Elk M1 Security Panel Integration Release Notes

Content

Last modified: 09/16/20

Introduction

The Elk M1 Security Panel is tested and certified for integration with the ClareHome system. To integrate the Elk M1 panel, you will need access to the ELKRP configuration tool or a global caché device. The Elk panel must be configured with the settings required by the ClareHome system.

The instructions in this document are provided to help you quickly integrate the panel into the ClareHome system. It lists the settings required by ClareHome for the systems to sync and communicate properly. It is not intended to be a complete installation guide.

Follow the manufacturer's installation documentation, included with the product, when installing the M1.

Note: When making changes to the M1 panel, the project must be re-deployed for changes to take effect.

Supported features

The following features are supported in the M1.

Controls

The following commands are supported.

Note: The controls set the security panel’s state.

- **Arm:** This command arms the panel.
- **Disarm:** This command disarms the panel.
- **Arm Away:** The panel arms in away mode, activating the entire security system (internal and external).
- **Arm Stay:** The panel arms in stay mode, turning off the home’s internal motion detectors.
- **Bypass Zone:** This command allows the user to set the alarm as normal but ignores the alarm in the specified zone(s). When the bypassed zone is tripped, the alarm does not go off. For example, setting your Lanai as a bypass zone allows the pool cleaner to enter and work without triggering the home’s alarm.
- **Unbypass Zone:** This command removes the bypass setting of the zone.

Feedback

The following states are set in the security panel based on the commands received from the user.

Note: The feedback states can be used in Fusion to create rules and notifications. For example, when the security panel is disarmed by a family member, the welcome scene runs, turning on all lights and sending a notification to the homeowner that a specific family member has disarmed the system.

- **Partition status:** The system is either faulted, or ready.
- **Fire alarm:** The system’s connection to the fire alarm.
- **Ready to arm:** The system is ready to arm.
- **Arming:** The security system is now arming.
- **Zone status:** The real-time status of the zone – ready, faulted, bypassed, or troubled.
- **Armed:** The panel is currently in an armed state.
- **Armed away:** The panel is in the armed away state, fully armed.
- **Armed stay:** The panel is in the armed stay state, with only the outside motion detectors active.
- **Disarmed by:** The user who disarmed the panel.
- **Armed by:** The user who armed the panel.

Installation

A qualified technician should install Elk M1 security panels. Refer to the installation instructions that came with your device. Clare Controls does not assume any responsibility for damages caused by improper installation or connection to the network.

Using a serial connection with the Elk M1

After installing the M1, connect it to the ClareHome data network. To make the connection, you will need to attach a serial adapter, such as a Global Cache' iTach device or a SENA serial device server. You will also need a null modem cable, or a null modem adapter with a serial cable.

To connect the M1 to the ClareHome data network:

1. Attach one end of a null modem cable (with a male DB-9 connector), to the serial connector on M1 panel, and then attach the other end of the cable to the serial adapter device (Global Cache', SENA, or other).
2. Attach one end of a Cat 5 networking Ethernet cable to the port on the serial adapter device, and then attach the other end of the cable to a port on the ClareHome data network.
3. Configure the serial adapter with the port parameter settings in Table 1.

Table 1: Serial adapter settings

Serial Parameter	Setting
Baud Rate	115,200
Data Bits	8
Parity	None
Stop Bits	1

Notes

- To configure the serial adapter, follow the manufacturer's instructions included with the device.
- When using the M1 to communicate with ClareHome, the panel PIN must not end with a zero (0). Zeros are used as padding and are ignored.

Connecting the Elk M1 to the ClareHome project

After installing the panel, connect it to the CLIQ controller. The M1 requires a null connection. When using the M1 with a CLIQ.mini, you must use a USB to serial cable with a null modem adaptor.

To connect the Elk M1 to the CLIQ.mini:

Note: You will need the USB to serial cable (part number CLIQ-SEC-USB-01) and a null model adapter.

1. Attach the USB end of the USB to serial cable to a USB port on the CLIQ.mini.
2. Attach the opposite end of the USB to serial cable (DB-9 connector) to the null model adapter.

   – or –

   Move the jumpers on the M1 to support straight through communication.
3. Attach the opposite side of the null modem adaptor to the serial connector on the M1.

Configuring the Elk M1 for communication with the CLIQ

To ensure that the M1 can communicate with ClareHome, install your panel as instructed in the Elk M1 manufacturer installation guide. Configure the required settings listed below.

To configure the M1:

1. Enter *****, **8**. All of the function key LEDs begin to flash.
2. Enter the Go To Program code (default 9713). If the code is valid, the Service LED flashes, and the function LEDs illuminate steadily, indicating you should enter the device to program.
3. Enter **0**, **0**, ..., the address of the M1. The Armed LED illuminates until you enter a programming location.
4. Enter the programming location followed by the ... key. The Armed LED begins to flash. If this is a valid location, the Armed LED extinguishes, the Ready LED illuminates, and the binary data for the first segment of this location appears on the Zone LED.
5. To change the data, enter data followed by the * key. The location automatically increments to the next segment. The data for that segment displays. Repeat the procedure until the system reaches the last segment.
6. Set the locations with the data as follows:

Table 2: M1 required settings

Required settings	Location	Segment	Enabled bits
Feature report selection/partition feature selection	23	1	1---5---
	23	2	---4----
	23	3	-----678
	23	4	--------
	23	5	Reserved
Serial port selector	207		1
Baud rate (115,200)	208		2
Home automation protocol	209		1
Transition based broadcasts	210	1	-2--5-7-
	210	2	1-------
Command/request enables	211	1	-2-45678
	211	2	12345---
	211	3	12345678
	211	4	--345678
LCD keypad address	212		192

Note: When setting the panel PIN in the M1, do not end the PIN with zeros (0). Zeros are used as padding and are ignored.

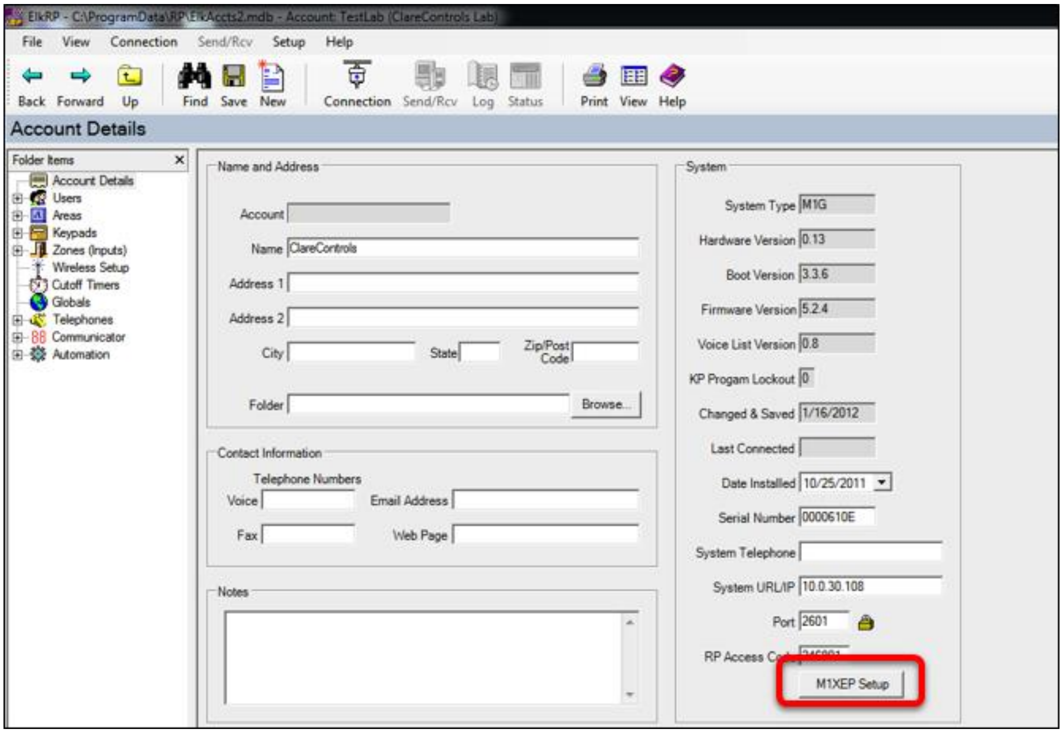
Configuring the panel with ElkRP

Configure the M1 panel using the ElkRP Windows programming tool.

