Review, as well as allowing custom colouring of the generated Review in the Review List to assist in distinguishing between Review generated from different sources.
- **Log Review Task Action:** Review generated by a Log Review Task Action will now be automatically associated with the Entities and Integrated Devices associated with the triggering event.
- **Personal/System Layouts:** Added the ability to export layouts from the Manage Layouts dialog. Exported Layouts can be imported back into Integriti through the 'Import Data' functionality. Imported layouts wil always be imported as System Layouts.



- **Entity Selection Dialog:** Improvements to the behaviour of the Site filter to further assist in filtering the entities to select from by their Site.
- **Schindler Card Codec:** Added Schindler Card Codec to default Entities. This can be used by creating a new 'Custom Software Codec' Card Format, with their 'Custom Enhancement Codec' referencing the Custom Enhancement 'Schindler Card Codec'.
- **License Manager:** Added support for entering multiple licenses at once. This allows license keys to be entered directly from the license details email.



- **Cleanup Database Task Action:** Added 'Days To Purge' option to allow the lower bound of the purge to be specified. This should be set to the maximum number of days the purge should occur over in order to improve the performance of the purge.
  The purge will cleanup items with a time anywhere between 'Purge Before (Days)' + 'Days To Purge' days before the action is executed and 'Purge Before (Days)' days before the action is executed.
- **Filters/Reports:** Filters and reports on Users, Doors and Areas are now able to select entity-specific properties from the User, Door and Area states, rather than only having access to the core state properties.
- **Title Bar:** Integriti's window title now contains details of which panel is currently selected in that instance of Integriti.



- **Icons:** Updated a number of icons across Integriti to improved, higher quality icons.
- **Permissions Report:** Added the option to 'Exclude Inactive Permissions' from a report's results. When enabled, expired and not started permissions will not be included in the report.
- **Schematics:** Improved drag-drop functionality to support dragging multiple entities from an Entity list onto an empty space on a Schematic Map. This will add all of the dragged entities as separate icons on the Schematic they are dropped onto.

- **User Associated Area/Location:** Changing a User's associated Area or Location will now automatically update the User's Position to that or the centre-point of the Area/Location. This allows Alerts associated with a User to be shown in Schematics, even when the current Area/Location isn't associated with the Alert and an RTLS system isn't being used. All Alerts associated with Users with positions updated in this way (as opposed to being updated through an RTLS system) will show up at the centre of the Area the User is currently in.
- **Mobile Reader:** Added support for manually moving Users into the Muster Area directly from the Mobile Reader application. This allows Users to be marked as being in the Muster Area even when they don't have their credentials on them.
  NOTE: The manual muster functionality requires an updated version of the Mobile Reader Application to be used.
- **Sample Reports:** Added First Badge of Day sample report to show the first user access and total access events for each day over a 2 month period.
- **Integriti CS:** Added support for configuring partitioned Controllers in Integriti CS. This can be done by creating a 'New Partitioned System' from the Integriti CS interface and enrolling the Controller into the auto-created Partition.

Issues Resolved

- **Keywords:** Resolved issue resulting in Entities not being added to Keywords when attempting to add from the Navigation Tree. This includes both dragging Entities onto the Keyword in the Navigation Tree and using the Edit Keyword Dialog to add Entities.
- **Controller Enrolment:** Controllers will now be enrolled into the Site specified in the Controller enrolment dialog, rather than always being enrolled into the top level site.
- **CSV Import:** Resolved potential issue that could result in blank Cards being associated with a User after a CSV import in some situations.

Documentation

- **Biometric Integrations:** Added manual describing the configuration and use of Biometric Integrations in Integriti.
- **RTLS Integrations:** Added manual describing the configuration and use of RTLS Integrations in Integriti.
- **Keylocker Integratons:** Improvements to KeyLocker manual to include details on configuring anti-passback for Keylocker integrations.
- **Integration Manuals:** Moved integration manuals to 'doc\Integrations'.
- **Schematics Editor:** Added new Schematics Editor Manual detailing use of the Integriti's Schematics editor. This supersedes the existing 'Integriti Software – Schematics' manual.

Bug-Fix Release (v 20.1.4)

February 2021 - 20.1.4

Improvements

- **Card Review (AURM):** AURM requests now support site code card numbers with leading zeros.
- **Door Schedules:** Changes to Door Schedules are now audited.
- **HID Mobile Credential:** Added support for HID's latest portal to ensure compatibility with newly created HID accounts. This option will be selected by default for new HID Mobile Credential Communication Handlers. Existing Communication Handlers can be updated to use the new portal if required by setting the HID Client Portal Version to 'Origo (2.2) – AWS IDP'.
  NOTE: Upgrading systems connecting to 'Cert' or 'Pre-Production' HID Portal environments will need to verify their HID Mobile Credential Communication Handler configuration after updating, and ensure the 'HID Client Portal Environment' property is set correctly.
- **HID Mobile Credential:** Added the option to manually specify the Invitation Link for systems using Email or SMS senders to send invitations. Upgrading systems will continue to use the previous default Invitation Link.

Issues Resolved

- **Card Review (AURM):** AURM requests no longer incorrectly alter the Review text to say 'Inactive Card'.
- **REST XML Interface:** Added support for self-closing ref elements in XML documents passed to the REST interface.
- **Module Editor Dashboard:** Resolved issue that resulted in changing the selected Controller in the Navigation Tree not updating the Dashboard to display the newly selected Controller when both Controllers were in the same Site.
- **Schematics:** Resolved issue resulting in the Status Text not showing in the status window for the selected element when 'Show Status on Mouse Hover' was disabled for that Schematic Map.
- **Licensing:** 'Additional Server Node (High Availability/Load Spreading)' now functions as described , with the **original** server not being included in the license count. The required number of licenses should match the total number of additional servers, not the number of servers in total.
- **Licensing:** Resolved an issue where doors managed by the Salto SHIP integration were incorrectly using Integriti Door licenses instead of 3rd Party Door Licenses. This could result in sites being unable to create more Integriti doors even though there were enough licenses.
- **Review Sender:** Performance improvements using the Review Sender on large systems.
- **Integrations:** Integrations that don't support a persisted connection will now have a state of 'Online' rather than always being marked 'Offline'.
- **Keywords:** Keywords can now be associated with Entities directly from the Entity editor.
- **Controller Data Sync:** A single Controller with a disconnected Level 5 kit is no longer able to stall data-sync for other Controllers.
- **XML/REST Interface:** Resolved potential issue querying review using legacy query syntax.

Documentation

- **Biometric Integrations:** Added manual describing the configuration and use of Biometric Integrations in Integriti.
- **Mimic View:** Updated manual to include details on using additional clients with the Mimic Viewer.
- **XML/REST Interface:** Added details on Session Management and Authentication to XML/REST Interface documentation.

Bug-Fix Release (v 20.1.3)

November 2020 - 20.1.3

Issues Resolved

- **CSV Import:** Controller and Site/Partition mappings configured in the CSV mappings will now be used for imported data.
- **CSV Import:** Resolved issue resulting in imported data not being saved into the Navigation Group specified in the CSV Import Settings.
- **Multi-Select Edit:** Resolved issue resulting in some properties not being editable from the multi-select editor.
- **Entity Lists:** Resolved issue resulting in the Time Since Last Update column not updating correctly in some scenarios.
- **Schematics:** Resolved issue that could result in custom single-click action configurations being lost when updating from v20.0 or earlier.
- **Integrations:** Refreshing Child Devices now creates the child devices in the site of the parent device, rather than in the default site.
- **Access Review:** Resolved issue that could result in Credentials being incorrectly associated with non-Card (PIN, etc) access review.
- **Review Window:** Resolved potential issue that could result in Review Windows not showing correctly for some Operator Types after updating from v20.0 or earlier.
- **Review:** Resolved potential error writing access review for some Card badges.
- **KONE Lift HLI:** Lift Access events occurring on the KONE system will now be logged to Review in real time.
- **CCTV Viewer:** Resolved potential issue resulting in video streaming (both live and playback) not showing any footage for some integrations.
- **Guard Tour:** The Skip Guard Tour and Start Guard Tour actions now use the User currently on the Guard Tour triggering the action when triggered from a Guard Tour. This allows steps in the current Guard Tour to be automatically skipped, and new Guard Tours to be automatically started by the User currently on another Guard Tour.
- **Guard Tour:** The Skip Guard Tour and Start Guard Tour actions are now able to automatically use the current Guard Tour Definition when triggered from a Guard Tour. This saves having to manually program the Guard Tour Definition property of the actions when configured in a Guard Tour's actions.

Improvements

- **System/Personal Layouts:** The currently selected site is now automatically saved in the current System/Personal Layout. This will be updated when the Layout is updated, and loaded when the layout is loaded. This replaces the 'Change Current Site' button in GateKeeper.
- **Control Workstation Task Action:** A Muster View can now be selected as one of the Items to Show.

Bug-Fix Release (v 20.1.2)

October 2020 - 20.1.2

Issues Resolved

- **HID Mobile Credential:** Added support for connecting to Origo HID Mobile Credential accounts using HID's AWS IDP portal.
- **Photo ID Design:** Resolved error that could prevent opening Photo ID Designs containing a QR Code.
- **Layouts:** Resolved potential error loading Personal and System Layouts containing multiple floating windows.
- **List Contents Advanced Report:** Resolved issue resulting in not being able to change the List Type property of List Contents reports.

Bug-Fix Release (v 20.1.1)

September 2020 - 20.1.1

Issues Resolved

- **Server Heartbeat Timeout:** The Server Instance's Heartbeat Timeout can no longer be set to a value that could result in the server incorrectly being marked as offline. Server Heartbeat Timeout will now be automatically updated to a more sensible value if the value entered is too short or too long.
- **Credential Last Used Time:** The Last Used time for credentials now supports Card Numbers with leading zeros.
- **Credential From Review:** Adding Credentials from a Review Record will now find existing credentials with leading zeros in the Card Number.
- **User Credentials:** Resolved potential error using the Enter Number dialog to add a Credential to a User on systems containing credentials using the 'Hashed Credit Card' Card Format.
- **Integration Servers:** Improved speed of stopping the integration servers.
- **Upcoming Door Schedules:** Added Free Access Time Period to Upcoming Door Schedules dialogue.
- **Entity Lists:** Improved default column sizing.
- **Filter Editor:** Resolved issue that could result in some properties not correctly showing the value editor.
- **System Designer/GateKeeper Startup:** Resolved potential issue resulting in the saved layout not loading correctly when opening System Designer/GateKeeper.
- **CCTV Viewer:** Resolved potential issue resulting in the system locking up when opening multiple video streams in quick successions (e.g. via the Control Workstation Task Action)
- **CCTV Viewer:** Resolved issue resulting in showing video from Alerts generated from Integration Review records not being able to show associated video.

VERSION 20.1

August 2020 - 20.1

CCTV Layouts

CCTV Layouts allow for collections of cameras to be stored, along with the layout of the CCTV viewer, and restored at a later point in time. This allows a view to be brought up as required to show a specific set of cameras in a specific layout. CCTV Layouts can be triggered either manually from a list in System Designer/GateKeeper or automatically through the Control Workstation Task Action.



