inner range

INTEGRITI

INTEGRATION
INVIXIUM BIOMETRIC PLUGIN

MANUAL V1.0

INNERRANGE.COM

CONTENTS

OVERVIEW 4
Audience 4
PREREQUISITES 4
Supported Invixium terminals/software/firmware 4
Invixium IXM Web tool 5
IMPLEMENTATION CONCEPTS 6
Topology 6
Master Terminals 8
Managing Configuration Data 9
Single terminal configuration 9
Master devices 11
Parent node configuration 12
User Management 12
Managing user cards 13
Managing Face biometrics In Mixed ROSTO / non-ROSTO Environments 13
Support For QR Code 15
QR code on TOUCH3 Biometric reader 15
Support for OSDP 15
Identification and Verification modes 15
INITIAL SETUP 16
Installation 16
Configuration 17
Biometric System Configuration (Parent node) 17
Biometric Reader Configuration 18
Biometric Configuration 20
QR code settings 21
Wiegand Input Settings 21
Wiegand Output Settings 22
OSDP 22
Card Formats configuration 23
Parity bits 23
Operational considerations 24
Networking 24

Copyright © Inner Range PTY LTD July 2026

Keeping terminal's clock synchronised....24
COMMANDS....25
Biometric Device Commands....25
TROUBLESHOOTING....26
Common mistakes....26
Enabling Telnet....26
Retrieving Device Logs....27
BIOMETRIC CAPABILITIES....28
Core Biometric Capabilities....28
Advanced Biometric Capabilities....29

Copyright © Inner Range PTY LTD July 2026

OVERVIEW

The integration extends Integriti Access Control capabilities by incorporating advanced biometric authentication technology from Invixium Biometric.

Invixium Readers can be used to enrol Biometric data and synchronise with Integriti. Users will be automatically synced with the desired permissions and credentials saved into Integriti. The Invixium readers are physically connected to IR Access Control panels using Wiegand or OSDP interfaces - enforcing access control with biometric precision.

This integration connects to every biometric reader directly, without an intermediary server.

For general description of Integriti Biometrics integrations, refer to the “Integriti Integrations - Biometric.pdf” document found in Doc\Integrations subfolder of your Integriti installation. For specifics of this integration, refer to CAPABILITIES

For detailed description of Invixium biometric devices, their configuration, specific functionality and application to actual production environment, please refer to resources available on www.invixium.com.

Audience

The document is designed for a security integrator who is familiar with IR Access Control solutions and has a good grasp of how biometrics can be applied in secure Access Control environments.

It is recommended to read this documentation in its entirety before beginning any individual installation steps, as the document contains examples and specific instructions that an integrator should become familiar with before modifying any live systems.

PREREQUISITES

- Integriti edition: Professional, Business or Corporate
- Integriti version: v26 or higher
- Integriti product license version: v26 or higher
- Licensing Information
  - This integration requires the ‘Integriti Integration - Biometric Management’ (PN: 996969) license.
  - In addition, you will also need the ‘Integriti Managed Biometric Reader’ (996970) license for each reader connected to the system.

Supported Invixium terminals/software/firmware

The plugin was built and tested against the following versions of IXM SDK software:

- IXM SDK version 3.0.122.0

The release was tested against the following terminals/firmware:

- IXM ROSTO FR2: Firmware v10.000.043.000
- IXM TFACE FP2: Firmware v6.003.022.000
- IXM TOUCH3: Firmware v11.000.015.000

Copyright © Inner Range PTY LTD July 2026

Invixium IXM Web tool

The Invixium integration v1.0 does not rely on using Invixium IXM Web tool. The integration offers a ‘practical set’ of configuration parameters which should be sufficient for majority of deployments. A customer will only need to use IXM Web if their terminals must be configured beyond what is supported by the integration.

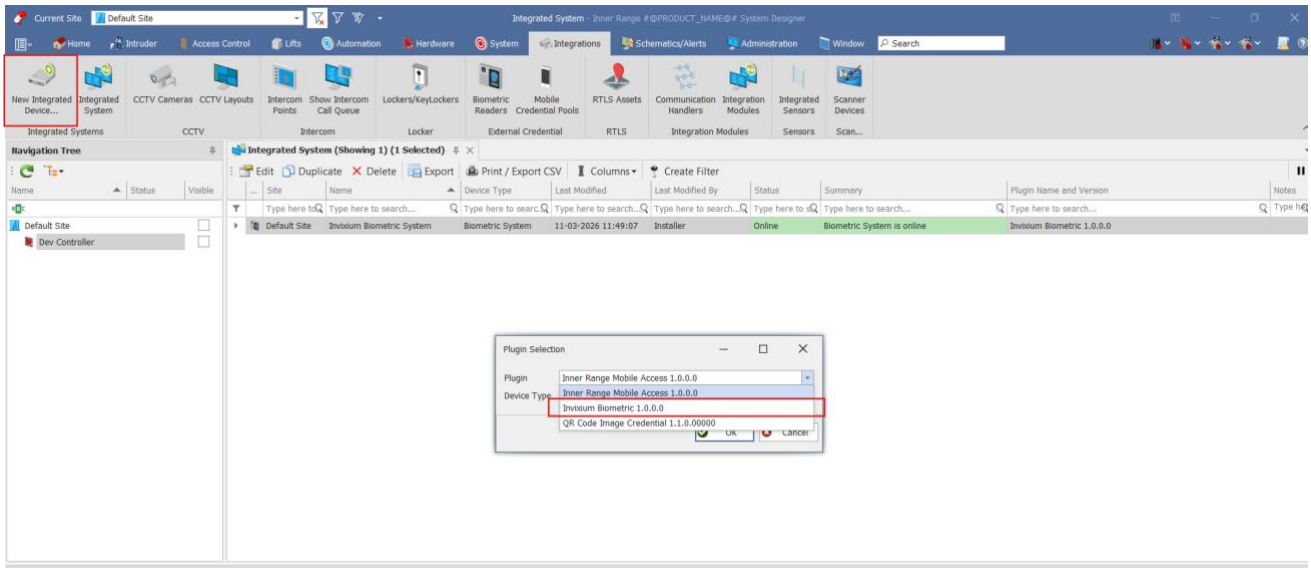
Customers should be aware that IXM Web tool is subject to licensing and is not free to use beyond initial period of one year. Contact your Invixium representatives for specific instructions.

Copyright © Inner Range PTY LTD July 2026

IMPLEMENTATION CONCEPTS

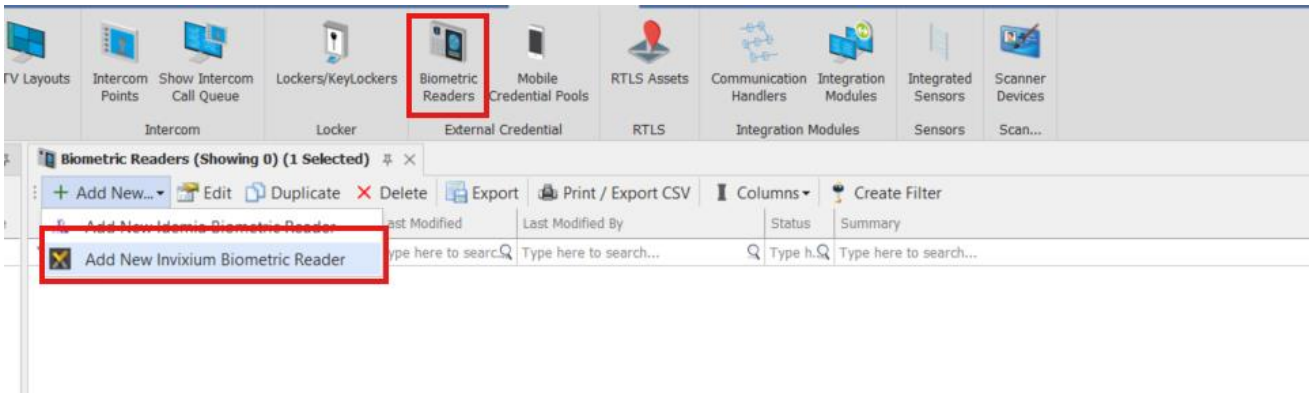
Topology

The parent node - Invixium Biometric System - is added as an Integrated Device. There should be strictly one instance added. Its main function is to run Events Listener and Heartbeats Listener.

