integriti
INTEGRATED SOLUTIONS

INTEGRITI SINE 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

Description

The Sine Integration is designed to manage the access control side of the Visitor Management process by handling requests made from the Sine system, including generating Users for Visitors, assigning them Permissions based on their Host and creating credentials to be used at Sine readers and turnstiles throughout a designated site.

The Sine Integration also handles manual Deprovision requests 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

- Provisioning:
  - On a request from Sine, assigns a User to represent the Visitor of a Visit, either creating a new one or finding a User with a matching email address.
  - Assigns permissions to this User based on the provided Host, matched against an existing User's email address.
  - Creates a credential based on a configured Card Template.
- Activating:
  - On this request, the Integration will activate the Credential given to the Visitor's User, allowing access to the permissions assigned to them in the Provisioning process.
- Deprovisioning:
  - On this request, 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 Sine Integration
- Create new Sine Integrated Device
- Configure Integrated Device
  - Configure URL
  - Set Card Template
    - Use Refresh Device to use Template/Format created by Integration
  - Set Sine Email Custom Field
    - Use "New Field" to create a new email Custom Field
- Save Integrated Device
  - Ensure Integration is now running
- Apply SSL Certificate to Port Integration is listening on
- Configure Network Settings
  - Open ports receiving Requests
  - Set destination of traffic to machine running Integration
- Use Sine Dashboard to configure Sine-side Integration Settings
  - Save these settings to confirm the Integration can receive Requests.

Integriti Sine Plugin

Required Integriti Version License

The Integriti Sine Integration requires an Integriti Pro/Infiniti v21 license or higher to be present on the product key running the integration.

Minimum Installed Integriti Version

The Integriti Sine Integration is only compatible with an installation of Integriti Pro or Infiniti that is v19.0 or higher.

Licensing Requirements

The Integriti Sine integration requires the “Visitor Management Integration” license (part number 996935) are required.

Tested Against

The Integriti Sine Integration v1.2 was built and tested against Sine v0.167.4.730dd84cb

Configuration

Installation

Close all instances of the Integriti software suite on the PC to install the integration on, including stopping all running Integriti services (if installing on the Integriti server).

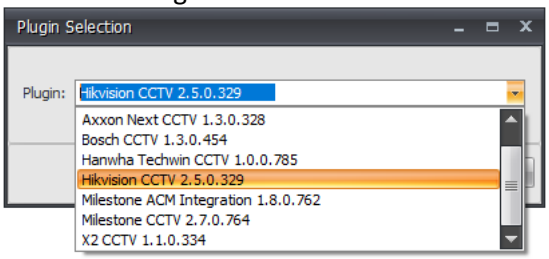
Download and run the Sine Integration installer on all Integriti servers first, before running on all client workstations that will be interacting with the integration; including updating the integration’s configuration and invoking commands.

After the installation has completed, remember to start all of the services that were stopped prior to running the installation.

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.

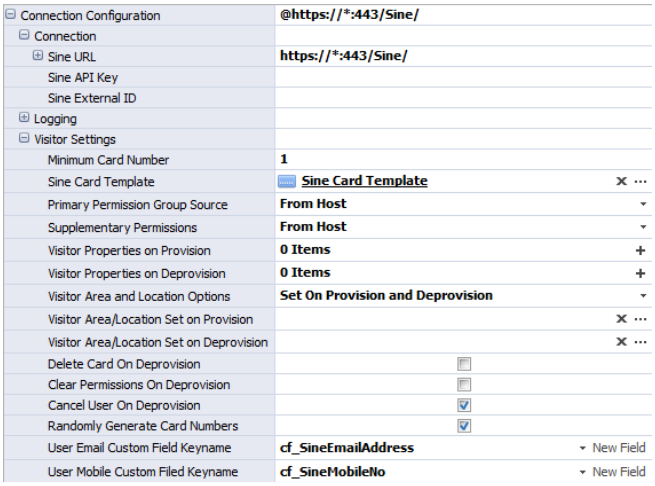
3. In the editor window that appears, give the newly created device a Name and optionally enter some Notes describing the device.

4. **Persisted Connection Run Mode** - Select the preferred Persisted Connection Run Mode. This is necessary for features such as event and camera state monitoring. This typically does not affect the ability to view video or invoke commands on this device and its child devices.