To configure the panel using the ElkRP programming tool:

1. Launch the ElkRP programming tool.

2. Click **M1XEP Setup**.



ElkRP - C:\ProgramData\RP\ElkAccts2.mdb - Account: TestLab (ClareControls Lab)

Account Details

Name and Address
- Account:
- Name: ClareControls
- Address 1:
- Address 2:
- City:
- State:
- Zip/Post Code:
- Folder:

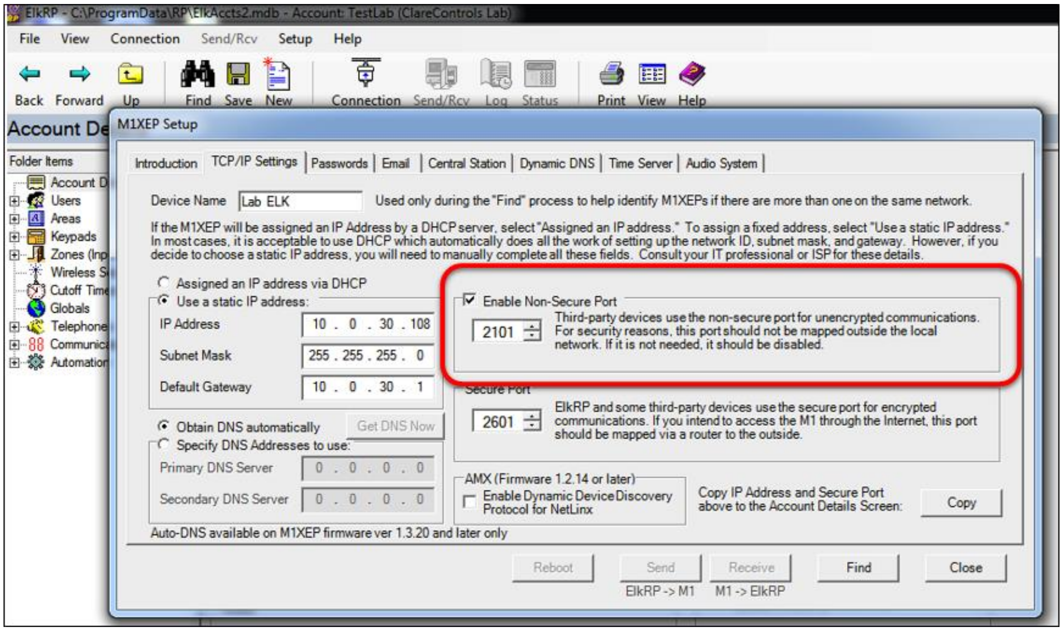
Contact Information

Telephone Numbers
- Voice:
- Fax:
- Email Address:
- Web Page:

Notes

System
- System Type: M1G
- Hardware Version: 0.13
- Boot Version: 3.3.6
- Firmware Version: 5.2.4
- Voice List Version: 0.8
- KP Progam Lockout: 0
- Changed & Saved: 1/16/2012
- Last Connected:
- Date Installed: 10/25/2011
- Serial Number: 0000610E
- System Telephone:
- System URL/IP: 10.0.30.108
- Port: 2601

3. Click the **TCP/IP Settings** tab, select the **Enable Non-Secure Port** checkbox, and then in the field enter the port number 2101.



ElkRP - C:\ProgramData\RP\ElkAccts2.mdb - Account: TestLab (ClareControls Lab)

M1XEP Setup

Device Name: Lab ELK — Used only during the "Find" process to help identify M1XEPs if there are more than one on the same network.

If the M1XEP will be assigned an IP Address by a DHCP server, select "Assigned an IP address." To assign a fixed address, select "Use a static IP address." In most cases, it is acceptable to use DHCP which automatically does all the work of setting up the network ID, subnet mask, and gateway. However, if you decide to choose a static IP address, you will need to manually complete all these fields. Consult your IT professional or ISP for these details.

○ Assigned an IP address via DHCP

● Use a static IP address:
- IP Address: 10 . 0 . 30 . 108
- Subnet Mask: 255 . 255 . 255 . 0
- Default Gateway: 10 . 0 . 30 . 1

● Obtain DNS automatically

○ Specify DNS Addresses to use:
- Primary DNS Server: 0 . 0 . 0 . 0
- Secondary DNS Server: 0 . 0 . 0 . 0

Auto-DNS available on M1XEP firmware ver 1.3.20 and later only

☑ Enable Non-Secure Port: 2101 — Third-party devices use the non-secure port for unencrypted communications. For security reasons, this port should not be mapped outside the local network. If it is not needed, it should be disabled.

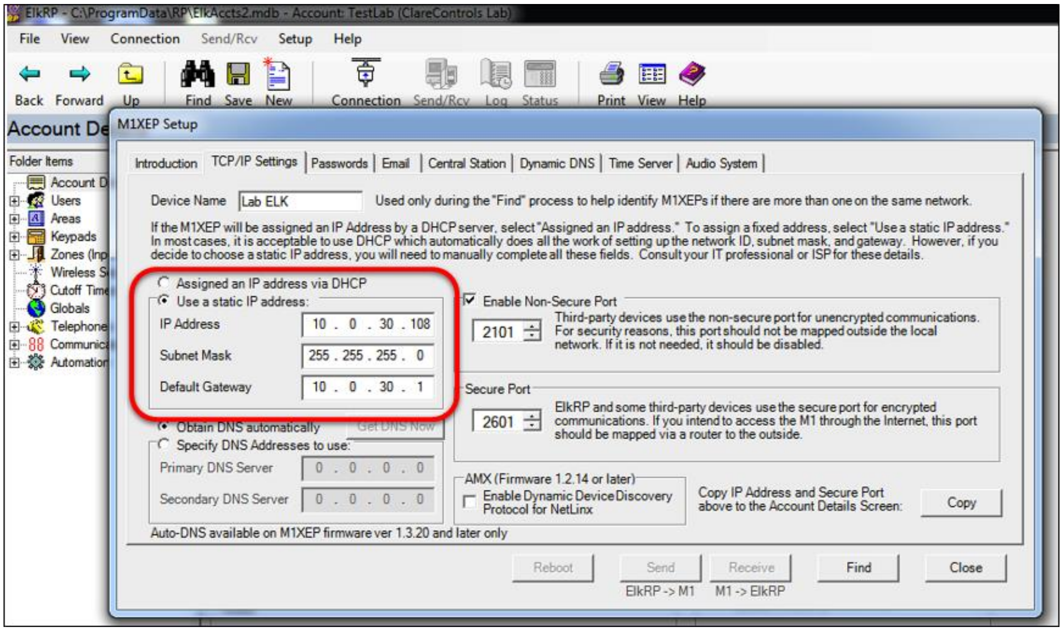
Secure Port: 2601 — ElkRP and some third-party devices use the secure port for encrypted communications. If you intend to access the M1 through the Internet, this port should be mapped via a router to the outside.

AMX (Firmware 1.2.14 or later)

☐ Enable Dynamic Device Discovery Protocol for NetLinx

Copy IP Address and Secure Port above to the Account Details Screen:

4. Select **Use a static IP address**, and then configure the static IP address information.



Device Name: Lab ELK — Used only during the "Find" process to help identify M1XEPs if there are more than one on the same network.

If the M1XEP will be assigned an IP Address by a DHCP server, select "Assigned an IP address." To assign a fixed address, select "Use a static IP address." In most cases, it is acceptable to use DHCP which automatically does all the work of setting up the network ID, subnet mask, and gateway. However, if you decide to choose a static IP address, you will need to manually complete all these fields. Consult your IT professional or ISP for these details.