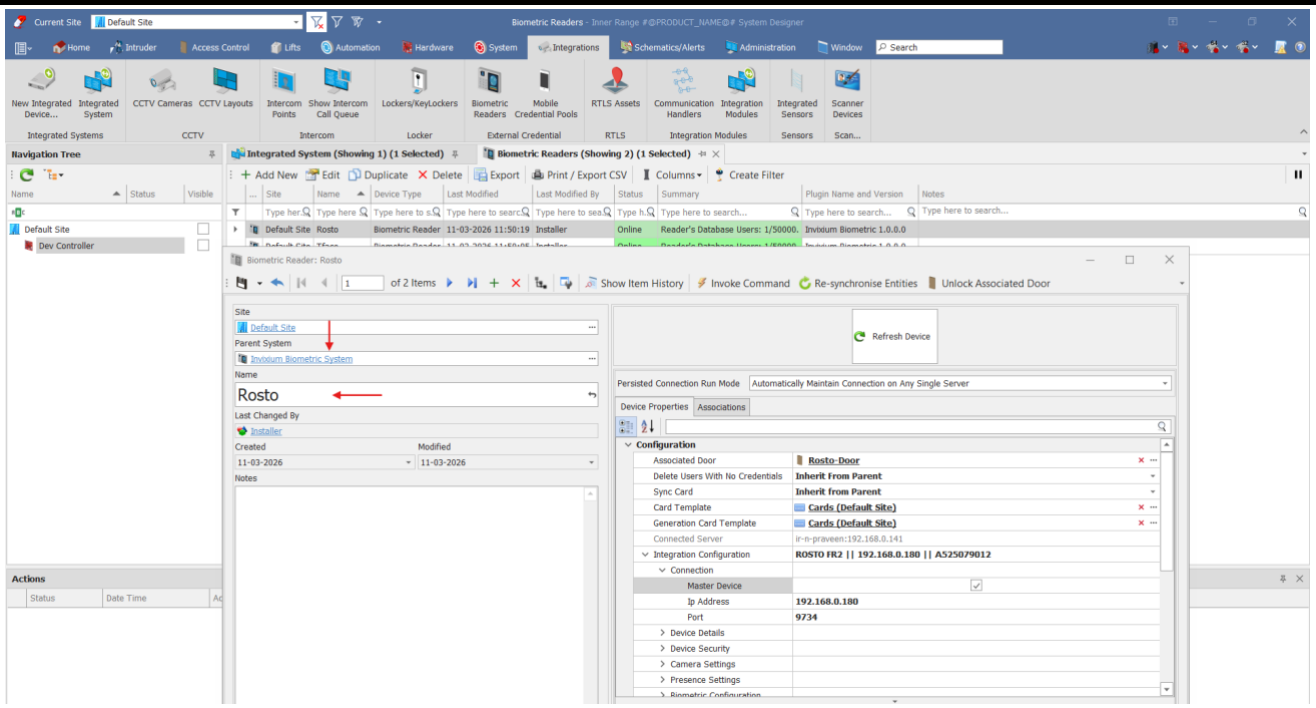


The parent node status will be shown as Online if both listeners are operational, even without a single terminal added.

Biometric terminals must be added separately from Biometric Readers tab by clicking on “Add New Invixium Biometric Reader”. There is no auto-discovery. A terminal device’s Parent System field must point to Invixium Biometric System.



Copyright © Inner Range PTY LTD July 2026



The integration maintains separate TCP/IP connection to every registered terminal. There is no 'in-between server' acting as an intermediary.

The communications are two-way:

The integration connects to a terminal device to send commands and save/retrieve configuration.

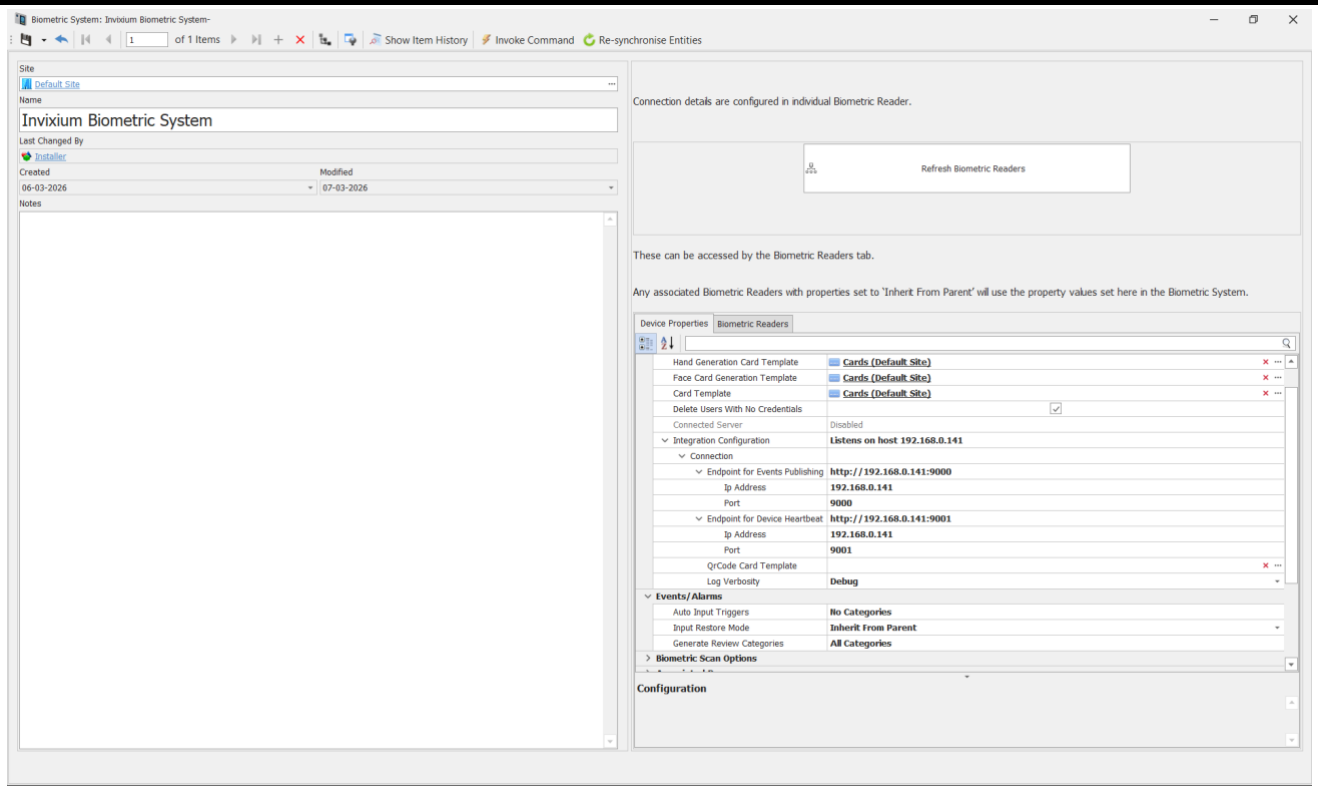
The integration maintains a single instance of Events Listener to receive asynchronous notifications/events from devices.

- The Events Listener's configuration is part of the integration's parent node configuration.
- The Events Listener's <address>:<port> is sent to every child biometric terminal, so it knows who to report to.

The integration maintains a single instance of Heartbeats Listener, to receive asynchronous heartbeats notifications from devices.

- The Heartbeats Listener's configuration is part of the integration's parent node configuration.
- The Heartbeats Listener's <address>:<port> is sent to every child biometric terminal, so it knows who to report to.

Copyright © Inner Range PTY LTD July 2026



Note: further in the Configuration section of this chapter, we refer to both listeners as ‘Listeners’ for brevity.

Master Terminals

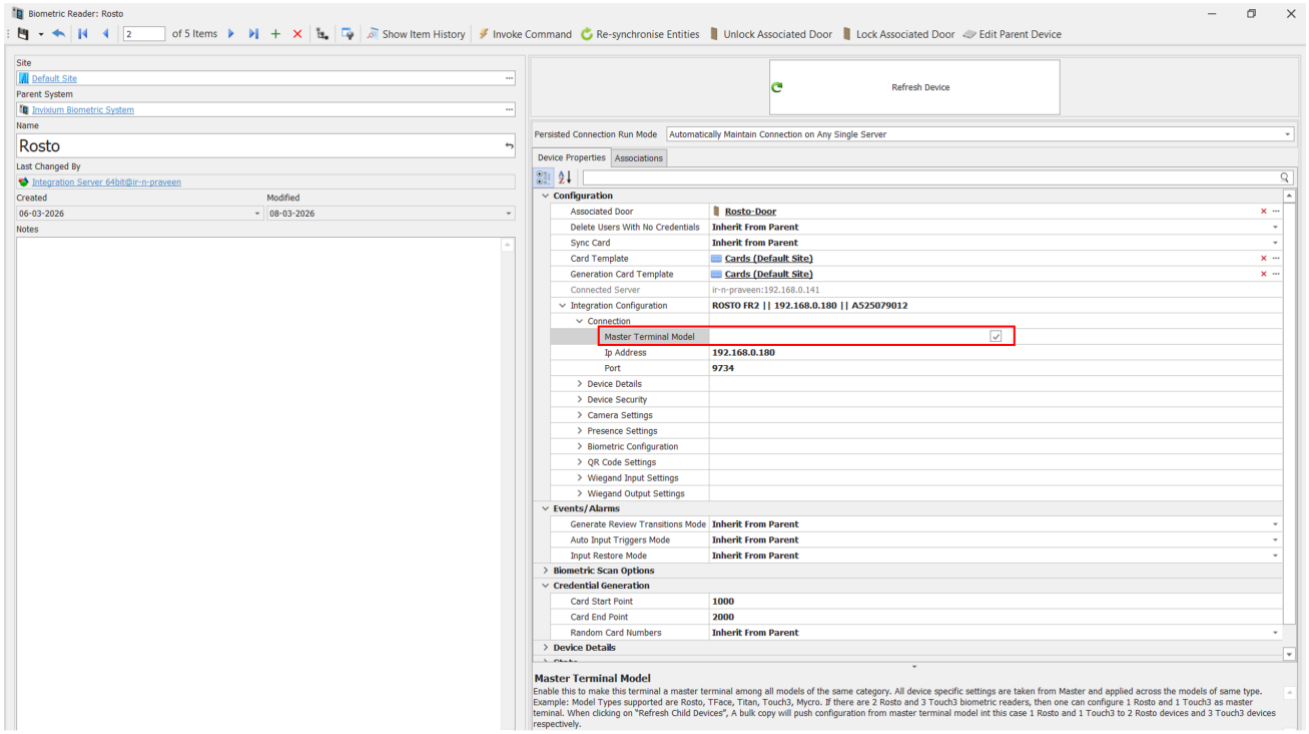
The Integration supports the concept of a ‘Master Terminal’. A master terminal’s configuration can be replicated to all other devices of the same model.

