integriti
INTEGRATED SOLUTIONS

INTEGRITI TRAKA KEYLOCKER PLUGIN

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

ASIAL MEMBER
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
GOLD MEMBER

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

Certified System
Quality
ISO 9001

Table of Contents

UPDATING TO V1.3 AND NEWER FROM V1.2 AND OLDER **2**

DESCRIPTION **3**

INTEGRITI TRAKA PLUGIN **3**

REQUIRED INTEGRITI LICENSES 3
MINIMUM INSTALLED INTEGRITI VERSION 3
REQUIRED INTEGRATION LICENSE 3
TESTED AGAINST 3

DEVICE ATTRIBUTES **4**

SETTING UP HTTPS IN TRAKA **5**

USER SYNCHRONISATION **5**

SYNCHRONISED USER PROPERTIES 5
USERS AND TRAKA REGIONS 6
ASSIGNING ITEM ACCESS GROUPS 6
SYNCHRONISING CARDS WITH USERS 7
Syncing with Multiple Cards *7*
Utilising Custom Card Formats for Transforming Card Data *7*

TROUBLESHOOTING **8**

Updating to v1.3 and Newer from v1.2 and Older

Please note that in version 1.3 of the Traka Integration, an error was fixed related to data cached on using 'Refresh Device'. When upgrading to v1.3 or newer, ensure that the Device is refreshed once the upgrade is completed.

Description

The Integriti - Traka integration provides two functions: User synchronisation and Event logging. User information within Integriti can be synchronised with Traka to facilitate ease of administration and mitigate data entry inconsistencies. Alarms and events can be sent from Traka into Integriti to leverage Integriti's powerful alarm management and reporting capabilities.

Integration Features

- Integriti - Traka User Synchronisation:
  - Integriti Users may be sent to Traka Web to be used with Traka Lockers.
  - Includes an option to also synchronise Integriti Users' Card Data to be used with Traka.
  - Note: This is a one-way synchronisation; changes made to a User through Traka on synchronised users will not be reflected in Integriti and may be deleted when Integriti pushes User updates.
- Traka Event Logging:
  - Events and Alarms from Traka will appear in Integriti Review to be leveraged for reporting and alarm management.

Integriti Traka Plugin

Required Integriti Licenses

The Integriti Traka KeyLocker Integration requires an Integriti Pro/Infiniti v23 license or higher to be present on the product key running the integration.

Minimum Installed Integriti Version

The Integriti Traka KeyLocker Integration is only compatible with an installation of Integriti Pro or Infiniti that is v22.0 or higher.

Required Integration License

This Integration also requires the "KeyLocker Integration" license (part number 996934).

Tested Against

The Integriti Traka keylocker plugin v1.3 was built and tested against the Traka Web v3.6.

Device Attributes

Connection	
Login Name	**SuperAdmin**
Password	**********
Traka Hostname	**192.168.140.200**
Traka User Sync Port	**10700**
Traka Event Listener Port	**10699**
Traka Connection Type	**Traka**
Use HTTPS	☑
Certificate Validation Mode	**Specified Thumbprint**
Certificate Thumprint	
Request Timeout	**00:01:00**
Logging	
Log Verbosity	**Debug**
User Sync	
Sync Users	☐
Sync User PIN	☐
Card ID Contents	**Card Number**
Event Manager	
Listen For Events	☑
Module Ping Interval In Seconds	**15**

Connection Details

- *Login Name* – The Username of the User to connect to the server with. The User should have sufficient permissions configured to allow use of all of the features of the plugin to be used.
- *Password* – The password of the User to connect to the server.
- *Traka Hostname* – The hostname of the machine hosting the Traka Integration Engine.
- *Traka User Sync Port* **–** The port to connect to. Default value is 10700
- *Traka Event Listener Port* – The port on which the Event Manager will listen for Events from Traka. Default value is 10699
- *Traka Connection Type* – The type of connection the Integration should use.
- *Use HTTPS* – If set, the Integration will use HTTPS when connecting to Traka.
- *Certificate Validation Mode* **–** Select the validation mode to use when connecting to Traka with a certificate.
- *Certificate Thumbprint* – Enter the thumbprint of the certificate used by the Traka HTTPS connection when its validation mode is 'Specified Thumbprint'.
- *Request Timeout* – The time before requests made by this Integration will timeout.

