Ademco/Honeywell Vista ICM (Internet Connection Module)

The following is based on a Vista ICM connected to a Vista 20P unit running “in2 fusion image\_2.2.3 - Mon Jun 4 14:18:12 MDT 2007” and may contain factual errors and pure guesswork.

# Operating System and Software

The device operating system is uClinux (<http://www.uclinux.org>).

The web server is boa ([www.boa.org](http://www.boa.org)).

Script aliases can be viewed in the /etc/boa.conf file.

The main application running communications between the ECP bus, devices, and Ethernet is named Fusion. It would seem that it provides a scripting runtime that is relatively straightforward and should provide a nice clean way to hack the behavior of the device. Sample files are located in the /var/fusion/devices folder.

# Network Ports

|  |  |  |
| --- | --- | --- |
| Port | Protocol | Description |
| TCP 23 | Telnet | Provides Telnet access to the device. |
| TCP 80 | HTTP | Provides web browser access. |
| UDP 3947 | UDP Datagrams | Broadcasts various system events and information. |
| TCP 50003 | Unknown/ASCII | Provides a continuous stream of updates of text that is displayed on the alarm system’s display panel. Can be changed in advanced setup. |

# Telnet Access

The device has a Telnet server running. There is only one user account, root, and the password is “42666263”.

# Web Tools

## Client Access

Normal client access is available from a web browser from <http://myhome/setup> or <http://1.2.3.4/setup> where 1.2.3.4 is the IP address of the unit.

## Configuration

To access the device setup, open <http://myhome/setup> or <http://1.2.3.4/setup> from a web browser. The product documentation will provide additional details.

## Debugging Utilities

The device provides a nice amount of debugging utilities directly over the web interface. There are two particularly interesting pages: <http://myhome/debug> and <http://myhome/show_vars>. You’ll also want to look at <http://myhome/debug_output> to see what options are available.

# Tips

## Backup Settings

Before you access the device via Telnet or make any changes, make a backup of the settings

## Update to Latest Firmware

Be sure to update to the latest firmware, currently 2.2.3. It also seems that the device definitions don’t get auto-updated and thus you may have an old version of the honeywell\_vista.dve file active. If this is the case, you may be missing various commands/macros, such as the Refresh macro.

One way to force an update of the device file is to make a copy of the latest available version in the /var/fusion/devices folder with a different name, and then go through the web setup to change the file used.

## Security

As you’ve probably noticed, the device is wide open and doesn’t provide even HTTPS access. For this reason, it would probably be a good idea to keep this device on a separate network by adding an extra network card into one of your computers instead of having it connected to your LAN.

## Digging Deeper

Try adding the “Network” device with “Web” or an IP camera to get additional packet types to be sent.

# HTTP Commands

The following table lists some of the more interesting commands that may be sent using a GET request.

|  |  |  |
| --- | --- | --- |
| Path | Query Parameters | Description |
| /cmd | ?cmd= | Sends the given command to the group, unit or node. |
| /cmd\_list |  | Displays a list of all available commands. |
| /debug |  | Displays node, port and unit information. |
| /show\_vars |  |  |
| /show\_flash | ?boot  ?ethmac  ?bootarg  ?settings  ?Sector=[0 – 34] | Prints a hex-dump of the requested item. |

## cmd Command

All commands start with /cmd?cmd= and are appended with a tick value. The tick value should be optional from non-web browser applications. For example:

<http://myhome/cmd?cmd=(0.0.0)Monitor_1_1_2023468919>

In addition to the commands below, you can send any item that is defined in the [macro] section on the /show\_vars page. Commands begin with the target identified by (Group#.Node#.Unit#). The following table displays sample values. Parameters are separated by an underscore.

|  |  |
| --- | --- |
| Command | Description |
| (0.0.0)Monitor\_0\_0\_AppletID\_[Name] | Switches the content sent to the feedback port (?) |
| (0.0.0)Select\_1\_1 | Requests the security module to report its ID. |
| (0.1.1)Refresh | Requests the security module send out the following variables:  display  ArmStatus  Ready  ZS.[1-16] |

# UDP Packet Contents

The following describes most of the structure and contents broadcast by the UDP port.

