OnGuard v1.1 Integration
for v7.0, v8.0, and v8.5 systems

⚠ Verify that you have the most current version of this document from **www.hvacpartners.com**, the **Carrier Partner Community** website, or your local Carrier office.

Important changes are listed in **Document revision history** at the end of this document.

Contents

What is the OnGuard Integration?

The OnGuard® Integration consists of a collection of add-ons that allow the i-Vu® Pro building automation system and an OnGuard® security system to work together. The OnGuard® Integration enables the i-Vu® Pro system to utilize actual occupancy data in control program logic by monitoring entry and exit events.

Included in the .zip file...	Purpose
Data Connector (page 6) *(onguard.addon)*	You must install the OnGuard® Data Connector add-on before installing any of the other OnGuard® .add-on files. The i-Vu® Pro application can track Occupancy through the security system.
Advanced Occupancy Scheduling (page 9) *(onguard-scheduling.addon)*	Based on historical occupancy trends, the add-on will write predicted scheduling to the i-Vu® Pro system which will allow for optimized energy usage.
Integrated Alarm Management (page 11) *(onguard-alarms.addon)*	Facility staff and security staff can monitor each other's alarms so that either team can dispatch appropriate personnel regardless of who is currently on shift. It also enables OnGuard® Action Groups to initiate control of the i-Vu® Pro system equipment.
Integration Helper Files (page 11) *(OnGuardIntegrationHelper.zip)*	This zip file includes: • alarm-manager.logic-script – Snap script that is used to add configured alarm points to your program. • onguard-alarms.logicsymbol – Logicsymbol that is used by the script above. It includes a template for the microblocks to be added to your program.

See "Installing an Add-on User Guide" for more information on the following:

- Installing an add-on
- Applying a license
- Running an add-on
- Upgrading an add-on

Requirements

- Carrier i-Vu® Pro v7.0 or later system with the latest cumulative patch
- Carrier hardware, if your application requirements include running logic for the transference of data to or from the OnGuard® system
- OnGuard® system with Administrator privilege:
  - v7.5 or v7.6 ONLY, using OpenAccess interface - versions later then 7.6 are not certified compatible at this time
  - Appropriate license applied for OpenAccess (Please see Lenel® pricebook)
  - Single sign-on configured and enabled
- Building Integration Platform (v1.11) (see the Building Integration Platform's installation guide):
  - Building Integration Platform Service installed
  - OnGuard® Connector Service installed
  - Username, password, and port number for the Building Integration Platform
- Network connectivity between the i-Vu® Pro Server, OnGuard® server, and Building Integration Platform server

When upgrading to i-Vu® Pro v8.0

If you are running the OnGuard Integration with a pre-v8.0 version of i-Vu® Pro, perform the following steps when you upgrade to i-Vu® Pro v8.0:

1 During the upgrade to i-Vu® Pro v8.0, choose to keep your existing add-ons. Add-on configurations will be saved.

2 Uninstall Building Integration Platform (BIP) v1.10, following the instructions in the *Building Integration Platform Installation Manual*.

3 Install BIP v1.11, following the instructions in the *Building Integration Platform Installation Manual*.

Running the OnGuard add-ons with i-Vu® Pro v8.0 or v8.5

When running the OnGuard add-ons with i-Vu® Pro v8.0 or v8.5, it may appear that your server is using more memory than it should. This occurs because v8.0 uses a newer version of Java, and most of the memory it reports as used is actually free.

If you would like to see a more accurate report of memory usage, perform the steps below on your i-Vu® Pro server:

1 Go to the **i-Vu Pro<x.x>\bin\launchers** folder.

2 Open the **i-Vu Pro server.launch** file in Notepad.

3 Add this line: `cjgreen.monitoredapp.config.gcimpl=-XX:+UseParallelGC`

4 Save the file.

5 Open the **i-Vu Pro service.launch** file in Notepad.

6 Add the same line of text as above, and save the file.

7 Restart **i-Vu Pro**. Memory usage should now display as significantly lower.

BIP installation and configuration details

To enable communication between the WebCTRL and OnGuard servers, the Building Integration Platform (BIP) must be installed on a server that can connect to both application servers. Refer to the following documents to install and configure the BIP:

- *Building Integration Platform Installation Guidelines*

- *Building Integration Platform Commissioning User Manual*

The BIP is designed to support multiple integrations. This section describes the steps needed specifically for the OnGuard Integration.