CCTV Layouts can be created by simply clicking on the CCTV Layout button (pictured above) at the bottom right of the CCTV Viewer and selecting 'Create New CCTV Layout'.

For full details on creating, viewing and updating CCTV Layouts, see the relevant section of the 'Integriti Integrations – CCTV' manual.

CCTV Surrounding Cameras View

The Surrounding Cameras View allows for physical relationships between CCTV Cameras to be configured and displayed in the CCTV Viewer. The Surrounding Cameras View shows the selected camera, as well as the cameras configured to be N, NE, E, SE, S, SW, W and NW of the selected camera, all in a CCTV Viewer. Clicking on one of the associated cameras will adjust the view to show the surrounding cameras of the camera that was clicked on. This allows for an object to be easily tracked across multiple cameras, simply by clicking on the camera stream that the object moves to.

For full details on configuring and using the Surrounding Cameras View, see the relevant section of the 'Integriti Integrations – CCTV' manual.

NEDAP LPR Integration

The NEDAP LPR integration allows for license plates from a NEDAP LPR camera to be configured as Credentials on a User directly from the license plate. Configuration is as simple as creating a NEDAP Card Format, associating it with a Card Template and entering the license plate as a Credential in the User.

Full details on configuring the NEDAP LPR Integration can be found in the 'Integriti Integrations – LPR' manual.

Contact Trace Report

Quickly and easily find out who a user may have been in contact with over a given time frame.
The contact trace report analyses historical access logs to determine who the “subject” of the report has been in contact with.
Depending on how your access system is set-up, multiple processing options are available, to give the most accurate and useful information possible.

Same Room Detection – “Location Change” records are analysed to determine where people have been, this works best with read-in read-out
Used Same Door Detection – “Access Event” records are analysed to determine when people used the same door within a configurable time.

Review Categories

The following Review Categories have been added or modified in this release:

- Site Code Card (simulated)
- Direct Entry Card (simulated)

Anywhere using a filter on Review Category should be reviewed to ensure these changes won’t effect existing filters. Places Review Category filters can be found include:

- Review Filters
- Operator Type Filters
- Scheduled Task Triggers
- Reports
- Saved Layouts

Improvements

- **CCTV Viewer Digital PTZ:** When in Digital PTZ mode while viewing a video stream in the CCTV Viewer, the mouse wheel will now zoom the stream in on the mouse cursor, rather than the top-left corner of the stream.
- **CCTV Export:** When exporting CCTV footage, the file name and Evidence Item comment can now be specified using a format string. This allows for contextual information, such as the export time and the camera name to be easily placed into the resulting file name and/or Evidence Item comment.
- **Intercom Call Queue:** Added the option to specify whether commands executed from the call queue dialog are run against the Origin or Destination of the selected call queue item. This can be especially useful when attempting to unlock an associated door from the dialog, where now the location of the Door can be selected (either the Origin or Destination of the call).
  NOTE: Running commands against both the Origin and Destination of a call queue item must be supported by the Integriti Intercom Integration being used.
  NOTE: Not all Call Queue Items may contain both an Origin and a Destination device. Where either device is not available, all commands will be performed against whichever device is available.
- **User RTLS Position:** Review is now logged when a User’s Area or Location is changed as a result of their position changing via an RTLS integration. The generated Review is in the same format as the current Area/Location review that is generated when a User’s Area or Location changes via Door access, allowing all location changes to be conveniently filtered and reported on.
- **Find Entity Form:** Added optional site filter when selecting an Entity to assist in findng specific Entities in multi-site systems.

- **Communication Handlers:** Communication Handlers can now be restarted directly from the Communication Handler list by selecting 'Restart Communication Handler' in the context menu.
- **Simulated Card Badge:** Simulated Card Badges can now be simply distinguished from physical Card badges from the associated Review Record through the new 'Simulated' Card Revew Categories.
  NOTE: This feature requires v20.1 Controller firmware.
- **Card Data Review:** Card Info Review Records now contain additional information about the Card where available. This can include the Site Code, the Credential type and the Card Number.
- **Format Strings:** Format strings now support default values where no value is found for a specified keyword, rather than leaving the value blank in the resultant format string.
  The default value can be specified by using the following format for the format string token: '{[PropertyName]:|[DefaultValue]|}' or '{[PropertyName]:[FormatSpecifier]|[DefaultValue]|}'.
- **Credit User Qualifications:** Credit User Qualification triggers now have the option to choose whether to increment or decrement the selected Custom Field's value when the trigger is activated. This makes it simpler for User Qualifications to be used in situations where access can be temporarily granted or denied based on events in Review or from an integration.
  Upgrading systems will automatically be set to decrement, keeping the existing behaviour.
- **Integrated Device:** Integrated Devices can now have their connection configurations edited in the multi-select editor, allowing the connection configuration to be configured for multiple Integrated Devices at the same time.
- **Review Sender Communication Handler:** Added new Review Search Mode option to allow a lookback period to be specified when sending Review. This allows for the time period over which missed Review will be sent by the Review Sender once it is received to be restricted.
- **Entity List:** Columns showing Entity Types can now be filtered and sorted in the Entity List.
- **X Reference Report:** Added support for showing references to Controllers in the X Reference Report.
- **User Programming:** A User's Tenancy Area can now be set to an Area List containing one Area per Controller. This allows for improved multi-Controller support, allowing specifying a Tenancy Area for each Controller rather than only allowing one.
- **User Programming:** A User's Default Floor can now be set to an Lift Floor List containing one Lift Floor per Controller. This allows for improved multi-Controller support, allowing specifying a Default Floor for each Controller rather than only allowing one.
- **Active Directory User Sync:** Member counts for each Active Directory group are now shown in the editor for the Communication Handler when selecting Groups To Monitor to assist in determining which groups contain Users.
- **Control Workstation Task Action:** Intercoms and other Integrated Devices can now be selected to be shown when using an Item Display Mode of 'Use Selected Item/s'.
- **CSV Import:** Improved behaviour when importing nested items to no longer add blank values when there is no value in the mapped column for the row.
  Where at least one property in a nested mapping is mapped to a column in the CSV, the nested value will only be added if at least one of these mappings has a value in the CSV.
  Constant nested mappings, where all rows of the nested mapping are determined by Constant Value Transforms will always be imported.
- **DB Object Filter:** Filters can now be created to show a filtered list of finalised Alerts, rather than just active Alerts.
- **Operator Permissions:** Added new Operator Permission to prevent Operators with specific Operator Types from viewing Finalised Alerts

Issues Resolved

- **Schematics:** Alerts now honour the Z coordinate of the source of the Alert when showing on Schematics. This prevents Alerts from showing on all Schematics covering the X, Y coordinates the Alert is generated at, and instead only shows on the Schematic at the correct Z coordinate.
- **Schematics:** Resolved issue resulting in mouse hover text being shown for map elements, even when they're obscured by another element.
- **Schematics:** Resolved issue resulting in Single-Click Actions not working on clients translated to a different language to the client they were programmed in.
  NOTE: Single-Click Actions may need to be re-programmed on translated systems.
- **CCTV Playback:** When playing associated CCTV footage from a Review Record, the default playback time is now sent in the timezone of the event, rather than the timezone of the client, to ensure the correct footage is played.

Bug-Fix Release (v 20.0.3)

July 2020 - 20.0.3

Issues Resolved

- **Data-Sync:** Improved efficiency of the "Disallow Changes From Controller" data sync mode.
- **Data-Sync:** Added "Upload Sync Behaviour"options.
  NOTE: These options can disable parts of the "upload from controller" data synchronisation and result in field controllers being out of sync with the server.
  Settings other than "Normal" should only be enabled if keypad editing is disabled, and under instruction from Inner Range Support.
- **Active Directory User Sync:** Added support for nested mapping to be configured with only Constant Value Transformations (and not be mapped to any AD Columns) to allow the same nested value to be given to all synched Users.

Bug-Fix Release (v 20.0.2)

June 2020 - 20.0.2

Issues Resolved

- **CSV Import:** Performance improvements when using nested mappings.
- **CSV Import String To Entity Mapping Transform:** Improved loading time of configuration UI and performance when used in an import.
- **CSV Import Name Lookup Transform:** Site is now selectable in the configuration UI when 'Limit Results To Site' is selected.
- **CSV Import Name Lookup Transform:** Resolved issue that could result in the 'Cast as Type' value specified not being persisted.
- **User Import:** Improved performance on large sites when importing Users (Via XML, CSV, REST XML).
- **Review Sender Service:** Improved performance when large numbers of connections are made to the Review Sender service from a third party.
- **Dot Net Support:** Added support for Dot Net v4.8.0.528372.
- **Human Readable Report:** Resolved potential error when viewing the Human Readable Report on a Controller.
- **Biometric Integrations:** Resolved issue that could cause the license check to fail when opening a Biometric Integration's Acquire Card dialog.

Bug-Fix Release (v 20.0.1)

June 2020 - 20.0.1

Issues Resolved

- **Review List:** Fixed issue resulting in several entity commands not working correctly when activated from the Review List's context menu.
- **System Designer/GateKeeper Layouts:** Fixed issue resulting in sometimes being unable to manually change the current Layout.
- **Integriti CS:** Resolved issue that could prevent logging into CS systems after transferring them between instances of CS.
- **Edit Door:** Newly created Doors now have a Door Type by default.
- **Control Workstation Task Action:** Fixed issue that resulted in previously configured Control Workstation Task Actions not being able to show Schematic Maps when triggered.
- **Custom Fields:** Resolved issue that caused large Custom Field text values to not save correctly (> 700 characters). The new limit on Custom Field text values is now approximately 4000 characters.
- **Schematic Maps:** Fixed error preventing viewing or editing certain Schematic Maps.
- **Intercom Call Queue:** Fixed issue resulting in Layouts not saving correctly when they contain an Intercom Call Queue window.
- **Intercom Call Queue:** Fixed issue that could result in some calls not showing up in the Intercom Call Queue.
- **Integration Auto Input Restore:** Improvements to the behaviour of the Auto option of Auto Input Restore Mode to only restore Inputs when events of types with a corresponding Auto Input Trigger configured are received.
- **Integration Persisted Connection:** Resolved issue that could prevent multiple Integrated Devices from having persisted connections running simultaneously.
- **Ethernet Bridge:** Ethernet Bridge firmware can now be updated through System Designer.
- **Communication Handlers:** Fixed issue preventing creation of EkoTek, Schindler and several other types of Communication Handlers.
- **HID Mobile Credential (Origo):** Resolved issue that could result in a connection to the Origo HID Mobile Credential system not being able to be established.
- **Review Triggers:** The 'When' option of Review, Custom Item Changed and Door/Area Triggers now correctly restricts the trigger to only be triggered when the specified Time Period is active.
- **EkoTek RTLS Listener:** Fixed issue that prevented Remote Logs received via the EkoTek Listener Communication Handler from producing Review and saving associated hardware.
- **X Reference Report:** Fixed potential error that could sometimes prevent running X Reference Reports.
- **Muster View:** Resolved issue that resulted in Users showing up as ungrouped lists in Muster Views, rather than being grouped by the Location they're currently in.
- **SkyTunnel:** Resolved issue that could result in connections to Controllers via SkyTunnel failing in some scenarios.