## Packet Types

|  |  |
| --- | --- |
| Values | Description |
| 0x01, 0x03 | Node Discovery/Network Info |
| 0x01, 0x04 | Unit Info |
| 0x02, 0x04 | Variable |
| 0x04, 0x01 | Command/Trigger |

## Header

The following is a common header shared by all packet types.

|  |  |  |
| --- | --- | --- |
| Bytes | Format | Description |
| 00 – 01 | UInt16 | Packet type |
| 02 – 03 | UInt16 | Unknown. Possibly part of the packet type. Seems to be 0x00, 0x01 always. |
| 04 – 05 | UInt16 | Time code |

## Node Discovery – 0x01, 0x03

There are two versions of this packet, both with very similar content. The Vista ICM was set to a static IP address and using DHCP was not tried. Type 0 may be related to DHCP.

### Type 0

|  |  |  |
| --- | --- | --- |
| Bytes | Format | Description |
| 06 – 07 | UInt16 | Subtype: 0x00, 0x00 |
| 08 – 09 | UInt16 | hb\_chksm |
| 10 – 11 | 2 bytes | Unknown |
| 12 – 13 | UInt16 | Data length |
| 14 – 19 | 6 bytes | Unknown |
| 20 – 23 | 4 x UInt8 | Device IP address |
| 24 – 27 | 4 bytes | Unknown |
| 28 – 33 | 6 x UInt8 | Device MAC address |
| 34 – 39 | 6 bytes | Unknown |
| 40 - 49 | 10 bytes | Unknown. Last byte potentially “flags” |
| 50 | UInt8 | Auto incrementing number |
| 51 | Byte | Unknown, potentially padding |
| 52 - 69 (Data length) | ASCII | sbrnd value terminated by 0x0A and padded with 0x00 as necessary |

### Type 1

|  |  |  |
| --- | --- | --- |
| Bytes | Format | Description |
| 06 – 07 | UInt16 | Subtype: 0x00, 0x01 |
| 08 – 09 | UInt16 | hb\_chksm |
| 10 – 11 | 2 bytes | Unknown |
| 12 – 13 | UInt16 | Data length |
| 14 – 19 | 6 bytes | Unknown |
| 20 – 23 | 4 x UInt8 | Device IP address |
| 24 – 27 | 4 x UInt8 | Device IP address |
| 28 – 33 | 6 x UInt8 | Device MAC address |
| 34 – 39 | 6 x UInt8 | Device MAC address |
| 40 - 49 | 10 bytes | Unknown. Last byte potentially “flags” |
| 50 | UInt8 | Auto incrementing number |
| 51 | Byte | Unknown, potentially padding |
| 52 – 69 (Data length) | ASCII | sbrnd value terminated by 0x0A and padded with 0x00 as necessary |

## Unit Info – 0x01, 0x04

This packet contains a subset of the variables for a unit.

|  |  |  |
| --- | --- | --- |
| Bytes | Format | Description |
| 06 – 07 | UInt16 | Subtype (?): 0x00, 0x01 |
| 08 – 09 | UInt16 | checksum |
| 10 – 11 | UInt16 | Unit number |
| 12 – 13 | UInt16 | Data length |
| 14 – 19 | 6 bytes | Unknown |
| 20 – 23 | 4 x UInt8 | Device IP address |
| 24 – 27 | 4 x UInt8 | Device IP address |
| 29 – 33 | 6 x UInt8 | Device MAC address |
| 34 – 39 | 6 x UInt8 | Device MAC address |
| 40 – 51 | 12 bytes | Unknown. Last byte is potentially “flags” |
| 52 – Data length | ASCII | Subset of variable values as “key=value”, delimited by 0x0A, and padded with 0x00 as necessary. |

## Variable – 0x02, 0x04

This packet contains a variable value. This may be sent by the SendVar() command in device scripts. This is easily the most interesting packet as it will contain the text that is displayed on the alarm panel, along with information about the state of zones (faults) and whether the alarm is armed.