Master Terminals are optional; however, in production environment all terminals of same type are expected to have similar configuration; using master devices simplifies management of your terminals and helps avoiding mistakes.

There should be strictly **zero or one** master terminal designated for each model type, i.e. if you use ROSTO and TFACE terminals in your deployment, you need one ROSTO master terminal and one TFACE master terminal.

The below screenshot shows how a terminal is designated as a Master:

Copyright © Inner Range PTY LTD July 2026



Managing Configuration Data

Term: *DB* – Integriti Database

Single terminal configuration

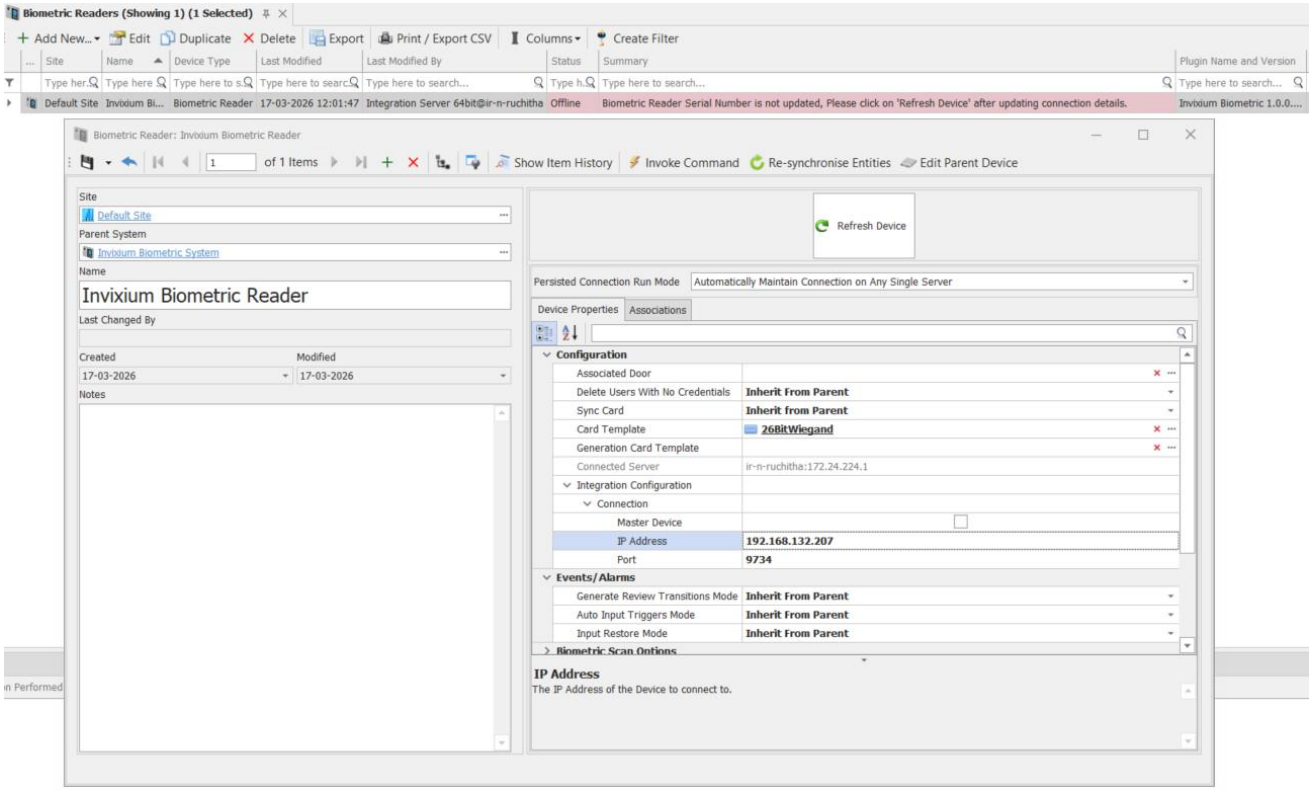
The list of configuration parameters offered by the integration is a ‘practical subset’ of all existing configuration parameters. This ‘practical subset’ was composed in consultation with Invixium specialists.

The list of parameters is different for each device model, reflecting specifics of the model.

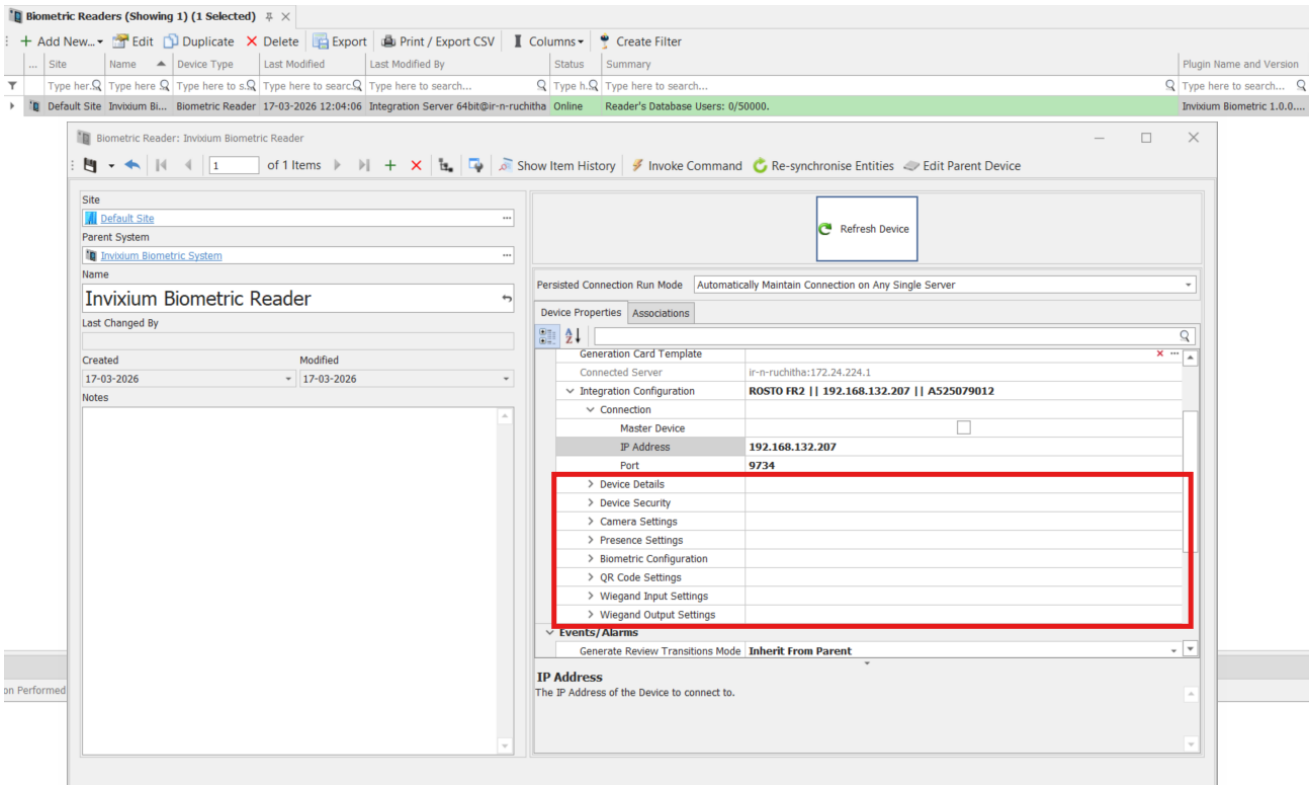
Note: to configure parameters which are not exposed by the integration, a customer needs to use Invixium IXM Web software.

Initially, the configuration UI shows values from the DB. For a newly added device it will show only its connection parameters; other fields will be empty.

Copyright © Inner Range PTY LTD July 2026



Clicking the Refresh button will retrieve configuration from the device, populate the UI fields and automatically save it to the DB.



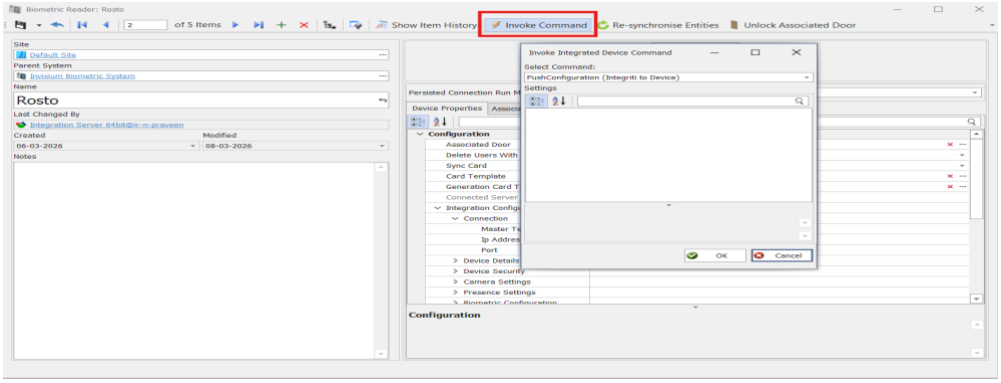
Copyright © Inner Range PTY LTD July 2026

- The Refresh operation automatically pushes the Listeners parameters to the device.
- Attempting to Save a non-complete configuration, without prior Refresh, will result in an error, which will be visible in the Biometric Readers list:



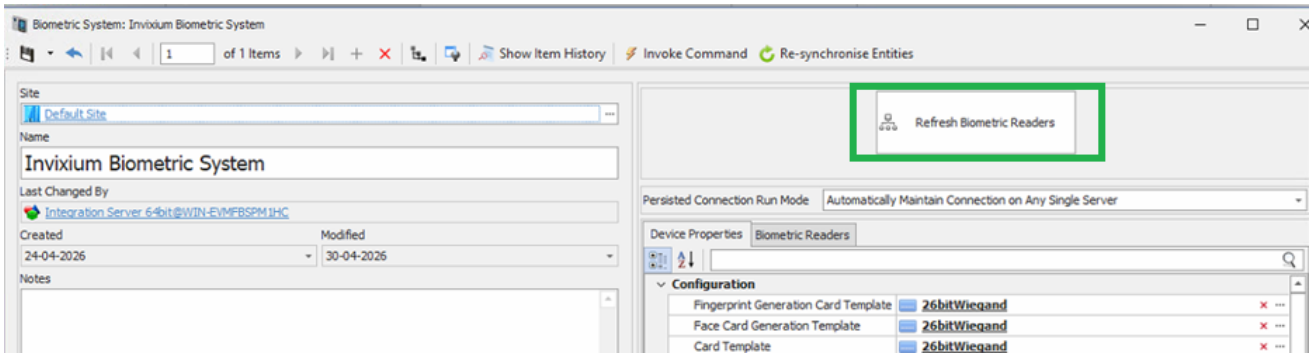
Clicking the ‘Save’ button collects configuration data from the UI and saves to the DB and to the device.

Note: invoking Command >Push Configuration command is equivalent to clicking Save.



Master devices

To push the master terminal configuration to all devices of same type, click the Refresh Biometric Readers button on the parent node.



If there is no dedicated master terminal for a particular model type, the operation will use each terminal’s actual configuration data.

Q: Can I prevent a specific terminal’s configuration from been overwritten by a master terminal data?

A: You cannot. We recommend configuring master terminal first and broadcast its configuration to all your devices, before configuring specific device’ parameters. Once master configuration is applied to your devices, you may consider disabling the “master terminal” designation completely, to continue with device-specific configuration tasks.

Copyright © Inner Range PTY LTD July 2026

Q: what about device-specific configuration, such as Network settings and OSDP ID? Are they going to be overwritten by the Master's data?

A: No. Network settings and OSDP ID will remain intact.

Parent node configuration

Parent node contains configuration of the Events Listener and Heartbeats Listener endpoints. The endpoints address: port parameters must be sent to every child device.

Clicking the parent node's Save button will automatically push the Listeners parameters to every child device.

The Refresh Biometric Readers button refreshes children devices configuration. For those terminal models which have a designated master device, the configuration will be taken from the master; otherwise, each terminal will be updated by reading its specific configuration from the DB.

Note: When pushing a master device configuration to terminals, the updated configuration will be automatically saved in each terminal's configuration data in DB.

User Management

An Integriti User will be automatically sent to relevant terminal devices, based on a user's door permission and devices' association with doors.

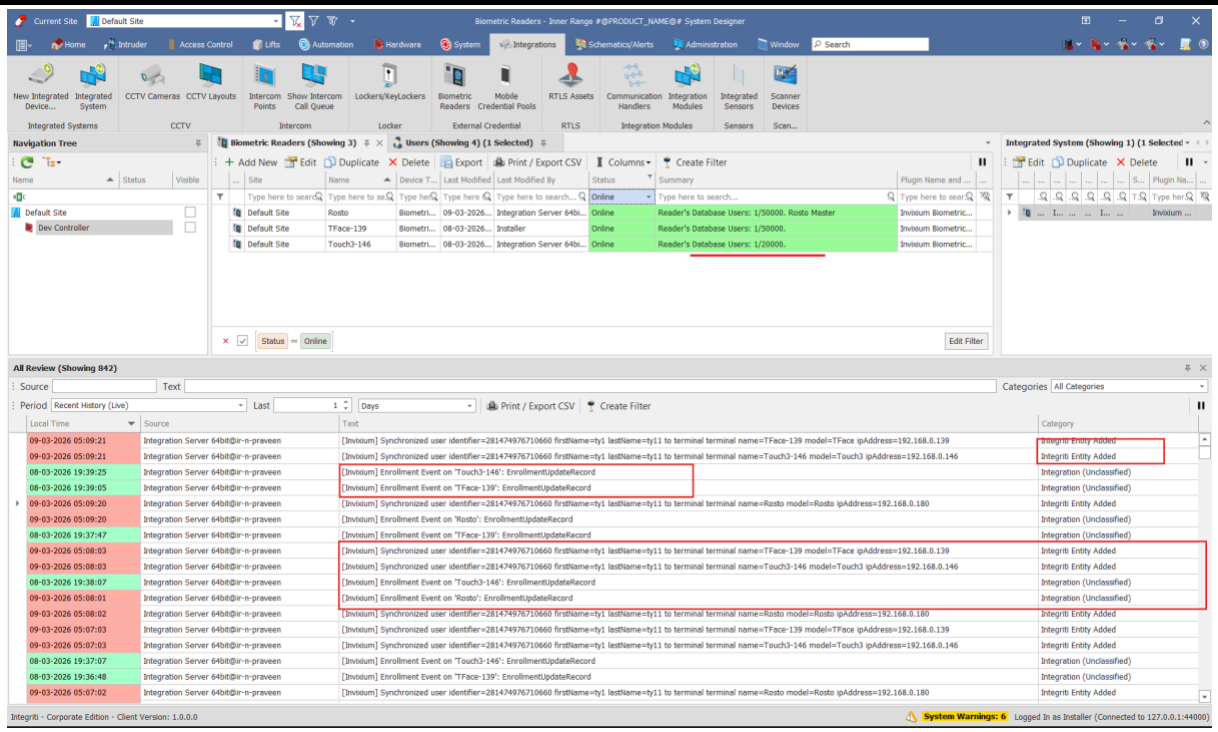
An Integriti user will be automatically deleted from a device if a device's door gets removed from the user's permissions.

It is permissible for an Invixium terminal used for user enrolment to not be associated with any door. In this case, a user's biometric data will not be saved to the device. Do not be surprised if after successful enrolment your face is not recognised by the enrolment terminal.

Q: Is it possible to find out if a device contains specific Integriti user's data?

A: Not directly. Indirectly, you can search in Integriti Review to see if it contains a "User Added To Terminal" entry for the user. Use Review filters with categories "Integriti Entity Added" or "Integriti Entity Deleted", or Enrolment Event under Integration category.

Copyright © Inner Range PTY LTD July 2026



Q: Is it possible to re-submit a specific Integriti user to all relevant devices without changing user data?

A: No. The “Re-synchronise Entities” button/command sends all users data.

Managing user cards

Consistent with Integriti’s Biometrics integration approach, the integration can generate a new virtual card during enrolment or use a user’s existing credential. Generating a new “just for biometrics” virtual card is recommended, to avoid dealing with issues like a real card being lost/damaged/stolen.

A card associated with a user’s biometrics during enrolment will be designated as a Default card of this user. The following snapshot shows a user’s record in IXM Web, with two cards, one of them a default one:

Card details

Serial Number	Card Technology	Status	Default	Facility Code	Issue Level	Activation	Expiry
1609	Smart	Active	Yes	100			
1502	QR Card	Active	No				

When pushing a user’s data into terminals, the integration will submit their default card, plus all cards associated with a template referenced by the “CardTemplate” parameter, plus any QR code credentials. This ensures that a user will be able to execute Card+Bio interaction with terminals using a real card or QR code.

Managing Face biometrics In Mixed ROSTO / non-ROSTO Environments

Copyright © Inner Range PTY LTD July 2026

Face biometric data captured by ROSTO devices only works with ROSTO terminals. In a mixed environment, the integration must keep a user's ROSTO face biometric data separately from their non-ROSTO face biometric data. At the same time ensuring that a user only needs to enrol their face once, regardless of the enrolment terminal's model.

This works as follows:

There are two types of enrolment:

1. **Live enrolment** - when a user shows their face to a device camera. The result of enrolment is a biometric 'blob' (a summarized digital representation of the enrolled face), and actual face image.
   After successful live enrolment, the integration will set a person' profile picture to the image returned by the enrolment, but only if there is no profile picture yet.
2. **Image-based enrolment** – instead of presenting a real face, a person's face photo can be sent to a terminal for algorithmic processing. The result is a biometric 'blob'.

When a user, who has already been live-enrolled on ROSTO, needs to be loaded for the first time into a non-ROSTO terminal, the integration will automatically execute image-based enrolment with this terminal. The returned biometric blob will be saved in the DB, used for all consequent downloads into non-ROSTO terminals.

The same logic works in a reverse direction, when a user was live enrolled on a non-ROSTO terminal.

Important: The plugin executes automatic image-based enrolment **only** if a user has already been live-enrolled.

Copyright © Inner Range PTY LTD July 2026

Support For QR Code

All Invixium terminal models, except MYCRO, support QR code presentation. By default, QR processing is disabled on terminals, and needs to be explicitly enabled as described here.

If enabled, a terminal will expect a QR code to be presented to it as per Card Access Rule settings inside the individual devices Biometric Configuration Parameters.

The Parent Node' *Card Template for QR Code* configuration parameter is used by the plugin only to differentiate QR credentials from other credential types: a credential of that type will be automatically sent to terminals together with the rest of user data.

Note: QR code presentation flow is managed by Card Access Rule configuration.