Event Manager

- *Listen For Events* – If enabled, a Traka Module will be setup to send Events to this Integration.

User Syncing

- *Sync Users* – If enabled, Users from Integriti will be synchronised to Traka.
- *Card ID Contents* – Choose the source of data to populate a Traka User's Card ID field.
- *Custom Card Format* – The Card Format that will be used to convert a User's Card Data for Traka.

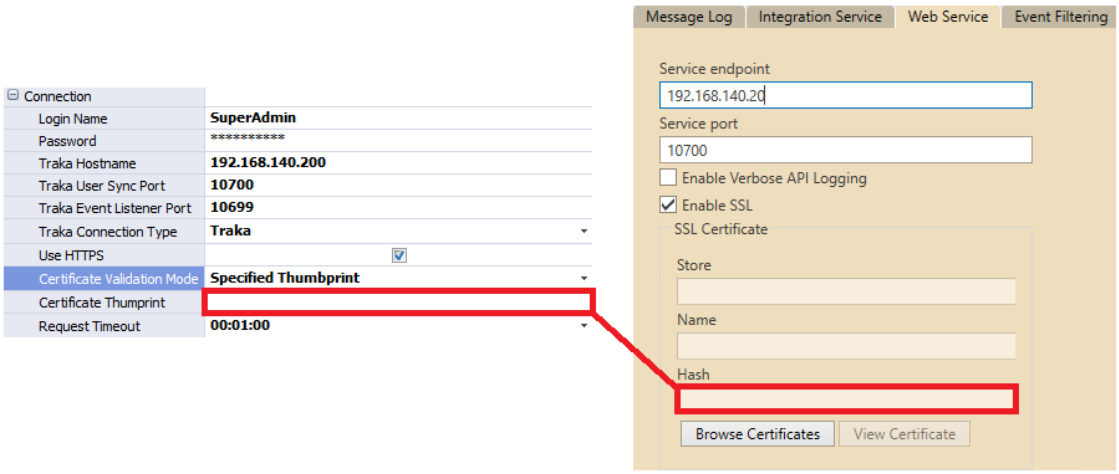
Setting Up HTTPS in Traka

HTTPS can be used to communicate with Traka which can be enabled in the Integrated Device using the “Use HTTPS” property and certificate settings in it. However, this also requires some set up in the Traka Monitor on the machine hosting the Traka Software.

With the Traka Monitor open, navigate to the “Web Service” Tab. To enable this functionality, tick the “Enable SSL” check box, then select a certificate to use by clicking “Browse Certificates”.

When using the “Specified Thumbprint” option in the Integration, you can compare the “Certificate Thumbprint” property in the Integrated Device and the “Hash” field in the Traka Monitor to ensure the two match.

Note: The thumbprint cannot be copied directly from the “Hash” field of the Traka Montior and will need to be taken from elsewhere.



User Synchronisation

Synchronised User Properties

As part of the User synchronisation process, the following User fields are sent to Traka:

- First Name (required)
- Last Name (required)
- Active Date
- Expiry Date
- User Expired
- Security or Qualify PIN

It will also synchronise the custom fields created by the Integration:

- Traka Keypad ID
- In All Traka Regions

Users and Traka Regions

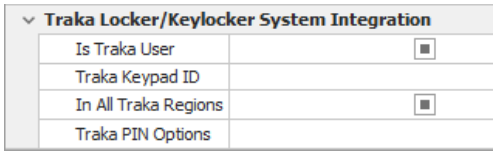
A User that will be synchronised to Traka must belong to at least one Region in Traka to be valid due to Traka's requirements for Users to have one Region.

There are two ways that a User can belong to a Region:

1. Having the 'In All Traka Regions' custom field ticked
2. Being assigned an Item Access Group via Permission Groups assigned to the User.

