INTEGRITI BOSCH SECURITY ESCORT INTEGRATION

Document created with reference to Integriti Professional software version v19.1.0.15471

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

ASIAL MEMBER
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
GOLD MEMBER

Certified System
Quality
ISO 9001

Integriti Bosch Security Escort Integration Manual

Table of Contents

Integriti Bosch Security Escort Plugin Compatibility

Required Integriti Version

The Integriti Bosch Security Escort Plugin is only compatible with an installation of Integriti Pro or Infiniti that is v19.1.0 or higher.

Tested Against

The Integriti Bosch Security Escort plugin was built and tested against the following:

- Bosch Security Escort software v3.1.0

Configuration

Installation

Close all instances of the Integriti software suite on the PC to install the integration on, including stopping all running Integriti services (if installing on the Integriti server).

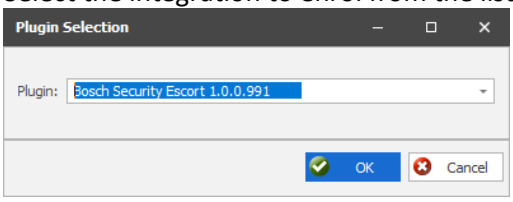
Download and run the integration's installer on all Integriti servers first, before running on all client workstations that will be editing and invoking commands on the integration.

After the installation has completed, remember to start all of the services that were stopped prior to running the installation.

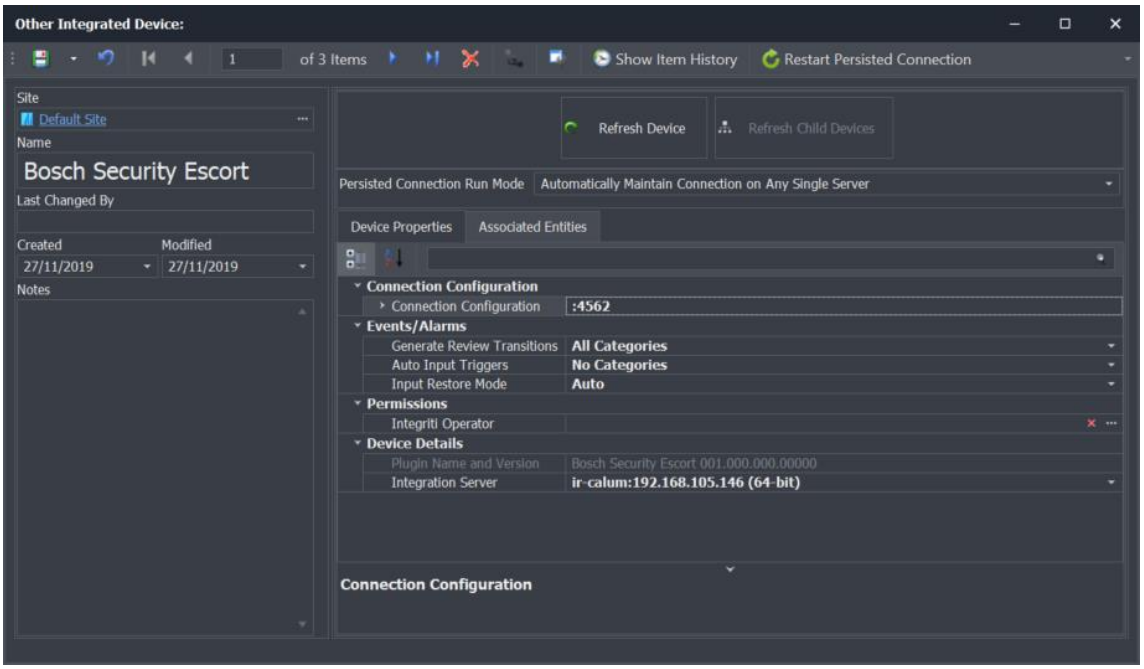
If reverting to an earlier version of an Integriti Integration, ensure that the currently installed version of the integration is uninstalled prior to installing the earlier version.