   The following options are available for the Persisted Connection Run Mode:
   Automatically Maintain Connection on Any Single Server – This is the recommended option if a persisted connection is to be enabled and will ensure that there is always one Integriti Integration Server connected to the 3rd party system, 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 connect to the 3rd party system. If the specified server goes offline, the integration will lose its connection to the 3rd party system until the specified integration server comes back online.
   Simultaneously Maintain Connection on All Servers – This option will establish a persisted connection to the 3rd party system on every Integriti Integration Server at the same time. This can result in the most simultaneous connections 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 one fewer connections being made to the 3rd party system at all times This may be useful if only a limited number of simultaneous connections are permitted by 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 the Sine system. For more details on how to configure integration specific properties, please refer to the "Device Attributes" and "Preparing Integration for Requests" sections below.
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 the Sine system and start listening for incoming requests.

Device Attributes



Connection

- *Sine URL* – The Base URL that the Sine Integration will listen for requests on. “Verify/”, “Provision/”, “Activate/” and “Deprovision/” are added to this URL to listen for the associated requests. It follows the following structure: “https://{Hostname}:{Port}/{BasePath}/
    - *Hostname* **–** The hostname used in the URL. Setting this to “*” will make the Integration listen on any hostname that targets the host machine.
    - *Port* – The Port the Integration will listen on for requests.
    - *Base Path* – The base path of the URL. By default this is set to Sine
- *Sine API Key* – A custom Key passed with each Sine Request to ensure that requests are coming from a verified source.
- *Sine External ID* – An ID used to uniquely identify and match with individual Sine Site Integrations.
    - **Note:** The Sine API Key and External ID can be entirely made up and set to any value. For example, the API Key could be “Sine Integriti {Site} Integration” with an external ID being set to a Guid value. These two values should also match the equivalent fields in the Sine Dashboard settings, as seen in the “Configure Sine To Send Requests” section.

Visitor Settings

- *Minimum Card Number* – The minimum Card Number that can be assigned to credentials generated by the Integration.
- *Sine Card Template* – The Card Template used to create Credentials for Visits.
- *Primary Permission Group Source* – Choose from where a Visitor's Primary Permission Group is taken on a Provision Request. The options include "From Host", "From Host's Permission Group Custom Field" and "Specified Value", taking the Primary Permission Group from the field below.
- *Primary Permission Group* – An optional property for a Permission Group that will be assigned to Visitors as their Primary Permission Group on a Provision Request.
- *Supplementary Permissions* – Choose the set of extra Permissions given to Visitors on a Provision request. Options include "None" or "From Host".
- *Visitor Properties On Provision* – A List of properties to be populated when a Visitor is Provisioned. Refer to the "Configuring Visitor Properties On Provision/Deprovision" section below for more information on how to configure this field.
- *Visitor Properties On Deprovsion* – A List of properties to be populated when a Visitor is Deprovisioned.
- *Visitor Area And Location Options* – Options for assigning a Visitor and Area or Location during a Visit. Options include "Set None", "Set On Provision", "Set On Deprovision" and "Set On Provision and Deprovision".
- *Visitor Area/Location Set On Provision* – The Area or Location that will be set on a Visitor on Provision. Leaving this blank will clear the Area/Location of the Visitor. Is only set when Options is set to "Set On Provision" or "Set On Provision and Deprovision".
- *Visitor Area/Location Set On Deprovision* – The Area or Location that will be set on a Visitor on Deprovision. Leaving this blank will clear the Area/Location of the Visitor. Is only set when Options is set to "Set On Deprovision" or "Set On Provision and Deprovision". Leaving this blank will clear the Area/Location of the Visitor.
- *Delete Card On Deprovision* – If set, a Card associated with a Visit will be deleted when a Visit is Deprovisioned.
- *Clear Permissions On Deprovision* – If set, a Visitor's User will have their permissions cleared on a Deprovision request.
- *Cancel User on Deprovision* – If set, a User will be Cancelled, preventing all access requests from the User, when a Visit is Deprovisioned.
- *User Email Custom Field Keyname* – The Keyname of the Email Custom Field for uniquely identifying Users (Hosts or Visitors) with Sine. The "New Field" button can be clicked to create a new custom field for this purpose.
- *User Mobile Custom Field Keyname* – The Keyname of the Mobile Custom Field that is updated/maintained by Sine on visit provisioning.

