INTEGRITI PROXYCLICK VISITOR MANAGEMENT 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

Certified System
Quality
ISO 9001

Table of Contents

Description

The Proxyclick Integration is designed to manage the access control side of the Visitor Management process by handling events in the Proxyclick system, including generating Users for Visitors, assigning them Permissions and creating credentials to be used at readers throughout a designated site.

The Proxyclick Integration also handles check-out events by suspending the credential associated with the Visit, preventing the Visitor from accessing the site further, but preserving the associated User for future use as well as record keeping through Integriti's Audit feature.

Integration Features

- Visitor management:
    - When a visit is created or updated in Proxyclick, assigns a User to represent the visitor, either creating a new one or finding a User with a matching email address.
    - Assigns permissions to this User based on the host, matched against an existing User's email address.
    - Creates a credential based on a configured Card Template.
- Check-in:
    - On check-in, the Integration will activate the Credential given to the Visitor's User, allowing access to the permissions assigned to them in the Provisioning process.
- Check-out:
    - On check-out, the Integration will suspend or delete the credential from the Visitor's User, preventing them from further accessing the site or permissions assigned to them.

Configuration Checklist

- Install Proxyclick Integration
- Create new Proxyclick Integrated System
- Configure Integrated System
    - Configure Proxyclick account credentials and URL
    - Set email address custom field
        - Use 'New Field' to create a new custom field.
    - Set Proxyclick Location
        - Refresh Device to auto-fill this or populate the drop-down list.
    - Set Card Template
        - Use Refresh Device to automatically create a Card Template and Card Format.
- Save Integrated Device
    - Ensure Integration is now running
- Apply TLS Certificate to the port the Integration is listening on
- Configure Network Settings
    - Open ports receiving requests on the firewall
    - Set port forwarding destination of traffic to machine running Integration
- Use Proxyclick Dashboard to configure webhook settings

Integriti Proxyclick Integration Compatibility

Required Integriti Version License

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

Minimum Installed Integriti Version

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

Licensing Requirements

The Integriti Proxyclick integration requires the "Visitor Management Integration" license (part number 996935).

Tested Against

The Integriti Proxyclick Integration v1.0 was built and tested against version 1 of the Proxyclick API, as was available at the time of release.

Initial Setup

In order to set up the Proxyclick Integration, the following steps must be performed.

Installation

1. Close all instances of the Integriti software suite on the PC to install the integration on and stop all running Integriti services on the Integration server.
2. Download and run the Proxyclick Integration installer on all Integriti servers first, before running on all client workstations that will be interacting with the integration, including updating the integration's configuration and invoking commands.
3. After the installation has completed, remember to restart all of the services that were stopped prior to running the installation.
4. 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 (for supported OS's) 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. For this Integration, the Persisted Connection is responsible for checking the status of existing visits upon restart and listening for webhook events. The following options are available:
   - **Automatically Maintain Connection on Any Single Server** – This will ensure that there is always one Integriti Integration Server listening for webhook events, 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 receive webhook requests. If the specified server goes offline, the integration will stop listening until the specified integration server comes back online.
   - **Simultaneously Maintain Connection on All Servers** – This option will establish a connection to the 3rd party system and listen for webhook requests on every Integriti Integration Server at the same time. This can result in the most requests 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 fewer requests being made to 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 Proxyclick. For more details on how to configure integration specific properties, please refer to the following steps and 'Device Attributes' section.
6. Select the Save button to save the newly created device.

Save and close the editor window for the new device and, if enabled, a persisted connection will automatically begin to Proxyclick, merge existing visits and updates for today, and start listening for further events.

Host/Visitor Custom Fields

A custom field is required to identify the Integriti User associated with Proxyclick employees and visitors by email address, corresponding to the email address in Proxyclick. The custom field keyname that should be used is selected under the 'Core Visitor Settings' category in the Integrated System attributes. An existing custom field may be selected using the dropdown; alternatively, a new custom field can be created using the 'New Field' buttons, creating an appropriate field for use with the Integration.

Additional data to import from Proxyclick to Integriti may be selected in the 'Extra Visitor Data' category.

