INTEGRITI HIKVISION BIOMETRIC INTEGRATION MANUAL

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

Integriti Hikvision Biometric Integration Manual

Table of Contents

Biometric Capabilities

Core Biometric Capabilities

Feature	Feature Description	Ver	Y/N
Fingerprint Biometrics	The Integration supports the use of Fingerprint Biometric Readers	21	✗
Face Biometrics	The Integration supports the use of Face Biometric Readers	21	✓
Hand Biometrics	The Integration supports the use of Hand Biometric Readers	21	✗
Receive Events from the Biometric System	The Integration supports incoming events to Door readers.	21	✓
Create Child Devices from Biometric Configuration	Child Biometric Readers will be created based on the Reader configuration on Refreshing Child Devices	21	✗
Associate Biometric Readers with Entities	Cameras loaded from the Biometric system can be associated with Integriti Entities to allow direct control of one from the other.	21	✓
Connect to Biometric Reader	Connect to Individual Biometric Readers instead of operating through a Server or System managing all connected readers.	21	✓
Connect to Biometric System	Connect to an overarching Biometric System which manages each Biometric Reader allowing to automatically connect to all Biometric Readers connected to the system.	21	✗
Configure Biometrics from the Web Interface	Use the Integriti Web Interface to Enrol and Manage Biometric System or Readers.	21	✗
Trigger Actions in the Biometric System	Trigger actions or commands in the Biometric system directly from Integriti.	21	✓
Sync Time (via NTP)	Sync the time of the Biometric system and Integriti to match via an NTP.	21	✗
Display Connection Status to Biometric System	Display whether or not Integriti is currently connected to the Biometric system.	21	✓

Feature	Feature Description	Ver	Y/N
Receive Events/Alarms from the Biometric System	Log events/alarms occurring on the Biometric system to Integriti's Review.	21	✓
Trigger Integriti Actions on Biometric Events/Alarms	Trigger actions to automatically occur in Integriti whenever specific events/alarms are received from the Biometric system.	21	✓
Generate Alerts from Biometric Events/Alarms	Automatically generate and restore Alerts tied to a specific reader in Integriti whenever specific events/alarms are received from the Biometric system.	21	✗

Advanced Biometric Capabilities

Feature	Feature Description	Ver	Y/N
Automatically Load Biometric Configuration	Refreshing Child Devices will automatically populate all readers configured in the Biometric System into Integriti when run. If not supported, reader configuration will need to be manually entered into Integriti.	22	✗
64-bit Integration Server Support	The integration supports being run on the 64-bit integration server.	22	✓
Show Biometric Status	The current online/offline status of configured Biometric Readers will be visible directly through Integriti.	22	✓
Categorised Review Records	Review generated by the integration will have a different category for different event types, allowing for easy filtering of specific Biometric events	22	✓
Trigger Inputs on Biometric Event	Inputs in Integriti can be automatically triggered and restored when specified types of events are received from the Biometric system.	22	✓

Integriti Hikvision Biometric Integration Compatibility

Licensing Requirements

The Integriti Hikvision Biometric Integration requires an Integriti/Infiniti v22 license or higher to be present on the product key running the integration.

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.

Minimum Installed Integriti Version

The Integriti Hikvision Biometric integration is only compatible with an installation of Integriti Pro or Infiniti that is v21.1 or higher.

SDK Version

The Integriti Hikvision Biometric plugin was built and tested against the following versions of software:

- ISAPI version 2.6 Feb. 2020

Tested Against

- DS-K1T673DWX Face Recognition Terminal; firmware version 3.3.12 build 220906
- DS-K1T341AM Face Recognition Terminal; firmware version 3.2.30 build 220210

Configuration

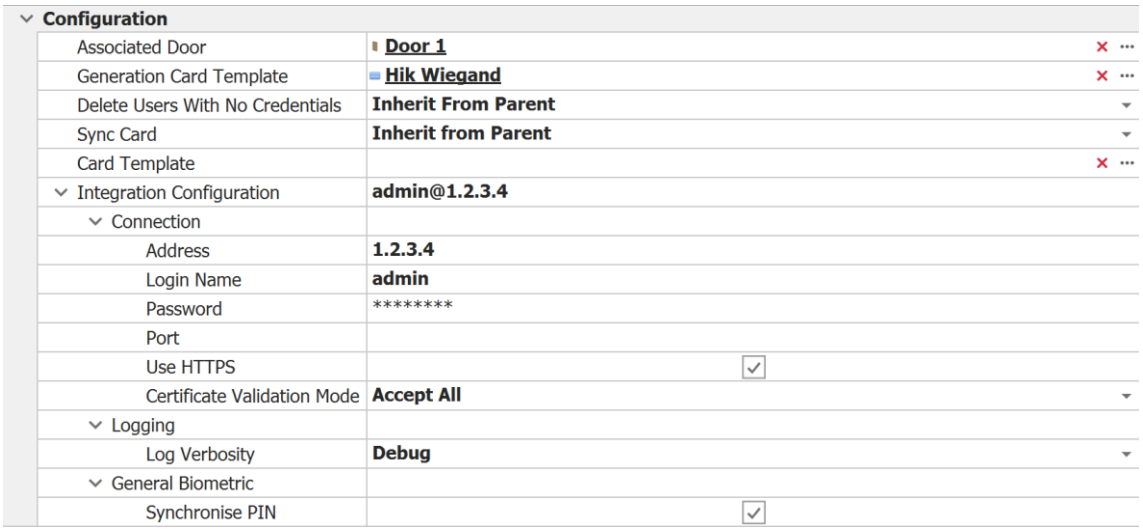
This section specifies the Hikvision Biometric Integration specific configuration details. Please refer to the 'Integriti Integrations – Biometric' manual for a detailed description on how to fully configure and use Biometric integrations in Integriti/Infiniti. Once Biometric Readers are configured, ensure to Refresh Device prior to using the integration. This will ensure all default configuration properties and device details are pulled from the device and will configure the device with the necessary default settings to ensure the reader is ready for use.