VERSION 20

March 2020 - 20.0

V20 Licensing Change

A major part of the Integriti V20.0 release involved assessing and evaluating the full Integriti hardware and software licensing model. These changes include new product editions, each including a different set of features, changes to existing licenses and the removal or combining of several existing licenses, among other things.
For the full details on the licensing changes included in Integriti V20.0, see 'Integriti License Change Release Notes.pdf' for a full breakdown of the changes.

Client Connection Licensing

We have simplified and improved how client licensing works.
There are no longer separately priced & counted fixed, floating & web interface licenses, they are all replaced by a single "Client License", which is included as part of the Integriti Product Edition.

> All existing sites' fixed / floating / web licenses will be automatically converted to additional client seats, providing additional client connections on top of what is included as part of the Integriti Product Edition.
>
> The functionality that used to be provided by "fixed workstation licenses" is now a core feature, and is covered in the "Reserved seats" section below.

Each "Client License" allows:

1. Up to 4 Clients from a single workstation (2x System Designers + 2x Gatekeepers)
   or
2. A single Web Interface session

Additionally, a single local "System Designer" login is ALWAYS permitted from any Activated Server.

Reserved Seats
Client Seats can be *reserved* (from the License Manager in system designer) for either:

- Workstations (existing fixed workstations)
- Operators

Reserving client seats ensures your most important workstations / operators are always able to access the system.
Reserving a seat for a specific Operator is a new feature with V20.0, allowing that operator to always be able to log in, regardless of the workstation they are at.

Remote Disconnect
Operators with reserved seats will always be able to login with a Gatekeeper or System Designer client from anywhere. Even if they are logged in somewhere else and all seats are taken, the login window will present a list of the operator's existing sessions, so one can be chosen to be closed.

Integrations

- **License Plate Recognition**: Added option to LPR Card Formats to not badge detected License Plates at the associated Reader if they don't have a matching Card programmed in Integriti.
- **Export CCTV Footage**: Added option to export the 'current frame' when exporting CCTV footage from the video viewer. This will export the frame currently showing in the viewer when the command is invoked.
  NOTE: Export Current Frame is not supported by all integrations, and requires a supported integration to function.
- **Video Viewer**: Individual video streams can now be dragged between different viewer panels, and between different instances of System Designer and GateKeeper on the same computer.
- **Video Viewer**: Added support for using the mouse wheel to zoom in and out when viewing video streams.
- **Default PTZ Speed**: CCTV Cameras and CCTV Recorders now have the option to specify default Pan, Tilt and Zoom speeds to be used when sending these commands from the video viewer. This allows easy overriding of the default PTZ speeds to make the camera move faster or slower as required.
  These properties should be set to the percentage of the built-in default PTZ speeds to use, with 100 specifying to use the built-in default PTZ speed. Set to 0 to use the defaults specified in the device's parents, where the device has a parent, and the built-in defaults where it doesn't.
  NOTE: This feature requires a supported CCTV integration for these properties to have any effect.
- **Integration Server Startup**: Improved integration server startup speed and error handling.
- **Intercoms**: Added the option to specify an unlock time to be used when unlocking associated doors on an Intercom Point. This can be configured through the 'Associated Door Unlock Time' property in either the Intercom System's configuration, or overridden in the Intercom Point's configuration. Leaving the unlock time configured as zero will maintain the previous behaviour of unlocking the associated door/s indefinitely.

Display Themes

Display Themes allow customisation of the look of Integriti lists, allowing the selection of font, text colour and background colour of rows/items in a list based on the configuration or current state of each item. This gives the ability to make individual rows stand out from the rest based on custom criteria, allowing for an improved workflow and better visibility of the status and configuration of items in the list.

- **Disabling Themes:** Added the ability to disable Display Themes to prevent them being automatically used by Entity Lists. Display Themes associated with a Filter will still be used, even when disabled.
- **Review Categories:** Improved editor used when selecting Any Of or Not Any Of values for Review Display Theme's Category property.
- **Display Theme Rules:** Display Theme Rules can now use a custom filter to specify rules more complicated than can be configured in the default rule editor.
- **Display Theme Rules:** Integrated Device and Communication Handler state properties can now be selected for Display Theme Rules.
- **Dark Themes:** Added the option to specify Display Themes as 'Prefered For Dark Themes'. This allows for Display Themes to be prioritized based on whether the skin of the currently active theme is dark or light, where multiple Display Themes have the same preference. This opens up the option to configure a different Display Theme for dark and light skins and have

the correct one always be used, helping ensure better colour contrast with the skin's built in background and text colours.

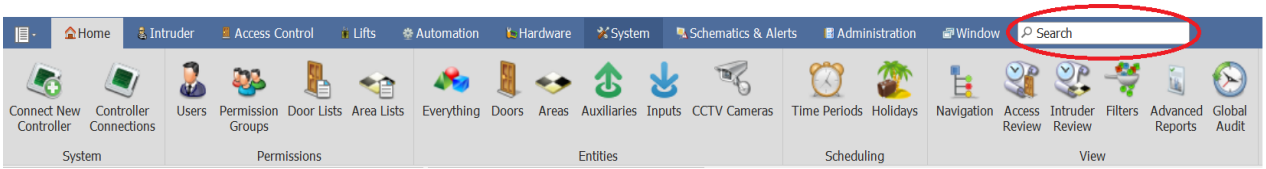
- **Default Display Themes:** Default Display Themes have been added for a number of types, allowing for default colouring of these lists and easier customisation of the default colouring.

XML Rest API

- **Compression:** Added the ability to use GZIP compression on large XML responses
- **Review:** Added the ability to long poll for new Review Records
- **Virtual Card Badge:** Virtual Card Badge now supports specifying a Door to badge at by name.
- **Virtual Card Badge:** Can now wait for panel ack or Access Review to ensure the command was executed successfully

Improvements

- **Disconnect Clients:** Client connections can now be remotely disconnected from the Client Connections list in System Designer by Operator's with sufficient permissions.
- **HID Mobile Credential Integration:** Added support for the HID Mobile Credential Origo (subscription) portal. Newly created HID Mobile Credential Communication Handlers will be created referencing the new portal.
  To create a new HID Mobile Credential Communication Handler using the Secure Identity Services (perpetual) portal, the HID Client Portal Version of the Communication Handler should be set to 'Secure Identity Services (1.0)'.
- **Controller Short Name:** For multi-Controller systems, a short name can now optionally be added to Controllers to prefix the Address of each Entity in that Controller. This can assist in identifying which Controller each Entity belongs when viewing Entities from across multiple Controllers.
- **Themes:** Improved theme selection to allow selection of a colour scheme for supported themes.
- **Ribbon Search Bar:** Added a search bar to the ribbon in System Designer and GateKeeper to allow ribbon items to be easily searched for.



- **Alerts:** Added option to Alert Definitions to not execute the 'Retriggered' Action when the Alert is restored.
- **Alerts:** Added new 'Maximum Activations' and 'Maximum Outstanding Alerts' options to Alert Definitions.
  Maximum Activations limits the number of times a single Alert can be retriggered. Once the configured value is reached, the Alert will no longer be retriggered and future retriggers of the Alert will be ignored. This option will be automatically set to 500 by default on updating systems.
  Maximum Outstanding Alerts limits the maximum number of un-finalized Alerts in the system for the Alert Definition at any one time. Once the configured value is reached, no further Alerts will be generated for that Alert Definition until the outstanding Alerts are finalized. This option will be automatically set to 500 by default on updating systems.
  This feature helps prevent "runaway alarms" from consuming excessive system resources and valuable operator time.
- **License Manager:** UI improvements to make relevant information on licensed features and client seat usage more visible.
- **Review List:** Commands for Entities associated with a Review Record can now be performed directly from the context menu of the Review in the Review List.

- **Send Action:** Actions can now be directly sent as either an Assert or a Deassert by simply pressing the corresponding button, rather than having to change a dropdown value, in the Send Action dialog.
- **Ekotek RTLS Integration:** The unassociated hardware dialogs now show all known hardware of the selected type, allowing all existing hardware associations to be managed from this dialog.
- **Ekotek RTLS Integration:** Users can now be to assigned Repeater hardware in addition to an Area or Location, allowing for alarms triggered from Repeaters to be viewable on Schematic Maps.

Issues Resolved

- **User List:** Resolved issue resulting in sorting by and filtering on the 'Credentials' and 'Permissions Summary' columns in the User Entity list not working.
- **Guard Tour Summary:** Resolved issue resulting in colouring of rows not being applied when printing a guard tour summary's steps.

Important Notes

- V20 firmware is recommended for the best experience using V20 software.

Notes For REST XML Technology Partners

- Changes have been made to the way Custom Field Values are serialized in the REST XML interface. See the Generated REST XML Documentation's 'Compatibility Notes' for further details

Bug-Fix Release (v 19.1.5)

June 2020 - 19.1.5

Issues Resolved

- **Database Update:** Improved the speed of running the database update script when updating from v19.1.2.
- **Controller Sync:** Resolved an issue that could occasionally cause a data sync stall on multi-controller systems.
- **Review Sender Service:** Improved performance when large numbers of connections are made to the Review Sender service from a third party.
- **Dot Net Support:** Added support for Dot Net v4.8.0.528372.
- **User Import:** Improved performance on large sites when importing Users (Via XML, CSV, REST XML).

Improvements

- **Apartments:** Can now have numbers greater than 255. NOTE: Integriti Controller Firmware v19.1.3.37707 or higher is required to make use of this change.

Bug-Fix Release (v 19.1.4)

April 2020 - 19.1.4

Issues Resolved

- **Controller Data Sync:** Improved & optimized the 'disallow controller changes' data-sync mechanism.
- **User Access Report:** Resolved potential error when running User Access Reports when logged in as an Operator with an Operator Type with insufficient permissions.

Improvements

- **Apartments:** Can now have numbers greater than 255. NOTE: Integriti Controller Firmware v19.1.3.37707 or higher is required to make use of this change.

Bug-Fix Release (v 19.1.3)

March 2020 - 19.1.3

Issues Resolved

- **Cyrillic Character Support:** Resolved issue that resulted in Cyrillic characters in Entity names showing in Review as '?'.
- **KONE Access Integration:** Reduced the number of simultaneous active connections the Kone integration has to Kone at any one time. This reduces the required number of Kone connection licenses required for the Kone integration to be used. The Kone Access Integration requires at least 3 Kone connection licenses to be present in the Kone system for the integration to function correctly.
- **KONE Access Integration:** Changing the Expiry Date/Time of an Integriti User now correctly updates the Kone Access Right Expiry.
- **KONE Access Integration:** Resolved issue that resulted in the Kone integration being unable to sync the re-assigning of a Card from one User to another
- **Control Workstation Task Action (Play Sound):** Resolved issue that could result in parts of the GateKeeper UI not updating correctly when multiple Control Workstation Task Actions that play sounds are triggered in quick succession on the same Workstation.

