INTEGRITI TRITON SENSOR INTEGRATION MANUAL

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Integriti Triton Sensor Integration

Table of Contents

Sensor Capabilities

Core Sensor Capabilities

Feature	Feature Description	Ver	Y/N
Receive Events from the Integrated System	Log events/alarms occurring on the Integrated system to Integriti's Review.	24	✓
Trigger Integriti Actions on the Integrated System Events/Alarms	Trigger actions to automatically occur in Integriti whenever specific events/alarms are received from the Integrated system.	24	✓
Generate Alerts from the Integrated System Events/Alarms	Automatically generate and restore Alerts tied to a specific Integrated Endpoint in Integriti whenever specific events/alarms are received from the Integrated System.	24	✓
Automatically Show Footage from Associated Cameras	CCTV Footage can be directly viewed from associated CCTV cameras, or Integrated Sensor alarms where the Integrated Sensor has an associated Camera.	24	✓
Trigger Inputs on Integrated System Event	Inputs in Integriti can be automatically triggered and restored when specified types of events are received from the Integrated System.	24	✓
Associate the Integrated Sensors With Entities	Integrated sensors loaded from the integrated system can be associated with Integriti entities to allow direct control of one from the other.	24	✓
Create Child Devices From the Integrated system Configuration	Child Integrated Sensors will be created based on the Integrated system configuration.	24	✓
View and Control Integrated Endpoints on Schematics	Integrated Sensors can be added to Schematic Maps in Integriti and directly viewed and controlled directly from the Schematic. Each Endpoint state is immediately visible on the Schematic where available.	24	✓
Sync Time (via NTP)	Sync the time of the Integrated system and Integriti to match via an NTP.	24	✘
Automatically Control Integriti Entities on Integrated System Events	Automatically control Integriti Entities on integrated system events. For example, automatically unlocking an associated Door on an event being received from a sensor.	24	✓

Advanced Sensor Capabilities

Feature	Feature Description	Ver	Y/N
Automatically Load Integrated system Configuration	The Refresh Child Devices command is not supported by the Triton Integration. Integrated Sensor information will instead be automatically populated as updates are received from Triton Sync.	24	✘
64-Bit Server Support	The integration supports being run on the 64-bit integration server.	24	✓
Show Integrated Sensor Status	The current online, offline or alarm status of configured integrated sensors will be visible directly through Integriti.	24	✓
Display Connection Status to the Integrated System	Display whether Integriti is currently connected to the Integrated System.	24	✘
Trigger Actions in the Integrated System	Trigger actions or commands in the Integrated System directly from Integriti.	24	✘
Categorised Review Records	Review generated by the integration will have a different category for different event types, allowing for easy filtering of specific events	24	✓

Integriti Triton Sensor Integration Compatibility

Licensing Requirements

The Integriti Triton Sensor Integration requires an Integriti/Infiniti v24 license or higher to be present on the product key running the integration.

Additionally, sufficient IoT Sensor Integration licenses (PN: 996972) to allow for the number of sensors to use in the system are required. Any unlicensed sensors will still show up in Integriti; however, alarms and sensor updates will be unavailable for them.

Minimum Installed Integriti Version

The Integriti Triton Sensor integration is only compatible with an installation of Integriti Pro or Infiniti that is v24.0 or higher.

Tested Against

The Integriti Triton Sensor plugin was built and tested against the following versions of software:

- Triton Sync, as of February 2024

Known Issues

- Test events, sent via the 'Trigger a test event on an active integration' section of the Triton Sync Integrations configuration, are currently not supported.

Setup

This release of the Triton sensor integration works by listening for HTTPS requests from the Inner Range integration of the Triton Sync cloud service. To set up the Triton sensor integration, it is necessary to prepare the Integriti integration server to receive HTTPS requests connections from the Internet.

To set up the Triton sensor 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. 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.
3. Download and run the Triton Integration installer on all Integriti servers first, then run it 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 restart all of the services that were stopped prior to running the installation.

Integriti Configuration

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 integrated system 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 listening for webhook events.
5. **Connection Configuration -** On the 'Device Properties' tab, under 'Connection Configuration', configure the integration specific properties, including details on listening for requests. Note the API Key that is displayed in the editor. For more details on how to configure integration-specific properties, please refer to the Configuration 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, the integration will begin listening for events.