QR code on TOUCH3 Biometric reader

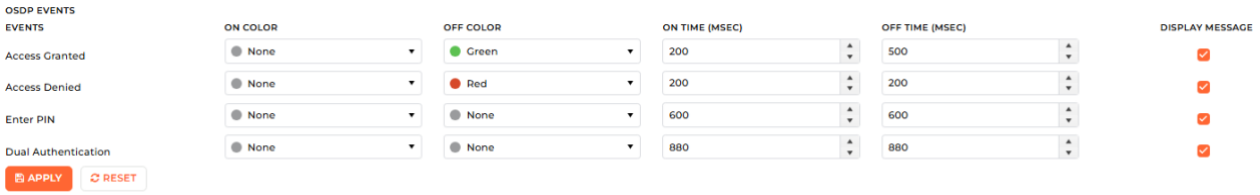
For using the QR code on TOUCH3 Biometric reader, in addition to the settings already configured in the UI, go to the device settings > QR-Code section and enable "Camera Preview" (device navigation path – Settings -> General Settings > QR Code Authentication).

This will ensure the QR code is properly seen by the camera, as the camera view and QR code will be made visible on screen to the person presenting the code to the reader, and processed in time.

Support for OSDP

Invixium terminals can be connected to controllers as a Wiegand reader, or as an OSDP reader.

IR controllers send fixed Granted/Denied osdp_LED commands; a terminal's LED settings must be configured accordingly, as shown below:



The integration automatically configures terminals with correct values. Customers should not be modifying those parameters without consulting with Inner Range and/or Invixium.

Identification and Verification modes

A biometric terminal contains a database of up to 50000 users, depending on a model.

When presented with a face or finger, it scans the entire list of users looking for a match. This is a very intensive and potentially long operation, referred to as *Identification*.

If Card+Face or similar interaction sequence is enabled on a terminal, a person first presents their card/QR before they are prompted to present their face or finger. In this case no lookup is needed, a terminal uses card/QR data to zoom onto a specific user record. The person's Face/Finger biometrics is compared with biometric data of the selected user record. This process is very efficient. It is referred to as *Verification*.

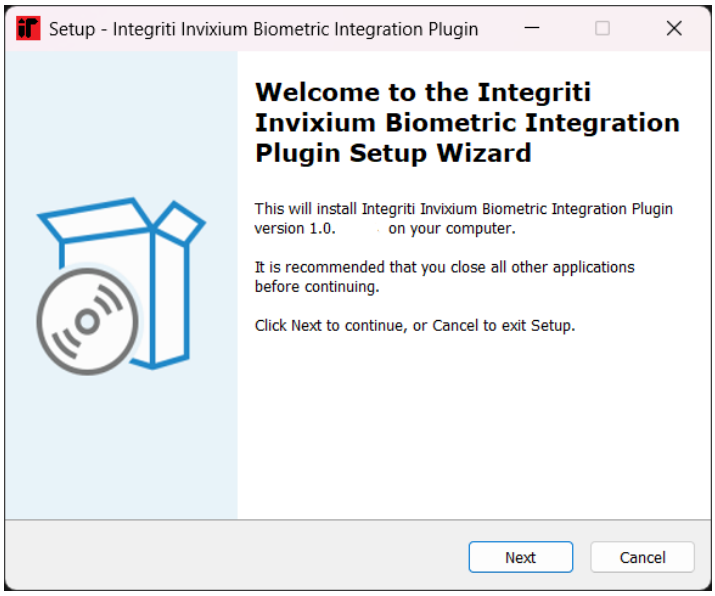
As a general remark: there are several configuration parameters affecting Identification and Verification behaviour of terminals. The interrelationship is complex; a customer should contact their Invixium partners to obtain help and specific instructions.

Copyright © Inner Range PTY LTD July 2026

INITIAL SETUP

Installation

Install the Integriti Invixium Biometric plugin executable on Integriti server running v25.2 or higher. Refer to the Release Notes for any Update considerations, if relevant.

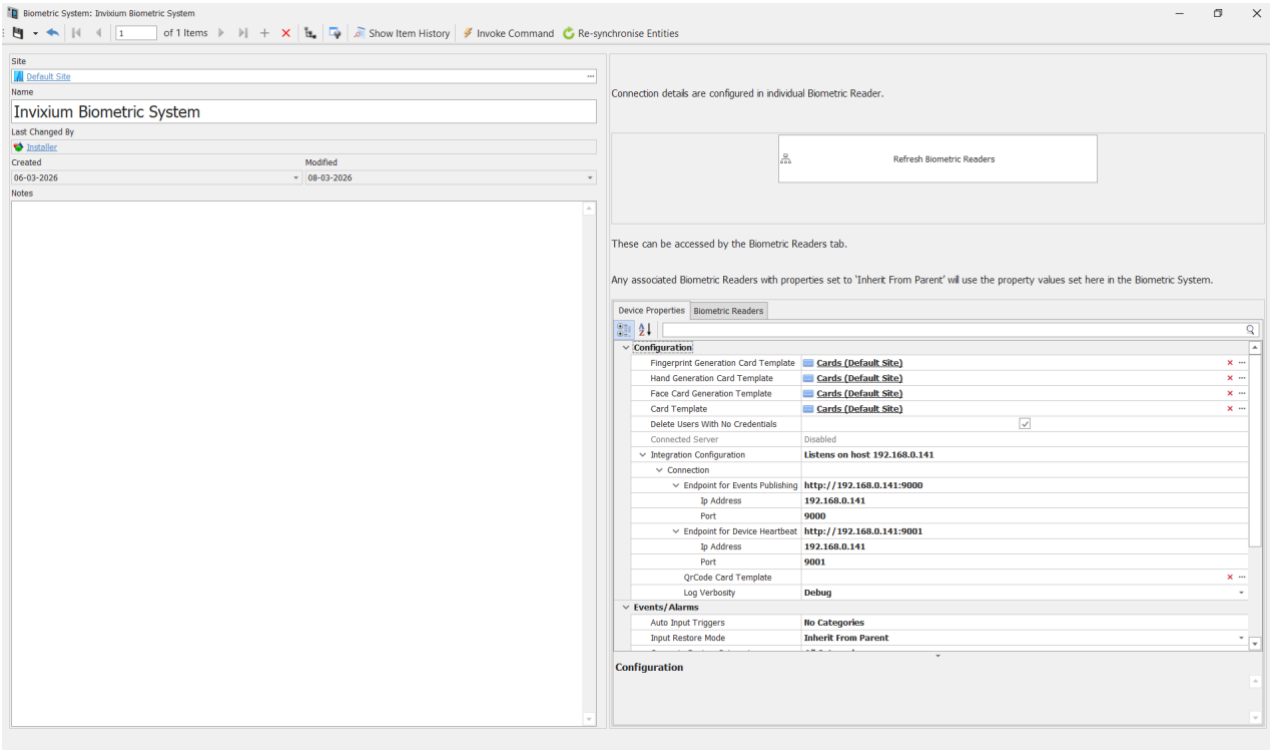


Copyright © Inner Range PTY LTD July 2026

Configuration

Biometric System Configuration (Parent node)

This section specifies the Invixium Biometric System (Parent node) specific configuration details.



Endpoint for Event Publishing – The IP Address and the Port to be used by Invixium biometric reader device to publish its events to Listener on Integriti. The default port is 9000, which is configurable. This port must be opened on the firewall for Inbound connections.

Endpoint for Device Heartbeat – The IP Address to be used by Invixium biometric reader device to publish device heartbeat event to Listener on Integriti. The default port is 9001, which is configurable. This port must be opened on the firewall for inbound connections.

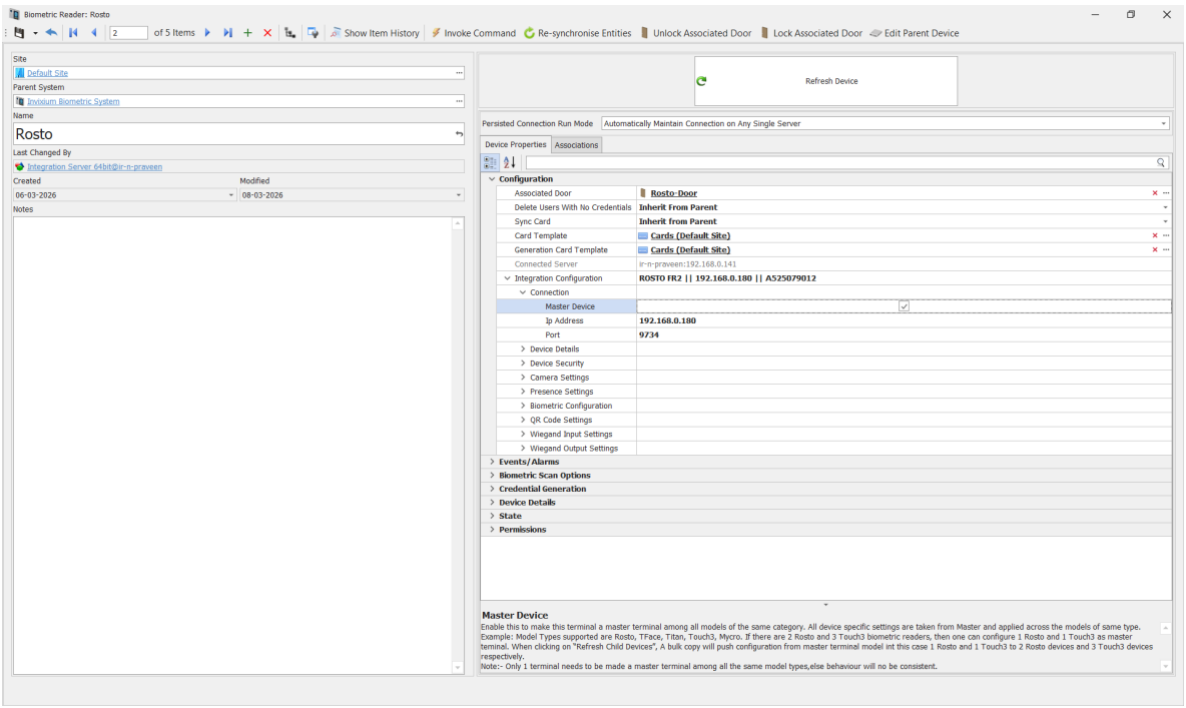
QR Code Card Template – Select a card template for QR code credentials. Will be used by the plugin to tell QR credentials from other credential types.