○ Assigned an IP address via DHCP

● Use a static IP address:

- IP Address: 10 . 0 . 30 . 108
- Subnet Mask: 255 . 255 . 255 . 0
- Default Gateway: 10 . 0 . 30 . 1

● Obtain DNS automatically

○ Specify DNS Addresses to use:

- Primary DNS Server: 0 . 0 . 0 . 0
- Secondary DNS Server: 0 . 0 . 0 . 0

Auto-DNS available on M1XEP firmware ver 1.3.20 and later only

☑ Enable Non-Secure Port: 2101 — Third-party devices use the non-secure port for unencrypted communications. For security reasons, this port should not be mapped outside the local network. If it is not needed, it should be disabled.

Secure Port: 2601 — ElkRP and some third-party devices use the secure port for encrypted communications. If you intend to access the M1 through the Internet, this port should be mapped via a router to the outside.

AMX (Firmware 1.2.14 or later)

□ Enable Dynamic Device Discovery Protocol for NetLinx

Copy IP Address and Secure Port above to the Account Details Screen:

5. Then add and configure the Elk M1 in Fusion.

Configuring in Fusion

Once configured, add and configure the Elk M1 in Fusion. This includes defining partitions and zones created when configuring the Elk M1, and then creating a service for each partition. Follow the steps below to configure your security system in Fusion.

Creating a partition

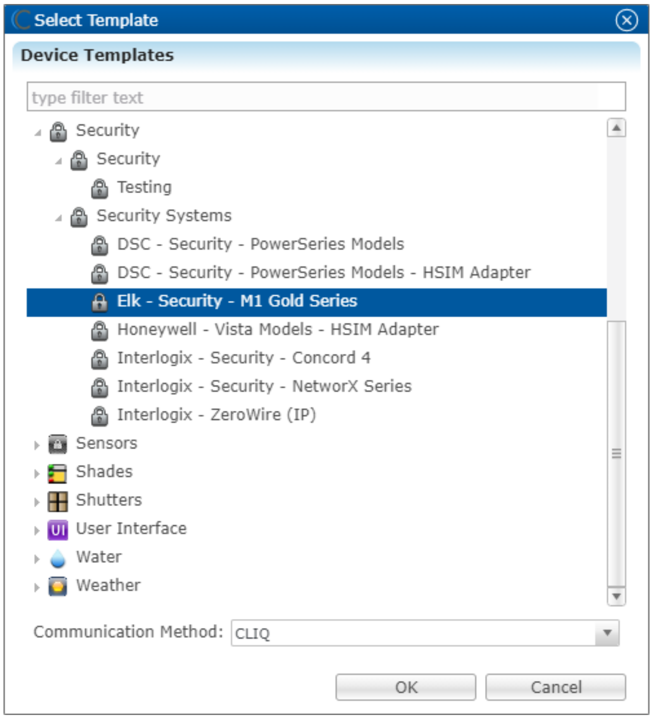
Begin by creating the partitions. Be sure that you create a partition for each partition you defined in your M1.

To add the M1 in Fusion:

1. Click the **Devices** tab, and then click the **New Device** button ⊕ to display the Select Template dialog.
2. Browse to **Elk - Security - M1 Gold Series**.

   Security > **Security Systems** > **Elk - Security - M1 Gold Series**

3. Select **CLIQ** in the Communication Method drop-down if you are using a CLIQ.host or a CLIQ.mini.



Select Template

Device Templates

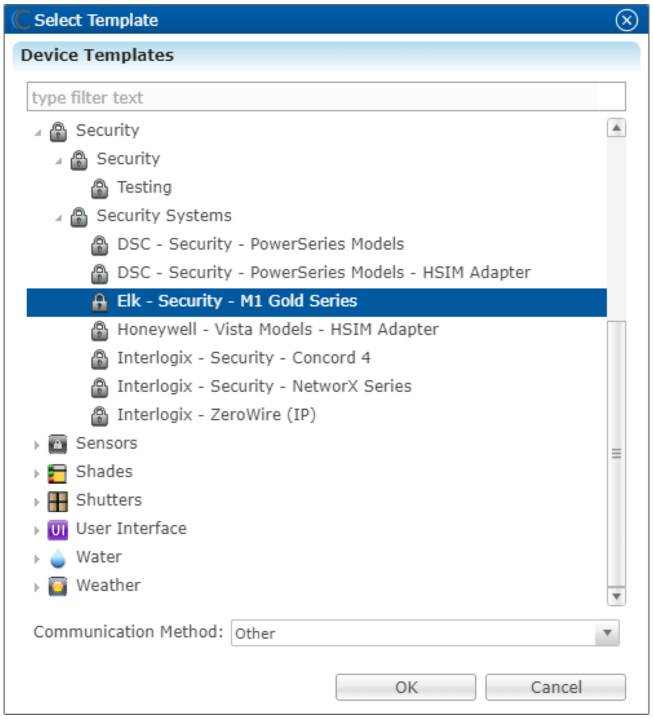
type filter text

- Security
  - Security
    - Testing
  - Security Systems
    - DSC - Security - PowerSeries Models
    - DSC - Security - PowerSeries Models - HSIM Adapter
    - Elk - Security - M1 Gold Series
    - Honeywell - Vista Models - HSIM Adapter
    - Interlogix - Security - Concord 4
    - Interlogix - Security - NetworX Series
    - Interlogix - ZeroWire (IP)
- Sensors
- Shades
- Shutters
- User Interface
- Water
- Weather

Communication Method: CLIQ

– Or –

Select **Other** in the Communication Method drop-down if you are using serial.



Select Template

Device Templates

type filter text

- Security
  - Security
    - Testing
  - Security Systems
    - DSC - Security - PowerSeries Models
    - DSC - Security - PowerSeries Models - HSIM Adapter
    - Elk - Security - M1 Gold Series
    - Honeywell - Vista Models - HSIM Adapter
    - Interlogix - Security - Concord 4
    - Interlogix - Security - NetworX Series
    - Interlogix - ZeroWire (IP)
- Sensors
- Shades
- Shutters
- User Interface
- Water
- Weather

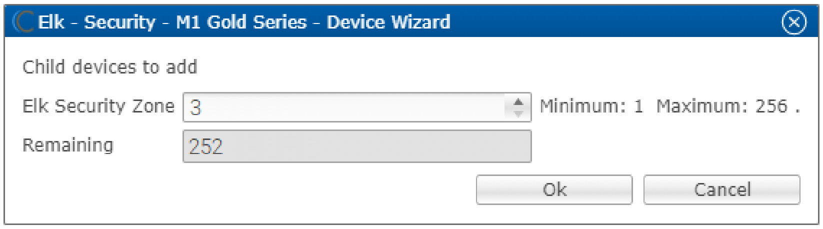
Communication Method: Other

4. Click **OK**.

5. The security Device Wizard displays. Select the number of zones, and then click **OK**.

   Notes

   - One partition is created automatically. Additional partitions must be added manually.
   - The number of zones you enter must match the number of zones defined in the M1 panel. In the example below, we create three zones.



Elk - Security - M1 Gold Series - Device Wizard

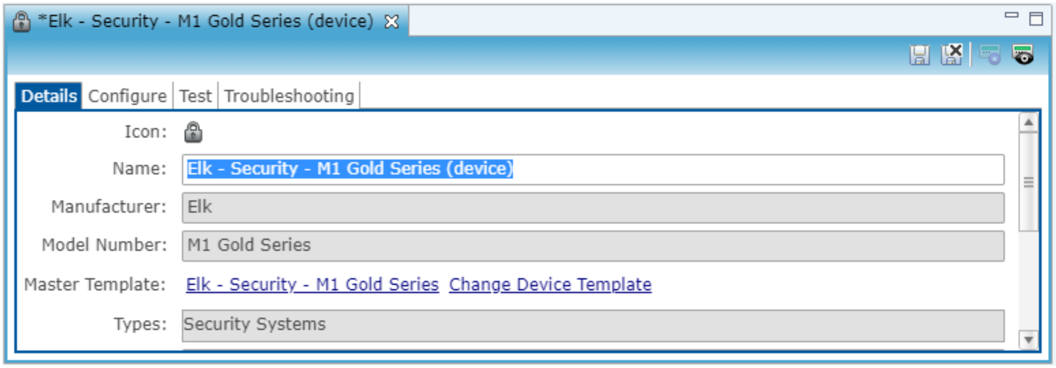
Child devices to add

Elk Security Zone: 3 Minimum: 1 Maximum: 256 .