Sample data values:

* “1.1.Ready=0”
* “1.1.display= Ready to Arm “
* “1.1.ZS.4=1”

|  |  |  |
| --- | --- | --- |
| Bytes | Format | Description |
| 06 – 07 | UInt16 | Data length |
| 08 – Data length | ASCII | Variable value as “Node#.Unit#.Key=Value” and padded/terminated with 0x00. |

## Command/Trigger/Event – 0x04, 0x01

This packet contains information about a command that was executed, such as arm, disarm, a zone fault, or an alarm event (fire, low battery, etc). This is likely to be the most reliable indicator of events. There can be one two three parameters passed with this packet. Zone trigger events are sent the first time the zone indicates activity and is reset after 30 seconds.

The high-level format is:

cmd=(0.0.0)\_T\_name:parameter1(parameter2,parameter3)

Sample data values:

cmd=(0.0.0)\_T\_Security:Disarmed

cmd=(0.0.0)\_T\_Security:Armed Away

cmd=(0.0.0)\_T\_Security:Office Window

|  |  |  |
| --- | --- | --- |
| Bytes | Format | Description |
| 06 – 07 | UInt16 | Data length |
| 08 – Data length | ASCII | Command value as “cmd=value” and padded/terminated with 0x00. |

## Vista Security Variables

The following table lists some common variables that are sent out by the ICM.

|  |  |  |
| --- | --- | --- |
| Variable | Known Values | Description |
| ArmStatus | 0 = Disarmed  1 = Arm stay  2 = Arm away |  |
| AlarmEvent | Numeric value | Alarm event count. A better option is to watch for the Alarm trigger. |
| display | “\*\*\*\*DISARMED\*\*\*\*”  “ Ready to Arm ”  “DISARMED CHIME”  “DISARMED BYPASS”  “ARMED \*\*\*AWAY\*\*\*”  “ARMED \*\*\*STAY\*\*\*”  “\*\*\*NIGHT-STAY\*\*\*”  “ARMED \*MAXIMUM\*”  “ARMED \*INSTANT\*”  “DISARM SYSTEM”  “Test In Progress”  “Busy-Standby”  “FAULT …”  “CHECK …”  “ALARM”  “EXIT ALARM”  “AC LOSS”  “SYSTEM LO BAT”  “LO BAT”  “RCVR Jam”  “Open Circuit”  “BYPAS …”  “Alarm Canceled”  “COMM. FAILURE ”  “ZONES FAULTED” “You may exit now”  “Hit \* for faults”  “MODEM COMM” | Alarm panel display text. Likely to be different between various Vista models. Text is usually padded with spaces on one or both sides to make up a 16 character string. The variable name is pre-pended with the device number such as “1.1.display=\*\*\*\*DISARMED\*\*\*\*”. |
| FireEvent | Numeric value | Fire event count. A better option is to watch for the Fire trigger. |
| ID | ECP bus device ID between 16 - 23 | The keypad ID given to the Vista ICM. |
| Ready | 0 = Not ready  1 = Ready | Whether the unit is ready. |
| ZS | 0 = No fault  1 = First fault  2 = Additional fault | Zone state. The variable name is pre-pended with the device number and appended with the zone number, for example “1.1.ZS.4=1”. |

## Vista Security Triggers

|  |  |
| --- | --- |
| Trigger | Description |
| Alarm | The alarm has tripped. |
| Fire | Fire sensor tripped. |
| Low Battery | Low battery warning. |
| Power Failure | AC power lost. |
| Power Returned | AC power restored. |
| Disarmed | System disarmed. |
| Armed Stay | Armed in stay mode. |
| Armed Away | Armed in away mode. |