BIP Installation

See the *Building Integration Platform Components* section of the *BIP Installation Manual* for which BIP services must be installed for the OnGuard Integration. Follow the instructions in that document to install each of the indicated services.

BIP Configuration

Refer to the *BIP Commissioning User Manual* to perform the following steps:

1 Refer to the *BIP Commissioning Access* section to log in as the default web admin user using the default credentials, then change the password for the default web admin user.

2 To set up additional web admin users:

   a) If the new user will not be authenticated with Active Directory or Single Sign-On, refer to the *Local Database User Creation* section to create the user in the BIP database.

   b) Refer to the *User Management* section to register the user with the role Admin with Web Login.

3 Register your Lenel-OnGuard System

   a) Refer to the *System Configuration > Add System Configuration* section to add a system. Select "Lenel-OnGuard" as your **System Type**.

   b) Refer to the *Register Lenel-OnGuard System* sub-section to complete the registration.

4 The Configuring the Server section of this document explains how to connect to a BIP Resource. Refer to the *Resource Registration > Add Resource* section to create a BIP Resource for this purpose with:

   a) **Resource IDs**: aaa, dipservice

   b) **Grant Type**: service

   c) **Scopes**: read, write

   d) **Access Token Time**: 1 month

IT considerations

The following information may be useful to network administrators.

Client	Server	Default Port	Traffic
i-Vu Pro – OnGuard® Data Connector	Building Integration Platform	TCP/IP 8443*	Building Integration Platform Rest API secured with TLS 1.2
i-Vu Pro – OnGuard® Data Connector	Building Integration Platform OAuth Service Provider	TCP/IP 8444*	Building Integration Platform OAuth Rest API secured with TLS 1.2

* The Building Integration Platform server ports default to 8443 and 8444, but can be customized in the field.

Building Integration Platform

The OnGuard® Data Connector add-on communicates with OnGuard® Server via the Building Integration Platform.

The OnGuard® Data Connector communicates to the Building Integration Platform using REST and Server Sent Event technologies. The REST APIs are secured using TLS 1.2 and authenticated using a username/password that is configured in the Building Integration Platform. Credentials for the service account are stored to a file by this add-on and secured using AES-128 encryption. The Server Sent Events are only accessible through the REST APIs, so they are secured in a similar way.

Configuring the Server

1 On the **Server Configuration** tab, enter the OnGuard Connector settings. See table below.

2 To allow a Self Signed Certificate, check the checkbox. Note: Choosing this option will result in a less secure configuration, therefore should only be chosen when you are unable to use a certificate signed by a certificate authority.

NOTE **Status** indicates **Connected** if configured properly. If errors occurred, view the **Activity Log** (to the right) to help diagnose what may be preventing the connection from being established.

Field	Notes
Host	The Building Integration Platform server IP address.
Port	Port number for the Building Integration Platform service.
OAuth Host	IP address of the server that the Building Integration Platform OAuth service is running on.
OAuth Port	Port number for the Building Integration Platform OAuth service.
Client ID	Client ID of the Building Integration Platform Resource associated with this integration.
Password	Client Password of the Building Integration Platform Resource associated with this integration.

NOTE You must configure your Lenel® OnGuard system with the System Name "OnGuard". You can edit this field in the Building Integration Platform's **System Configuration** tab.

Setting up the Data Connector add-on

To track occupancy through the security system, you must define one or more zones.

NOTE For the purpose of this integration, a zone is a geographical area for which occupancy can be detected through the activity of its associated badge readers.

Adding a zone

1 On the **Occupancy** tab, enter a unique name for the new zone in the **Add New Zone** field.

2 Press **Enter** to add the new zone – it appears in the list of zones below.

NOTE To remove a zone from the list, click the **Delete** (x) button to the right of the zone name.

Setting zone properties

1 On the **Occupancy** tab, click the zone you wish to configure in the **Zone** list.

2 Click **Config** in the **Occupancy** panel.

3 Select a value for the **Full Occupancy Count** lertethe zone.

The zone is considered fully occupied when the occupancy count reaches this number.

4 Enter a time for the **Reset Time**.

The occupancy count is automatically cleared at this time each day to ensure that each day's occupancy tracking does not accumulate errors from the day before.

NOTE If the add-on is shut down at any time, the last known occupancy count is retained.

Exporting and clearing the prediction history

Prediction history can be exported to a .csv file which is named after a selected zone. Exporting the prediction history purges all but the most recent 30 entries from the **Prediction History** panel.

On the **Scheduling** tab, select the desired zone, then click the **Export Predictions** button in the **Prediction History** panel.