Remaining: 252

6. The **Details** tab displays.

   Enter a name for your Elk M1.



*Elk - Security - M1 Gold Series (device)

Icon:

Name: Elk - Security - M1 Gold Series (device)

Manufacturer: Elk

Model Number: M1 Gold Series

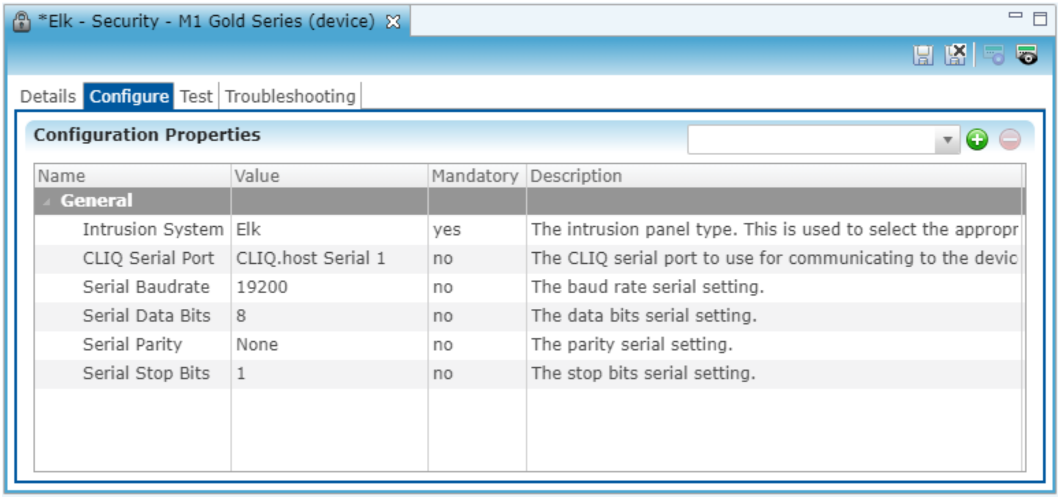
Master Template: Elk - Security - M1 Gold Series Change Device Template

Types: Security Systems

7. Click the **Configure** tab.

8. Configure the fields with the serial information.

   Note: Ensure that you select the proper value for the CLIQ Serial Port drop-down. CLIQ.host and CLIQ.mini each have port options.

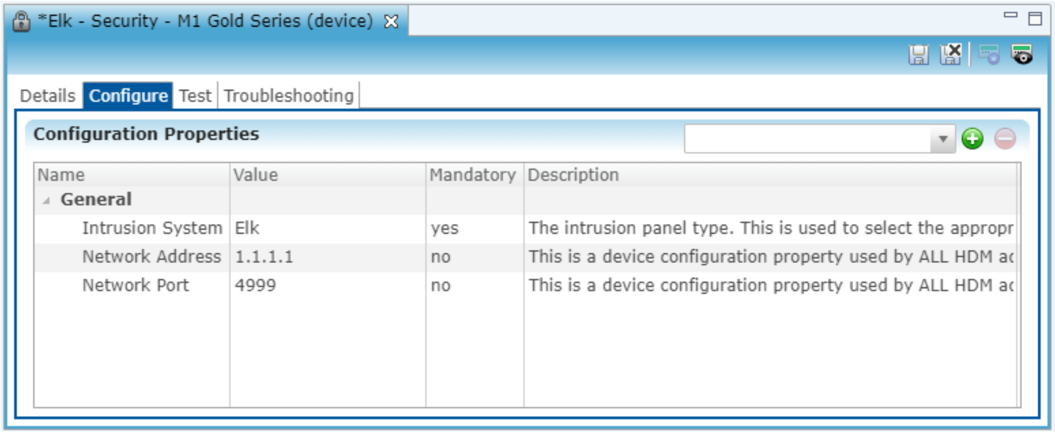


Name	Value	Mandatory	Description
General			
Intrusion System	Elk	yes	The intrusion panel type. This is used to select the appropr
CLIQ Serial Port	CLIQ.host Serial 1	no	The CLIQ serial port to use for communicating to the devic
Serial Baudrate	19200	no	The baud rate serial setting.
Serial Data Bits	8	no	The data bits serial setting.
Serial Parity	None	no	The parity serial setting.
Serial Stop Bits	1	no	The stop bits serial setting.

– Or –

Configure the fields with the correct IP information.

Note: The Network Address and Network Port are unique to your system.



Name	Value	Mandatory	Description
General			
Intrusion System	Elk	yes	The intrusion panel type. This is used to select the appropr
Network Address	1.1.1.1	no	This is a device configuration property used by ALL HDM ac
Network Port	4999	no	This is a device configuration property used by ALL HDM ac

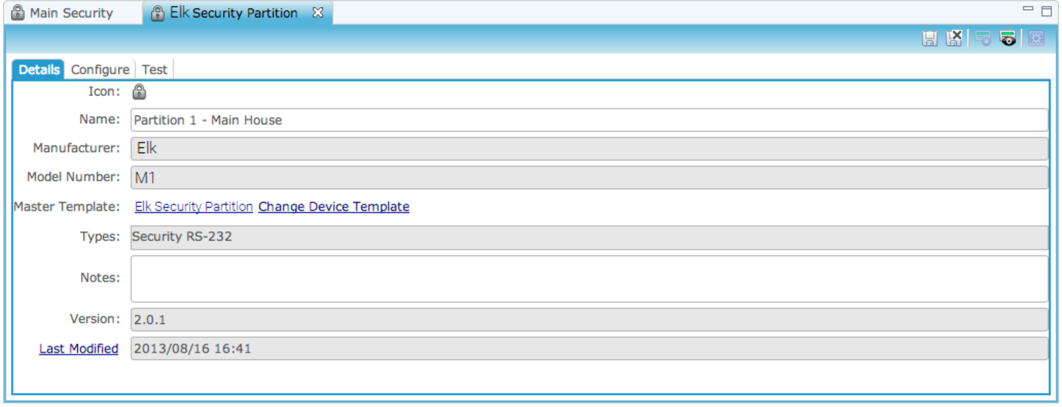
9. Click the **Save** button 💾.

To configure a partition:

1. Return to the **Devices** tab, and then double-click the first partition to display its **Details** tab.

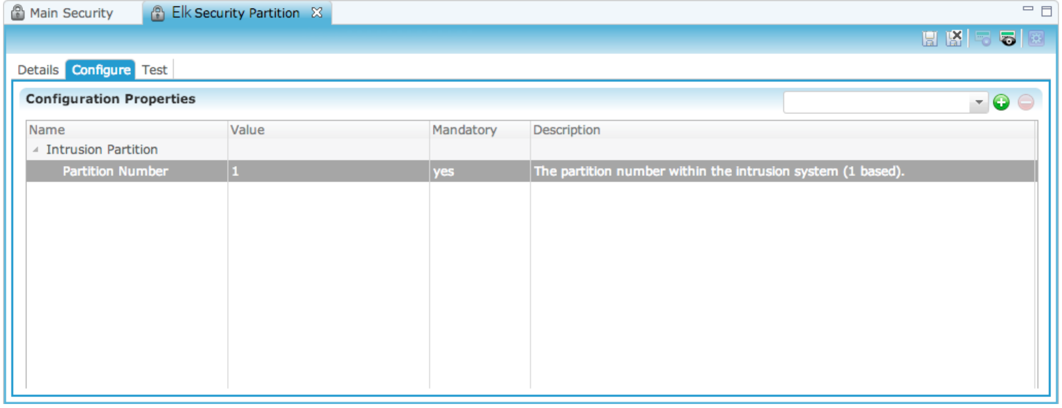
2. Enter a name for the partition.