Bug-Fix Release (v 19.1.2)

March 2020 - 19.1.2.15837

Issues Resolved

- **Editing Lists:** Resolved issue that could result in items being unintentionally removed from a List (Door List, Area List, etc) after editing the list from a Controller keypad.
- **Human Readable Report:** Resolved issue resulting in the Human Readable Report not running for many Controllers.
- **Permissions Report:** Resolved issue where having multiple identical qualifiers could result in rows being removed from the report.
- **Challenge Response:** When a Location is full, access requests are now automatically denied.
- **Review:** Direct Entry Cards are now correctly associated with Access events.
- **Photo ID:** Resolved issue that could sometimes result in the error 'A generic error occurred in GDI +' being shown when attempting to print a Photo ID.
- **Muster View:** The Count field now has the correct value when printing Muster Views.

Bug-Fix Release (v 19.1.1)

December 2019 - 19.1.1.15582

Improvements

- **RTLS CCTV Improvements:** Users now have their associated Area/Location automatically updated as their RTLS position changes. This allows CCTV footage to be shown directly from a User from all of the cameras associated with the Area/Location that their RTLS position shows them as being inside of.
  This can be configured by placing the Areas/Locations on a Schematic Map as Shape Elements covering their positions relative to the RTLS system, then pressing Auto-Allocate Positions to save the Area's/Location's position data. Once this is done, Users will automatically be moved to the Area/Location their current RTLS Position falls within as their position changes, automatically associating the Cameras associated with that Area/Location with the User, until they move to a new Area.
- **Alerts:** When grouping Alerts with a source of Review Filter by a Format String, all empty results of the format string are now automatically grouped, rather than always creating new results.
- **Muster Report:** Muster reports now have the option of selecting Locations and Muster Locations in addition to Areas and Muster Areas.
- **Time On Site Report:** Added support for Lift Access when using a Processing Mode of First/Last Badge.

Issues Resolved

- **Finalizing Alerts:** Resolved issue where Alerts could sometimes not be finalized after the triggering Entity was deleted.
- **Review:** The Review list no longer automatically un-pauses when selecting a record.
- **Invoke Integrated Device Task Action:** Resolved issue resulting in the configuration options not showing up for some Integrated Device command types when editing an Invoke Integrated Device Task Action.
- **Partitions:** Resolved issue where deleting partitioned Entities could sometimes result in Entities being incorrectly deleted from Controllers in other partitions.
- **Schindler Lift HLI:** Resolved issue resulting in Schindler Lift HLI Communication Handlers configured in Integriti v18 not working after updating Integriti without reconfiguring the Communication Handler.

Important Notes

- If using the Inner Range Mobile Reader Application, an update will be required in order to continue working with Integriti v19.1.1.

Notes For REST XML Technology Partners

- Changes have been made to the properties of User State in the REST XML interface. See the Generated REST XML Documentation's 'Compatibility Notes' for further details.

VERSION 19.1

November 2019 - 19.1.0.15471

Schematics Improvements

Viewer:

- **Element Labels:** Elements can now have a label shown about them positioned relative to the element (top / center / bottom, left / center / right). The contents can be customized in the element presenter, showing the linked item name by default.
- **Custom Hover Text:** When the mouse moves over map elements, useful information about the element can be shown. This information is customizable in the element presenter.

Editor:

The editor has several productivity improvements to accelerate the creation of high-quality schematic maps. More will come with future releases, but here are some highlights in this release:

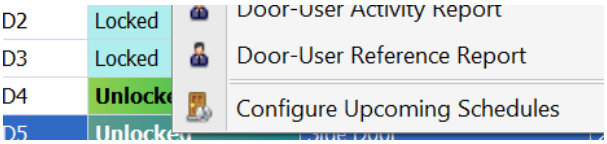
- Management of elements in the Element List has been enhanced. Elements now have an icon for their type, an editable description, and visibility and lock control.
- Usability when inserting and editing of elements has been improved.
- Previewing of layer visibility

Door Schedules

When you know you need a particular room unlocked for an upcoming event, you can now create a “Door Schedule” in advance. Schedules can be managed and reported on from the new “Door Schedules” list in “System Designer”.



Schedules can also be managed from the context menu of any door in either “System Designer” or “Gatekeeper”. This functionality is also available when right-clicking a door from a schematics map.



Inactive Credential Used

When cards are marked as lost / stolen / damaged are used, the system now creates new review events specifically for these events, and associates the user with the card review events.

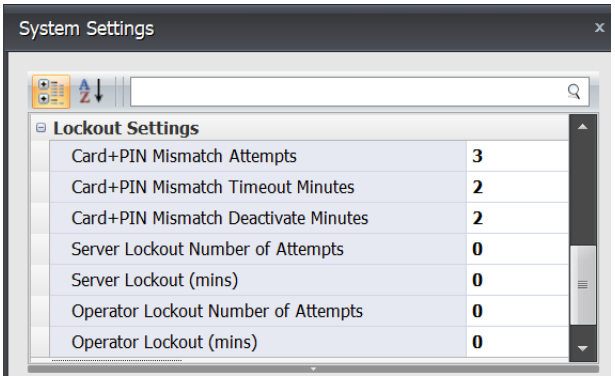
This allows the creation of Alert Handlers or automatic actions when a “blacklisted” card is used anywhere in the system.

Improved Lockout Capabilities

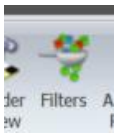
Configured in “System Settings”, operators and / or credentials can be temporarily locked out of the system when too many incorrect login / access attempts are made.

Card+PIN Mismatch activates when a user presents a valid card at a reader, but then enters an incorrect PIN.

Operator Lockout activates when an operator uses an incorrect password.



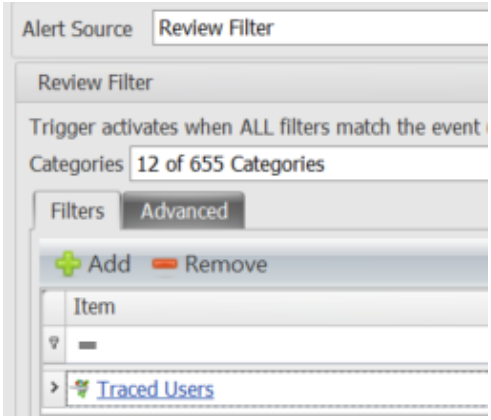
Powerful New Uses for “Filters”



Pre-Defined “Filters” have always been part of Integriti, but now filters can also be used in other areas of system programming.

Improved Review Trigger Filtering

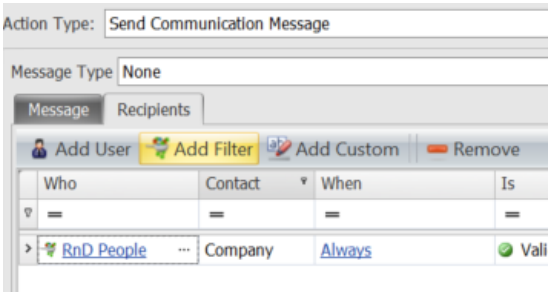
Review triggers (as used in Scheduled Tasks, Alert Definitions, etc) now allow ‘Filters’ to be referenced to identify the events to trigger on.
A filter may simply be a ‘Review Filter’ (perhaps specifying just access granted events), but additionally, a filter can narrow down events based on which entities the review event refers to.



For example, a ‘Custom Field’ called “Under Probation” could be defined on “Users”, and a filter created to only display the Users with this option enabled. An ‘Alert Definition’ could then be created to trigger whenever a user under probation is denied access to a door.

Send Communication Message

Messages recipients can now be specified by referencing a ‘Filter’ instead of manually including each user.
This allows you to easily broadcast a message to all member of a department / group, or any other criteria you can filter on (perhaps just the people in a particular area).



Strongly Typed Credentials & 2 Factor Authentication

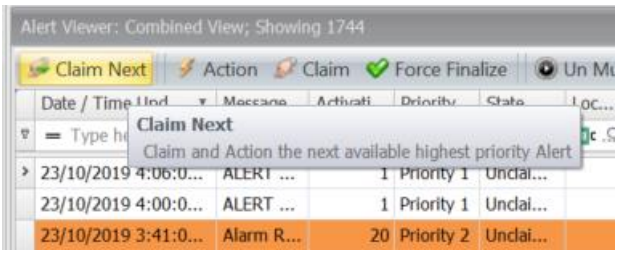
Credentials (formerly known as cards) are now identified (by the Credential Type in their Credential Template) as one of the following categories:

- Card
- Face
- License Plate
- Fingerprint
- Eye

Door / Lift Type programming can then require a specific type of credential, or even any 2 (or 3) types of credential. This allows many more access control scenarios to be defined, like requiring both card and biometric credentials to access a door or allowing facial recognition during the day for faster user processing but disabling that mode in the evening.

*This feature requires V19.1 Controller Firmware.

Other Improvements



- **Alerts**: The new ‘Claim Next’ button allows operators to quickly move on the next most important alert in Gatekeeper.
- **Alerts**: Alert Views are now able to utilize ‘Display Themes’ so the appearance of alerts can be customized for each site.
- **Alert Responses**: The workstation ‘host name’ and client type are now recorded against each alert response.
- **Control Workstation:** Reset Schematics Zoom (all maps / all ‘default’ maps).
- **Pin Mismatch:** Configure in "System Settings" - after a number of incorrect PINs, the card is deactivated for the specified number of minutes (requires V19.1 firmware)
- **Control Workstation Task Action** - Added Auto-selection logic to either only control client from context, or auto-select clients based on Operator and Workstation ranks
- **Integrations** - Added 'Restart Persisted Connection' command to plugins to allow restarting a connection from the context menu
- **Review List** - Exclude & Include Category menu options now apply to all selected rows
- **Review Events:**
  - Inactive card review events now reference the associated user
  - Server start-up now creates a review event
  - When any Integrated Device command is invoked an event is logged.
- **New System Warnings:**
  - New system warnings when low drive space is detected.
  - New system warnings when Servers are offline.
- **Assign System Inputs**: Automatic ‘System Area’ input programming can now use a different process group for door forced alarms
- **Web Interface**: The server-side session inactivity timeout (configured in Operator Type) is now enforced in the Web Interface.
- **Time On Site Report**: Can now include “Door Unlock” events when using the first / last processing mode.
- **Communication Messages:** HTTP Content can now be enabled for the message body.

- **CSV Import:** The ID (Address) property now works when mapped for Entities – and can be used as a key
- **CCTV:** Show Associated CCTV Footage on a User will now show the CCTV footage for that User's associated Area/Location
- **Task Actions:** When invoking an Integrated Device Command, the device can now be selected automatically based on the triggering context
- **Kone Access Integration**: Improved user interface and added compatibility with more Kone card formats.