Associating microblocks with a zone

A control program can be designed to operate on zone occupancy data from the integration. Do this by associating microblocks in the control program as targets to receive the zone occupancy data. The microblocks are updated 1 minute after startup and every 5 minutes following that. There are four different microblocks that can be configured.

Microblock	Maps too...	And represents...
Occupancy Count	an AV microblock	how many people are currently badged into a zone.
Full Occupancy Count	an AV microblock	the number of people that would be considered 100% occupied.
Occupancy Percent	an AV microblock	the percentage of people in a zone based on the Occupancy Count/Full Occupancy Count.
Comm status	an MSV microblock	the communication status with the Building Integration Platform. MSV values must be configured in the microblock: 1=Comm Failed 2=Comm OK 3=Subscriptions Pending This value is updated both periodically and on change of value.

Auto-mapping with predetermined reference names

Use these predefined reference names in the equipment file:

Set this reference name...	to start with...	for this microblock type
Occupancy Count	onguard_occ	AV
Full Occupancy Count	onguard_full_occ	AV
Occupancy Percent	onguard_pct_occ	AV
Communication Status	onguard_comm_stat	MSV

1 On the **Occupancy** tab, click the zone you wish to configure in the **Zone** list.

2 Click **Microblocks** in the **Occupancy** panel.

3 When the **Equipment** panel appears, navigate the Equipment tree and select the equipment with the predefined reference names (see table above).

4 Drag the selected equipment from the tree to any slot in the **Microblocks** section.

NOTES

- All the predefined reference names will be assigned to the associated points. Depending on the system size, this operation may take a few seconds.

- To remove a microblock association, click the **Delete** ( ) button to the right of the microblock name.

Manual mapping of reference names

1   On the **Occupancy** tab, click the zone you wish to configure in the **Zone** list.

2   Click **Microblocks** in the **Occupancy** panel.

3   When the **Equipment** panel appears, navigate the Equipment tree and select a microblock to associate.

4   Drag the selected microblock from the tree to the corresponding slot in the **Microblocks** section.

NOTE To remove a microblock association, click the **Delete** ( ) button to the right of the microblock name.

Associating badge readers with a zone

Each zone can be assigned entrance badge readers to detect how many people have badged into a zone. Each unique badge entry event increments the occupancy count for that zone. When the badge is detected in another zone the occupancy count is decremented in the original zone and incremented in the new zone.

NOTES

- If no readers are configured under an OnGuard® device panel, the OnGuard® device panel will not show up under **Peripheral Devices**.

- A badge reader can only be mapped to a single zone. Readers that are already mapped will be grayed out (disabled) in the **Peripheral Devices** panel.

- Use the electrical drawing to determine which Access Control Devices belong to which zone.

To associate a badge reader

1   On the **Occupancy** tab, click on the zone you wish to configure in the zone list.

2   Click **Associated Devices** in the **Occupancy** panel.

3   When the **Peripheral Devices** panel appears, select a reader to associate.

      NOTE The items in the list are retrieved from the configuration of the connected OnGuard® system.

4   Drag the selected reader to the **Associated Devices** section.

NOTE To remove a reader association, click the **Delete** ( ) button to the right of the reader name.

Setting up the Advanced Occupancy Scheduling add-on

Advanced Occupancy Scheduling is an add-on that predicts and schedules occupancy based on past occupancy data. The schedule that is generated contains no undefined regions and the whole day is scheduled with off and on times. For example, a 9-5 schedule would be written with midnight to 9am as off, 9am-5pm as on and 5pm to midnight as off.

The Occupancy Schedule Optimizer algorithm provided with the algorithm schedules optimal building area operational schedules based on actual building usage patterns. This add-on compares security card logs to occupancy count information in user-defined areas and then schedules equipment based on the average time the area reaches a user-defined occupancy threshold.

The add-on functions by associating data by day of the week and maintaining rolling data sets of the last five occurrences. For example, the add-on schedules equipment on Monday based upon the usage patterns of the five most recent Mondays. This allows the algorithm to accommodate variations of occupancy among the different days of the week and adapt over time as usage patterns change.

The Occupancy Percentage parameter allows the user to define when the building is considered occupied for the purposes of scheduling using a percentage value. For example, for an area with full occupancy of 100 people, setting the parameter to 5% results equipment being scheduled ON when the algorithm predicts five or more occupants will be present. Increasing the parameter conserves energy by allowing a larger occupancy count to be considered unoccupied, with the converse true for reducing it.