Card Template

A Card Template is required to create credentials for visitors using the Integration. It is suggested to create a Card Template and Format using 'Refresh Device' on the Integrated System. If no Card Template is already provided, this will create and assign one using the following attributes:

- Card Format
  - Name: Proxyclick Card Format
  - Card Type: Wiegand Site (Complex)
  - Wiegand Card Type: NBit
  - Total Bits: 26
  - Card Number Offset: 1
  - Card Number Length: 24
- Card Template
  - Name: Proxyclick Card Template
  - Card Format: Proxyclick Card Format

Note: A different Template can be used in place of one generated by the Integration, however, only when a different reader or card number encoding method is needed for the system.

Webhook Listener URL

The integration server will listen for HTTPS requests matching a URL pattern that can be configured as seen below:

˅ Listener URL	**https://*:443/Proxyclick/**
Hostname	*
Port	**443**
Base Path	**/Proxyclick**
Webhook Password	*******

This URL defines two key things:
- The hostname the Integration will listen on in the private network it belongs to
- The port and base path of the URL target to be configured in Proxyclick.

Setting the hostname to '*' will make the Integration listen for any requests with the matching port and path that are sent to the server hosting it. You can also specify an IP address of a NIC on the hosting server to restrict the Integration to listening for requests sent to that IP only as well as having a matching port and path.

In addition, a 'Webhook Password' should be specified under the 'Connection' category to authenticate webhook requests using basic HTTP authentication. If this is used, the same password must be specified in the Proxyclick webhook settings, along with the username 'proxyclick'.

Note: If multiple Integrated Devices are being used to communicate with multiple Proxyclick sites, then the Base Path property must be appended or prepended with some string to ensure that the Integrated Systems are not listening on the same URL.

Firewall Configuration

If there is a firewall running on the Integration Server or network, it will be necessary to allow access to the port used by the Integration through the firewall. To allow access using Windows Firewall, follow these steps.

1. From the Start menu, open 'Windows Defender Firewall with Advanced Security.
2. Select the 'Inbound Rules' category.
3. Select 'New Rule'.
4. Select the 'Port' rule type.
5. Select TCP and enter the listening port number configured above.
6. Select 'Allow the connection'.
7. Ensure that the rule is enabled for the type of network configured on the Integration Server computer.
8. Give a name (such as 'Integriti Proxyclick Integration') and optional description, then save the rule.

Port Forwarding

If the Integration is hosted on a server on a private network, it is likely that some Port Forwarding rules will need to be set up on routers to ensure that requests from Proxyclick can reach the server hosting the Integration.

This step requires two things:
- The Port number on which the requests will be sent
- The local IP address of the machine that hosts the Integration

The Port number is simply the Port that was set in the Integrated Device settings as part of the URL set up, and the Port Forwarding rules will need to use the IP address of the host machine as a destination, so that traffic on the opened port will be sent to the Integration.

Assigning TLS Certificate

It is strongly recommended that the webhook requests use HTTPS to ensure the security of the connections made between Proxyclick and Integriti. This means that the server running the Proxyclick integration will need a SSL/TLS Certificate to be bound to the Port it is configured to listen on. This certificate cannot be self-signed, as that will not be viewed as valid by Proxyclick. The steps involved to bind this certificate to the Integration's port on the host machine will vary depending on the Operating System of the host machine.

This step may not need to be taken for public facing machines that already utilise HTTPS communications. If the Integration is running on a machine such as this, an existing TLS certificate may be used with the Integration. So long as the certificate is valid for the Integration server, no further steps need to be taken.

Configuring Proxyclick to Send Requests

Once the above steps have been completed, it is necessary to configure a webhook integration in Proxyclick to send events to the Integration.

1. Open the company dashboard in the Proxyclick web application.
2. Click ⚙ 'Settings' in the sidebar.
3. Select the 'Integrations' category.
4. Select 'Settings' under 'API and Webhooks'
5. Click 'Add Webhook'
6. Enter any name for the webhook.
7. Enter the destination URL via which the Integration can be reached. This will include the public hostname or IP address of the Integration server and the Base Path specified in the Integrated System attributes.
8. If a Webhook Password is to be used, enable Authentication and provide the username 'proxyclick' and the Webhook Password specified in the Integrated System Attributes.
9. Ensure that the following events are enabled: visitor check-in, visitor check-out, visit created, visit updated, meeting deleted
10. Save the webhook settings.