   In our example below, the first partition is named “Partition 1, Main House.”



Icon:	
Name:	Partition 1 - Main House
Manufacturer:	Elk
Model Number:	M1
Master Template:	Elk Security Partition Change Device Template
Types:	Security RS-232
Notes:	
Version:	2.0.1
Last Modified	2013/08/16 16:41

3. Click the **Configure** tab.
4. In the **Value** field, enter the partition number.



Configuration Properties

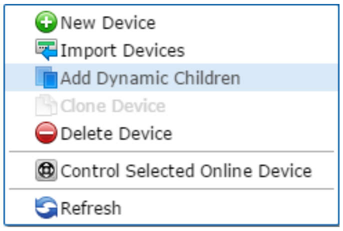
Name	Value	Mandatory	Description
Intrusion Partition			
Partition Number	1	yes	The partition number within the intrusion system (1 based).

5. Click the **Save** button .

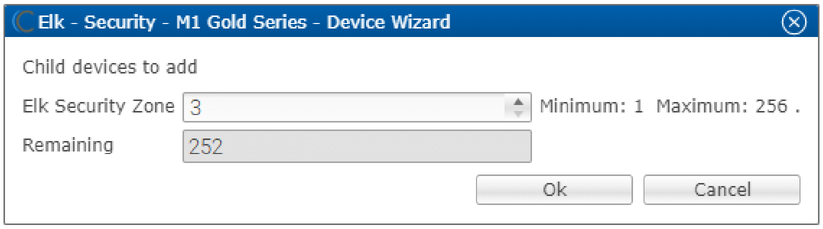
To manually add partitions to the security system:

Note: When adding partitions, be sure that you do not duplicate the partition numbers. Each partition number must be unique.

1. Return to the **Devices** tab.
2. Right-click the partition, and then select **Add Dynamic Children**.



3. The security Device Wizard displays.



Elk - Security - M1 Gold Series - Device Wizard

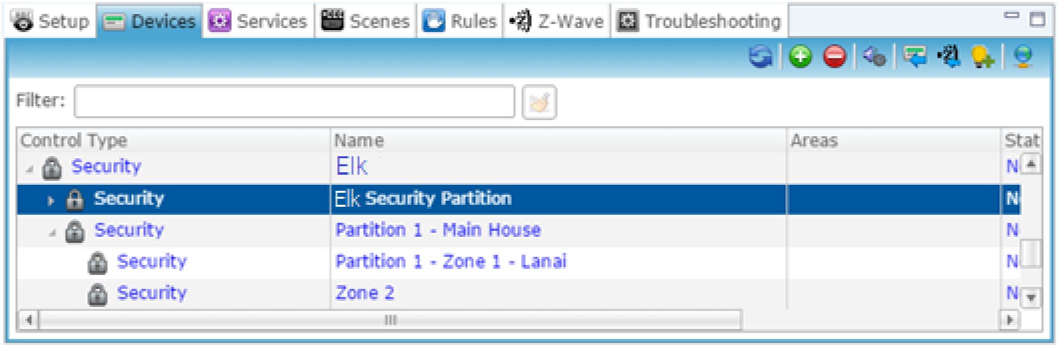
Child devices to add

Elk Security Zone: 3 Minimum: 1 Maximum: 256 .

Remaining: 252

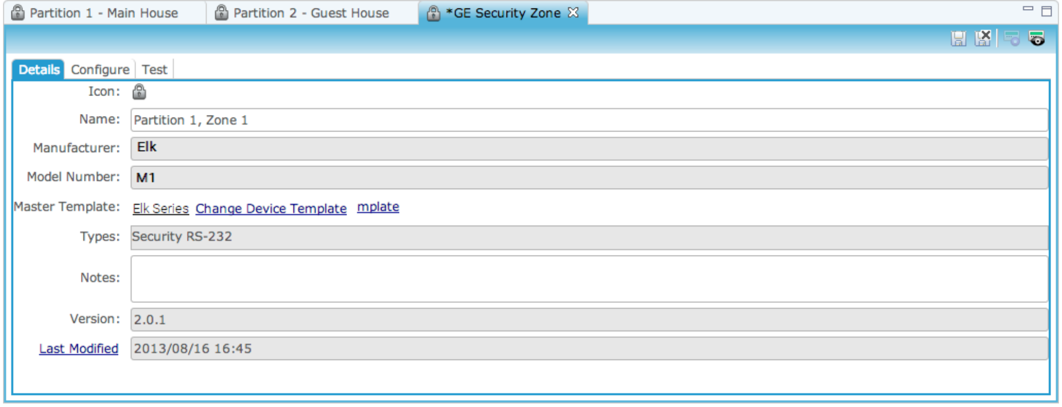
4. Select the number of partitions, and then click **OK**.

5. Return to the **Devices** tab and browse to the first security partition to configure.



Control Type	Name	Areas	Stat
Security	Elk		N
Security	Elk Security Partition		N
Security	Partition 1 - Main House		N
Security	Partition 1 - Zone 1 - Lanai		N
Security	Zone 2		N

6. The **Details** tab displays. Enter a name and notes for the device if desired, and then click the **Configure** tab.



Icon:

Name: Partition 1, Zone 1

Manufacturer: Elk

Model Number: M1

Master Template: Elk Series Change Device Template mplate

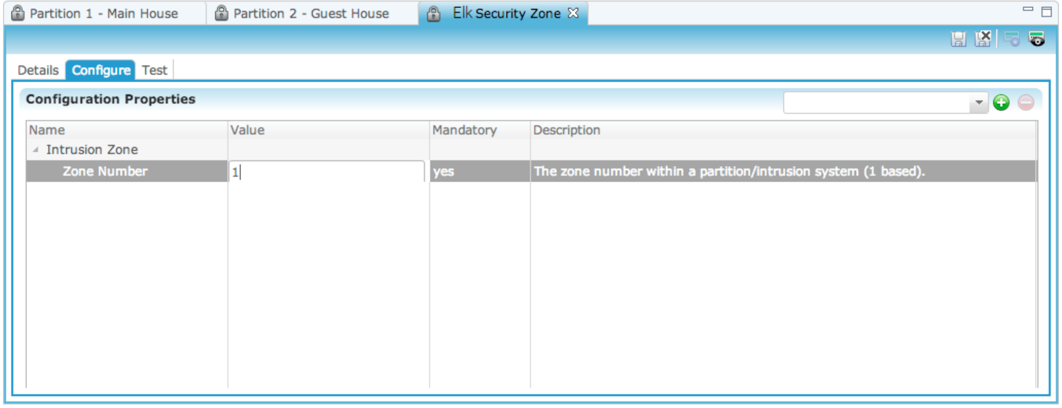
Types: Security RS-232

Notes:

Version: 2.0.1

Last Modified 2013/08/16 16:45

7. Expand the Intrusion Partition drop-down, and then enter the partition number in the **Value** field.



Configuration Properties

Name	Value	Mandatory	Description
Intrusion Zone			
Zone Number	1	yes	The zone number within a partition/intrusion system (1 based).

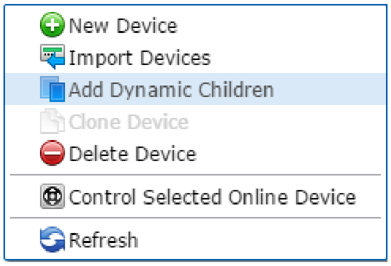
8. Click the **Save** button .