The next section describes how Item Access Groups can be associated with Permission Groups and how this assigns the Groups to a User.

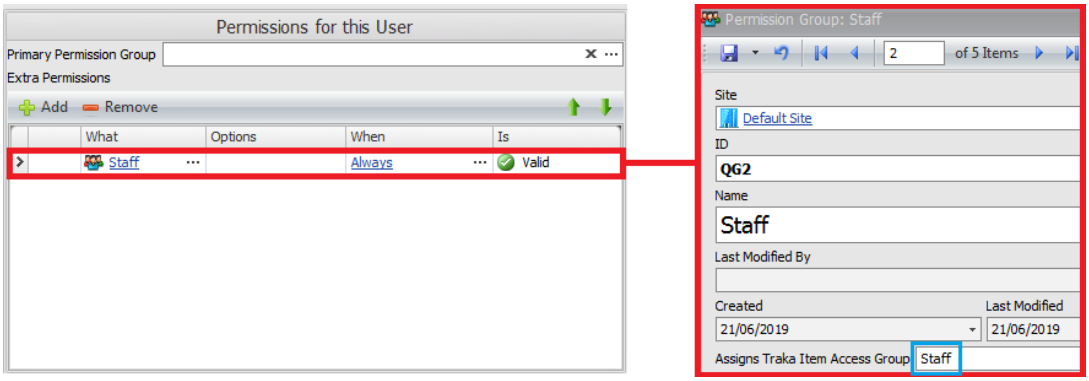
Note: The 'Is Traka User' and 'In All Traka Regions' custom fields can be found in a 'Null' state for Users that existed before the Integration was created and these Custom Fields were created. This can be seen in the image beside this note.



Users that are in this state will have these values treated as False.

Assigning Item Access Groups

Item Access Groups determine the items that a Traka User has access to. To assign Item Access Groups to a User synchronised from Integriti, we assign Permission Groups that are associated with an Item Access Group.



When editing a Permission Group, you can use the "Assigns Item Access Group" custom field to choose an Item Access Group that it will represent. This field is populated when "Refresh Device" is used on the integration's Integrated Device. Then, simply assign Permission Groups to Users to be synchronised in order to assign the User that Item Access Group.

In the example above, the Item Access Group "Staff" has been assigned to the Permission group of the same name, then when the "Staff" Permission Group is assigned to a User, it will assign the "Staff" Item Access Group to that User in Traka.

The custom field may not be visible by default unless a custom layout is used for the Permission Group editor. To access the custom field, refer to the 'Accessing Custom Field Without a Property Grid' section of the 'Integriti Keylocker Integration Manual' documentation provided with the Integriti core software.

Synchronising Cards with Users

A User's Card ID can be synchronised with the User to Traka for use with lockers in the system. The contents of the Card ID field can be configured in the Integrated Device under the "Card ID Contents" property.

Syncing with Multiple Cards

If Users use multiple cards within Integriti and require card syncing to Traka, which only allows for one Card ID to be used per User, the Card Template Ranking custom field can be leveraged to give priority to certain Card Types. The lower the number assigned to the Template, the higher priority the Template is considered by the Integration.

Note: The Integration considers Templates with no entry in its custom field to be of the lowest priority. As such, it is suggested that values are only assigned to Templates used with the Integration that need to be high priority to keep the amount of values that need to be assigned to a minimum.

Utilising Custom Card Formats for Transforming Card Data

The Integration also allows Operators to assign a Card Format to be used in place of the Integration's standard Card Data transformation. This can be assigned in the Integration's configuration using the "Custom Card Format" field.

This feature is typically only used if a system is using a Custom Card Format for the Keylocker system, but can also be used to transform card data to a different desired format.

Troubleshooting

New Traka Users stuck on "In Progress" status

Traka Users may get stuck in this state with no access to Traka Systems when Traka Web is configured to not set Users to Active on Systems by default.

This behaviour can be changed through the Traka Web Admin program, selecting "Default Settings" and setting the below property to "True":