Issues Resolved

- Resolved an issue that caused some review windows to incorrectly filter out all review.
- Filters – Collection Contains filters can now be saved

Bug-Fix Release (v 19.0.1)

August 2019 - 19.0.1.15054

Improvements

- **Lift Integrations:** Schindler & Kone ACI now allow inspection / editing of the “service data”. This should only be done on instruction form Inner range support staff.
- **Kone ACI Integration:** Lift car allocation events can be associated to the Lift-Floor area.
- **Kone ACI Integration:** Configuration now uses drop down combo boxes.
- **Review Sender:** The ‘Remote Server” can now be specified by either DNS name or IP address.
- **Filters:** Day of Week filters can now use “Any Of”
- **Card Enrolment:** SIFER enrolment station now supports CSN cards (using the Direct 88 format).
- **CCTV Export:** The status of a CCTV footage export is now displayed at the end of the export, to make it clearer if the export succeeded or failed.
- **Remote CS Connections:** The “Allow CS Remote Connection” license is no longer required to remotely administer small systems with Integriti CS (regardless of the Smart card level).

Issues Resolved

- **Schindler Lift Integration:**
  - Resolved an issue that caused deleted cards to stall user-sync.
  - Deleting users who are already deleted no longer causes an error.
  - User sync failures no longer stall data-sync (errors are logged to review)
- **Partitioned Systems:**
  - CSV Import now supports importing users into a partition.
  - irentities exported systems (ie from CS) can now be imported into a partition.
  - Card ‘collision detection’ logic is now ‘Partition Aware’, supporting legitimate duplicates.
  - Partitioned entities inside sub-sites have their address ‘Short Name’ correctly updated.
  - Partitioned entities in global user permission rows no longer written to all partitions.
  - Partitioned programming referenced no longer incorrectly behave like global references.
- **CCTV Viewer:** The timeline now more accurately matches the current playback time.
- **CCTV Export:** Resolved potential errors exporting CCTV footage in some scenarios.
- **User Interface:** Improved UI responsiveness in the Edit User screen.
- **Alert Definitions:** The default Alert handler is now disabled.
- **Schematics:** Resolved an issue that caused Layers to hide some elements.
- **Control Workstation Task Action:** Improved performance of the Show Items option when the Task Action is triggered multiple times in close succession.
- **Review Windows:** Resolved an issue that sometimes caused no events to be shown.
- **Time Trigger:** Resolved issue resulting in the Start Time of a Time Trigger being lost when changing the frequency of the trigger in the editor.
- **Active Directory:** Resolved issue resulting in the error ‘The Server does not support the requested critical extension’ when attempting to perform an AD import on large Active Directory Databases (>~20,000 Users).
- **Active Directory:** Distinguished Names of Groups and OUs are now visible from the editor in the Active Directory Communication Handler.

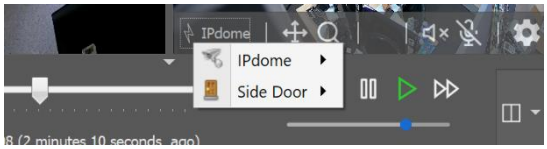
VERSION 19

June 2019 - 19.0.0.14739

New & Improved Camera Interface

The CCTV camera interface has been completely overhauled, and now supports:

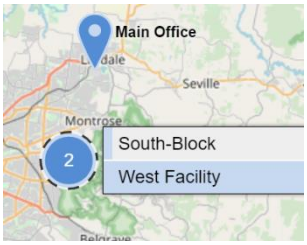
- Multiple standard layout configurations.
- Control Items associated with cameras directly from the video stream.
- Easily navigate with the timeline.
- Export short clips or snapshots to file or the Evidence Vault (requires integration support).
- Control PTZ tours directly from the video stream.
- Aspect ratio can optionally be enforced on a per camera basis.



- New layout options, including “N + Main” layouts that are designed to show many thumbnail camera streams, and allow operators to click on any of them to bring that camera to the Main large display.

Schematics

- **Map Group Clustering**: Zooming out now displays your buildings as “Icons:
  - Isolated buildings are shown with names “location icons”
  - Zooming out further will group buildings into “cluster icons”
  - Icons turn red to indicate the presence of alerts
  - Clicking on a cluster shows a menu to jump to your chosen map.
- **Editor:**
  - Improved UI for the positioning of maps within a map group
  - Improved UI for rotating and positioning map elements



Evidence Vault

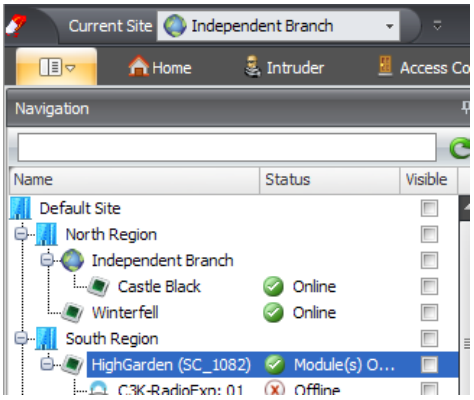
Evidence Vault is an interface that allows any file to be stored and retrieved for later use.

- **Cryptographic Fingerprinting:** Evidence is stored with MD5 and SHA-256 cryptographic hashes, so tampering with any evidence extracted from the vault can be detected.
- Compatible CCTV Integrations can store clips (or snapshots) directly into the Vault.
  - Footage associated to Alerts can be stored in the Vault automatically (for example via the ‘Save Associated Footage to Evidence’ action in the Created Actions), or manually from the context menu.
- Configure the storage location (UNC) in ‘System Settings’:
  - Only the Server requires access, so evidence can be secured, and won’t bloat your database backups.

Operator permissions give fine grain control over who can store or retrieve evidence items.

Partitioned Systems

Version 19 introduces “Partitioned Sites” allowing the creation of Users (and other ‘global entities’) that only exist within the ‘Partition’ they were created in.



- Create new ‘Partitions’ from the “Site Navigation Tree” in System Designer.
- Users in Integriti’s existing ‘Global Partition’ are still truly global.
- Choose your current “working site” from the new selector in the title bar.
- Partitions can contain multiple ISCs & IACs.
- Each ‘Partition’ can have its own local ‘User 1’.
- Card / PIN uniqueness is only enforced within a partition.
- Partitions are entirely isolated from each other.

For more information refer to the “Integriti Partitioned Systems Guide” located in the ‘docs’ folder.
*This feature requires a license.

High Level Camera Alarm Integration

Your integrated devices (Cameras / Intercoms / etc) can now trigger inputs in Integriti’s sophisticated intruder detection capabilities.

- Configure in integrated device properties.

Communication Handlers

- New **Kone ACI HLI:** Sync users and access events with Kone’s next generation lift ACI platform.
- New **ModBus TCP Slave**: Allows 3rd parties to use the Modbus protocol to monitor and control Doors / Areas / Auxiliaries & Inputs.

Alerts

- Pre-Defined Alert Responses allow operators to more efficiently close issues, and enforce consistency to enable better reporting.
- All Alert Sources now support “Finalize only when alarm conditions are restored. Additionally, ‘restore’ event can be either counted (existing functionality) or a single restore can clear many triggers.
- New review ‘Categories’ filter for the Intruder Events Alert Source – This allows the exclusion of some XMIT categories, or states – for example to exclude Tamper Events.

Quality of Life Improvements

- **System Warnings:** New system warnings when low drive space is detected.
- **Control Workstation:** Reset Schematics Zoom (all maps / all ‘default’ maps).
- **Control Workstation:** Can now ‘Load System Layout’.
- **Operator Compliance Restrictions:** “Ensure Maximised” removes the ability to “restore down” the main GateKeeper application.
- **Workstation & Server** entity lists can now display their last know OS and .NET versions.

Bug-Fix Release (v 18.2.3)

May 2019 - 18.2.3.14706

Issues Resolved

- **HID Mobile Credential Integration:** Fixed an issue that prevented assigning HID Mobile Credentials when using the counted license.
- **Controller Data Sync:** Fixed an issue that could result in Controllers being unable to sync data while connected to Integriti.
- **Operator Challenge Response:** Improved processing when multiple 'Challenge Definitions' match an access request (ie. are for the same door):
  - All open 'Challenge Windows' now receive new requests.
  - All open 'Challenge Windows' are now updated by any relevant response.
- **Operator Challenge Response:** Challenges can now be actioned from the 'Past Challenge Viewer' if performed before the challenge times out.
- **Operator Challenge Response:** Multiple Challenge Definitions can now be viewed simultaneously in Integriti Gatekeeper.
- **Card Parity:** 38-bit cards with high card numbers now have their parity calculated correctly.
- **Day of Week Filters:** Resolved an issue that prevented review triggers (Scheduled tasks / Alert Definitions / etc) containing 'Day-of-week' filters from working correctly.
- **Format Strings:** Where previously invalid tokens using the new curly brace format in a format string were left in the resulting text, invalid tokens are now removed. This will affect format strings used in such places as Alert Response Plans, Log Review Task Action, Challenge Definitions, etc. NOTE: People using the legacy '%' syntax should update their format strings to use the new curly brace notation.
- **Format Strings:** Added support for entering literal curly braces by entering '{{' or '}}'. If any single curly braces are currently being used as literal curly braces in a format string, they should be replaced with the new double curly brace notation.
- **Active Directory User Sync:** Fixed an issue that resulted in not some Active Directory Groups being missing from the 'Groups To Monitor' property of the Communication Handler on larger sites.
- **Schematics Map Viewer:** Fixed potential issue that could result in the Status Summary or Command panels not being visible or resizable.

Bug-Fix Release (v 18.2.2)

March 2019 - 18.2.2.14467

Issues Resolved

- **Arm Area Window:** Pause button now moves when the window is resized.
- **Reports:** Fixed an issue that prevented operators without a 'Name' from running reports.
- **LPR:** License plates now support Unicode characters.
- **Programmed Inputs List:** Improved performance on large systems.
- **Alerts:** Resolved an issue that caused the 'Escalate Alert' task action to occasionally not work.
- **Schindler HLI:** Incompatible cards no longer interrupt user card syncing.
- **Schematics:** Copy / paste / delete 'Edit mode' keyboard short-cuts no longer have any effect in 'View Mode'.
- **Audit:** Resolved: 'Show History' occasionally showing the history of another entity.
- **Photo ID:** Fixed an issue that caused barcodes to be printed the same for every card, when printing cards for multiple users at the same time.

Bug-Fix Release (v 18.2.1)

February 2019 - 18.2.1.14187

Issues Resolved

- **Schematics Editor:**
  - Status bar show position and size.
  - Resolved some grouped item visibility issues.
- **Schematics:** Fixed Single Click Actions from touch screens.
- **Guard Tour:** Resolved an issue starting tours created in V18.2.0.
- **Muster View**: Windows can be opened in a new Tab.
- **Sounds**: Resolved an issue that caused Alert sounds to be lost during a version upgrade.
- **HID Mobile Credential**: Updated to current HID production URL.
- **CS Edition**: Resolved issue that prevented customizing list views (ie adding new columns).
- **Panel Connectivity**: Fixed an issue that could potentially cause controllers to stop data-sync & control functionality on networks with occasional very high latency.
- **Lists:** Reduced flicker in review & other rapidly changing lists.
- **User Editor:** Fixed an error that occurred when exporting some User photos.
- **Display Themes:** Improved Display Theme colour blending.
- **Commissioning Report:** Sims II group number is now correctly reported.
- Resolved an issue that caused custom enhancements to not compile on some touchscreen equipped clients.