Log Verbosity – Only the 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.

Once the Biometric System Parent Node has been configured above, individual Biometric Readers can be added.

Copyright © Inner Range PTY LTD July 2026

Biometric Reader Configuration

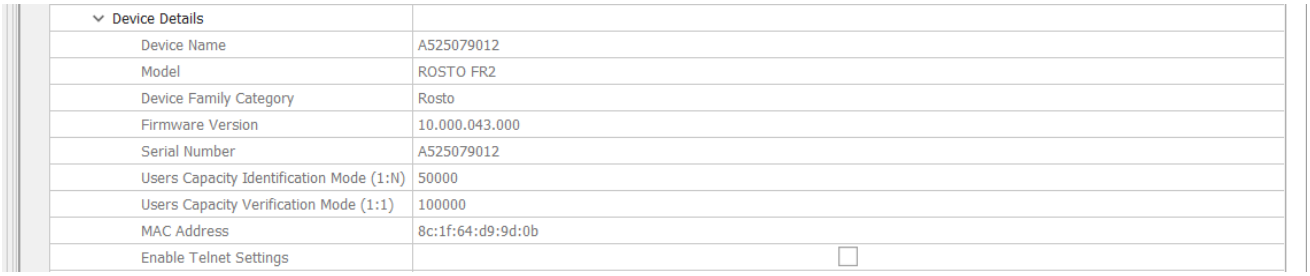


Master Device – Enable this to make this terminal a master device.

IP Address – The IP Address of the Device to connect to.

Port – TCP Port. Default port is 9734. This value can be configured and changed on the device and the port will need to be opened on the firewall.

Device details –describes device's hardware and firmware. Read-only. Populated by pressing Refresh Device.



Device Security – This setting is available only in device models ROSTO, TFACE, TITAN and TOUCH3, but not in MYCRO device model as this is only finger biometric with no display or screen.



Device Pin – This is a numeric pin and should be of length of 4 to 10 digits long. Default is 0000

Copyright © Inner Range PTY LTD July 2026

Disable App Menu on Device –when application menu is disabled, you can still access it by entering pin. By default, app menu is enabled on device.

Lock App Menu on Device – locking disables access to the menu completely. By default, the option is turned off.

Note: This option requires the *Disable App Menu* option to be set.

Display Timeout – Tells how much time display will stay awake. Default value is 600 seconds.

Camera Settings – This setting is available on device Models ROSTO, TFACE, TITAN and TOUCH3 but not MYCRO. TOUCH3 only has “Enable Face Detection” regarding detection and not identification as it is majorly for fingerprint.



Camera Flash Option – Based on the brightness of the room, you can set the LED flashlight to one of the following: ON, OFF, Auto. In the case of a perpetually dark room, users can select “ON” for Flash, to ensure that the face is captured properly. For rooms that have varying levels of darkness throughout the day, “Auto” should be selected.

Enable Face Detection – Select the option to ensure that during authentication, users are asked to show their faces properly. If enabled this is used behind scenes for detection. When enabled even in identification, detection is done with the same captured face even in Identification flow.

Enable Face Auto Identification – Enabling Auto Identification will always keep the camera turned on.

Enable Live Face Detection – Enabling Live Face Detection will ensure that only a LIVE face is detected and prevents spoofing via static photos for face detection.

Enable Multiple Face Detection – Enabling Multiple Face Detection will grant access to the user whose face is closest to the camera. If Multiple Face detection is OFF, the Device will not grant access if there are multiple faces in the frame.

Enable Visual Face Detection Help Guide – Enabling Face Capture Guides will display an orange colour box on the camera to indicate users need to show their faces within that box only.

Enable Capture on Touch – Enabling Capture on Touch will ensure that the camera captures the face on touch.

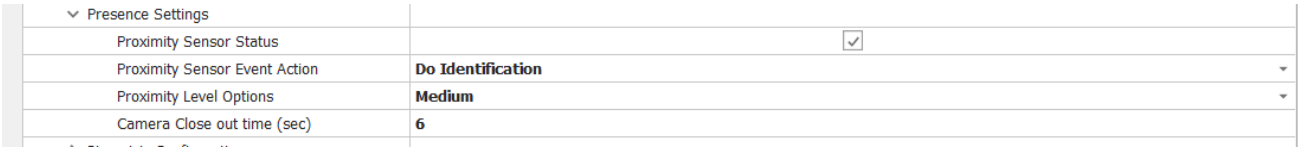
Enable Auto Focus with Presence Detect – Enabling Auto Focus with Presence Detect will ensure that the camera auto-focuses as soon as the presence of a face is detected on it.

Preview Resume Time (sec) – Enter the duration (in seconds) after which the Camera should resume once authentication using other biometric options, such as fingerprint or card is done. The default duration for resuming preview is 5 seconds. Range is 1 to 5.

Copyright © Inner Range PTY LTD July 2026

Face Capture Sound – Set the value for face capture audio volume. Range of value is 1 to 100.

Presence Settings – This setting is available in device models ROSTO, TFACE and TITAN. But not in TOUCH3 or MYCRO device models.



Proximity Sensor Status – Check this to enable Presence Detection. When presence is detected, the device turns the sensor on and starts capturing an image. Enable the “Presence Detect” feature to detect presence and turn the sensor ON only when a user is detected or else it will turn OFF. Here sensor refers to face or finger sensor. By default, this will always be on.

Proximity Sensor Event Action – When presence is detected, Proximity sensor will perform selected action. This action can be “Turn the LCD display On / Active” or “Do Identification” or “Both”. Both is present only in TFACE and TITAN device models

Camera Close out time (sec) – Enter the time duration (5 to 120 seconds) up to which the camera should remain open after a presence is detected. The default timeout duration is 8 seconds. This feature maintains an optimal throughput, particularly during continuous multiple detections.

Biometric Configuration

This setting is available in device models ROSTO, TFACE, TITAN, TOUCH3 and MYCRO. Based on device model only some options will be available for each device.

Finger Biometric Access Rule – In finger biometric access rule, Finger Biometric authentication and any addition identification is asked for based on selection. There is combination of Card, Face, finger, pin options in the dropdown menu. By default, only finger is selected. In ROSTO device model, this dropdown option itself will not be available. In TFACE, TITAN device models both Face and finger are present. In TOUCH3 and MYCRO only Face option is not present.

Card Access Rule – Defines which of supported user interaction sequences (such as Card+Face+Pin, for example) to follow. An interaction is always triggered by a person presenting his card or QR code to a terminal.

Note: the card data sent to a controller after completing an interaction, depends on two factors:

1. Wiegand Output card format for Verification mode.
2. Choice of Default or Actual card

Face Access Rule – Defines which of supported user interaction sequences, triggered by a person presenting his face or finger to the terminal, to follow.

Wait Time(sec) – Edit the amount of time before authentication times out between 3 and 60 seconds. By default, authentication times out after 10 seconds

Biometric Device Mode – Select either "Verification" or "Identification".

Identification is the default mode.

Selecting "Verification" will disable biometric capabilities of the terminal, forcing it to operate as a *card_reader_with_lookup* device – after a card swipe, the card data will be verified against the

Copyright © Inner Range PTY LTD July 2026

terminal's list of users; if there is a match, the actual card data or a user's *default card* will be sent to a controller. The "*which card to send to controller"* choice is configurable:

Biometric Device Mode	**Identify**
Disable Biometric Verification	Verify
Disable Pin Verification	Identify

In "Identification" mode, the terminal operates as a normal biometric reader device. It can also handle user interaction sequences which are triggered by presenting a card or QR code (Card+Face, etc)

Verify Finger Biometric Security Level – Accuracy of user verification can be set to "Low", "Medium", "High", "Very High", or "Maximum". "Medium" is the default accuracy.

Identify Security Level – Accuracy of user identification can be set to "Low", "Medium", "High", "Very High", or "Maximum". "Medium" is the default accuracy.

Spoof Level – You can set Spoof Level settings to prevent fake finger authentication. This is present in some of the Lumidigm sensor supported devices like TITAN.

Disable Biometric Verification – If checked, this will disable the Biometric (Finger & Face) Access Rule. All other credentials will be asked as per the access rule set inside card access rule. By default, this setting is unchecked.

Disable Pin Verification – If checked, this will disable the Pin verification for user. By default, this setting is unchecked. This is option is not present in MYCRO device model.

Disable Identification – If checked, this will disable the Identification when the device is in Identification Mode. By default, this setting is unchecked.

Face Verification Level –Accuracy of face matching in *verification* mode. "Medium" is the default accuracy.

Face Identification Level – Accuracy of face matching in *identification* mode. "Medium" is the default accuracy.