9. Repeat steps 1 through 8 for each partition.

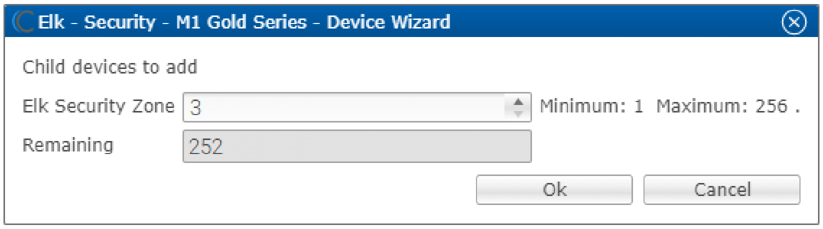
To manually add zones to a partition:

1. Return to the **Devices** tab.

2. Right-click the first partition, and then select **Add Dynamic Children**.



3. Fusion has added the first zone for you. Enter the number of additional zones for this partition.



Elk - Security - M1 Gold Series - Device Wizard

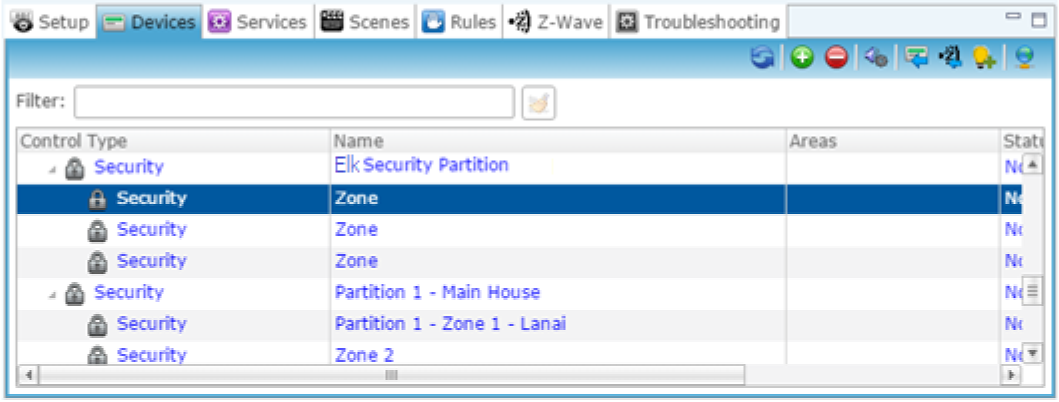
Child devices to add

Elk Security Zone 3 Minimum: 1 Maximum: 256 .

Remaining 252

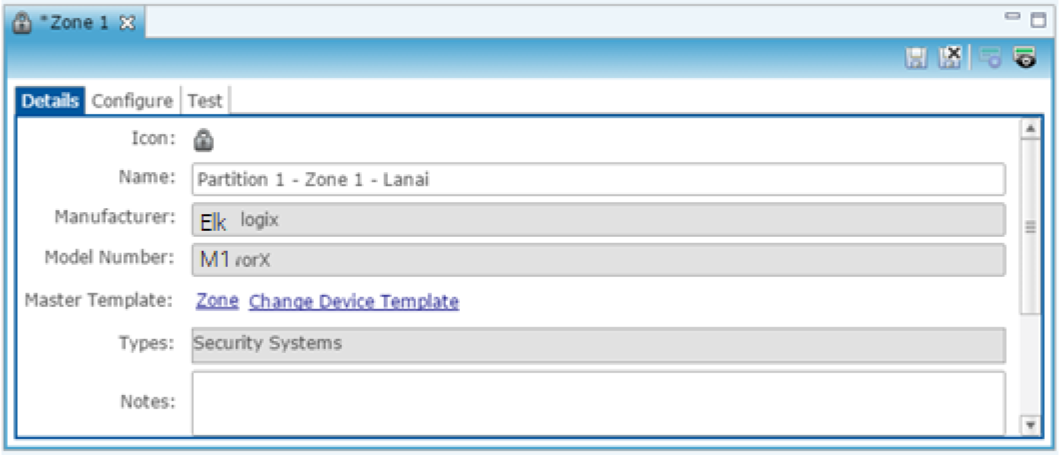
4. Click **OK**.

5. Return to the **Devices** tab, and then browse to the first security zone to configure.



Control Type	Name	Areas	State
Security	Elk Security Partition		No
Security	Zone		No
Security	Zone		No
Security	Zone		No
Security	Partition 1 - Main House		No
Security	Partition 1 - Zone 1 - Lanai		No
Security	Zone 2		No

6. Fusion displays the **Details** tab for the first zone. Name the zone.



Icon:

Name: Partition 1 - Zone 1 - Lanai

Manufacturer: Elk logix

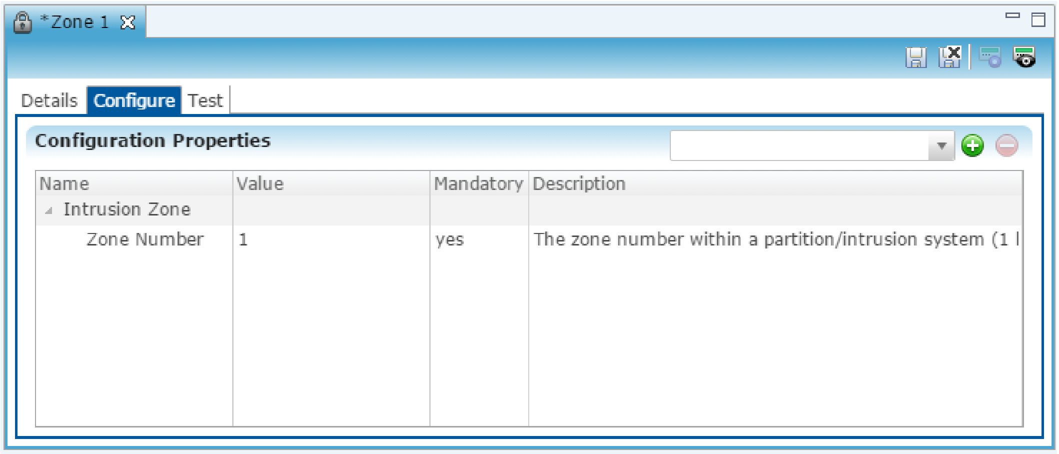
Model Number: M1 rorX

Master Template: Zone Change Device Template

Types: Security Systems

Notes:

7. Click the **Configure** tab, and enter the zone number in the **Value** field.



Configuration Properties

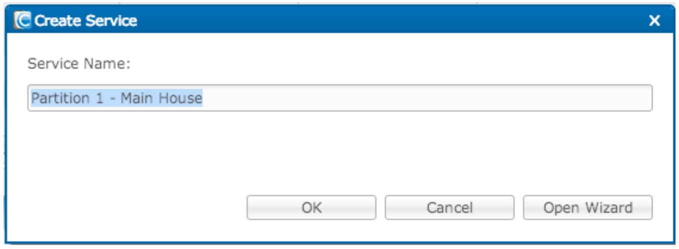
Name	Value	Mandatory	Description
Intrusion Zone			
Zone Number	1	yes	The zone number within a partition/intrusion system (1 I

8. Click the **Save** button 💾.

9. Repeat steps 1 through 4 for each partition, and 5 through 8 for each zone.

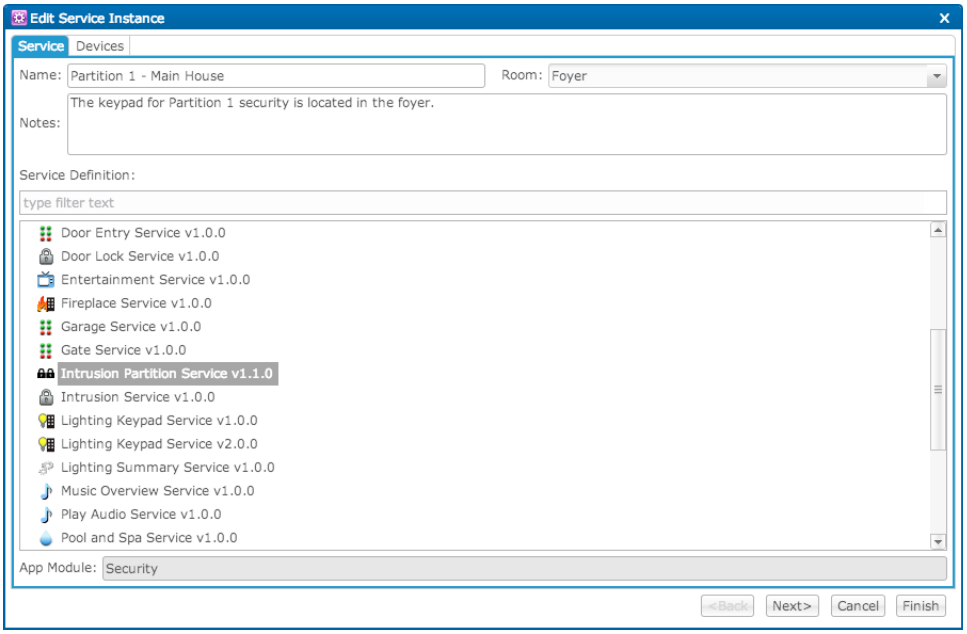
To create a service for a partition:

1. Click the first partition in the list to display its **Details** tab, and then click the **New Service Instance** button to display the Create Service dialog.