Enrolment

1. In Integriti System Designer, select 'New Integrated Device' from the System tab.
2. Select the integration to enrol from the list that appears and press Ok.



NOTE: The same version of each integration must be installed on both the Integriti Integration Server and on the Integriti Client Workstation that is enrolling the integration for it to be enrolled.
If the desired integration does not appear in the drop-down list, ensure that both the 32-bit and 64-bit Integriti Integration Servers are running.

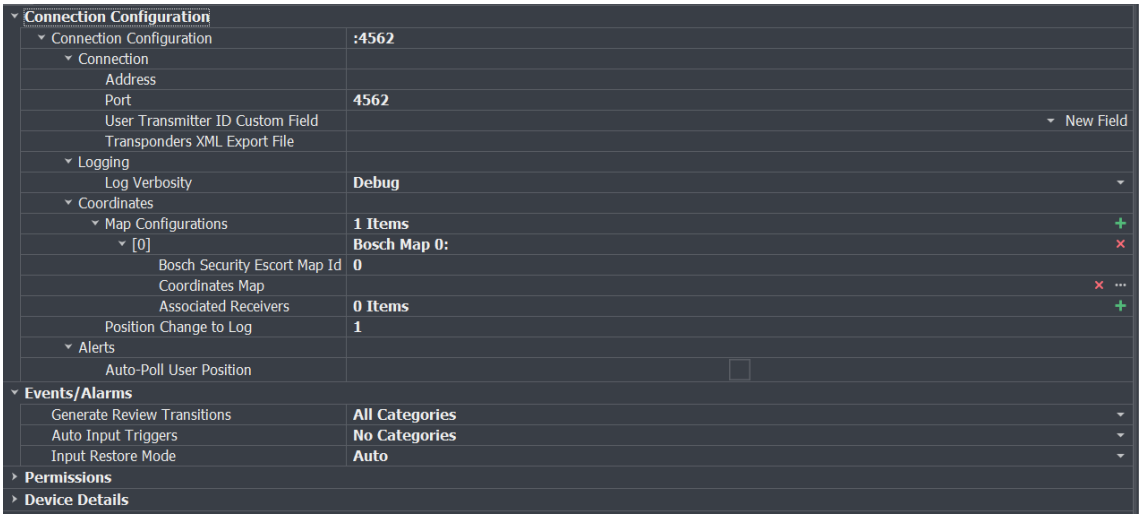


3. In the editor window that appears, give the newly created device a Name and optionally enter some Notes describing the device.

4. **Persisted Connection Run Mode** - Select the preferred Persisted Connection Run Mode. This is necessary for features such as event and camera state monitoring. This typically does not affect the ability to view video or invoke commands on this device and its child devices.

   The following options are available for the Persisted Connection Run Mode:
   Automatically Maintain Connection on Any Single Server – This is the recommended option if a persisted connection is to be enabled and will ensure that there is always one Integriti Integration Server connected to the 3rd party system, provided at least one Integriti Integration Server is available.
   In high availability systems, if the Integriti Integration Server that this device's persisted connection is running on goes offline, the persisted connection will automatically start up again on another running server.
   Maintain Connection on the Specified Server – This option will run the persisted connection to the 3rd party system only on the specified server and no others. This is the best option to use if only one of the available Integration Servers is able to connect to the 3rd party system. If the specified server goes offline, the integration will lose its connection to the 3rd party system until the specified integration server comes back online.
   Simultaneously Maintain Connection on All Servers – This option will establish a persisted connection to the 3rd party system on every Integriti Integration Server at the same time. This can result in the most simultaneous connections to the 3rd party system, and can result in duplicate Review Records being logged for events received from the 3rd party system.
   Disabled – Disables the persisted connection to the 3rd party system for this device. This option should only be used if event and state monitoring are not required from this device and will result in one fewer connections being made to the 3rd party system at all times This may be useful if only a limited number of simultaneous connections are permitted by the 3rd party system.