Ports Used

The following ports are used for communication between the Integriti Hikvision Biometric integration and the Biometric devices. These ports should be configured in the Integriti Integration Server and any Integriti Client Machine's firewalls to allow the integration to be used.

- Port specified in Connection Configuration

Connection Configuration



Connection

Address – The IP address of the device to connect to.
Login Name – The administrator user name to use to log in to the device.
Password – The administrator password to use to log in to the device.
Port – TCP port to connect on. If left empty, the standard port will be used. This is 443 if HTTPS is selected or 80 otherwise.
Use HTTPS – Whether to use HTTP over TLS to connect to the device.
Certificate Validation Mode – When using HTTPS, specifies whether the connection should continue when the device does not have a valid certificate.
Certificate Thumbprint – When 'Certificate Validation Mode' is set to 'Specified Thumbprint', the SHA-1 certificate thumbprint that should be accepted. It should be specified as 40 hexadecimal digits, case insensitive, with no separators.

Logging

Log Verbosity – Only logs of the specified level or higher will be logged. If Warning is selected, only Warning, Error and Fatal logs will be written to the log.

General Biometric

Synchronise PIN – When enabled, users synchronised to the Integrated Device will have their security PIN synchronised. This can enable authentication by entering the PIN on the device in addition to or instead of face authentication, depending on the configuration of the device. See the device's user manual for more information.

Biometric Integration Configuration

Generation Card Template – Required to generate Biometric Credentials. Read more in the Biometric Integrations manual. Specify a Card Template to use when creating new credentials for this Integrated Device. Any new credentials created will be associated with this Card Template - Existing Credentials used by this Integrated System will maintain their existing Card Template.
When the device is connected to an Integriti reader module, the Card Format used by the selected Card Template should match the configuration of the device. See the Wiegand Configuration section for more information.
Other – Read more in the Biometric Integrations manual.

Biometric Integration Notes

When the integrated system is set up, Integriti will synchronise users and associated face records to the device to allow Integriti users to authenticate with the device. When removing a face record or permission to the associated door from a user in Integriti, the user and associated face record will be deleted from the device, removing their access to it. This shall also be done if the Card representing that face record is set to an inactive state that is considered permanent revocation. If the Card state is set to an inactive state that is considered temporary, the user and face record will remain, but their access permission on the device will be temporarily revoked, resulting in an error message when the face is presented.

Reassigning an existing Card representing a biometric credential to another user in Integriti is not supported.

Persisted Connection

This integration allows a persisted connection to be set up with a biometric reader. This allows access control events to be received from the reader in real time and recorded as review events in Integriti.

An active persisted connection indicates that there is an underlying persisted network connection active from the Integriti integration server to the reader, using arming mode. This may fail if there are more existing arming connections than the device allows. The integration will automatically restart the connection if expected heartbeat messages are not received for 90 seconds.