Service Name: Partition 1 - Main House

2. Click **Open Wizard** to display the Service Instance dialog, select Intrusion Partition Service, and then click **Next**.



Name: Partition 1 - Main House

Room: Foyer

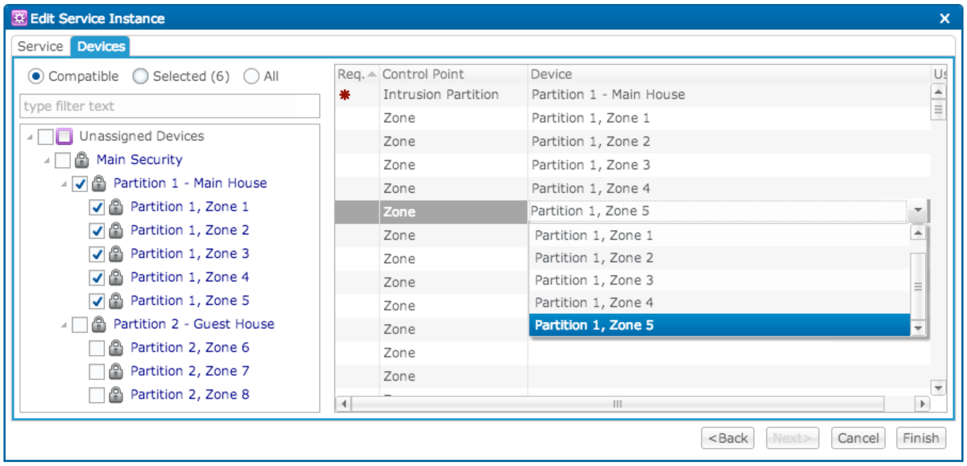
Notes: The keypad for Partition 1 security is located in the foyer.

Service Definition:

- Door Entry Service v1.0.0
- Door Lock Service v1.0.0
- Entertainment Service v1.0.0
- Fireplace Service v1.0.0
- Garage Service v1.0.0
- Gate Service v1.0.0
- **Intrusion Partition Service v1.1.0**
- Intrusion Service v1.0.0
- Lighting Keypad Service v1.0.0
- Lighting Keypad Service v2.0.0
- Lighting Summary Service v1.0.0
- Music Overview Service v1.0.0
- Play Audio Service v1.0.0
- Pool and Spa Service v1.0.0

App Module: Security

3. Fusion displays a checkmark for the selected partition and its zones. If not, select the partition and zones on the left side of the window.



● Compatible ○ Selected (6) ○ All

- □ Unassigned Devices
  - □ Main Security
    - ☑ Partition 1 - Main House
      - ☑ Partition 1, Zone 1
      - ☑ Partition 1, Zone 2
      - ☑ Partition 1, Zone 3
      - ☑ Partition 1, Zone 4
      - ☑ Partition 1, Zone 5
    - □ Partition 2 - Guest House
      - □ Partition 2, Zone 6
      - □ Partition 2, Zone 7
      - □ Partition 2, Zone 8

Req.	Control Point	Device	Us
*	Intrusion Partition	Partition 1 - Main House	
	Zone	Partition 1, Zone 1	
	Zone	Partition 1, Zone 2	
	Zone	Partition 1, Zone 3	
	Zone	Partition 1, Zone 4	
	Zone	Partition 1, Zone 5	
	Zone		
	Zone		
	Zone		
	Zone		
	Zone		
	Zone		
	Zone		

- Partition 1, Zone 1
- Partition 1, Zone 2
- Partition 1, Zone 3
- Partition 1, Zone 4
- **Partition 1, Zone 5**

4. Set the control points for the partition and zones.

   On the right side of the window, click inside the **Devices** field, and then select a zone from the dropdown list.

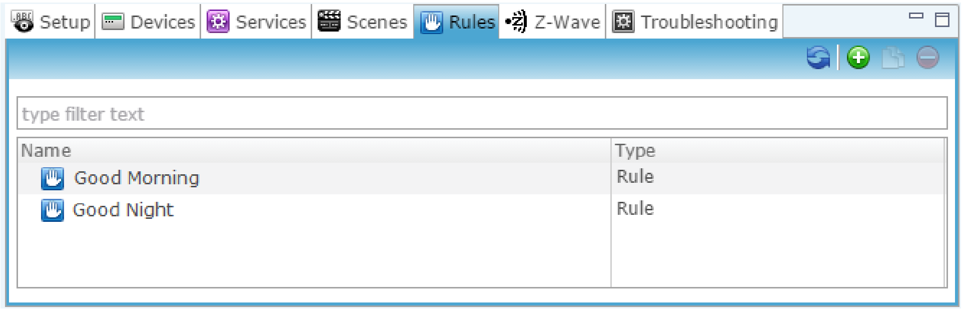
5. Click **Finish**, and then deploy your project.

Configuring rules with the M1

The following example sets an Armed-Away rule. When the M1 is set to Arm-Away, the Goodbye – Lights Off scene runs.

To create an Armed-Away mode rule in Fusion:

1. Access your project, and then click the **Rules** tab.

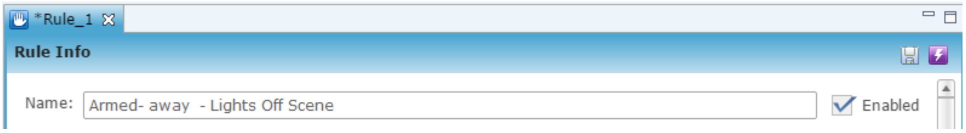


type filter text

Name	Type
Good Morning	Rule
Good Night	Rule

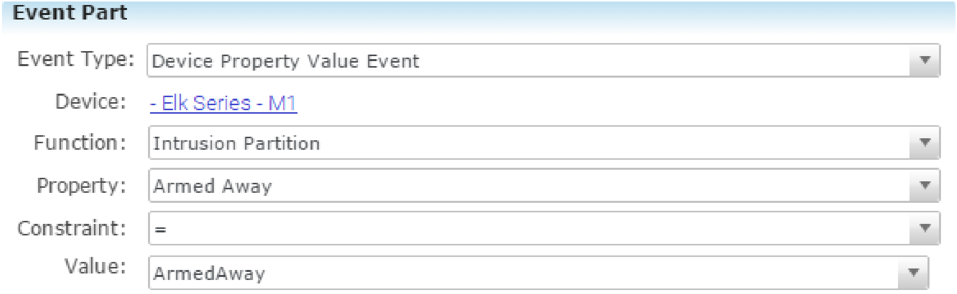
2. Click the **New Rule** button ⊕.