QR code settings

Available in all device models except MYCRO.



QR Code Status – Enable/disable this to turn QR Code Authentication feature ON or OFF. Invixium device treats QR Card as any other Card and can be part of Card Access Rule.

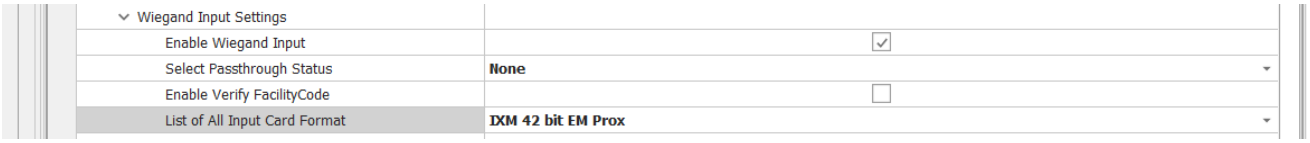
QR Code Auto On – Enabling this feature will open the camera automatically to scan the QR-Code

QR Code Scan Type – For all Invixium biometric devices, QR Code scanning type is "Normal" by default.

Wiegand Input Settings

This setting is available in device models ROSTO, TFACE, TITAN, TOUCH3 and MYCRO. Below are settings on UI screen

Copyright © Inner Range PTY LTD July 2026



Enable Wiegand Input – By checking the checkbox, one can enable Wiegand cards being read by the device.

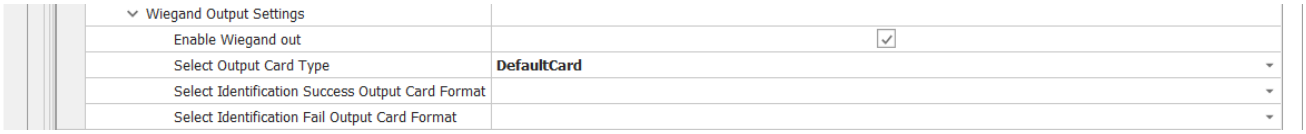
Select Passthrough Status – Options under this are None, Wiegand Passthrough and Card Passthrough. This is the way in which data is communicated by the biometric device to the controller. Wiegand Passthrough will send entire Wiegand data to the controller. Card-Passthrough will send only the custom card data to the controller. Defines the terminal's behaviour when acting as a card reader device.

Enable Verify Facility Code – By checking the checkbox, will enable verifying of Facility Code of the card.

List of All Input Card Formats – This is a multi-selection dropdown box. Invixium biometric devices support up-to a maximum of 5 Card Formats. Make a selection of card formats and save. Only 4 card formats are default provided for every Invixium Biometric Device. Note:- For purpose of ease, one can add card formats into master terminal device via IXM web application. Use this terminal to retrieve configuration and edit / save accordingly. Then copy this configuration across all other devices of same device type.

Wiegand Output Settings

This setting is available in device models ROSTO, TFACE, TITAN, TOUCH3 and MYCRO. Below are settings on UI screen



Enable Wiegand Out – the option controls whether the terminal will send card data to a controller, or not. For all practical purposes, it must always be enabled.

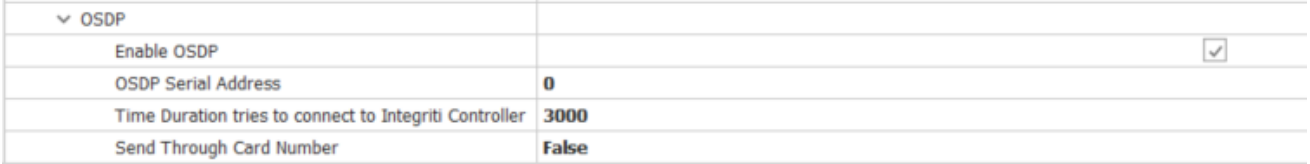
Select Output Card Type – Selecting Default Card will send same card details for all the identification of specific user and selecting Actual Card will send actual card detail to the controller.

Select Identification Success output card format – The card formats populated are the one's that have been configured on Master Terminal Device. Selected card format that will be on successful identification of user and send to controller. Only one can be selected and UI is dropdown for selection.

Select Identification Fail output card format – Selected card format will be used for sending reserved card data on failed identification of user.

OSDP

Set of parameters controlling terminal's behaviour as OSDP card reader.



Copyright © Inner Range PTY LTD July 2026

Card Formats configuration

Each terminal comes with a preset ‘factory defaults’ list of card formats; those cannot be modified or erased.

The integration offers a mechanism for extending the ‘factory defaults’ card formats list.

The plugin installer places a card formats definition file, called **ConfigurableCardFormats.json**, into **IRPlugins\PreRequisites\InvixiumBiometrics** folder. The file supplied by the installation executable contains a list of ‘popular’ card formats.

- 26-bit Wiegand with Sitecode

  The entry is disabled, as it is also one of the ‘factory defaults’ formats.
- 48-bit Corp 1000
- 35-bit Corp 1000
- HID 37 Bit (H10302)
- Sifer 56bit with Sitecode

Card formats defined inside the file will be automatically loaded into every terminal.

A customer can edit the file and add new format definition to the list. Restart the integration to push new card format definitions into terminals.

Each entry within this file has a unique ID. The first 20 positions (IDs) are reserved for card formats configured from IXM Web tool, in case a customer uses it.

When adding a new format, ensure that it’s ID is unique. The ID range for additional formats added by the user should start from 21.

The file structure contains definition of ***EraseBeforeLoad*** parameter. When set to True (default), the integration will wipe all existing card formats from a terminal, before loading the new set. If False, the integration will not erase anything; existing card formats with same identifiers as in configuration file will be replaced, new entries will be added.

Q: Why do we ever need EraseBeforeLoad == false?

A: A customer can use IXM Web to configure card formats, in addition to using the mechanism described in this chapter. EraseBeforeLoad=false will preserve the formats created by IXM Web.

Parity bits

The structure allows configuring card formats with or without Parity bits. The Sifer 56bit entry can be used as an example. Be aware that Integriti controllers do not perform Wiegand bits verification at all, so there is not real need to have Parity Bits configuration as part of card format.

Copyright © Inner Range PTY LTD July 2026

Operational considerations

Networking

To receive asynchronous notifications from Biometric devices, the following Inbound rules must be configured on the Integriti Integration Server Firewall:

- 9000 for Invixium Device Push Notifications
- 9001 for Invixium Device Heartbeat Notifications

To communicate to devices, the SDK uses port 9734. This port must be enabled on the firewall for Outbound connections.

Keeping terminal's clock synchronised

It is important to keep terminal clock synchronised with Integriti servers and controller's time. We recommend configuring a scheduled task which runs periodically (at midnight?) and invokes the *Set Device Time* command on each connected terminal.

Copyright © Inner Range PTY LTD July 2026

COMMANDS

Biometric Device Commands

Many commands are offered via context menu, when Right-Clicking on a terminal in SystemDesigner/GateKeeper Biometric Devices page.

Most of the below commands are integrator/admin level commands that a normal Integriti user would not ordinarily need to access for day-to-day operations. Careful consideration should be made to restricting this category of device within existing Operator Type granular permissions so that only authorized operators may view, edit, or otherwise issue commands against these devices.

The following commands are supported:

Push Configuration This command pushes configuration saved in Integriti DB to Biometric Device.

Set Device Time Sets Time on Biometric Device.

Delete All Users Deletes All Users on Biometric Device.

Delete All Logs Removes all logs stored on the reader. Logs correspond to Transaction Logs.

Reboot Device Restarts the device.

Factory Reset Resets all data to factory state on the device.

Restore Device Configuration to Default Restores Device Configuration to Default. All settings that are provided via Integriti can be restored back to their default state. Option is provided to Restore all settings at once or each specific setting.

Enable/Disable Telnet on Device Enables or disables telnet on the device. Used for Troubleshooting.

Download Device Logs Use the command to download device logs. May be needed for Troubleshooting.

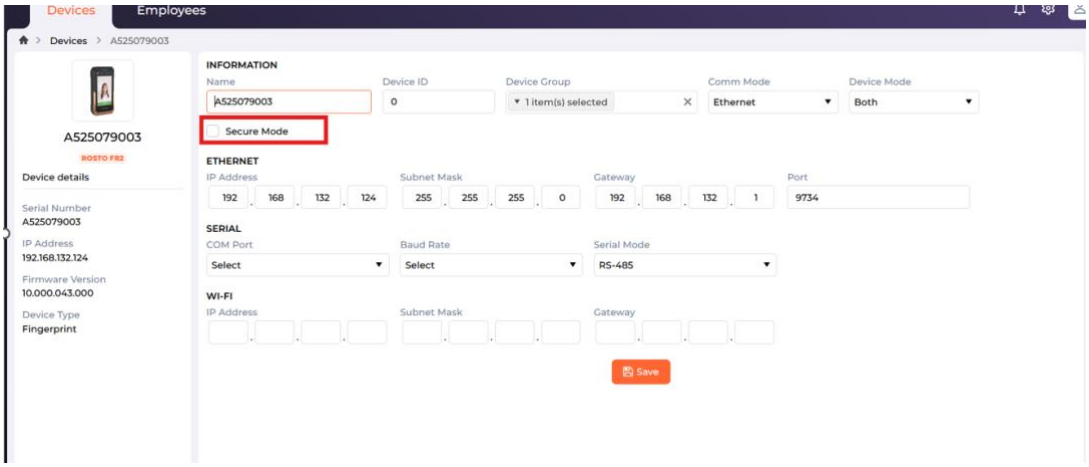
Update Firmware Upgrades Firmware via providing path to the .bin file of the new firmware version.