VERSION 18.2

November 2018 - 18.2.0.14056

Schematic Maps & RTLS

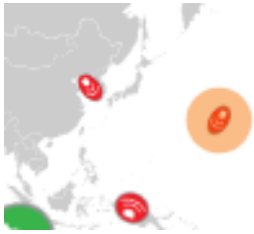


New "Map Groups"
See all of your schematic maps as one giant interactive vector map.

- Zoom in on individual maps for high detail, or zoom all the way out to see a helicopter view of your entire installation.
- Multi-Level complexes can overlay maps, allowing you to choose the level you are interested in.
- Position maps over a worlwide "street view"
- Auto-rotate – as you zoom in on a particular map, it will automatically re-orient to the map's "design orientation"

Schematics Vector Editor - Schematic maps are easier than ever to create, as the new Vector Engine is now used when designing your maps for a true WYSIWYG experience.

Alerts & RTLS
Applying co-ordinates to entities in the system allows Schematic Group Viewers to automatically zoom in on the relevant areas.

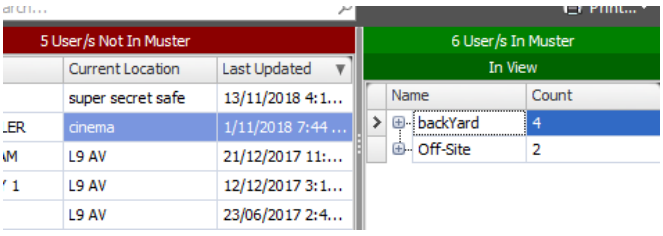


Co-Ordinates can be applied to Doors, Areas, Inputs, Users, Alerts, Cameras & Intercoms by Integrations to 3rd party providers.

Once a map has been "located" (by placing it on a map group) you can easily update the geo-location for all items on the map from the Map editor with the new "Auto Allocate Positions" feature.

Alerts automatically inherit the RTLS geo-location of the items that triggered them. This enables the Alert to be visualised as an Icon on the appropriate map. (choose an element presenter in map properties).

Live Muster View

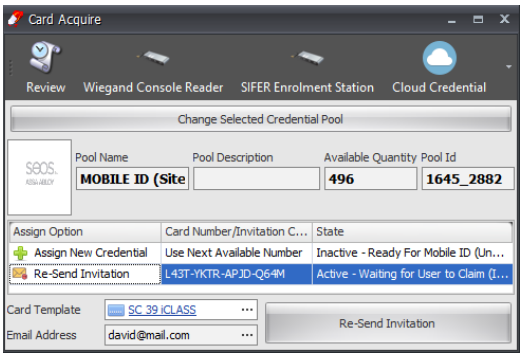


Provides an interactive view of where everyone is during an evacuation - Similar to the Muster feature of the Mobile Reader Application.

Configure "Muster Views" from System Designer -> Access Control -> Muster View.

Use a "Location List" to determine which areas or locations are included in the the view, and the "Muster Point" check box in Area & Location Programming to indicate which areas are "safe".

HID Mobile Credentials



Allocate and manage HID Mobile Credentials from within the Integriti User Editor.

Configure the new “Cloud Credential Service” to:

- Monitor the progress of allocated credentials
- Send customised Email / SMS Invitations to Users

*This feature requires a license.

REST / XML 3rd Party Interface

- New Session Cookie (when security is enabled):
  - The session cookie validity is configurable from 5 to 60 minutes
  - Allows a significant performance improvement
- Control License now allows “Virtual Card Badges”

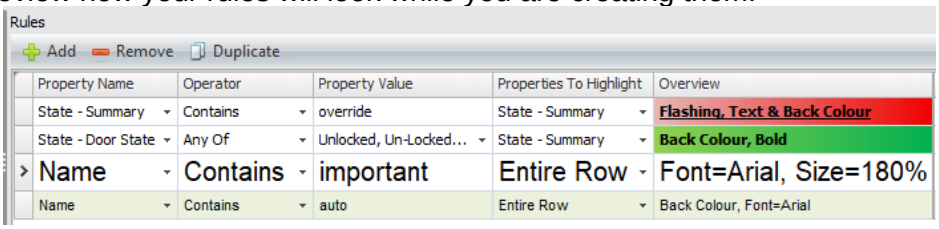
Active Directory Integration (Users)

- New editor makes working with large AD’s much easier.
  - A Tree makes choosing OU filters or AD Groups much easier.
  - Test import now shows any attributes that contain no data at the bottom.
- Improved support for Group based filtering. (Including the AD “Built-in Groups”)
- When configured to sync Cards, new cards are now created in the “Import Settings -> Default Site”.
- Performance improvements.

Display Themes

Customising the look of Integriti lists is easier and more powerful than ever, thanks to a “Display Theme” overhaul:

- Customise either the whole row, or just the field you choose.
- Rules can change every aspect of a row or item:
  - **Font**, including bold / italic font modifiers
  - **Colour**, separate foreground / background colour.
  - **Flashing**, make important alerts / states really stand out!
  - **Gradients**, an optional 2nd background colour allows gradients
- Increase (or decrease) the size of specific rows.
- Preview how your rules will look while you are creating them:



Remember: ‘Filters’ can use a specific ‘Display Theme’

Alerts Workflow Improvements

- **"Control WorkStation" Action:** Added the option to specify where the dock window for items shown should be opened. It is now possible to select from:
  - Opening the item in the current 'default' window if one is available, otherwise creating a new 'default' window
  - Using an already open window for the same type of item, otherwise opening in a new window
  - Always opening in a new window
- **"Control Workstation" Action:** Added the ability to show entities from the context of the action, rather than only showing the explicitly selected items. This means that the CCTV footage or Schematics Map shown will dynamically change depending on which entities the context of the action references, only showing the relevant footage/map each time.

Operator Permissions & Layouts

- **Layouts:** Added the ability to select a default dock window to use for showing CCTV footage and Schematic Maps from context menu commands, rather than always opening in a new tab. This allows the 'Show Video' and 'Show In Map' commands to always show the corresponding item/s in a selected Window, which can be stored as part of a layout, allowing multiple items to be shown one after the other, all in the same window. The default window can also be used to ensure items opened using the Control Workstation command always open in the same location.
- **Operator Restriction:** Added the ability to prevent an Operator Type from being able to change the default sorting of Entity Lists. This allows information to be laid out in a set format, with priority items always showing at the top.
- **Operator Restriction:** Added the ability to prevent an Operator Type from being able to apply filters to columns in Entities Lists. This ensures that no Entities can be hidden from view due to a filter being applied to the list.
- **GateKeeper Restriction:** Added the ability to prevent an Operator Type from closing GateKeeper, ensuring the software is always left open.
- **Restore Layout:** Added a button to the ribbon to easily restore a layout back to its saved settings, reverting any changes made to the layout since it was last saved.
  - **Operator Restriction:** The new 'Can Factory Reset Layout' option can prevent operators from unloading their assigned layout.

Quality of Life Improvements

- **Operator Types Editor:** Type categories are now organised by their location in the System Designer ribbon, and can be manually searched by name when looking for a specific type. A new "Top Level" check box makes it easy to change all settings.
- **Guard Tour Editor:** A tree view (similar to the "Running Tour" view) makes it easier to create groups in Guard Tours.
- **Guard Tours:** Operator 'View permissions' on Guard Tour Definitions now apply to the running Guard Tours window.
- **Scheduled Tasks:** Next Time Trigger column is now a DateTime instead of a string
- Triggers:
  - All Triggers: Added an optional "TimePeriod" qualifier (with invert bit)
  - Review / Door/Area Triggers: Added User match mode to allow them to only work for some users.
  - Using DoorLists in Door / Area Triggers now required only a server restart to pick up changes in door list programming (as opposed to re-editing the trigger).

  - The ability to specify just access granted / denied / or either to Door Area Triggers
- **Door Editor:** added support for 2 badge arm modes, and allowed editing from the arm mode from within the reader edit fly-out.
- **Timed Door Unlock:** When unlocking a door from the software, the prompt asking for the unlock duration now defaults to the unlock time for the door, (or 5 seconds if a time is not specified)
- **Reports:** The new “X Reference” Report shows direct relationships between entities in the system - for example, which users have been assigned certain permission groups.
- **Email Sender:** Emails can now be sent in HTML format
- New License Plate Recognition:
  - **LPR: Coalesce Ambiguous Characters –** Optionally makes LPR more reliable by treating 1/I or O/0 as the same char.
  - **LPR: Ignore Case –** Optionally makes LPR case insensitive.
  - **‘Associated Door’** now correctly identifies the reader in all cases.
- Improved editor & display of ‘Notes’ Custom fields.

Issues Resolved

- **Rest/XML:** Resolved issue where multiple concurrent requests could occasionally return an invalid password error.
- Reduced flickering in live windows on busy systems (particularly review).

Bug-Fix Release (v 18.1.2)

August 2018 - 18.1.2.13952

Issues Resolved

- **Schematics:** Resolved a problem opening maps containing items they have no permissions to see.
- **Schematics:** Resolved issue that caused flip / rotate transforms to not always be applied in view mode.
- **Schematics:** Resolved issue that caused groups containing icons to be hidden.
- **Pager Message Sender:** Added “OK” as a valid message ACK. Custom ACK messages can now be configured.
- **Communications Handlers:** Any handlers that are stopped due to errors are now automatically re-started.
- **Review:** Resolved issue when selecting categories in review filters, or when filtering live review to “exclude category”.
- **System Warnings:** Removed the incorrect license warning when more than 100,000 users are in a controller with a Level 5 User expansion Kit.
- **Integriti Mobile:** Review dates are now in local time.
- **Entity State:** Fixed bug that caused state changes to be sent from the controller on the first connection after a “default” even when the controller “Prevent State Syncing” option was enabled.
- **EKOTEK:** Resolved issue that caused user state to not be created.
- **Permissions Editor:** Resolved an issue that caused permissions editors to display the error message: “Year, Month and Day parameters describe an un-representable DateTime”.

Bug-Fix Release (v 18.1.1)

July 2018 - 18.1.1.13342

Mimic Viewer

The Integriti Mimic Viewer is designed as a stand-alone installation of Integriti that maintains its own connection to an Integriti controller. This connection can be made alongside an Integriti Professional connection, via Ethernet or serial. Primarily, the Mimic Viewer is intended to allow local on-site schematic maps to be displayed that don't rely on an Integriti server that is located off-site.

For setups where a centralized Integriti Professional server is located off-site, if connectivity to the central server is lost then the controller will still function normally, but any software clients that are logged in will disconnect. Some of these software clients could be used to show fire alarm, duress or other site information on a monitor on the wall that are critical to OH&S. If this is the case, then the Mimic Viewer product is an ideal alternative that does not rely on internet connections.

For more detailed information about the Mimic Viewer, including usage examples and how to install and configure it, see the Integriti Mimic Viewer programming manual available on the Technicians Downloads section of the Inner Range website.

*This is a stand-alone Integriti product like Professional and Express and hence requires its own product activation key.