3. Enter a name for the rule, and then select the Enable Rule checkbox.



Name: Armed- away - Lights Off Scene ☑ Enabled

4. Configure the Event Part as below.
   - **Event Type:** Device Property Change Event
   - **Device:** Elk Series – M1
   - **Function:** Intrusion Partition
   - **Property:** Arm Away
   - **Constraint:** =
   - **Value:** ArmedAway



Event Part

Event Type: Device Property Value Event

Device: - Elk Series - M1

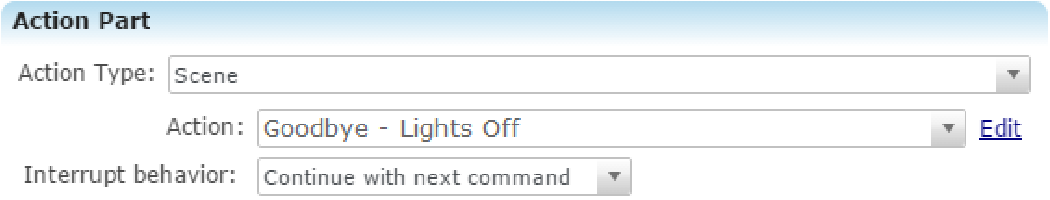
Function: Intrusion Partition

Property: Armed Away

Constraint: =

Value: ArmedAway

5. Configure the Action part as below.
    - **Action Type:** Scene
    - **Action:** Goodbye – Lights Off
    - **Interrupt behavior:** Continue with next command



Action Part

Action Type: Scene

Action: Goodbye - Lights Off

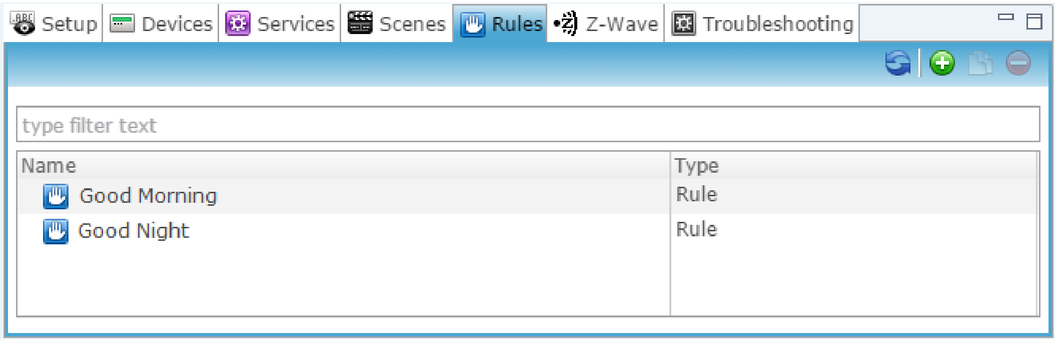
Interrupt behavior: Continue with next command

6. Click the **Save** button , and then deploy the project.

To create a disarmed by rule in Fusion:

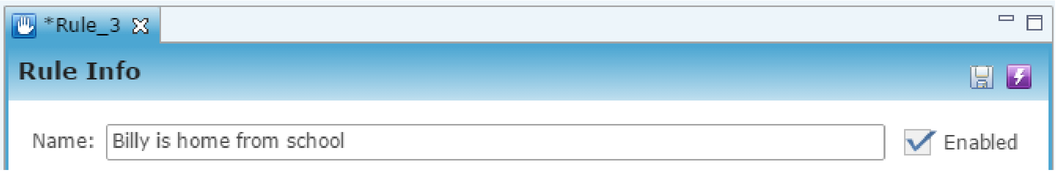
Note: The Elk panel must be configured with individual pin numbers assigned to people with access to the property. If the Elk panel is not configured with individual pin numbers, this rule will not work properly. To set pin numbers in the Elk see the documentation that came with the device.

1. Access your project, and then click the **Rules** tab.



Name	Type
Good Morning	Rule
Good Night	Rule

2. Click the **New Rule** button .
3. Enter a name for the rule, and then select the Enable Rule checkbox.

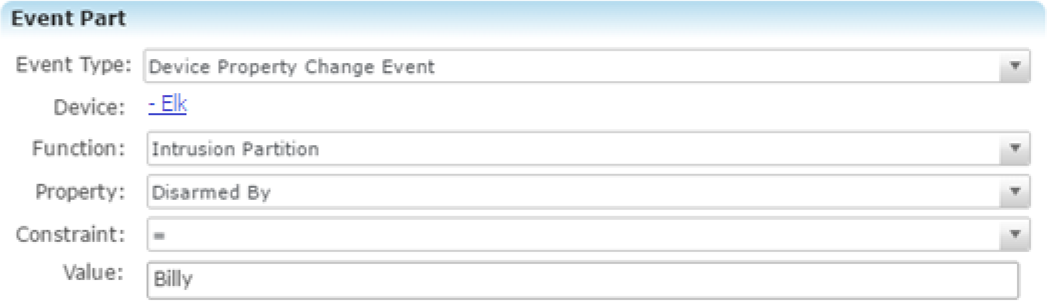


Rule Info

Name: Billy is home from school ☑ Enabled

4. Configure the Event Part as below.
   - **Event Type:** Device Property Change Event
   - **Device:** - Elk
   - **Function:** Intrusion Partition
   - **Property:** Disarmed By
   - **Constraint:** =
   - **Value:** Billy

     Note: The Value field must be identical to the name configured in the Elk panel.



Event Part

Event Type: Device Property Change Event

Device: - Elk

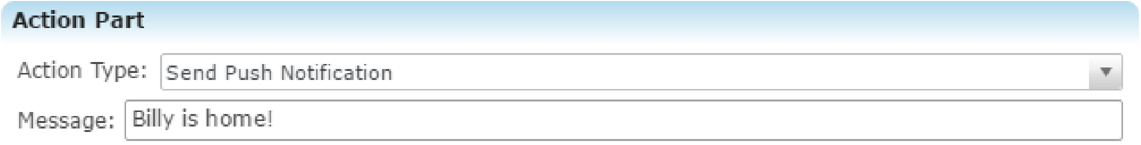
Function: Intrusion Partition

Property: Disarmed By

Constraint: =

Value: Billy

5. Configure the Action Part as below.
   - **Action Type:** Send Push Notification
   - **Message:** Billy is home!



Action Part

Action Type: Send Push Notification

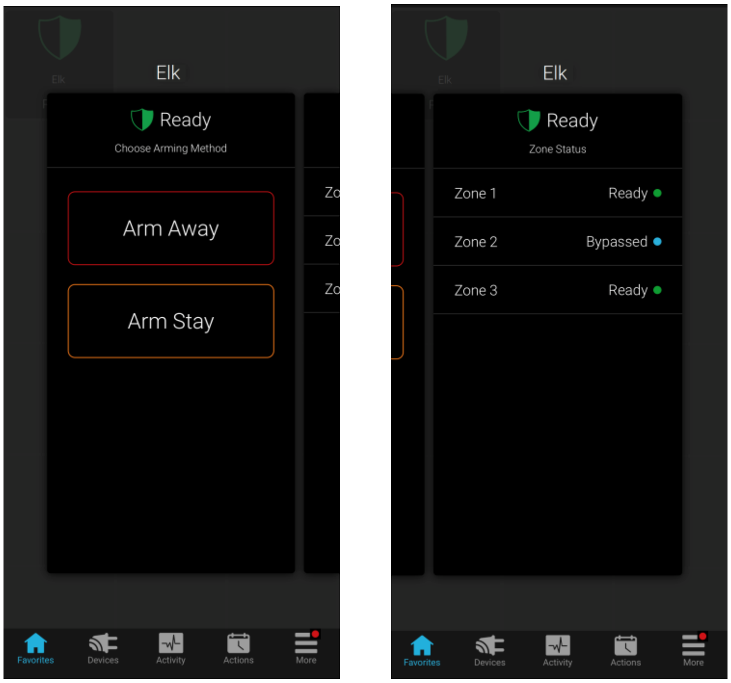
Message: Billy is home!

6. Click the **Save** button 💾, and then deploy the project.

User Interface

The following figures show the Elk controls in the ClareHome app.

Figure 1: **Elk Security System UI in ClareHome**



Zone 1 Ready
Zone 2 Bypassed
Zone 3 Ready

Contact information

Clare Controls, LLC.
7519 Pennsylvania Ave, Suite 104
Sarasota, FL 34243

General: 941.328.3991
Fax: 941.870.9646
www.clarecontrols.com

Integrator/Dealer Support: 941.404.1072
claresupport@clarecontrols.com

Homeowner Support (ClareCare): 941.315.2273 (CARE)
help@clarecontrols.com