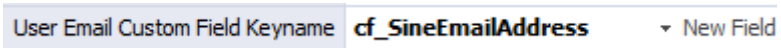
Preparing Integration for Verification

The Sine Integration will listen for HTTPS requests from a configured Sine System. Before configuring the Sine system to communicate with this Integration, make sure you have followed the following steps to prepare the Integration for use, as the Sine System will require the Integration to be running and complete a Verify Request, checking the API Key and External ID fields match those in Sine, in order to complete configuration.

Host/Visitor User Email Custom Field

The Sine Integration uniquely identifies Hosts and Visitors by Email Address, which is source from a Custom Field assigned to Users, specified in the Device Attributes as seen above. An existing email custom field can be specified in the device settings using the dropdown to select an existing custom field by its keyname. Alternatively, a new Custom Field can be created using the "New Field" button, as seen below, creating an appropriate field for use with the Integration.

Note: Visitors and Hosts are uniquely identified by this field, and Hosts in Check-ins from Sine must have an email address that matches a User in Integriti for the request to be successful.



Sine Card Template

A Card Template is required to create credentials for Visitors created by the Integration. It is suggested to create a Card Template and Format using "Refresh Device" on the Sine Integrated Device. It will create a Card Format and Template with the following properties:

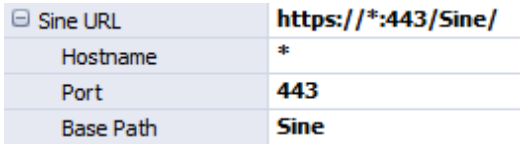
- Card Format
  - Name: "Sine QR Card Format"
  - Card Type: Wiegand Site (Complex)
  - Wiegand Card Type: NBit
  - Total Bits: 26
  - Card Number Offset: 1
  - Card Number Length: 24
- Card Template
  - Name: Sine QR Card Template
  - Card Format: Sine QR Card Format

This will also assign the Card Template in the device configuration if one has not been set yet.

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 a Sine Integration.

Sine URL for Requests

The Sine Integration listens on HTTPS for requests matching a URL pattern that can be configured as seen below:



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 the Sine System.

Setting the Hostname to "*" will make the Integration listen for any requests with the matching port and Base Path that are sent to the machine hosting it. You can also specify an IP Address of a NIC on the hosting machine to restrict the Integration to listen for requests sent to that IP only as well as having a matching port and Base Path.

The Sine System's request URLs, described in greater detail below, will have the same URL as appears above (next to "Sine URL"), with the hostname being replaced with the public hostname of the machine that hosts the integration. This could be the public IP Address of the machine hosting the Integration, or the hostname of a web hosted service that routes the request to the local machine. Each of the request URLs should then be appended with "Verify/", "Provision/", "Activate/" and "Deprovision/" to provide separate URLs for each of the requests the Sine system can make.

Note: If multiple Integrated Devices are being used to communicate with multiple Sine Sites, then the Base Path property can be appended or prepended with some string to ensure that the Devices are not listening on the same URL for the same requests.

Assigning SSL Certificate to Sine Integration Port

Sine Integrations are required to communicate over HTTPS for requests to ensure the security of the connections made between Sine and Integrations. This means that the machine running the Sine Integration will need an SSL 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 Sine. 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 with the certificate bound to the port the Integration is listening on, so long as the certificate bound to the port it listens on is not self-signed, no step may need to be taken.

Port Fowarding to Sine Integration

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

This step requires two things:

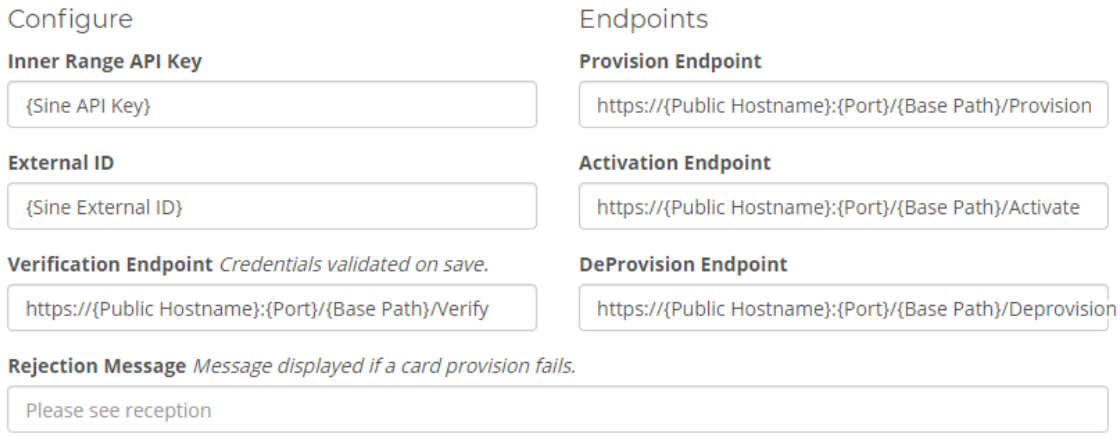
- The Port number on which the requests will be sent
- The local IP address of the machine that hosts the Integration

