AN-181

Protege GX Redwall Integration

Application Note

Last Published: 17-May-22 09:36 AM

Contents

Protege GX Redwall Integration

Protege GX Redwall integration is a licensed feature that allows you to implement Redwall laser scan detectors alongside your Protege GX system. Integration enables Redwall detectors to operate as Protege input expanders, and trigger alerts within Protege GX when motion is detected.

This application note covers:

- Supported software and firmware versions
- Integration prerequisites
- Configuring the integration
- Trouble input mapping
- Input mapping

How It Works

The Protege GX controller communicates with the Redwall detectors over ethernet, some directly and some via the Redwall IP Encoder (PIE-1).

The fourth octet of the detector's IP address is automatically assigned as its device ID, which is used to identify the device on the network.
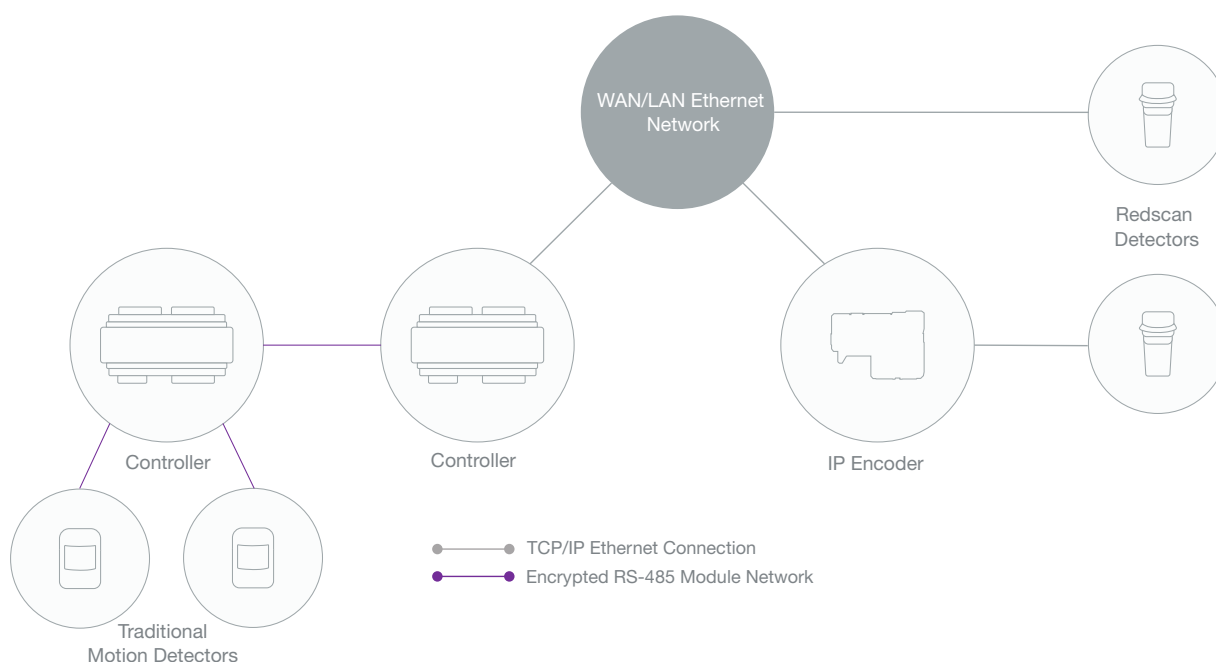
Each Redwall detector is configured as an input expander within Protege GX. The inputs and trouble inputs associated with the detectors are mapped to specific Redwall event codes, enabling you to monitor the state of the detectors. As the states change, these inputs can also generate alarms within Protege GX.

Prerequisites

Before attempting this integration, ensure that the following requirements have been met:

Supported Versions

Protege GX Redwall integration is supported with the following tested and verified versions only:

Component	Version	Notes
Protege GX Software	Version 4.0.128 or higher	
Protege GX Controller	Supported versions: • 2.08.583-849 • 2.08.1268 or higher	Redwall integration is not supported in controller firmware versions 2.08.850-1267.
Redscan Manager	Version 4.1.3.0 **only**	This is the only version of the Redwall software that has been tested and validated for this integration. Other versions may be compatible, but have not been verified and may contain incompatible features.

Use an Arbitrary Number

Recent versions of Redscan Manager include a Detector ID option to 'Use an arbitrary number'. This option is **not** compatible with this integration.

The controller identifies each Redwall device by the fourth octet of the **Module IP address** as defined in the corresponding Protege GX input expander record. If an arbitrary number is assigned it will cause the Redwall device to send data that does not match the input expander records which have been programmed.

Protege GX License Requirements

License	Order Code	Notes
Protege GX Redwall Integration License	PRT-GX-RED	1 license per Protege GX server

Networking Requirements

Before you begin, ensure that the **subnet masks** of the controller and the Redwall devices are the same. For example, if the controller's subnet mask is 255.255.255.0, ensure that all Redwall devices use the same subnet mask. If the subnet masks are different, the Redwall device will appear online but input state changes will not be seen by the controller.

To view your controller's subnet mask, log in to the web interface and navigate to **Settings | Adaptor - Onboard Ethernet**. If you change the **Subnet Mask** you will need to **Save** the setting and then **Restart** the controller.

