inner range

UNIFIED VIDEO, ACCESS & SECURITY SYSTEMS

INCEPTION

Tech Guide - Integrations
June 2024

INNERRANGE.COM

INCEPTION

Contents

Overview

This technical note covers the integration functionality within Inception, documenting all steps required to connect the Inception system to a supported third-party system.

Introduction

Integrated Connections allow the Inception's functionality to be extended beyond the typical intruder and access control functionality already provided, providing rich integration into external systems. One such integration that Inception supports is Inner Range's own "IR Video" range, allowing the Inception to connect to, monitor, and control IR Video NVRs and cameras.

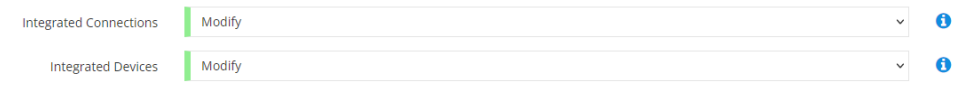
Integrations are represented in Inception as two different components: Integrated Connections and Integrated Devices. The Inception's connection to a third-party device, be it an NVR, camera, or some other device, is stored as an Integrated Connection. A *Refresh Devices* can then be performed against this connection to populate all devices linked to this connection. For example, if connecting to an IR Video NVR, an Integrated Connection is configured with the NVR's details, and then a *Refresh Devices* will pull in all cameras connected to the NVR and populate them in the Inception system as Integrated Devices. The NVR itself would also be configured as an Integrated Device, allowing for its state to also be monitored.

Configuration

Web Page Profile Permissions

This section will provide a walkthrough on fully configuring an Integrated Connection to an IR Video NVR that has multiple cameras attached to it. Before starting, ensure that the IP address of the NVR is known, as well as the NVR's administrator username and password.

First, ensure that the currently logged in user has the appropriate Web Page Profile permission to view and edit Integrated Connections and Integrated Devices. This can be done by navigating to *[Configuration > Users > Web Page Profiles]*, selecting the Web Page Profile linked to the user, and confirming that, under *Item Editing Permissions*, both *Integrated Connections and Integrated Devices* are set to *Modify*.

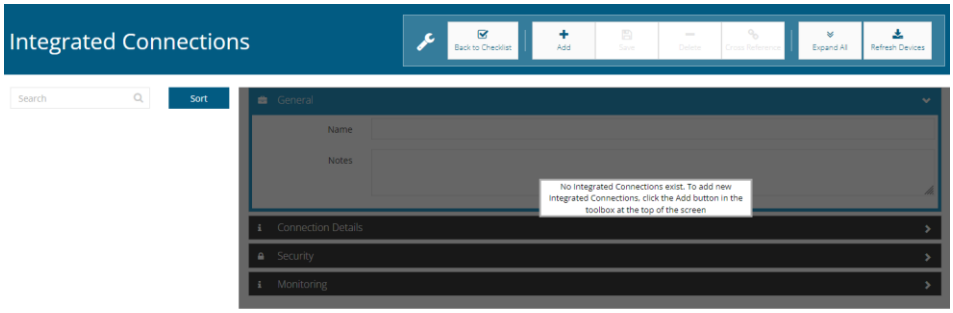


Configuration

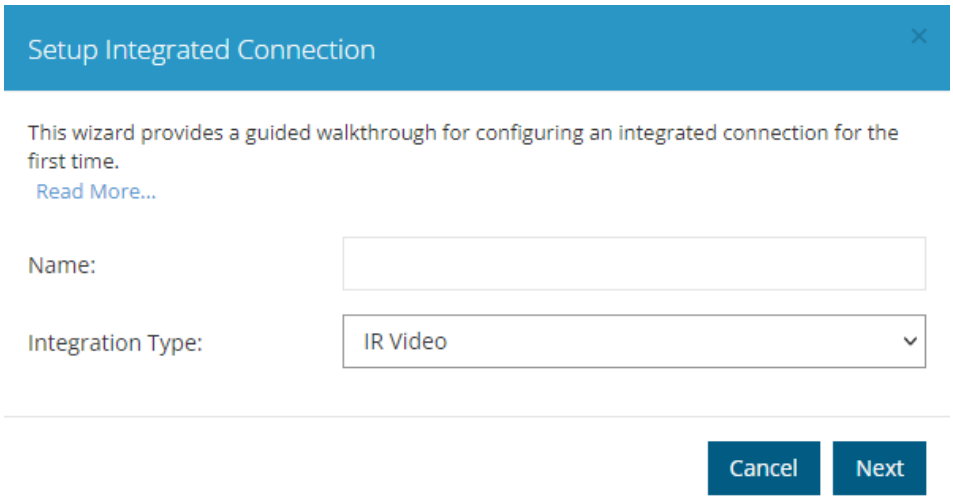
INCEPTION

Creating an Integrated Connection

Integrated Connections can be created and managed on a dedicated page, found by navigating to *[Configuration > Integrations > Integrated Connections]*.

