Horatio Quickstart Guide

Ben Peoples Industries
ben@benpeoples.com
412-254-4236

October 16, 2015

Contents

1 Introduction

Horatio consists of two components: the website and the Horatio Bridge Device (HBD). While the HBD handles data collection and actually interfacing with the physical lighting system, the bulk of the configuration actually happens on the website.

However, due to the many different network configurations available, the actual network configuration has to happen on the physical device.

2 Physical Installation

The HBD is a 1RU rack mount unit. We do not provide it with mounting screws, as different racks are different.

We do provide it with a 100-240VAC wall wart adapter. Do not plug it in until all other connections are made– there is no power switch, the HBD is on whenever there is power.

The rear connections include (2) ethernet ports, and (2) USB ports, one of which typically has a WiFi adapter in it. If you are installing in a facility that prohibits any WiFi, you should remove this.

3 Initial Configuration

You will need an HDMI capable display and a USB keyboard. Plug these into the front of the Horatio Bridge Device and power it up. If you have already powered it up, you do not need to power cycle, but you may be in an odd graphics mode. If the display receives signal but cannot display anything, you will need to power cycle the HBD by unplugging it and plugging it back in.

If you see a blank screen, press "enter" on the keyboard, and you should see a login prompt. Login with the username "config" and the password "config" (both without the quotes). If you have already configured the system, you may need to use a different password.

The system will walk you through a series of prompts. The only required tasks are to set up networking and test the connection to the VPN server to ensure that data is flowing from the HBD to the cloud.

3.1 Wireless

By default, the WiFi connection supports "WPA-Personal" encryption with a pre-shared key and SSID. If you use more complex methods of authentication, contact us for pre-configuration.

Most WiFi networks use DHCP, but if not you can assign a specific IP address.

The checkbox for "use as default gateway" should remain unchecked if this wireless network is not connected to the internet. Some systems will supply default gateway routing information for networks that do not route to the public

internet, leaving this checkbox off will actively suppress this connection as a route out.

3.2 Wired

The HBD comes standard with two ethernet interfaces, nominally called eth0 and eth1. Either can support DHCP

Please pay attention to which one you have connected to which network while you are configuring the system.

The checkbox for "use as default gateway" should remain unchecked if the network is not connected to the internet. Some systems will supply default gateway routing information for networks that do not route to the public internet, leaving this checkbox off will actively suppress this connection as a route out.

3.3 VPN Caveats

The VPN connection to our servers uses the Class B private network 172.25.26.0/24 by default. If any of your wired or wireless networks overlap with this (any address starting with 172.16.0.0 through 172.31.0.0 could indicate a potential overlap), contact us for available alternates.

The VPN connection is established to our server (vpn.horat.io / 104.197.144.231) on TCP port 443 from a random port on the HBD. This should traverse most sane firewall/NAT rules without configuration. We can configure the HBD to use a specific TCP port for VPN contact if you need strict routing rules, contact us for details.

4 GPS Antenna

The optional GPS module is used as an accurate time source for NTP. While the module we use does have an onboard antenna, the module requires an external antenna to be able to get GPS signals from within a rack.

We provide a SMA antenna connector on the rear of the HBD. Please note that there are two varieties of SMA: RP-SMA and SMA. The connector on the HBD is an SMA.

The antenna for the GPS must be an active antenna. A passive antenna will not be detected by the module. We can furnish a low-profile antenna with a 3m cable, or you can provide your own.

Cold-start on the GPS may take up to 15 minutes even with good signal. Do not be alarmed if the HBD takes a while to indicate that GPS is working.

5 Device Discovery

Once the networks are configured, we recommend running device discovery. This will push information about the found devices to the cloud server, but

more importantly if you are not discovering devices that you know are on the system this could indicate a problem with the network configuration.

RDM Device Discovery is configured from the web interface.

6 Alert Configuration

On the website, alert configuration is a two step process.

The first step is on the Monitoring Configuration page (under the Monitoring menu). This page lets you set the check interval for devices. Devices can be configured to be checked from once every 5 minutes to once every 60 minutes. Our testing has shown 15 minutes to be a reasonably sane value, but you may want to increase this for some devices.

Checking the "Alert" box on this page will enable alerts for that device.

The second page is the Alert Config page (also under the Monitoring menu). This page has two main sections. The top section allows you to configure settings for all alerts, by severity. The bottom section lets you configure the alert conditions and severity for each device.

As indicated on the page, alert notifications cascade. This means if you add your e-mail to "Warning" alerts, it will also send you alerts for Error, Critical, Alert, and Emergency severities. There are two additional checkboxes for each alert level: checking "Send 24/7" will send SMS messages 24/7, not just during daytime hours. "Require Confirm" will keep sending an alert until someone acknowledges it (either by responding to the SMS or clicking a link in the email).

6.1 Severity

Severity for an alert is ranked in 8 levels from "Debug" to "Emergency"— this list is the same as used by the syslog system, so it may look familiar. You can distribute the alerts and notifications in whatever way makes sense to you.

6.2 Alert Case

Alert Case allows you to specify what sort of failure is required to trigger an alert. Some devices are flaky, but not actually in a failed state every time a check fails, so alerting on the first failure would cause false alarms.

Additionally, for protocols that support a heartbeat function rather than active monitoring, we provide an Alert Case for no update in a certain amount of time.

We can configure custom alert cases for you if you have some strange case.