Name of the webhook

Integriti Proxyclick Integration

Destination URL

https://example.com/proxyclick

Authentication 🟢

If the destination application requires basic HTTP authentication, please enable authentication and add username and password

Username

proxyclick

Password

●●●●●●●●●●

Trigger events

Select at least one

☑ Visitor check-in
☐ Visitor on-site
☑ Visitor check-out
☑ Visit created
☑ Visit updated
☑ Meeting deleted
☐ New booking
☐ Booking updated
☐ Booking deleted
☐ Employee check-in
☐ Employee check-out
☐ Employee check-in deleted

Device Attributes

Configuration	
∨ Connection Configuration	admin@example.com
∨ Connection	
Login Name	admin@example.com
Password	********
∨ Listener URL	http://192.168.0.157:34567/proxyclick/
Hostname	192.168.0.157
Port	34567
Base Path	/proxyclick
Webhook Password	************
Location Name	Sample Location ▾
∨ Logging	
Log Verbosity	Debug ▾
> Core Visitor Settings	
> Check-in and Check-out Settings	
> Visitor Permissions	
> Extra Visitor Data	

Connection

- **Login Name** – The email address to use to log in to Proxyclick.
- **Password** – The password to use to log in to Proxyclick.
- **Listener URL** – The local URL on which to listen for webhook requests. See the section 'Webhook Listener URL' for more details.
- **Webhook Password** – A password used to authenticate webhook requests.
- **Location Name** – The name of the Proxyclick location that this Integrated System should manage. If there is only one site accessible with your Proxyclick account, Refresh Device will automatically fill this in; it will also populate the drop-down list.

Core Visitor Settings

∨ Core Visitor Settings		
Email Address Custom Field	cf_EmailAddress ▾	New Field
Card Template	▪ **Proxyclick Card Template**	✕ ⋯
License Plate Card Template	▪ **License Plate**	✕ ⋯
Card Number Custom Field	**Card Number** ▾	

- **Email Address Custom Field** – The keyname of an Integriti User custom field to use to identify visitors and hosts by email address. This is required as it is used to identify the Integriti User associated with an employee in Proxyclick.
- **Card Template** – The Card Template used to create credentials for visits. This is required; if left empty, Refresh Device will automatically create a card template.
- **License Plate Card Template** – The Card Template used to create credentials for visits using the license plate specified in Proxyclick. This is optional; if no card template is specified, the Integration will not create license plate credentials.
- **Card Number Custom Field** – The name of the Proxyclick custom field that defines the card number to create for a visit if provided. If left empty, the Integration will not create credentials this way.

Check-in and Checkout Settings

⌄ Check-in and Check-out Settings			
Enforce Visit Times	**Start and End Time**		⌄
Card Handling on Check-out	**Suspend Cards only**		⌄
Clear Permissions on Check-out		☐	
Cancel User On Check-out		☑	

- **Enforce Visit Times** – Specifies whether to set a visitor's User's start and/or expiry time based on the scheduled start and end times of the visit. If set, the visitor User will be considered expired outside the scheduled times, even if still checked in.
- **Card Handling on Check-out** – Specifies what to do with the Cards assigned to a visitor when the visitor checks out or the visit ends.
    - **Suspend Cards only** – Suspends the Cards, preventing them from being used but preserving all data.
    - **Suspend Cards and remove from visitor** – Suspends the Cards and removes them from the visitor's list of assigned Cards.
    - **Delete Cards** – Deletes the Cards from the Integriti database. New Cards will be created if the visitor's status is reset to Expected.
- **Clear Permissions on Check-out** – If set, a Visitor's User will have their permissions cleared when the visitor is checked out.
- **Cancel User on Check-out** – If set, a User will be Cancelled, preventing all access requests from the User, when the visitor is checked out.