Issues Resolved

- **Card Printing:** Resolved issue that sometimes resulted in User Details not being shown when printing a Card.
- **Site Defaults:** Resolved issue that caused the Site Time and Review Playback Buffer Site properties to not be inherited from parent Sites when not set in a child Site.
- **Guard Tour:** Fixed potential error when showing CCTV footage for a Guard Tour in a new tab.
- **Guard Tour:** Added ability to modify whether or not a Group Step is ordered.
- **System Performance:** Optimisations to system load times.
- **Integriti Mobile:** Fixed incorrect door states shown for DOTL and Door Forced states.
- **Review:** Review from foreign Controllers now correctly translates the names, and references the "other" Controller's items.
- **EkoTek Listener Service:** Fixed bug resulting in received location updates not being generated.
- **EkoTek Listener Service:** Fixed issue preventing associating multiple Repeaters with the same Area/Location.
- **EkoTek Listener Service:** Fixed an issue where System Warnings were not removed from Entities when these alarms were claimed in the EkoTek software.
- **EkoTek Listener Service:** Fixed issue that could result in 'Multiple Entity' problems stopping the service rather than just displaying a warning.
- **EkoTek Listener Service:** Claimed/Raised alarms caused by Repeaters now only display the Repeater name once.
- **REST/XML Interface:** Fixed issue that caused the DateTimeGenerated field to be overwritten with the current insertion time. This now only happens if the DateTimeGenerated is more than 1 day in the future.
- **Communication Services:** Fixed issue that prevented the IPXmit, Review Receiver and Review Sender Communication services from being able to start again after being stopped by the software without a server restart.

- **Schematics:** Added support for importing SVG files containing foreign elements.
- **Schematics:** Fixed potential issue resulting in some elements not showing up on a map until a state change occurred.
- **XML Import:** Fixed potential issue importing items into Integriti that could result in properties not getting set correctly.
    - **NOTE:** Items must be re-exported to resolve this issue.

Feature Updates

- **UI Update:** Resolved several issues when using high DPI displays.
- **Audit:** Changes to Integrated Devices and Communication Handlers are now audited.
- **Guard Tour:** Improvements to current step overview in the Guard Tour Summary.
- **Firmware Update:** Software now provides a warning when attempting to update a Controller's firmware to a version newer than the software version.
- **Operator:** Last Login and Login Count are now stored for Operators.
- **Schematics:** Added the ability to cancel setting an SVG file and a notification when taking longer than expected – The 'Esc' key can now be pressed while the image is being rendered to cancel the import (the progress form must be focused for this to work)

NEW IN VERSION 18.1

April 2018 - 18.1.0.13171

Schematics Animations

Make your maps come alive with flashing text and animations!
Default Element-Presenters have been updated to include visual indications when alarm / tamper states are active.
This can be customized in the element presenters “Animation Settings”.
Animations allow a 2-frame animation to be applied separately to the “Shape”, “Icon”, and “Label” formats within an element presenter (on conditions of your choice). Allows elements to flash or pulse, and also change size.

Guard Tour

“Guard Tour” helps you organise, log, monitor and execute routine security tasks, improving safety, security and accountability for your staff.

- **Real Time Tracking:** When personnel are conducting their predefined tasks, their progress can be monitored in GateKeeper.
- **Overdue Alerts:** When combined with Integriti’s powerful Advanced Alerts engine, email / SMS / popup-windows and more are all possible to ensure staff safety.
- **Flexible Grouping:** Tours can be broken down into groups of sub-steps, and optionally completed in any order. This allows guards to randomize the order of activities (making patrols more difficult to predict by would-be attackers)
- **Accountability & Dispute Resolution:** A comprehensive audit trail easily settles disputes about what patrols (and parts thereof) have been completed.
- **Automation:** As the Guard progresses through the tour, tedious tasks (like re-arming the cleared area) can happen automatically.
- **Scheduling:** Guard Tours can be started manually or as part of a pre-defined Schedule
- **Reporting:** With the reports module, you can always know which patrols were completed each week.

‘Guard Tour Definitions’ are created by the system integrator in ‘System Designer’, specifying in great detail what tasks should be performed in what order, and what should happen when they are completed (or not completed in the prescribed time).

Operators can the Start a Guard Tour manually from Gatekeeper, or the scheduler can automatically start Tours.
*This feature requires a license.

Alerts

The “Finalized Alert” can now show more information in the ‘Alert Summary’ about the history of an alert (including any notes an Operator may have left in responding to an alert)
This Data is also available to reports on Alerts.
The appearance of Alert Views can now be customised with Display Themes, and viewed with ‘Filters’.
*Alerts Definitions can now customize the formatting of the message (previously was just the review text).
*Alerts created with Review Triggers can now specify a separate review filter to be used as a ‘restore’

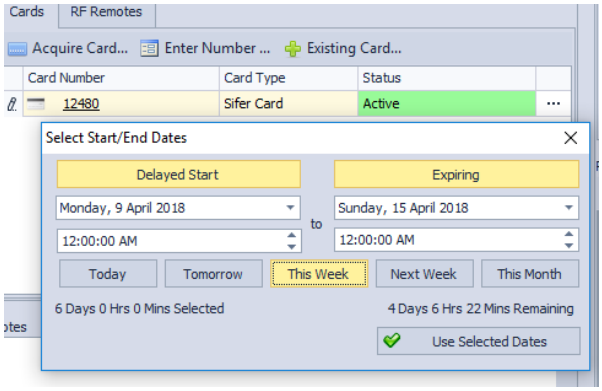
*Requires an Advanced Alerts license

64 Bit Integration Server

The new 64-Bit integration server allows new integrations to utilize expanded memory and resources available on 64-bit servers.
The existing 32-bit Server is still installed as well to support older integrations that require a 32-bit host.
Integriti will automatically load any plug-in with the correct Server.

Cards (Expiry & Temporary Replacement):

Individual Cards can now be expired (or given a future start date)
Convenient UI shortcuts facilitate common tasks, like when a User needs to be given a temp card for the day.
These are available from the User Edit Screen.
Cards now have new Status types so you can easily know / report on which cards are temp cards.
Cards also reference which card they are replacing, making it simple to track down the history of any cards.



More Powerful Custom Enhancements

Inner Range Professional services have more power than ever in being able to customize the Integriti platform to individual Customer requirements.
OnSave Triggers
Customized Context Menu Commands
*Custom Enhancements are quoted by Inner Range professional services on a per job basis.

Mobile Reader

With “Mobile Reader”, your Security Officers can easily verify personnel credentials, and perform evacuation mustering from their compatible mobile device.
Credential Check: Simply swipe a user’s access card instantly see the associated users on file photo, and relevant details. Guards can then activate (or de-activate) the swiped card on the spot.
Mobile Muster: In the event of an emergency, Security Staff can easily see who is still in danger (and where they are), as evacuating staff swipe at either fixed muster points, or directly at the “mobile reader”.
*This feature requires a license.

EkoTek Listener Communication Service

Monitor and track the location of assets and personnel with the new EkoTek Integration.
*This feature requires a license.

Quality of Life enhancements

- New **Review Filters** can now be easily created from existing windows
- **Schematics** can now handle a wider variety of SVG files.
- **LPR** – The License Plate Recognition feature now allows more control over which reader is used for LPR.
- **Time-On-Site Report:** A new mode allows processing based on 'Location Changed' review (as opposed to Access review)
- The **REST / XML** interface Documentation is available at http://127.0.0.1/doc/XmlApiDoc.html (when licensed and configured)
- **Reports:** Global parameters have now been added to reports to allow the report designer access to information like:
  - Who ran the report
  - Who / When the report was last edited
  - The date range of the report
- **Show on Map:** Right click on any item in a list, and you can easily open the schematics map this item resides on.
- **Grant Amnesty:** Right click on a user and choose 'Grant Amnesty' to easily resolve anti-passback issues.

- **Schindler HLI:** Custom fields can now use more 'Custom Field Types' (for example ComboBox can now be used where previously only a Text field was allowed)

Bug Fixes

- **Qualifications:** fixed an issue that caused qualifications with multiple triggers to sometimes fire all triggers actions when any trigger happens.
- **Schindler HLI:** Fixed bug that caused inactive cards to be sent to the external system as active cards

Bug-Fix Release (v 18.0.4)

March 2018 - 18.0.4.12783

Issues Resolved

- **Schematics:** Fixed issue that caused initial state to show incorrectly, (when many state changes occur during map load)
- **Application Layer HA**: Improved Server to Server communication security & robustness.
- **Scheduled Tasks:** Fixed issue that caused some tasks to no longer be editable (if created in older versions).
- **Photo ID:** Fixed an issue that caused long labels with black text, using the “best fit” sizing option to sometimes be truncated.
- **Photo ID:** Fixed issue that caused ‘delete’ to fail for some card designs.
- **Workstations:** New properties let you see when each workstation was last used (from system designer) and they can be deleted. Ensure no Task Actions (schedules / Alert Definitions / etc) reference a workstation before deleting it.
- **System Performance:** Optimised the System Designer Tree display of hardware state.
- **Active Directory Integration (Users):** Increased performance of user sync and fixed memory leaks.
    - **Note:** Upgrading customers may still have configurations that manually specify the ‘key’ field. This is no longer the recommended way. A manual key incurs significantly more performance overhead than using the newer (introduced in V4.1) ‘built-in’ custom field key. To change an existing system to use the newer method:
        1. Ensure a full sync has been completed with the newer software, and that all your AD Users have a correctly populated ‘cf_ActiveDirectoryGuid’ custom field.
        2. Ensure none of the column mappings have the “key” column checked. (this column is now hidden by default, it can be found by right clicking in the column headers -> Column Chooser.)

Bug-Fix Release (v 18.0.3)

January 2018 - 18.0.3.12579

Issues Resolved

- **Date/Time Editor:** Fixed an issue caused date editors (like User Expiry).
- **Gatekeeper:** Fixed label on Review Group in Window Tab.
- **Web Interface:** Resolved issue that caused the “Use HTTPS” option to not work.

Bug-Fix Release (v 18.0.2)

January 2018 - 18.0.2.12543

Issues Resolved

- **REST/XML:** Fixed an issue that caused some items to not be able to be deleted by Address.
- **Controller Connect Dialog:** Fixed occasional issue that caused the ‘Connect Manual’ window to not show up.
- **Reports / Filters:** ‘System Warnings’ can now be filtered / reported on.
- **SIFER enrolment station:** Made confirmation BEEP’s louder when cards are detected.
  SIFER large LED indicates the connection status:
  - White (SIFER has power, but is not connected)
  - Blue: The Acquire Card dialog is open and communicating with the reader.
  - Green (momentary flash) indicates a card was read.