5. **Connection Configuration -** On the 'Device Properties' tab, under 'Connection Configuration', configure the integration specific properties, including details on connecting to the 3rd party system.



Connection

- **Address –** Enter the address of the machine with the Bosch Security Escort Software installed. The Bosch Security Escort software must be running for a connection to be made.
- **Port –** Enter the port to use for communications with the Bosch Security Escort Software. This can be found (and configured) in the Bosch Security Escort Software under Network->System Directories and Network Address->Remote Control Listening Port.
- **User Transmitter ID Custom Field** - Select the Custom Field for storing the Bosch Security Escort Transmitter ID to associate with Users
- **Transponders XML Export File –** Export the Transponder Database from Bosch Security Escort as an XML file and place on the Integriti Integration Server. The path to this file should be specified here.
  The Transponder Database can be exported from Bosch Security Escort by opening the Transponder Database, selecting Export and making sure to export as XML.

Coordinates

- **Map Configurations –** Configure which Integriti Schematics are associated with which Bosch Security Escort Receivers. This should be left empty until after the device has been refreshed.
- **Position Change to Log –** Changes to a User's position will only be logged after they have moved more than this percentage of the area of the current map. Users changing floors will always have their new positions logged.

Alerts

- **Auto-Poll User Location -** Set to True to automatically poll the location of supported Users from the Bosch Security Escort system when those Users are associated with an active Alert. User location will be polled at the frequency specified in 'Auto-Poll User Location Frequency'.

- **Auto-Poll User Location Frequency -** Select the frequency at which to auto-poll for current User locations if 'Auto-Poll User Location' is enabled.

6. Select the Save button to save the newly created device.
7. Ensure ‘Transponders XML Export File’ has a valid file path and press the Refresh Device button. This will automatically populate the Map Configuration with the Bosch Security Escort configuration.
   It may be necessary to close and re-open the editor for the Bosch Security Escort Integrated Device for the new options to be loaded into the configuration.
8. Go through each of the Map Configurations and specify an Integriti Schematics Map to associate with the selected Security Escort map configuration. This will be used for converting coordinates from Bosch Security Escort to Integriti’s coordinates scheme. This Schematic should line up exactly with the Bosch Security Escort map, with each corner of this map being the same coordinate as the equivalent corner in the Bosch Security Escort software’s map.

Position Tracking

Updating User Position

Whenever a 'Position Change' event is received from the Bosch Security Escort Software, the location of any associated User will be updated automatically, ensuring that the User's location always matches the location sent from Bosch Security Escort.

Position Change Events

Position Change events are sent from Bosch Security Escort in three scenarios:

- When an alarm/event is active on a transponder, position updates will be sent on a regular basis, ensuring the user's position is kept up to date.
- If Auto-Poll User Position is enabled in the Integriti Integrated Device, all Integriti Users with a valid Bosch Security Escort transmitter, who are associated with an active Alert in Integriti, will have their current position will be requested at the frequency specified by Auto-Poll User Position Frequency.
  NOTE: 'Supervision' must be enabled for the associated Transmitter in Bosch Security Escort's Subscriber Database for the request for the User's current position to work.
- When a 'Request User Location' command is sent, if the specified transmitter is found, a corresponding Position Change event will be generated.
  NOTE: 'Supervision' must be enabled for the associated Transmitter in Bosch Security Escort's Subscriber Database for the request for the User's current position to work.

Associating User with Transmitter

For Position Changes to be associated with a User, it is necessary to associate the id of each transmitter from the Bosch Security Escort system with the corresponding User in Integriti. This can be done by setting the 'Bosch Security Escort Transmitter Id' property of each User to the ID of the Transmitter associated with them in Bosch Security Escort.
After doing this, any events received from the Bosch Security Escort software triggered by that Transmitter will automatically be associated with the specified Integriti User.
NOTE: The 'Bosch Security Escort Transmitter Id' property will only show up the User edit dialog AFTER the integration's persisted connection has started for the first time.