Visitor Permissions

⌄ Visitor Permissions			
Primary Permission Group Source	**From Visitor's Proxyclick Custom Field**		⌄
Custom Field Name	**Visitor Type**		⌄
Custom Field Value Mapping	**0 Items**		+
Supplementary Permissions	**From Host**		⌄

- **Primary Permission Group Source** – Choose how to assign a primary permission group to the User created for a visitor.
    - **From Host** – Gives the visitor the same primary permission group as the host.
    - **Specified Value** – Gives the visitor the specified primary permission group.
    - **From Host's Permission Group Custom Field** – Assigns the permission group whose name is specified in an Integriti custom field of the host's User.
    - **From Visitor's Proxyclick Custom Field** – Assigns a permission group according to the value of a Proxyclick custom field on the visitor, using a specified mapping.
- **Primary Permission Group** – When 'Specified Value' is selected, the primary permission group that should be assigned to visitors.
- **Custom Field** – When 'From Host's Permission Group Custom Field' is selected, the keyname of the Integriti User custom field that should determine the permission group for the user's visitors.
- **Custom Field Name** – When 'From Visitor's Proxyclick Custom Field' is selected, the name of the Proxyclick custom field that should determine the permission group for the visitor.
- **Custom Field Mapping** – When 'From Visitor's Proxyclick Custom Field' is selected, if this is left empty, the Integration will assign a permission group with the same name as the custom field value. To override this, specify a list of value-permission group pairs.

The first entry in this list with a value that matches the value of the Proxyclick custom field will assign its permission group to the visitor. If the custom field is left empty in Proxyclick, an entry with an empty value will be used if one is provided.

- **Supplementary Permissions** – Choose how to assign extra Permissions to the User created for a visitor.
  - **None** – No extra permissions will be added.
  - **From Host** – Gives the visitor the same extra permissions as the host.

Extra Visitor Data

∨ Extra Visitor Data		
∨ Visitor Properties	1 Items	+
∨ [0]	Field 'cf_MobileNo' set to Proxyclick f...	×
Property Name	**Mobile Number**	∨
Mode	**Keep updated**	∨
Value Source	**From Proxyclick Field**	∨
Field	**Mobile Phone Number**	∨
Visitor Area/Location Options	**Set on Check-in and Check-out**	∨
Visitor Area/Location Set on Check-in	◇ **Area 1**	× ···
Visitor Area/Location Set on Check-out	◇ **Area 2**	× ···

- **Visitor Properties** – A list of Integriti User properties and custom fields to be populated from Proxyclick visitor data.
  - **Property Name** – The name of the property or custom field in Integriti to populate.
  - **Mode** – Specifies when to import this data. If 'Keep updated' is selected, this property will be kept updated whenever the visit information is edited; otherwise, the property will be set at the specified time: on User creation, check-in or check-out.
  - **Value Source** – Specifies how to determine the value to set to the property or custom field.
    - **From Host** – Copies the value from the Host User.
    - **From Proxyclick Field** – Imports a value from a field in Proxyclick. This may be a built-in or custom field of the visitor or visit.
    - **Specified value** – Use a constant value for all visitors.
    - **Clear value** – Reset the property or custom field to an empty or default value.
- **Visitor Area and Location Options** – Options for assigning a Visitor's User an Area or Location during a Visit. An Area or Location may be assigned on check-in, on check-out or both.
- **Visitor Area/Location Set on Check-in** – The Area or Location that will be set on a Visitor on check-in. Leaving this blank will clear the Area/Location of the Visitor.
- **Visitor Area/Location Set on Check-out** – The Area or Location that will be set on a Visitor on check-out. Leaving this blank will clear the Area/Location of the Visitor.

Visitor Permissions and Defaults

Visitors will be assigned new or existing Users when visits are created with this Integration running. There are several settings in the Integration to ensure that Visitors get the correct permissions to a site, as well as other values that may need to be leveraged for related integrations. This section details how to configure the initial settings a Visitor's User will receive on Check-In.

Configuring Visitor Permissions

A Visitor's User can be given be assigned Permissions from several sources depending on the needs of the site, setting values for both the Primary Permission Group and Supplementary Permissions of any Visitor's User when checked-in.

"Primary Permission Group Source" will set where the Primary Permission Group assigned to a Visitor when it is Checked-in. The Permission Group assigned can be sourced from one of the following:

- **From Host** – Gives the visitor the same primary permission group as the host.
- **Specified Value** – Gives the visitor the specified primary permission group.
- **From Host's Permission Group Custom Field** – Assigns the permission group whose name is specified in an Integriti custom field of the host's User.
- **From Visitor's Proxyclick Custom Field** – Assigns a permission group according to the value of a Proxyclick custom field on the visitor, by name or using a specified mapping.