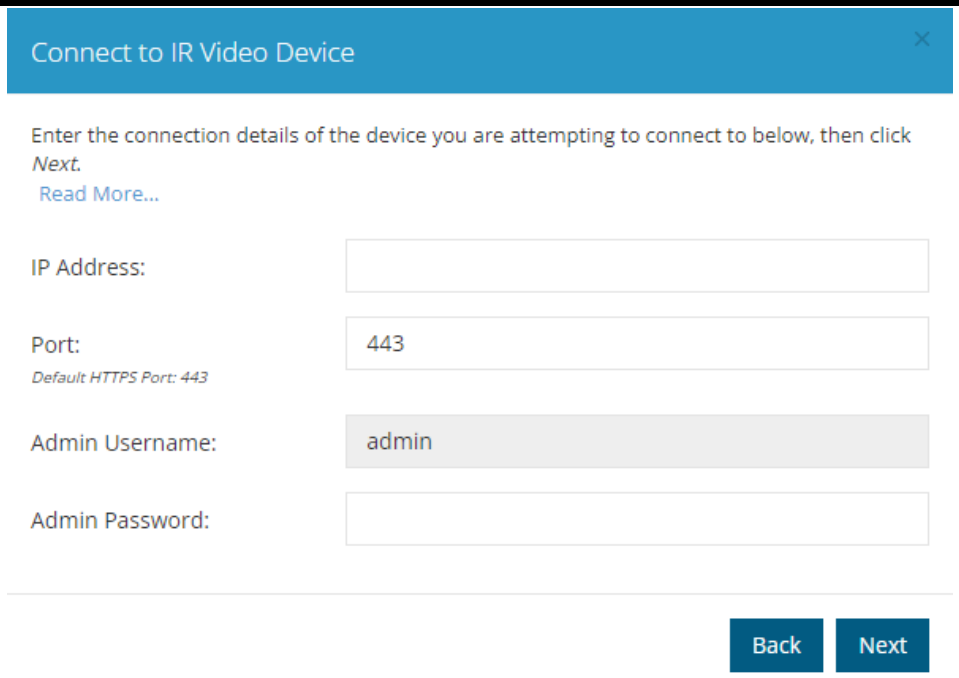


Upon clicking the *Add* button, a guided wizard will commence that will walk through the initial configuration and connection to a third-party device. Note that the Integrated Connection will not be saved until the wizard has been completed, removing any risk of half completed Integrated Connections persisting.