Finally, the Occupancy Schedule Optimizer algorithm conducts continuous data quality checks to ensure that irregular occupancy events, such as holidays, do not impact the scheduling function. Any data that deviates significantly from the rolling data set is discarded when predicting schedules.

Setting scheduling properties of a zone

TIP For the scheduling properties described below, you must have either the **Start Time** or **Stop Time** set to **Predicted** before you can configure **Algorithm** or **Occupancy Percent**.

1   On the **Scheduling** tab, click on the zone you wish to configure in the **Zone** list.

2   Click on **Config** in the **Schedules** panel.

3   Set both the **Start Time** and **Stop Time** to either **Predicted** or **Fixed**; if Fixed, select a time.

NOTE If **Predicted**, select an algorithm and a percent for occupancy.

4   Select an **Algorithm** from the droplist to use for the occupancy prediction.

5   Adjust the **Occupancy Percent** setting to modify how the selected algorithm predicts the start and stop time.

NOTE Use the **Reset All Occupancy Data** button (Reset All Occupancy Data) on the **Zone** panel to remove all data used by the occupancy schedule algorithm. The add-on must re-accumulate this data before the algorithm can make schedule predictions. Use this option after an extended period of unusual occupancy activity. For example, when a building has just come out of commissioning and is ready to start recording real occupancy data.

Associating schedulable items to a zone

1   On the **Scheduling** tab, click on zone you wish to configure in the **Zone** list.

2   Click on **Destinations** in the **Schedules** panel.

3   From the **Destination** panel, you can either add **Areas** and **Equipment** or **Scheduling Groups**:

- ○   In the **Areas and Equipment** section of the **Destination** panel, drag the desired **Area** or **Equipment** to the **Destinations** section of the **Schedules** panel.

- ○   In the **Scheduling Groups** section of the **Destination Panel**, drag and drop the scheduling group to the **Destinations** section of the **Schedules** panel.

NOTES:

- To remove a schedulable association, click the **Delete** () button to the right of the schedulable name.

- Toggle on and off the **Write Schedules** button () on the **Zone** panel to enable and disable the writing of predictions to system schedules.

- Use the **Export Predictions** button () in the **Prediction History** panel to export the prediction history to a .csv file named after the selected zone. Exporting the prediction history purges all but the most recent 30 entries from the **Prediction History** panel.

Setting up the Integrated Alarm Management add-on

Integrated Alarm Management is an add-on that enables the exchange of alarms between the i-Vu® Pro system and the OnGuard® system.

Setting up alarms from OnGuard to the i-Vu® Pro system

In order to send alarms from an OnGuard® system to the i-Vu® Pro system, you must define a mapping. The mapping describes the OnGuard® event source and the destination microblock which re-generates the alarm for the i-Vu® Pro system.

Adding an alarm mapping

1 On the **Alarms** tab, click **OnGuard to i-Vu Pro**.

2 Click the **Edit Events** button.

3 Click the **Add New Mapping** button.

4 In the **Mapping Configuration** panel, set the **OnGuard Source**:

    a) Click the **Event Type** slot, then select a type from the available choices.

    b) With the **Event Sub Type** slot now selected, select a sub-type.

5 In the **Mapping Configuration** panel, specify if this mapping should **Use Schedule**:

    ○ **No** will always transfer alarms regardless of the schedule.

    ○ **Yes** will only transfer alarms during the scheduled time range. See *Setting up the alarm transfer schedule* (page 14) for more information.

NOTES

- To remove a mapping, click the **Delete** () button to the right of the mapping.
- You can use an exported configuration to generate an equipment file containing your mapped alarm points. See **Exporting Zone Mapping** below. Alarm points will be given refnames as indicated in the **Refname Template** below.
- To add alarm points to an existing equipment file, locate the **i-Vu® Pro Destination** section on the **Mapping Configuration** panel to see the microblock refname template generated by the add-on. Use this template to construct a refname to be used in the equipment file to map this point to a BV microblock. See the refname template and example below.

    RefnameTemplate: almbv_p<panel>_d<device>_type<type>_subtype<subtype>

    All of the fields in <> above are numbers provided by the OnGuard system.

    EXAMPLE: almbv_p1_d4_type4_subtype8

    In this example, the alarm is from Panel 1, device 4, event type 4 (system), sub-event 8 (door forced open)

Adding Zone Mapping

Map the equipment files to the zones to receive OnGuard® events. Once the Zone Mapping is set up, any mapped OnGuard® events will be written to the mapped BV microblocks in the mapped Equipment file.