Bug-Fix Release (v 18.0.1)

January 2018 - 18.0.1.12501

Issues Resolved

- **User-Door Recent Activity:** Fixed an issue that caused the User Door recent activity window to sometimes show no results.
- **Operator Permissions:** Review events are only visible to operators who can 'see' the source 'control module'. This has always been the case, but is now also enforced from the Web Interface and Reports.
- **Operator Permissions:** Door Override commands can be hidden via the new 'Send Override Commands' option in operator types.
- **Schematics:** Resolved an issue that caused clients that updated via 'Auto-Client-Update' to not be able to render maps.
- **Schematics:** Fixed issues in the 'Bulk import maps' feature.
- **Schematics:** Fixed an issue that caused some clients to freeze when changing item colours in design mode.
- **User Qualifications:** Credit deductions are no longer Audited by default.
- **User Qualifications:** Fixed a bug that caused all credit deductions to be actioned whenever any single trigger activated.
- **Web Client:** Removed access to entity types Operators are not allowed to see (based on their permissions).
- **Web Client:** Fixed issues in list sorting / filtering
- **Web Client:** Fixed PIN editing of users
- **Web Client:** Custom fields are now editable
- **Web Client:** Fixed a bug that allowed the created timestamp to be overwritten

VERSION 18

January 2018 - 18.0.0.12448

Vector Schematics

An all new vector-based schematics rendering engine allows maps to smoothly zoom in & out forever while always looking crisp and professional.

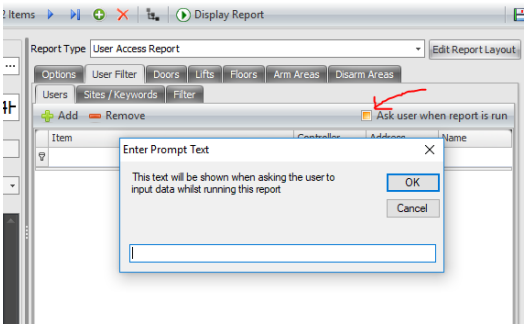
* See the section “Vector Schematics – New Features in detail” for more information on the Improvements to Schematics.

Review Event Log Improvements

The new ‘Review DBs’ list lets you see and manage where your review records are.
Review queries are cancellable, and show progress.
Introducing review ‘Categories’ (formally known as Transitions). Filters and reports now let you easily select categories and sub-categories when looking for review
All external Databases are now created with a ‘date range’, this is encoded in the name, as Year_Quater. For example, ‘IntegReview__2017_Q3_0’ will only contain review records that were **generated** in July, August, September or 2017.
New Database clean-up actions can now efficiently ‘obliterate’ all old review in accordance with your data retention policies.
The Application Server now has a **Review Ram Cache** to improve performance, the size of this cache can be configured in Administration -> Servers.

Interactive Reports

Each filter / property of a report can now prompt the user running the report for a value each time the report is run.
This means low level operators no longer need the rights to edit reports to just change a single parameter each time the report is run.



Operator Action Confirmation

Specific Doors / areas / list of the above can now be configured to prompt for a confirmation before control is allowed.
Lists must be explicitly configured for confirmation (it does not happen just because it's items are configured as such)
This is configured with the new ‘Requires Operator Confirmation’ option in entity programming.

Application Layer High Availability

Customers who require Enterprise grade reliability can now run multiple instances of the Integriti Services at the same time.
Controllers / Clients automatically connect to available nodes to ensure an “always on” experience.
This feature requires additional licensing and is quoted on a per site bases. Contact Inner Range Professional services for more information.

Licence Plate Recognition

Licence Plates can now be used as credentials when used with compatible CCTV Systems.
*This feature requires a license.

Sky Reader – Mobile Application Support

Guards can check the validity of credentials from their Android device (IOS coming soon). When valid cards are presented to the phone, an image of the PhotoID attached to the card is immediately shown.

IP XMIT Service – New Communications Handler

When enabled, all XMIT review records are transmitted to the connected automation system.
This feature requires no additional controller support, and is in addition to the native alarm reporting capabilities of the controller. This means if the controller has an alarm reporting comms task, and this feature is enabled, 2 messages would be sent to the control room for each alarm / restore.
*This feature requires a license.

Quality of Life enhancements

- Communication Handlers & Integrations can now have a “Run Mode” so they can be easily disabled, and can have a Server affinity.
- Communication Messages now have additional **local** ‘Created’ and ‘Sent’ times. (in addition to the existing UTC ones)
- User Access Report - Renamed "On Areas" and "Off Areas" tabs to "Arm Areas" and "Disarm Areas" respectively
- Report Configurations - Added Display Names, Categories and Descriptions to fields in Reports that didn't previously have one.
- Format Strings: Added new pre-sets for numeric and date datatypes
- XML / REST Interface can now perform any ‘control’ action by POSTing the XML.
- XML / REST Interface can now perform queries by POSTing an XML filter.
- XML / REST Interface can now retrieve users without pictures by specifying **User_noImages** as the type name.
- Commands invoked by operators from Edit Dialogs can no longer be ‘accidentally’ pressed when (for example) double clicking through a hyperlink. If the button is pressed within a second of the window coming to the foreground, a confirmation is required.
- Active Directory/CSV Import Transformations - Gave the option to limit search results to a particular site (and its child sites) for the Name Lookup Transformation
- Enrolling / presenting SIFER cards at a SIFER Enrolment Station now saves the CSN with the card.
- Server heartbeat frequency is now configurable
- Diagnostic ‘Log Viewer’ now has a handy “Zip for Export” button.
- LAN modules now have a Battery Life property (years). The system automatically sets the ‘Battery Needs Replacement’ value to true when it is too old, based on the programmed installation date, and the configured ambient temperature.
- Send user Messages can now use ‘System Settings’ to customize which senders are used

- Send PIN can also have its message customized / Translated via 'System Settings'
- Integriti Web: Added support for Custom Fields to user editor
- Recent Activity Report (from the right-click menu of any entity): Has been upgraded to use the regular review control. While it can no longer be arbitrarily sorted by any column, it now has the usual review context menu's, and colouring.
- Schindler Lift HLI: Access review is now given its own category, and is tied to the user, so they can show up in activity / access reports.

Issues Resolved

- CCTV Viewer - Added the actual error message to status message shown when starting video stream fails
- Review Filters in gatekeeper now show in 'real' Review windows that can be 'live' and are correctly coloured
- Format Strings: All date times (even custom fields) can now be formatted
- Cards: Fixed an issue that caused cards with 'all zero' data to be incorrectly sent to controllers (resulting in erroneous credential clashes)
- Item Editors - Fixed a bug that resulted in the 'Unsaved Changes' warning being shown when nothing has changed for some windows that contain 'filters'.
- Fixed an issue that caused database restores from some previous versions to not allow login due to 'insufficient client licenses available'
- Fixed an issue that prevented the importing of some Integrated Devices
- Disabled Time & Custom Item change triggers now correctly obey the 'disabled' setting.
- Web Interface: Made it impossible to delete the "What" entity, leaving a blank permission row

Vector Schematics – New Features in detail

- New file format support in addition to the current raster-based file formats.
  - SVG – Scalable Vector Graphics file format for map background, image elements and element presenters.
- Map Properties:
  - Background border colour and width.
  - Zoom settings: max and min zoom value for the map.
- Element Properties:
  - Selectable – specify whether the element can be selected through mouse clicks.
  - Zoom behaviour settings: This lets us control how the element will behave when the map grows and shrink during zooming in and out. The available options are.
    - Dynamic size: This attribute lets us describe how the element should size in relation to different zoom levels. Options available are:
      1. Element should size with background (the default);
      2. Maintain a constant size;
      3. Maintain a constant size within a specified zoom range.

Option 2 and 3 lets the element maintain a constant size even when the map grows and shrink during zooming in and out. For these two options the user needs to specify a zoom position. The zoom position tells where the element is going to stay on the map as the map grows and shrink during zooming. The options for zoom position in relation to the element are:

1. Top – Left
2. Top – Centre

3. Top – Right
4. Centre – Left
5. Centre – Centre: The default
6. Centre – Right
7. Bottom – Left
8. Bottom – Right
9. Bottom – Left
10. Specify A Position: For this the user will need to specify the Dynamic Size Zoom Position which are the mouse x and y position on the map.

In addition to specifying the zoom position, for option 3 the user will need to specify the zoom range for which the element size remains constant.

- Dynamic visibility: This attribute lets us control the visibility of the element in relation to zoom level. The options are
  1. Always Visible:
  2. Visible Within Range: The element will only be visible within a given zoom range. For this the user will also need to specify a zoom range.

- Element selection highlight:
  - Box selection for rectangle, icon and image elements.
  - Border/line selection for ellipse and line elements.
  - The selection is highlighted using animating dashed white and black lines overlaying each other. The selection animation occurs for only a brief period of time.
- Smooth transition:
  - Smooth zoom transition.
  - Fade in and out transition for element selection.
  - Fade in and out transition for element visibility.
- The map rendering is resolution independent. A 100% view means the map will be completely shown to fill the viewable area irrespective of the size of the viewing window.
- Zoom in and out buttons.
- A text box to specify a zoom level in percentage.
- A zoom and position reset button which centres the map at 100% zoom.

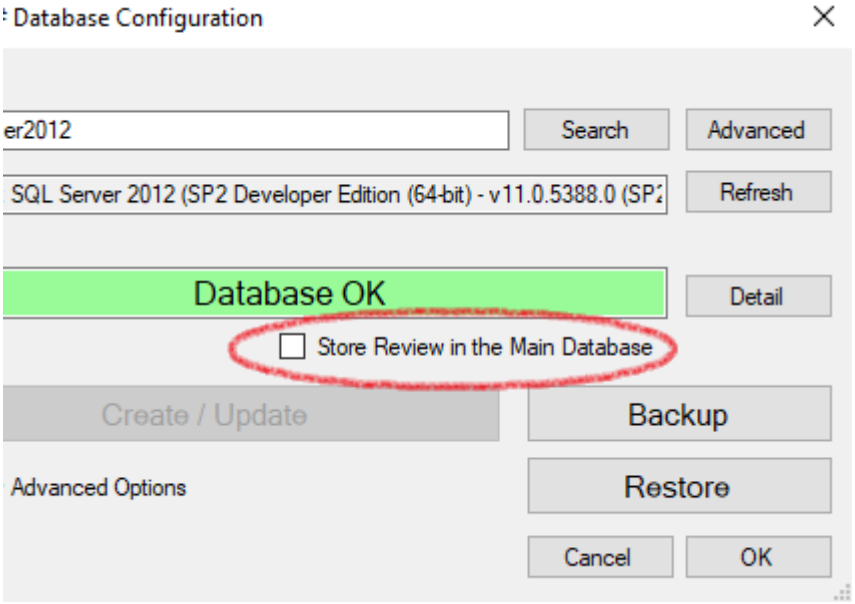
A movable and expandable (drop down) layers menu placed on the top left corner of the map. By default, when opening a new map, the layer menu is shown only when layers are available.

APPENDIX

V18 REVIEW IMPROVEMENTS

V18 significantly improves the 'Review' Event log subsystem

It is now strongly recommended that Review is not stored in the 'main database'.
Ensure the "Store Review in the Main Database" checkbox is NOT checked in the "Database Configuration" utility.



The Application Server will automatically migrate all historic review to the new system. Your system will continue to work as normal while this happens in the background, but historic review will not show up in filters / reports until the migration is complete. Migration typically occurs at approximately 100,000 events per minute.
Ensure enough **additional** disk space is available in SQL server to store all of the existing review **again** before upgrading to this version. (approx. 1GB per million review records)
If your old review was stored in external databases the additional disk space can will be freed once migration has completed. If existing review was stored in the main database, your DBA or Inner Range Professional services can 'shrink' your database to reclaim this space.