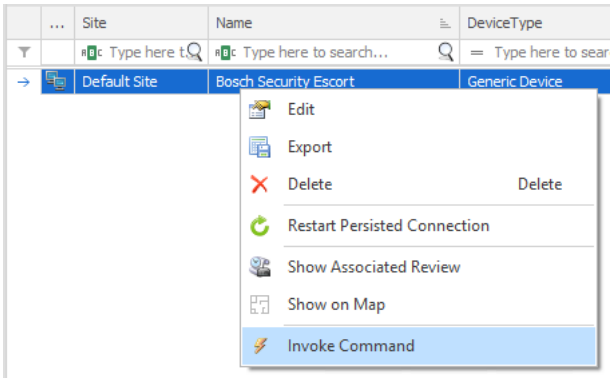
Coordinates Conversion

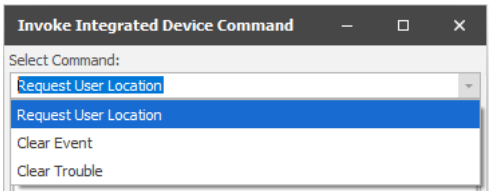
When Position Change events are received from Bosch Security Escort, the coordinates received will be automatically converted from the Bosch Security Escort coordinates scheme to the GPS coordinates used by Integriti.
This conversion is done using the Coordinates Map specified for the Receiver, lining the top left and bottom right corners of the map to line up with the Bosch Security Escort map. For the conversion to give the correct results, it is necessary for the background of the Integriti Schematic to line up exactly with the Bosch Security Escort map, thus ensuring a point in Bosch Security Escort lines up with the same position on the Integriti Schematic.

Invoking Commands

Invoking Commands on Bosch Security Escort

To perform a command on the Bosch Security Escort System through the Integriti software select 'Invoke Command' from the context menu of the integration for the selected server.





From the Invoke Integrated Device Command window that appears, select the required command from the dropdown box:

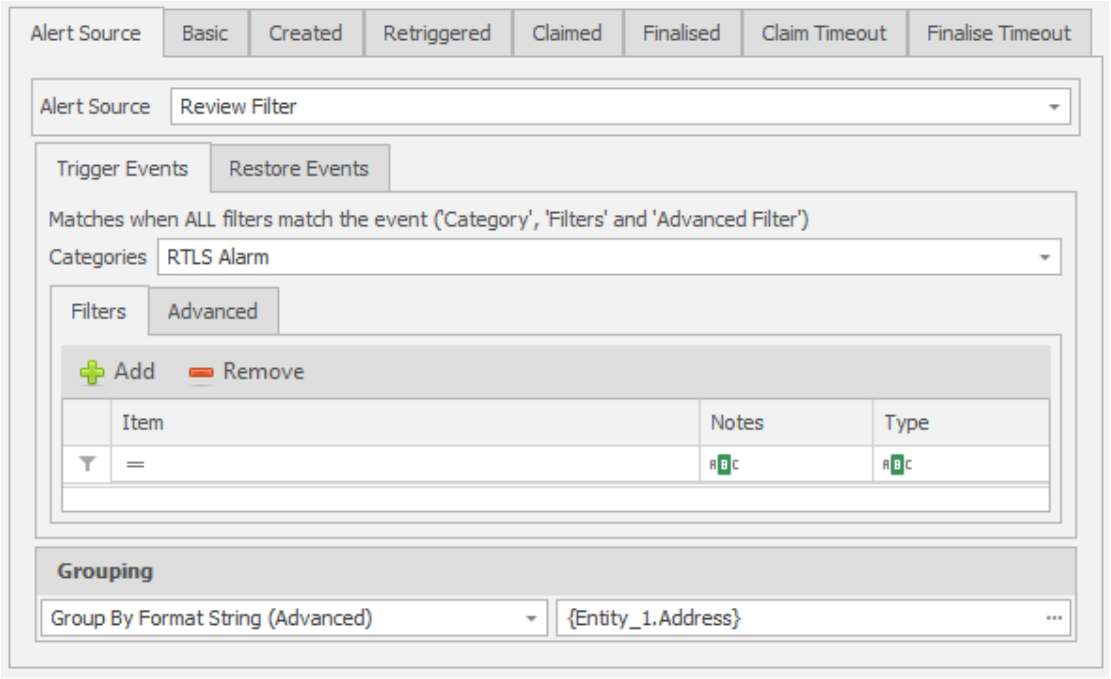
Request User Location	Sends a request for the Bosch Security Escort Software to retrieve the current location of the transmitter specified by the 'Transmitter Id'. If this command is successful, a Position review record will be generated by the integration, and any associated Integriti Users will have their location updated.
Clear Event	Either Clears or Silences any currently active events on the selected Transmitter. When triggering from an Alert that was generated from the matching Bosch Security Escort event, optionally set Alert ID to the ID of the Alert to automatically load necessary options from the triggering event.
Clear Trouble	Clears Trouble of the selected Trouble Type from the Transmitter/Point selected. Point Number should be left as 0 if clearing trouble on a Transmitter. This will remove notifications for the specified trouble on the specified device. When triggering from an Alert that was generated from the matching Bosch Security Escort event, optionally set Alert ID to the ID of the Alert to automatically load necessary options from the triggering event.

Alerts

Configuring Alerts for Bosch Security Escort Alarms

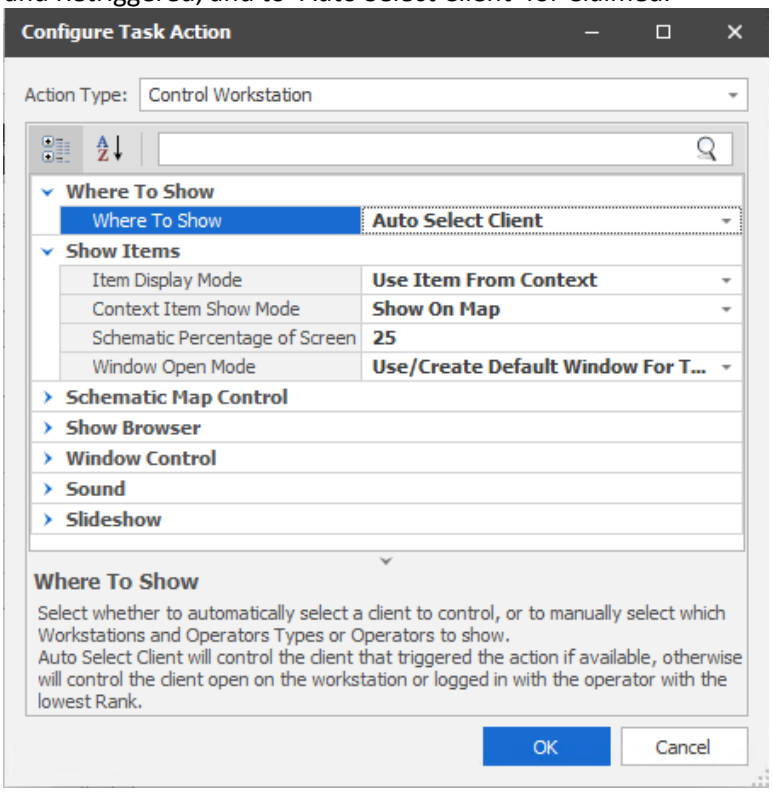
Alerts can be configured to be generated for Alarms occurring in the Bosch Security Escort system. These Alerts can be configured to automatically be generated and restored as the associated alarm is triggered and restored in Bosch Security Escort, and can be grouped to generate one alert per User when using transmitter alarms.