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.

Configuring Sine To Send Requests

Once the above steps have been completed, open the Sine Dashboard to configure a Site to communicate with this Integration. Once at the dashboard, click on “Sites” in the left side-bar, then “Settings” on the desired Site, then “Integrations”, then under “Current Integrations” click the gear symbol on the desired Integration to open its settings.

Below shows the settings fields and the associated Sine Integrated Device fields that each setting should be filled with:



For example, using the example configuration settings from Integriti seen in previous steps, the Verification URL entered into this section would be “https://{Public Hostname/IP Address}:443/Sine/Verify”.

Also ensure that the “Status” of the Integation, found near the bottom of the settings page is set to Enabled, as seen below:

Before saving these settings, ensure that the Integration in Integriti is running, as the Sine system will send a Verify request to confirm that it can communicate with the URL before saving changes. Then click the “Save” button. If an error is displayed by Sine, it is recommended to check the Integriti Log to find a detailed error message if the request was received by the Integration.

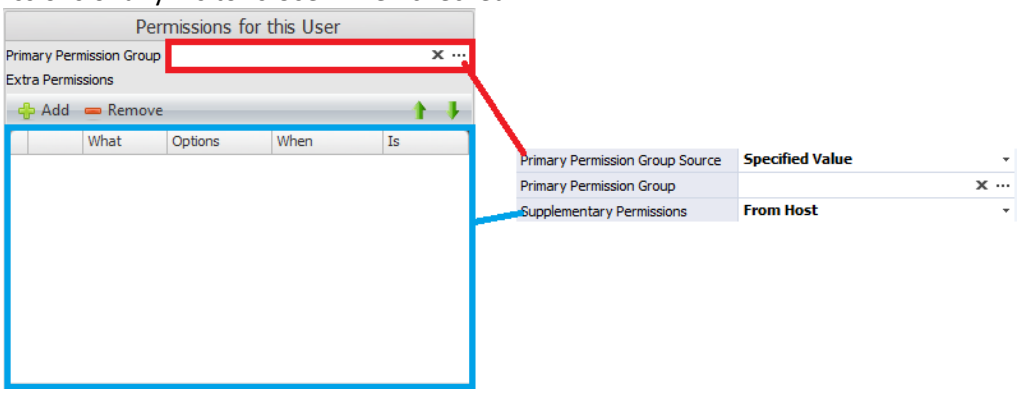
Once these settings have been successfully saved, the Integration is ready to be used.

Visitor Permissions and Defaults

Visitors will be assigned new or existing Users when they Check-In to Sine 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", where the Primary Permission Group of the Host User of the visit is used,
- "From Host's Permission Group Custom Field", where the Permission Group is chosen from one defined in the Host's "Sine Host Primary Permission Group Name" Custom Field.
    - **Note:** If using this option, the "Sine Host Primary Permission Group Name" Custom Field's dropdown can be populated with existing Permission Group name by clicking "Refresh Device" on the Sine Integrated Device.
- "Specified Value". Selecting "Specified Value" will reveal a "Primary Permission Group" field that can be used to select the Permission Group given to the Visitor.

"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 Provision/Deprovision

The Integration can be configured to set property values of a provisioned Visitor's User to some default value 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 "Default Visitor Property Values" 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 property names that can be used to specify defaults.

Then select the source of the value. This can either be set to:

- "From Host", to copy the value of this field from the Host of a visit to the Visitor, or
- "Specified Value", where a manually set value will be set to this field. You can then set the field "Specified Value" to be the value this field will be given on Check-in.
- "Clear Value", where a property is set to a default or empty value.