Listening Addresses

Integration HTTP listeners are based on HTTP.sys. Normally, the integration will listen for requests on all available IP addresses on the integration server. Optionally, it is possible to restrict integration HTTP listeners to specific IP addresses by configuring an IP listen list using the terminal command `netsh add iplisten`. If any IP addresses are added to the system's IP listen list, integration HTTP listeners will listen on the specified IP addresses only. For more information, see the Network Shell documentation.

The **Hostname** attribute in the Connection Configuration section may be used to restrict the listener to only responding to requests that specify the matching hostname in the URL, in addition to being received on a specific IP address if an IP listen list was configured above. This may be used to separate requests for multiple Triton Sync sites.

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 Triton 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 Triton Sync 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 required that the webhook requests use HTTPS with a valid and trusted TLS certificate. This means that the server running the Triton integration will need such a certificate to be bound to the port that it is configured to listen on. This certificate cannot be a self-signed one, as that will not be accepted by Triton Sync. The certificates must be installed in the integration server's Local Machine > Personal store; the steps to do this may vary slightly depending on the operating system.

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.

Triton Sync Configuration

The following steps must be completed to configure Triton Sync to send updates and alerts to Integriti.

1. Go to the Triton Sync portal page.
2. Select the Integrations tab. You must be using an administrator account to access this.
3. Enter the hostname to reach the Integriti integration server and the port number configured in Connection Configuration. The hostname must match the server's TLS certificate.
4. Enter the API Key noted above.
5. Click Save.

Configuration

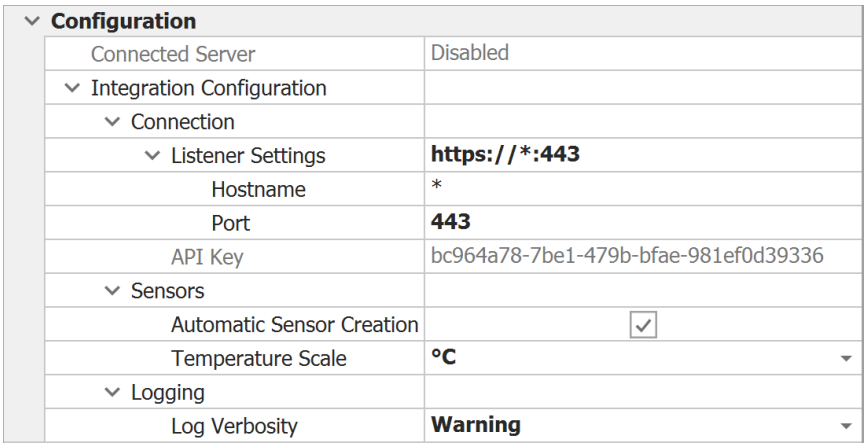
This section specifies the Triton Sensor Integration specific configuration details. Please refer to the 'Integriti Integrations - Core' manual for a detailed description on how to fully configure and use integrations in Integriti/Infiniti.

Ports Used

The following ports are used for communication between the Integriti Triton integration and Triton Sync. These ports should be configured in the Integriti Integration Server's firewalls to allow the integration to be used.

- 443 (or an alternative specified in Connection Configuration)

Connection Configuration



Connection

Listener Settings: Hostname – Set to '*' to have the integration accept any requests with a matching port number. Specify the hostname or IP address of a network interface on the hosting server to restrict the integration to listening for requests sent to that hostname or IP address only, as well as having a matching port.
Listener Settings: Port – Specify the port number on which to listen for requests. The default is 443.
API Key – A randomly-generated key that must be provided in the Triton Sync integration setup.

Sensors

Automatic Sensor Creation – Specify whether to automatically create and add integrated sensors corresponding to sensors that have been added in Triton Sync to Integriti. The devices will be added when a heartbeat or alarm message is received for a sensor that is not currently in Integriti. This is selected by default.
Temperature Scale – Choose whether to display temperatures in °C or °F within integrated sensor state attributes.

Logging

Log Verbosity – Only messages 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.