Configuring the Integration

Enabling Redwall Integration

Redwall integration needs to be enabled on each controller that communicates with Redwall detectors.

1. Navigate to **Sites | Controllers** and select the controller that will communicate with Redwall detectors.

2. If your controller has firmware version 2.08.884 or higher, module UDP is disabled by default and must be enabled to allow the controller to communicate with Redwall devices. Expand the **Commands** field and enter the following command:

   `EnableModuleUDP = true`

3. Go to the **Configuration** tab.

4. Expand the **Input expander integration** section and set the **Integration type** to Redwall.

5. Define the UDP **Port** the controller will use to receive Redwall event codes.

6. Define the **Module integration port** to be used for communication between the Protege GX controller and the Redwall scanner when it is operating as an input expander. If this is not defined, the default port is 9451.

7. Enable the **Redwall debug** option to create an audit of integration activity, which can be viewed in the Protege GX event log.

   This should only be used during initial configuration and should be disabled once the integration is operational, to avoid generating excessive unnecessary debug files.

8. Click **Save**.

If multiple controllers will communicate with Redwall modules, repeat these steps for each required controller.

Input Expander Configuration

Each integrated Redwall detector needs to be created as an input expander in Protege GX.

1. Navigate to **Expanders | Input expanders**

2. Select the **Controller** that will communicate with this detector, and **Add** a new input expander.

3. Assign a **Name** to identify the Redwall module.

4. Expand the **External integration** section and enter the **Module IP address** of the Redwall module.

5. Click **Save**.

6. In the **Configure module** popup:
   - Set the **Type** to PRT-ZX16-DIN
   - Assign an available **Physical address** for the module.
   - Set the **Outputs** to 0.
   - Click **Add now**.

7. Repeat for all Redwall detectors connected to the system.

Trouble Input Mapping

As the Redwall modules are configured to mimic Protege input expanders, Redwall trouble codes are mapped to specific trouble inputs on the Protege GX input expander record of the Redwall detector.

The trouble inputs available for each type of Redwall module are shown in the tables below.

To create the required trouble inputs for each Redwall detector:

1. Navigate to **Programming | Trouble inputs** and select the controller that this Redwall detector communicates with.

2. Create a trouble input record with a **Name** that identifies the trouble input and the Redwall detector.

3. Set the **Module type** to Input (ZX).

4. Set the **Module address** to the **Physical address** assigned to the input expander record representing this Redwall detector.

5. Set the **Module input** to the Protege GX Trouble Input Number corresponding to the appropriate Redscan Trouble Code, as defined in the tables below.

6. Navigate to the **Areas and input types** tab and assign the necessary configuration to trigger the required alarms for this trouble input.

7. Click **Save**.

The Redwall trouble codes are mapped to specific Protege GX trouble input indexes, depending on the type of Redwall module connected.

Redscan Module

Redscan Trouble Code	Protege GX Trouble Input Number
Tamper Failure	1
Disqualification Failure	10
Anti-Rotation Failure	11
Anti-Masking Failure	12
Trouble Failure	13
Soiling Failure	14
Module Offline	16

PIE-1 Module

PIE-1 Trouble Code	Protege GX Trouble Input Number
Tamper Failure	1
Trouble Failure	13
Module Offline	16

For the Module Offline trouble input, the controller sends a ping command to each of the programmed Redwall modules. Ping commands are sent every second with a response timeout of 2 seconds.

If a Redwall module has successfully registered as an input expander, it will be classified as offline after five missed ping commands (unless the controller has been power cycled or the Redwall service restarted).

If a Redwall module has never registered as an input expander (has no physical connection to the controller), the controller will check it only twice before marking it as offline. After two missed ping commands the next Redwall module will be checked for its online status. This is to increase speed and efficiency when determining the online status of Redwall modules.

Input Mapping for Event Code Reporting

Alarm codes are also mapped to specific inputs on the Protege GX input expander records.

The alarm code input mapping for each type of Redwall module is shown in the tables below.

To configure the required alarm code inputs for each Redwall detector:

1. Navigate to **Programming | Inputs** and select the controller that this Redwall detector communicates with.

2. Identify the inputs that were automatically generated for this Redwall module's input expander record.

3. Using the tables below, identify and **delete** the inputs that are not required for Redscan Alarm Code mapping.

4. Matching the **Module input** number to the appropriate Redscan Alarm Code below, rename the remaining inputs to identify the alarm code and the Redwall detector.

5. Navigate to the **Areas and input types** tab and assign the necessary configuration to trigger the required alarms for this alarm input.

6. Click **Save**.

The Redwall alarm codes are mapped to specific Protege GX inputs, depending on the type of Redwall module connected.

Input Mapping for Redscan Modules Using a 4 Zone Configuration

Redscan Alarm Code	Protege GX Input Number
A1	1
A2	2
B1	3
B2	4

Input Mapping for Redscan Modules Using an 8 Zone Configuration

Redscan Trouble Code	Protege GX Input Number
A11	1
A12	2
A21	3
A22	4
B11	5
B12	6
B21	7
B22	8

Input Mapping for PIE-1 Modules

Redscan Trouble Code	Protege GX Input Number
FR	1
NR	2
CR	3
FN	4