Copyright © Inner Range PTY LTD July 2026

TROUBLESHOOTING

Common mistakes

1. Leaving “Secure Mode” flag ticked, after configuring a terminal in IXM Web.

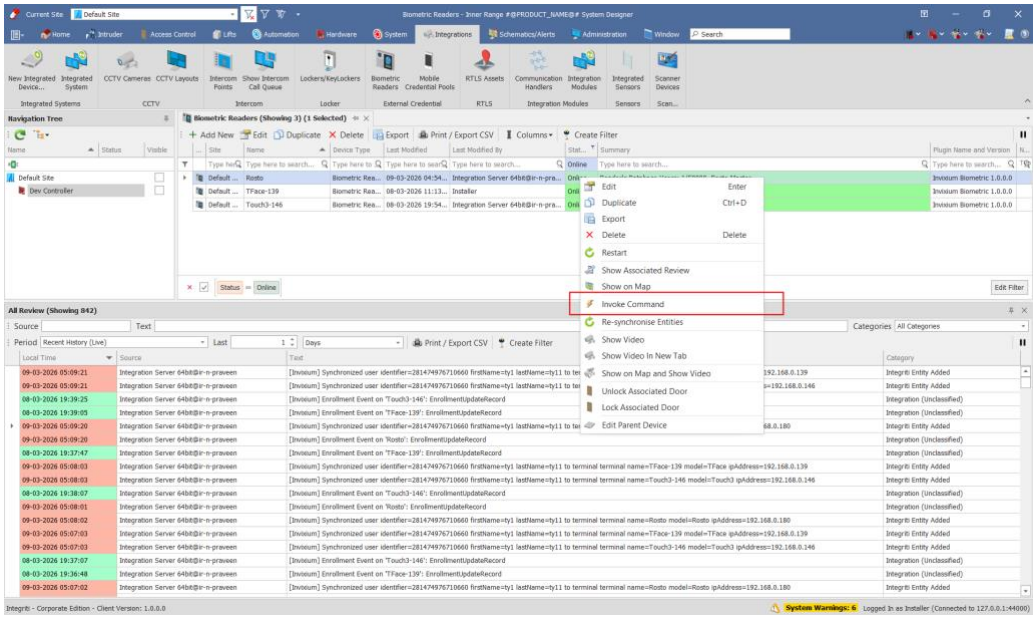


The Secure Mode flag “locks” the terminal to IXM Web, preventing any other applications, such as Integriti, from accessing the device. Make sure the ‘Secure Mode’ is unticked before exiting the IXM Web tool.

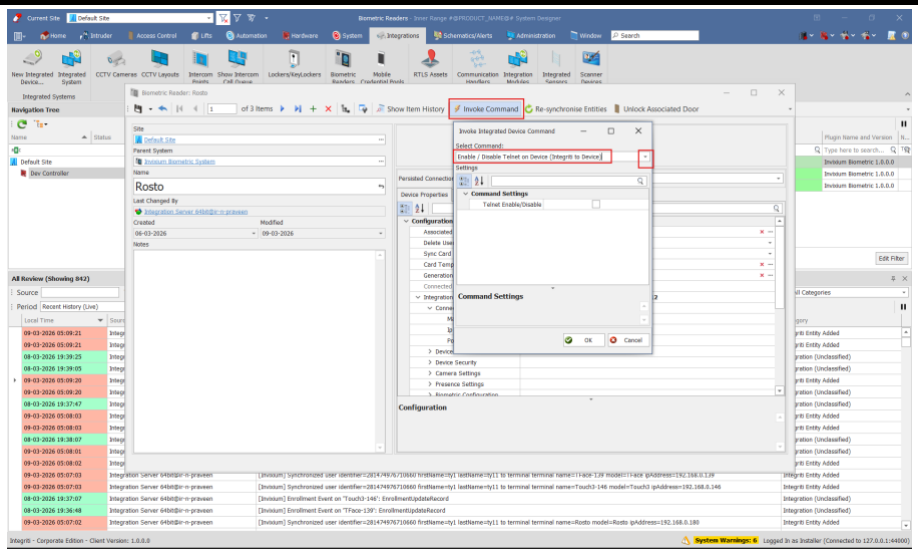
2. Overwriting correct Web Server IP Address and port parameters – which should point to Integriti server host – with invalid values from IXM Web UI.

Enabling Telnet

When there is need to troubleshoot a device, an Invixium support person may request ability to access device remotely, by enabling Telnet on the unit. Telnet can be enabled or disabled via “Invoke Command”.

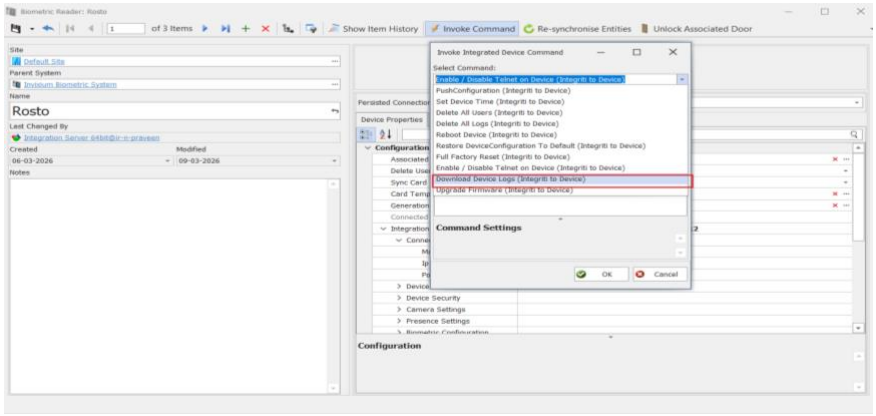


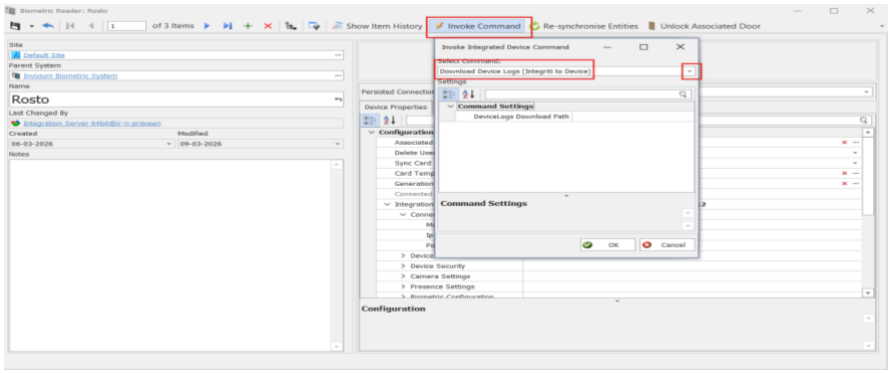
Copyright © Inner Range PTY LTD July 2026



Retrieving Device Logs

Retrieving Logs from a device and sharing with support team may become necessary for troubleshooting:





Note: the logs will be saved on a computer running Integriti IntegrationsServer64. When entering a destination folder for the logs, chose an existing folder on this computer. The name must be entered as a local path, like “c:\MySupport\InvixiumLogs”.

Copyright © Inner Range PTY LTD July 2026

BIOMETRIC CAPABILITIES

Core Biometric Capabilities

Feature	Feature Description	Y/N
Fingerprint Biometrics	The Integration supports the use of Fingerprint Biometric Readers	✓
Face Biometrics	The Integration supports the use of Face Biometric Readers	✓
Finger vein Biometrics	The Integration supports the use of Finger vein Biometric Readers	✗
Receive Events from the Biometric System	The Integration processes incoming notifications from the terminals	✓
Create Child Devices from Biometric Configuration	Child Biometric Readers will be automatically discovered and created on Refreshing Child Devices	✗
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.	✓
Connect to Biometric Reader	Connect to Individual Biometric Readers instead of operating through a Server or System managing all connected readers.	✓
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.	✗
Configure Biometrics from the Web Interface	Use the Integriti Web Interface to Enrol and Manage Biometric System or Readers.	✓
Trigger Actions in the Biometric System	Trigger actions or commands in the Biometric system directly from Integriti.	✓
Sync Time (via NTP)	Sync the time of the Biometric system and Integriti to match via an NTP.	✗
Display Connection Status to Biometric System	Display whether Integriti is currently connected to the Biometric system.	✓
Receive Events/Alarms from the Biometric System	Log events/alarms occurring on the Biometric system to Integriti's Review.	✓
Trigger Integriti Actions on Biometric Events/Alarms	Trigger actions to automatically occur in Integriti whenever specific events/alarms are received from the Biometric system.	✓
Generate Alerts from Biometric Events/Alarms	Automatically generate Alerts tied to a specific Camera in Integriti whenever specific events/alarms are received from the Biometric system.	✗

Copyright © Inner Range PTY LTD July 2026

Advanced Biometric Capabilities

Feature	Feature Description	Y/N
Automatically download Biometric Configuration into terminals	Refreshing Child Devices will automatically download saved configuration into terminals.	✓
64-bit Integration Server Support	The integration supports being run on the 64-bit integration server.	✓
Show Biometric Status	The current online/offline status of configured Biometric Readers will be visible directly through Integriti.	✓
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	✓
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.	✓

Copyright © Inner Range PTY LTD July 2026



Global Headquarters

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

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

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

Inner Range Canada
+1 (844) 588-0874
sales.canada@innerrange.com

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

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

INNERRANGE.COM