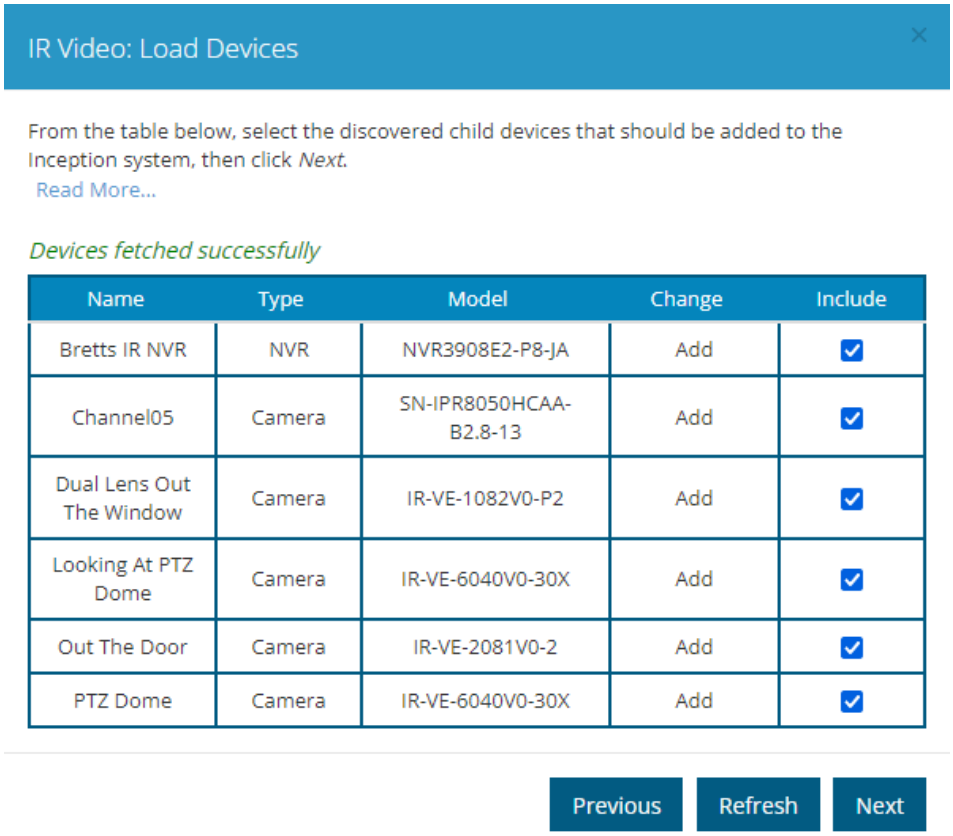


The *Setup Integrated Connection* step allows the naming of this Integrated Connection, as well as selecting the type of integration to use. As at the time of writing, the only supported *Integration Type* is Inner Range's *IR Video*, which is used to connect to our *IR Video* NVRs and cameras. Clicking *Next* will then move on to the *Connect to Device* step.

Configuration



Clicking *Next* will move on to the *Load Devices* step, where any child devices linked to this connection can be pulled.

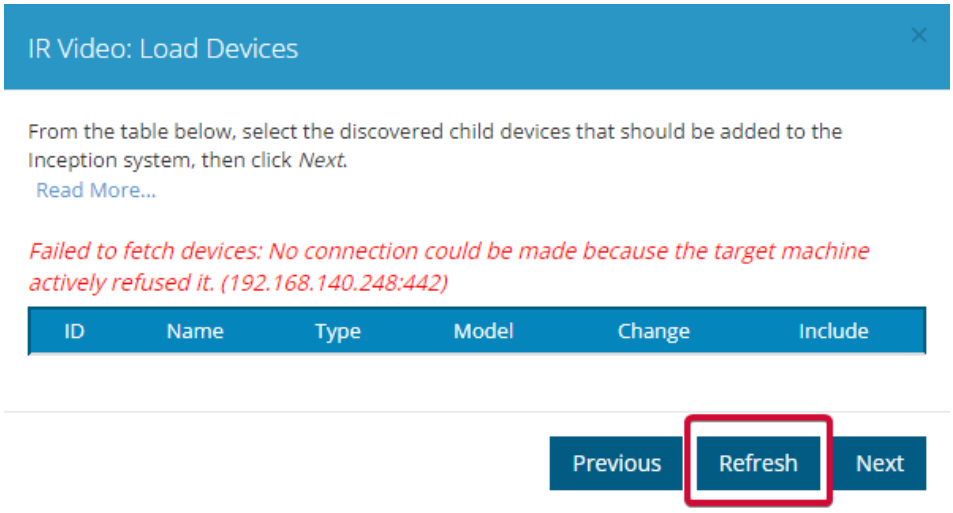


Configuration

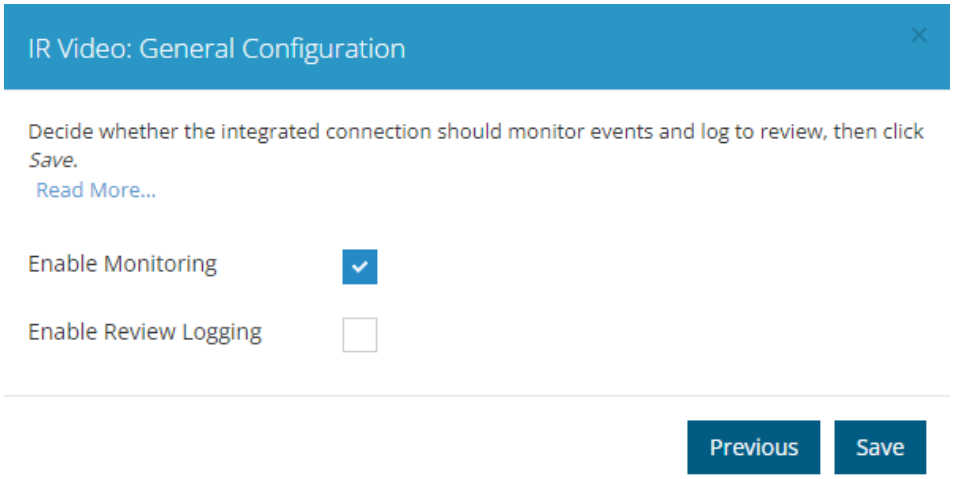
Upon this step being shown, the Inception system will automatically attempt to fetch all devices associated with this connection. The devices fetched could just be one device (for example, when connecting directly to a camera), or multiple devices (for example, connecting to an NVR and fetching both the NVR and all its connected cameras).