Check-in and Check-out Process

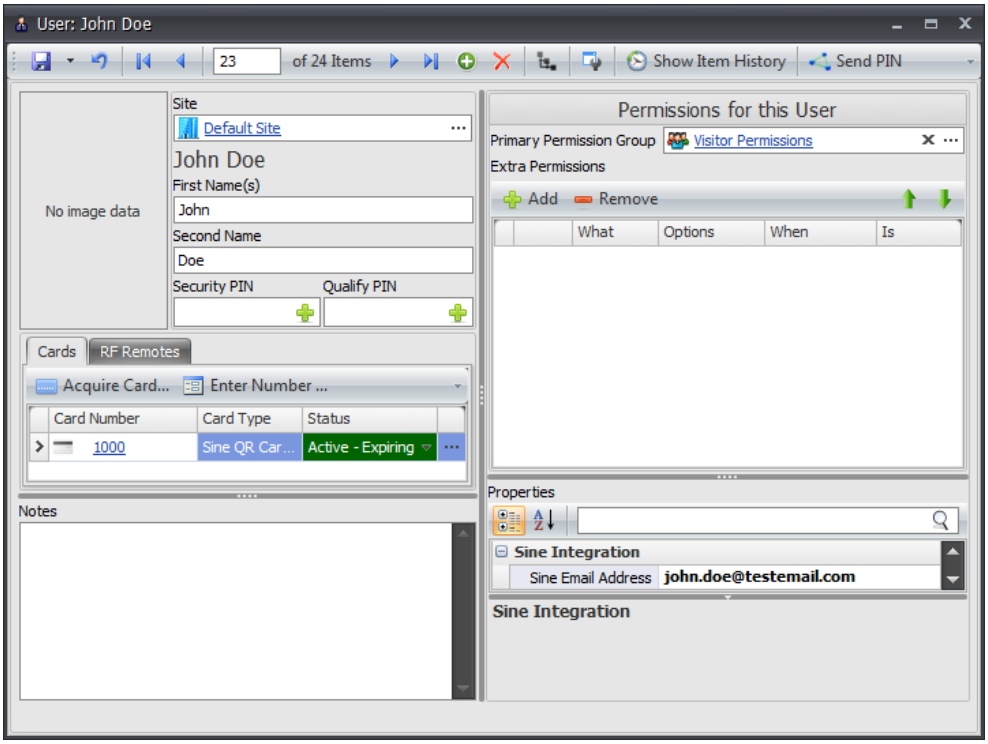
Before performing any check-ins, ensure that there are Users in the Integriti System that match with the emails of Hosts in Sine that will be hosting any Visits created by Sine. These Users will be used as sources for things like Permissions and a Visit will not be considered valid by the Integration unless the Host's email matches one belonging to a User in Integriti.

Check-ins

The following must be provided for a Check-in to be accepted by the Integration:

- Visitor
  - Non-empty First and Last Name
- Host
  - Email Address that matches an Integriti User's email address

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 if required or if it has no email address, create a new Credential for the User to use for the length of the Visit, and copy/assign any appropriate permissions or Property values specified in the Integrated Device's configuration. Below shows an example of a User created to represent a new Visitor:



The User will become active after the Valid period for the Visit begins, which is configurable in the Sine System.

Check-outs

When a check-out occurs, Visitor's User will be cancelled, preventing them from using credentials assigned to it to access any permissions assigned to them. The credential assigned to this user for a given Visit can also be deleted when check-outs are performed by setting the "Delete Card On Deprovision". The Visitor's User will not 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. However, the Integration can be configured to cancle a User, removing their ability to resolve any access requests, or have their permissions cleared when Deprovisioned.

Troubleshooting

Sine Dashboard Integration Settings are not saving	Sine will attempt to call on the Verification URL to ensure that the settings that were entered are valid. Make sure the Integration is running in Integriti and that the URL displayed in the Summary has the same Base Path following the Hostname and Port.
"The property '{Property Name}' was not a valid property Log Message"	This issue occurs when the Property Name of a Default Visitor Property Values does not match the name of a User's property. Check the property name of the property specified, or reselect it from the dropdown list to ensure it is spelled correctly.
Host Email does not exist, but there is a User that has that email	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.