"Supplementary Permissions" will set where any additional permissions are sourced. It can be set to "None", where no additional permissions are assigned to the Visitor, or "From Host" which like above takes the Permissions of the Host and also assigns them to the Visitor.

Configuring Visitor Properties on Check-in/Check-out

⌄ Visitor Properties	2 Items	+
⌄ [0]	Field 'cf_PhoneNumber' set to Proxyclick field 'Phone Number'...	✕
Property Name	Phone Number	⌄
Mode	Keep updated	⌄
Value Source	From Proxyclick Built-in Field	⌄
Field	Phone Number	⌄
⌄ [1]	Field 'Notes' set to custom field 'Visitor Type' on visit creation	✕
Property Name	Notes	⌄
Mode	Set on visit creation	⌄
Value Source	From Proxyclick Custom Field	⌄
Custom Field	Visitor Type	⌄

The Integration can be configured to set property values of a Visitor's User to ensure that required values are filled in for the Visitor's use on site. **Note:** This is an optional feature that does not need to be configured for the Integration to function.

To add a field to set, click on the "+" button in the 'Visitor Properties' field, as seen above. This will add a new entry in the list.

Next, the "Property Name" should be set to the Name of the required property. This field has a list of User property names and custom fields.

Select when the property should be set. The options are:
- **Keep updated** – Updates the value whenever the visit data is edited.
- **On creation** – Sets the property when the visitor User is created.
- **On check-in** – Sets the property when the visitor is checked in.
- **On check-out** – Sets the property when the visitor is checked out.

Then select the source of the value. This can either be set to:
- **From Host** – Copies the value from the Host User.
- **From Proxyclick Built-in Field** – Imports a value from a built-in field of the visitor in Proxyclick.
- **From Proxyclick Custom Field** – Imports a value from a Proxyclick custom field on the visitor or visit.
- **Specified value** – Use a constant value for all visitors.
- **Clear value** – Reset the property or custom field to an empty or default value.

Check-in and Check-out Process

Before performing any check-ins, ensure that there are Users in the Integriti System that match with the Proxyclick IDs or email addresses of employees in Proxyclick who will be hosting any visits. These Users will be used as sources for permissions and other data, and a visit will not be considered valid by the Integration unless the Host's email address matches one belonging to a User in Integriti.

Check-ins

The following must be provided for an event or visit update to be accepted by the Integration:

- Visitor
    - Non-empty First and Last Name.
- Host
    - The employee's email address in Proxyclick must match an Integriti User's data, using the custom field specified in the Integrated System attributes.

If any of the above requirements are not met, a Log will be written to the Integriti Log detailing the issue. Once these requirements have been met, the Integration will create the visitor's User if required and assign any appropriate permissions or Property values specified in the Integrated System's configuration. If a Card Number custom field was specified and a value is provided in Proxyclick, it will also create a new Card for the visitor to use throughout the visit. Below shows an example of a User created to represent a new Visitor:

Check-outs

When a check-out occurs, any Cards assigned to the User for the visit will be suspended, removed from the user, or deleted, depending on the Integrated System attributes. The Integration can be configured to cancel the User, removing their ability to resolve any access requests, and/or have their permissions cleared when checked out.

The Visitor's User will never be deleted during this process, in order to preserve the User's audit trail, as well as allowing the Integration to leverage an existing User for returning or frequent visitors.

Troubleshooting

The Integration is not creating or updating entities	Ensure that the port used by the Integration is not blocked by a firewall. Make sure the host's email address in Proxyclick matches a user in Integriti. If a webhook password was specified, make sure the Proxyclick webhook configuration uses the correct username (proxyclick) and the same password.
"The property '{Property Name}' was not a valid property Log Message"	This issue occurs when the Property Name of a Visitor Properties list entry does not match the name of a User's property or custom field. Check the property name of the property specified, or reselect it from the dropdown list to ensure it is spelled correctly.
Host's User cannot be found by email address, but there is a User with a matching email address	Ensure that the custom field keyname matched the Email Custom Field used by Integriti. It has also been observed in larger systems that, upon an integration restart, the Integration can take time to cache the email information of Users for use with Requests. Ensure that you give the Integration at least a minute to start up before requests are sent to it to avoid this issue.