The *Include* column allows the selection of which devices to save in the Inception system as Integrated Devices. Any that are not selected on this screen will not be saved in Inception. If in the future these devices are required to be present in the Inception system, a manual *Refresh Devices* will need to be performed (explained later in this document).

If the fetching of devices fails for any reason, an error code will appear above the table, and the *Refresh* button can be used to reattempt the device fetching.



Clicking *Next* will move to the *General Configuration* step.



Configuration

When *Enable Monitoring* is ticked, the Integrated Connection will receive all events sent from the connected device, including any events occurring on any child devices connected to this device as well. If *Enable Monitoring* is ticked, *Enable Review Logging* will appear as an available option. Ticking this will result in all monitored events also being logged to review.

NOTE: It is recommended to leave Enable Review Logging unchecked, as this can result in a large amount of extraneous review events being logged, which could result in the Inception's review limit being reached prematurely.

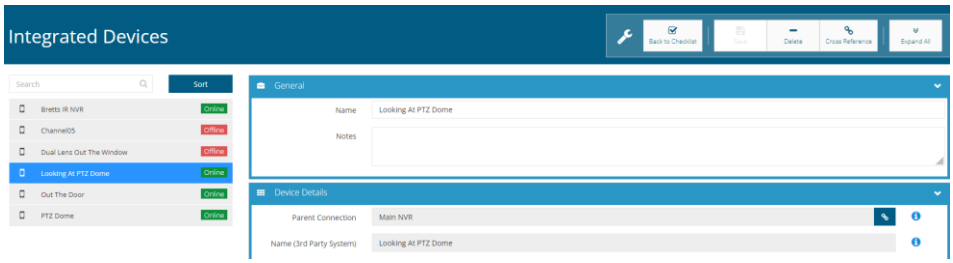
Clicking *Save* will finalize the Integrated Connection process, creating a new Integrated Connection in the Inception system with the settings provided during the wizard, as well as create a new Integrated Device for each device that was marked to be included during the *Load Devices* step.

If, in the future, the *Admin Password* of the Integrated Connection needs to be revealed, this can be done by clicking the little reveal button next to the *Admin Password* field.

This password can only be revealed if the logged in user has the *Allow Password Reveals* checkbox ticked within their *Web Page Profile*.

Integrated Devices

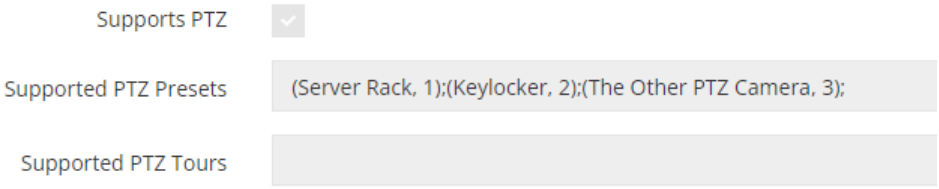
Once fetched from the third-party system, any Integrated Devices linked to an Integrated Connection can be found on the *Integrated Devices* page (*[Configuration > Integrations > Integrated Connections]*).



From this page, Integrated Devices can be managed and deleted as necessary, however they cannot be added. Each Integrated Device has a reference to its *Parent Connection*, as well as a button that directly links to that Integrated Connection.

Configuration

If the Integrated Device supports PTZ, then two additional properties will be displayed in the editor: *Supported PTZ Presets* and *Supported PTZ Tours*.



These values are provided by the Integrated Device and reflect what's been configured on the third-party system. If these presets are changed on the third-party system, a *Refresh Devices* will need to be performed on the parent Integrated Connection.

Refresh Devices

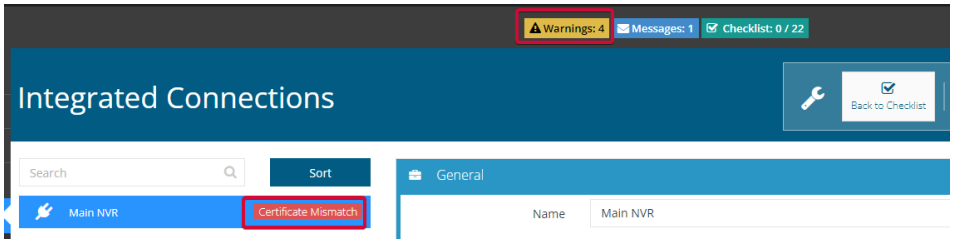
Once an Integrated Connection has been fully configured, it may still be required to repopulate Integrated Devices, due to new devices being added, or existing devices being configured/deleted. This can be done on the *Integrated Connections* page by selecting the Integrated Connection, then clicking on the *Refresh Devices* button.