The Alerts can be configured with the following settings:

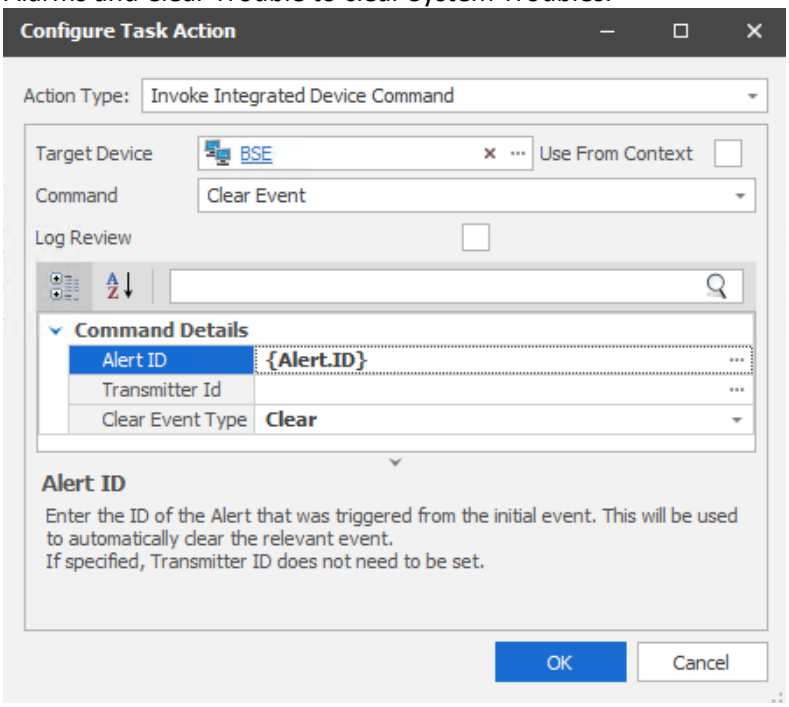


1. Set the Alert Source to ‘Review Filter’.
2. Under Trigger Events select which Categories to generate Alerts for. Select ‘RTLS Alarm’ for general transmitter alarms, ‘RTLS Lanyard Snatched Alarm’ or ‘RTLS Man Down Alarm’ for Lanyard Snatched and Man Down alarms on the transmitter, and ‘RTLS System Warning’ to generate alarms for System Troubles.
3. For Alerts triggering off Transmitter alarms, the Alerts can optionally be grouped by the User generating the Alert. This results in one Alert being generated for each User (or transmitter). This is done by setting Grouping to ‘Group By Format String’, and setting the format string to ‘{Entity_1.Address}’.
4. Under the Basic tab, enable ‘Refresh Alerts On Location Change’. This will automatically update the position of an Alert on the map as new Location Change events are received from Bosch Security Escort.
5. Optionally add a Control Workstation action on Created, Retriggered and/or Claimed to automatically show the User on the relevant Schematic when the Alert is created, retriggered or claimed. Where to show should be set to ‘Manual Selection’ for Created

and Retriggered, and to 'Auto Select Client' for Claimed.



6. To automatically clear the Transmitter Alarm/System Trouble in Bosch Security Escort when the Alarm is finalized in Integriti, add an Invoke Integrated Device Command Action on Finalised with the following settings. Use Clear Event to clear Transmitter Alarms and Clear Trouble to clear System Troubles.



7. Select the save button to save the newly created Alert Definition and start generating the configured Alerts.

Troubleshooting

Plugin doesn't appear in 'New Integrated Device' List	Restart the Integriti Integration Server and restart any instances of Integriti System Designer or Integriti Gatekeeper open on the computer experiencing the problem