1 On the **Alarms** tab, click **OnGuard to I-Vu Pro**.

2 Click the **Edit Zones** button to open the **Zone Map** and **Equipment** panels.

3 Drag the equipment from the **Equipment** panel to the desired zone in the **Zone Map** panel.

NOTE To delete a zone's association with a piece of equipment, click the **Delete** (x) button to the right of the zone.

Exporting Zone Mapping

You can export a JSON configuration file that contains the current **OnGuard to I-Vu Pro** Events and Zones to be used with Snap to build equipment for the selected Alarm Mappings.

1 On the **Alarms** tab, click **OnGuard to I-Vu Pro**.

2 Click on the **Export** (Export) button to download the current configuration file; this downloads an onguardmapping.json file.

Adding Alarm Manager Points to an equipment file

The JSON configuration file can be used in the Snap application to add the mapped points to an equipment file.

To add Snap Script to the Snap application:

1 In the Snap application add the "Scripts plug-in" (refer to Snap Help for this step).

2 In Snap select Tools>Scripts>Configure, then click **Add**.

3 Select the alarm-manager.logic-script from the onguard-integration.zip file.

4 Click **Ok**.

To add Snap Symbols:

1 Create a folder called "onguard_integration_helper" inside of <your_system_name>\extras\tools.

2 Select the onguardalarms.logic-symbol file from the onguard-integration.zip file; then move the file into the onguard_integration_helper folder created above.

To add OnGuard® Alarm Points to an equipment file:

Once the alarm-manager.logic-script and alarm-manager.logic symbol has been properly installed, OnGuard® Alarm points can be appended to existing equipment files with appropriate reference names.

1 Export the current Zone Mapping JSON configuration file (see Exporting Zone Mapping section above) and note where you download the onguardmapping.json file.

2 In Snap, open the equipment file that corresponds to the zone that you want to append the OnGuard® alarm points to.

3 Select Tools>Scripts>alarm-manager to open a script editor.

4 Press the **Execute** button in the script editor to run the script which will bring up a file dialog. Navigate to the onguardmapping.json file created in step 1.

5 Select the onguardmapping.json file and click **Open**.

6 From the drop-down list of available zones, select the zone that corresponds to your equipment file and click **Ok**. The Alarm Manager points are appended to the open equipment file.

7 Close the script editor.

NOTE If constructing an equipment file serving multiple zones, repeat steps 4 through 6 for different zone selections on the same equipment file.

Setting up alarms from the i-Vu® Pro system to OnGuard

In order to send alarms from the i-Vu® Pro system to the OnGuard® system, a source must be defined in the OnGuard® system to act as the originator of the alarms. There can be many sources defined for the i-Vu® Pro system to use, and each source can be configured to transfer i-Vu® Pro alarms by category.

The i-Vu® Pro alarms notifications that are sent to OnGuard® are:

○ Alarm is generated

○ Alarm is acknowledged

○ Alarm point returned to normal

Setting up the alarm source

1 On the **Alarms** tab, click **System Select** > **i-Vu Pro to OnGuard**.

2 Select the **OnGuard Source** to configure.

3 Under the **Category** column to the right, select each alarm category to enable for that source.

4 Next to each alarm category, specify when it should transfer alarms:
  • Select **No** to always transfer alarms regardless of the schedule.
  • Select **Yes** to only transfer alarms during the scheduled time range. See *Setting up the alarm transfer schedule* (page 14) for more information.

Setting up the alarm transfer schedule

For items that you have selected **YES** for **Use Schedule**, you must specify the alarm transfer schedule. The transfer schedule time range applies to both **OnGuard to I-Vu Pro** and **I-Vu Pro to OnGuard** alarms.

On the **Alarms** tab, set the following from the **System Select** column in the **Schedule** section:

Start Time - to start sending alarms

Stop Time - to stop sending alarms

Troubleshooting

If the connection is not successful and you receive an error message in the Activity Log panel, see the table below.

Error message	Solution
Error reading system id, No active system named OnGuard	Make sure your Lenel® OnGuard system is configured with the System Name "OnGuard". You can edit this field in the Building Integration Platform's **System Configuration** tab.
Error authenticating with DIP	Check **Allow Self Signed Certificate**. If using a signed certificate, uncheck after the connection is established. If using a self-signed certificate, leave it checked.

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
9/12/23	All topics	Removed references to versions newer than v8.5	AC-PM-RB-R
7/28/22	Requirements	Updated version requirements	AC-PM-LO-O-LO

* For internal use only