This will repull a list of all linked devices from the Integrated Device and display them in a table. From here, any desired changes can be included, then applied by clicking *Apply Changes*.

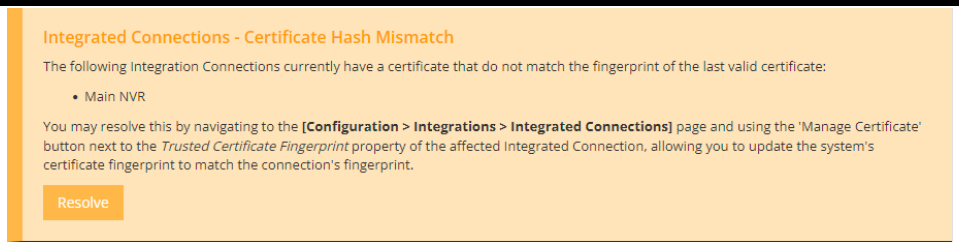
HTTPS Connection Management

To promote and ensure network security, all Integrated Connections created in the Inception system are configured to use HTTPS, and this cannot be changed. Upon initial connection, the Inception will collect store the *Trusted Certificate Fingerprint* of the third-party device's certificate.

If the *Trusted Certificate Fingerprint* stored in Inception is detected to be different than the connected device, due to the certificate changing on the third-party device, the Integrated Connection will refuse to connect to the third-party device and a system warning will be generated on the Inception system.