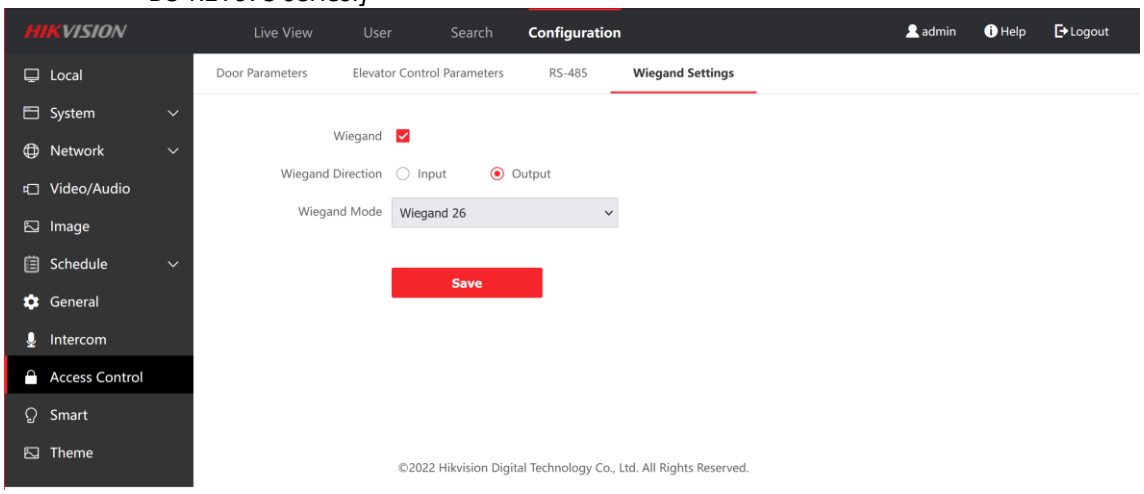
Wiegand Configuration

Some Hikvision biometric devices, such as the DS-K1T673 series face recognition terminals, can be wired to an Integriti reader module via Wiegand, allowing them to be used in place of a card reader.

When wiring the integrated device to a reader module, the Wiegand ground (normally a black wire) should be connected to the V0 pin of a reader port, and the D0 (green) and D1 (white) connections to the respective Wiegand data pins. If the integrated device is powered separately, it is not necessary to connect the +VR pin. These connections may vary depending on the device; see its user manual for more information.

To configure Wiegand output on the device, navigate to the appropriate configuration page similar to Configuration > Access Control > Wiegand Settings, and configure the Wiegand settings similar to the following. The screenshot below is specific to the DS-K1T673 series, but the exact options may vary between devices; see your device's user manual for more details.

- **Wiegand:** Enabled
- **Wiegand Direction:** Output/Send
- **Wiegand Mode:** Wiegand 26 *[Other Wiegand formats are not supported with the DS-K1T673 series.]*



When using Wiegand 26-bit mode, the selected Card Format for this connection in the reader module attributes should be '26Bit Wiegand'. For reference, the correct settings for this mode are as follows:

- **Card Type:** Wiegand Site Code
- **Reverse Bytes:** False
- **Total Bits:** 26
- **Site Code Offset:** 1
- **Site Code Length:** 8
- **Card Number Offset:** 9
- **Card Number Length:** 16
- **Issue Number Offset:** 0
- **Issue Number Length:** 0

Card numbers and the site code specified in the card template must be within the valid range for the card format being used. For 26-bit Wiegand, the valid range of site codes is 0~255 (decimal) and for card numbers is 0~65535.

After Cards generated for external credentials in Integriti have been synchronised to the device, when a user successfully authenticates with the device, it will send the site code

specified in the Generation Card Template along with the card number from the recognised user to the Integriti reader module.

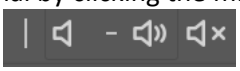
Note: It may be necessary to manually sync entities from the server to the controller for this to be correctly recognised.

Video Viewer

It is possible to monitor a video feed from a Hikvision face recognition terminal using the Hikvision CCTV integration. To do this, set up a CCTV System for the device with that integration in addition to the Biometric Reader. The server address, name and password in the CCTV System attributes should be the same as in the Biometric Reader attributes, to point to the face recognition terminal.

Refreshing child devices of the CCTV System will populate a single camera in Integriti providing access to live video from the device.

When viewing video on a Hikvision face recognition terminal using the Hikvision CCTV integration, it is possible to begin streaming audio from the device using the volume buttons on the camera control bar, shown below. Audio may also be transmitted from the client computer to the face recognition terminal by clicking the microphone button.



For more information, see the Hikvision CCTV integration manual and the Integriti Integrations – CCTV manual.

Commands

Biometric Device Commands

The following commands can be performed on a Biometric device:

Control Attached Door	Remotely locks or unlocks a door wired to the biometric reader. It is also possible to disable the door so that authentication on the reader will not unlock it.

Troubleshooting

Persisted connection or other operations fail with an 'Unauthorized' error	• Ensure the device is not locked due to too many authentication failures. • Note that the username and password are both case sensitive.
Persisted connection fails with a 'Not Found' error	• If a connection was recently stopped, allow the integration to automatically retry after 10 seconds. • Are there already the maximum number of arming connections allowed by the device?
Persisted connection fails with an invalid certificate error	• Configure the integration server to trust the device's certificate or set the Certificate Validation Mode to Specified Thumbprint and specify the correct thumbprint. A Web browser may be used to obtain the thumbprint. See Connection Configuration for details. • Alternatively, set the Certificate Validation Mode to Accept All.
User Start and Expiry times not converted correctly	• If the time zone on the device is different from the integration server's time zone or has changed, it is necessary to Refresh Device.
Authentication on the device results in a 'Card Access Denied - Unknown Card' review alert in Integriti	• If the card number in the review alert is incorrect, ensure that the Wiegand settings on the device match the Card Format selected for the reader and the card number and site code are in range for that Card Format. • Manually synchronise entities from the server to the controller or wait a few minutes.