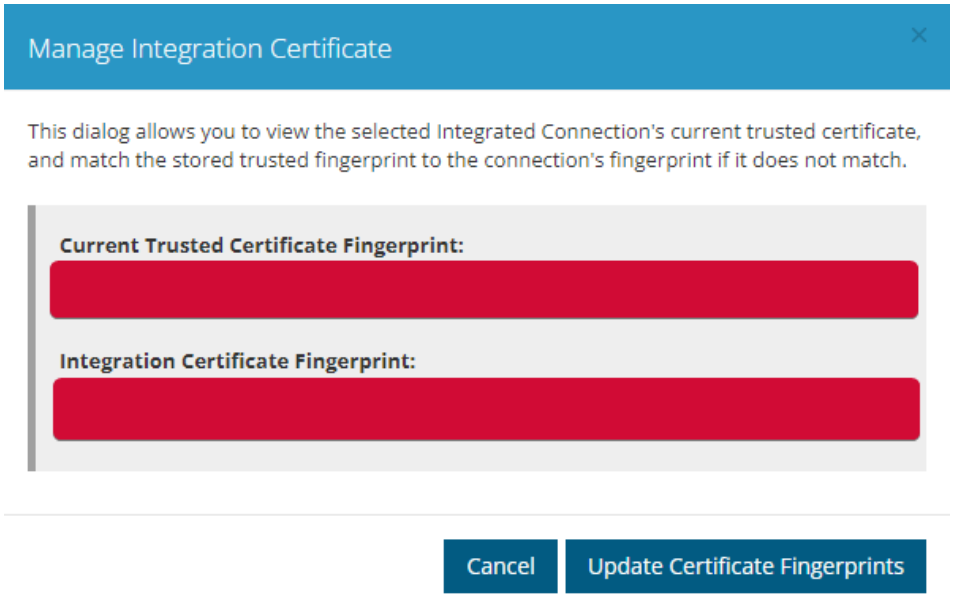


Configuration



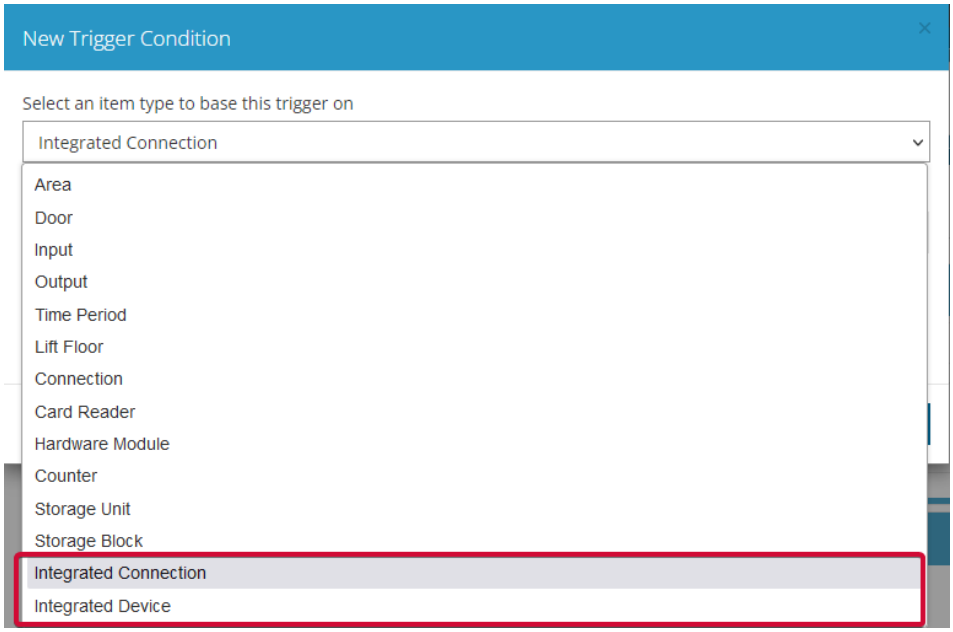
To resolve this issue, the stored *Trusted Certificate Fingerprint* must be updated to match the new certificate fingerprint of the third-party device's certificate. This can be done manually, by editing the *Trusted Certificate Fingerprint* field, or can be automatically updated by clicking the link button next to the property.

Clicking this button will open a dialog that allows the automatic matching of the stored *Trusted Certificate Fingerprint* with that of the third-party device.



Automated Action Triggers

Events that come through from both Integrated Connections and their linked Integrated Devices can be used as triggers for Inception's Automated Actions. When configuring an Automated Action's trigger condition, two new trigger types are now available: *Integrated Connection* and *Integrated Device*.

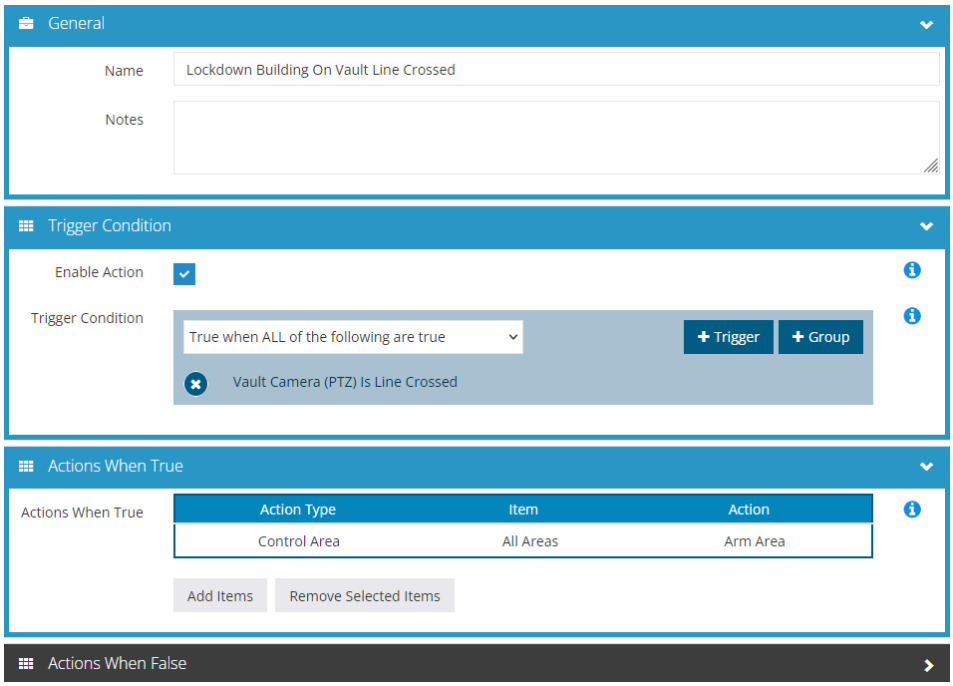


Once an item type is selected, the specific connection/device and the desired state can then be selected. Integrated Connections currently only have one state that can be monitored, *Connection Error*, while Integrated Devices have the following state options:

- Device Offline
- IP Conflict
- Cable Disconnected
- Network Disconnected
- Illegal Access
- Video Signal Lost
- Video Signal Abnormal
- Disk Alarm
- Disk Full
- Disk Attenuation
- Motion Detection
- Physical Alarm Input
- Line Crossed
- Double Virtual Fence
- Loitering Analysis
- Illegal Parking
- Intrusion Analysis

Configuration

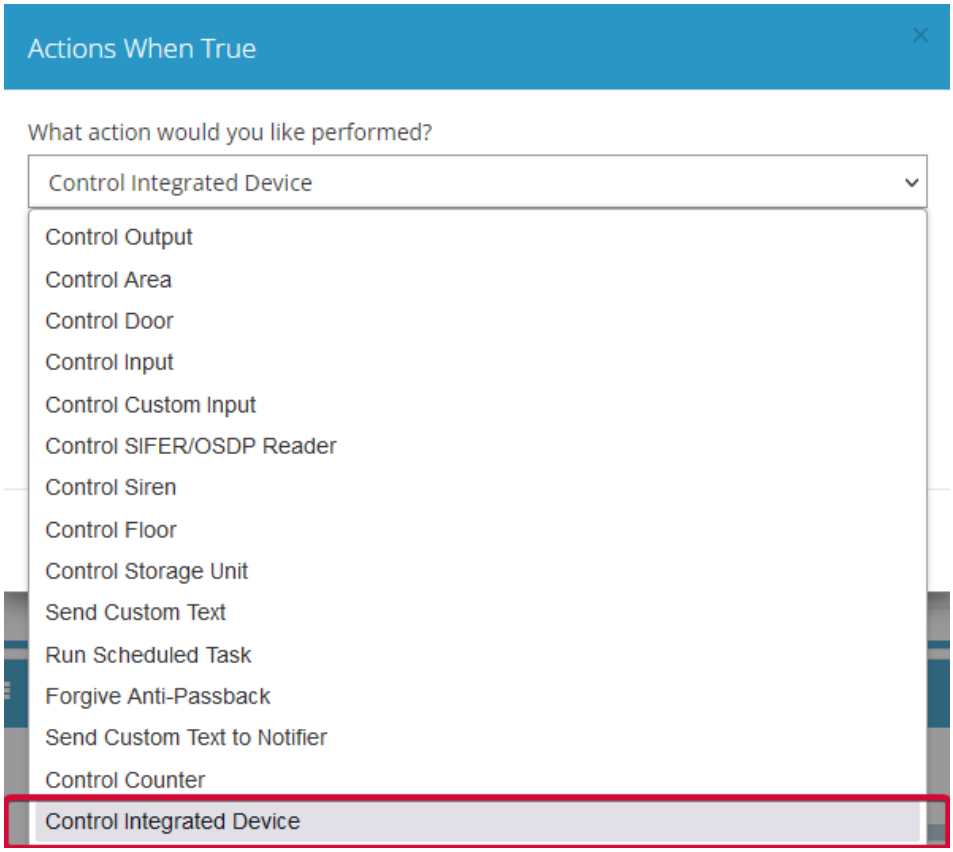
Once configured, any event of the selected type will correctly transition the Automated Action's state between *True* and *False*. For example, the following Automated Action will arm all areas in a building once a line crossed event has been detected from a vault camera:



With this configuration, once the select camera (*Vault Camera (PTZ)*) sends a *Line Crossed* event to the Inception system, the Automated Action's state will transition to *True*, and the Inception will arm all areas on the system.

Automated Action Actions

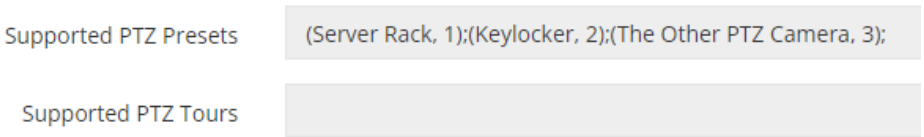
Automated Actions can also be used to send commands to connected Integrated Devices. When adding a new entry to either *Actions When True* or *Actions When False*, a new *Control Integrated Device* option is now available as an option.



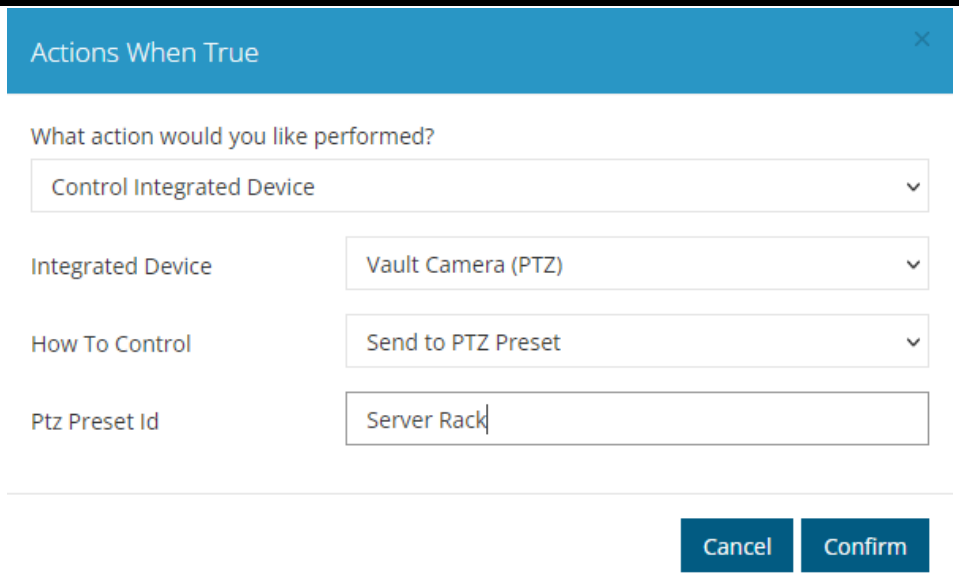
Once a target Integrated Device has been selected, the following control types can be selected:

- Send to PTZ Preset
- Control PTZ Tour
- Control Physical Output

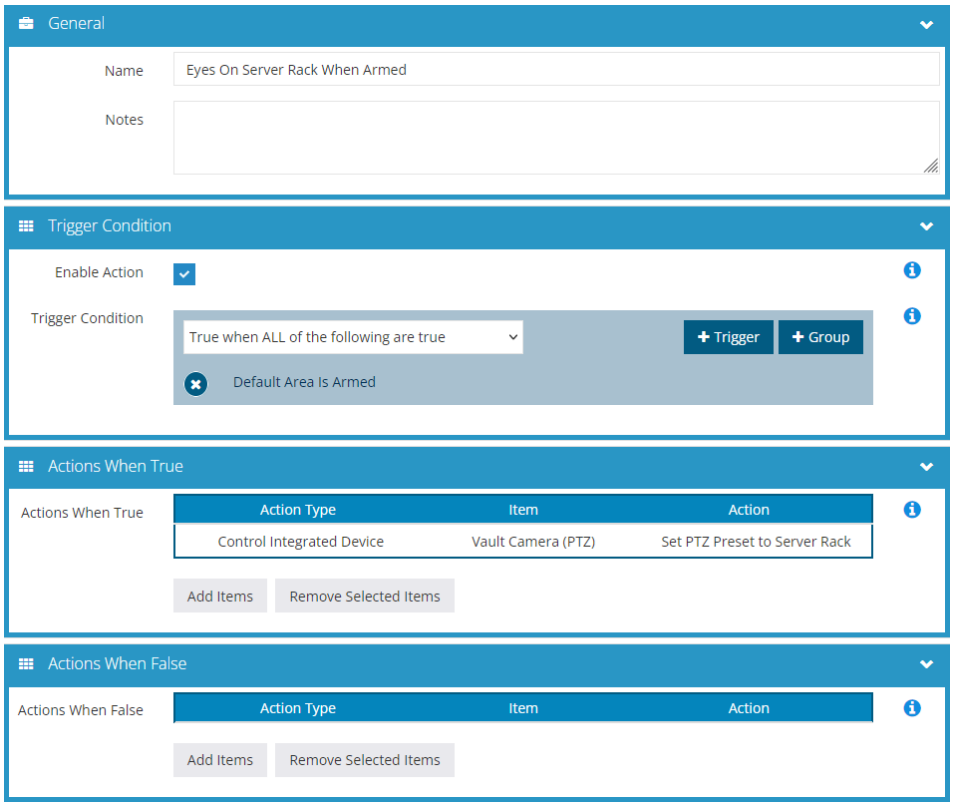
An Integrated Device's available PTZ Presets and PTZ Tours, if any, can be found within the Integrated Device's settings, under *Supported PTZ Presets* and *Supported PTZ Tours* respectively. These can then be copied across into relevant field within the Automated Action's action definition.



Configuration



For example, the following Automated Action will send a PTZ camera to the *Server Rack* PTZ preset upon the *Default Area* being armed.



Global Headquarters

Inner Range Australia
+61 3 9780 4300
anz@innerrange.com

Inner Range United States
+1 (844) 588-0874
usa@innerrange.com

Inner Range United Kingdom
+44 (0) 845 470 5000
uk@innerrange.com

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

Inner Range Middle East
+971 4 8067100
middleeast@innerrange.com

Inner Range India
+91 80 4070 3333
asia@innerrange.com

INNERRANGE.COM

July 2024