OneLINK Bridge AV Interface

Current Release

OneLINK Bridge 1.3.0
December 20, 2019
New Features

- If you restore factory defaults, the OneLINK device now requires an initial setup step to make the administrative controls and other functionality available. In this initial step, you must set the admin password. This is also required for initial access to OneLINK devices that ship with this version of firmware. See Initial Set-Up Procedure. After completing the initial setup, you have the option of enabling features that are now disabled by default. At this time, setting the admin password is the only task in the initial setup procedure.
- Preliminary support for far-end access to camera presets in certain soft conferencing clients.
- OneLINK Bridge factory default settings can now be restored by pressing and holding the Display IP Address button while rebooting the device.
- Added support for long press right-clicking on iOS devices.
- When static IP addressing is selected, the administrator can specify a DNS server.
- Echo cancellation can now be enabled and disabled via Telnet command:
  `audio { line_in_1 | line_in_2 } echo-cancel { get | on | off | toggle}`

Improvements

- Security improvements include changes to the default settings for:
  o HTTP access is disabled. To connect using HTTPS, type `https://` followed by the IP address. Because Vaddio uses self-signed certificates, your browser will present warning messages indicating that you are trying to access an unsafe website; however, this is a secure connection to the OneLINK device and traffic will be encrypted.
  o Telnet access is disabled.
- Disabled TLS v1.1 protocol. More recent protocols continue to be supported.
- The Telnet command `network settings get` now includes the OneLINK device's hostname in the information it returns.
- Telnet commands to set hostnames and other user-definable strings now accept hyphens.
- In the admin web interface, some settings have moved from the DIP Switches tab to other tabs of the System page.
- The default setting for UVC mode has been changed to Client Custom for better out-of-the-box compatibility with major soft conferencing clients. This does not change the OneLINK device's stored settings; however, if you need to restore factory defaults, you may need to change this setting afterward.
- Exporting data to an Android device now works properly.
- In some situations, UVC control did not perform as expected unless a network connection was available.
- In certain situations, the OneLINK device passed RS-232 communication at the rate it was received, rather than enforcing the baud rate set in the web interface.
- In some cases, the web interface did not load properly if the computer had recently accessed another Vaddio device at the same IP address. This has been fixed.
- Occasionally, the OneLINK Bridge could lose its HDBaseT connection to the camera if the camera remained in standby for extended periods. This has been fixed.
- Disconnecting the OneLINK cable from a camera and connecting it to a OneLINK EZIM without removing power to the OneLINK Bridge could result in flickering video in the USB stream and on the SDI output. This has been fixed.

Notes

- Cameras connected to OneLINK devices may also need a firmware update to continue to accept IP control.

Release History

OneLINK Bridge 1.2.0
November 9, 2018
New Features

- Added UVC control support for Vaddio native HDBT Cameras to enable far-end control when used with some 3rd Party soft codec clients like Zoom that support UVC standards.thing.

Improvements

- Added display of OneLINK connection status and far-end camera IP address for Vaddio native HDBT cameras to the web UI.
- Added USB stream active/inactive notifications to the web UI.
- Enabled DNS-SD device discovery, controllable as a toggle in the security page of the web UI.
- Enabled HDMI video feed between Cisco Precision 12x cameras and Cisco SX20 units running newer CE series firmware.
- Fix for USB playback audio sometimes halting when USB record streaming is stopped.

OneLINK Bridge v1.1.2
July 24, 2018
Improvements

- Miscellaneous internal code improvements.

OneLINK Bridge 1.1.1
June 28, 2018
New Features

- Security features include:
  - Added ability to disable the telnet server on the device.
  - Added ability to disable the HTTP server on the device. When this is disabled, HTTPS must be used to connect to the web UI.
  - Added ability to configure HTTPS certificates from the web UI.

Improvements

- Security improvements include:
  - Improved internal firewall settings.
  - Disabled TLS v1.0 protocol.
- Control/configuration updates include:
  - Added tooltips to the main navigation bar in the web UI when it's collapsed.
  - Added support via Telnet control commands to request current temperature readings from a connected OneLINK Bridge device.
  - Added ability to toggle auto mic mixer inputs in the web UI.
  - Improved readability for Telnet control error messages.
  - Updated system time zone data.
  - Enable import of configuration exported from previous versions of software.
  - Enable some user settings to persist across page refreshes in the web UI.
  - Removed "sleep" Telnet control command
  - Master mute state is now reflected in the per-channel mute states on the web and via Telnet control.
  - Interoperability improvements with Internet Explorer® 9 through IE11.
  - Various other minor updates

- Functional improvements and updates include:
  - Added support for Level B SDI audio and video.
  - Added support for passing video and audio from an HDCP-protected source via HDMI.
  - Improved handling of video input when external source changes feeds.
  - Improved several items relating to increased HDBaseT performance.
  - Interoperability improvement for USB streaming with Windows® 10
  - Various other minor updates

OneLINK Bridge 1.0.1
August 9, 2017

Notes

- Initial release.

Initial Set-Up Procedure

Recent security improvements to Vaddio products have changed the way you interact with this product when you set it up for the first time.

What's new

- The product now uses the more secure HTTPS protocol, rather than HTTP.
- You must set the admin password using the web interface. Until the admin password is set and any other initial tasks are completed, the control and administrative interfaces are not available.
- You will not be able to open a Telnet session to this product until you set the password using the web interface.
- You will need to set the admin password again if you restore factory defaults.

Refer to the product's manual for specific instructions to discover its IP address and access its web interface.

Connect using HTTPS

Before the product is configured, HTTP access is disabled. To access the web interface, type `https://` followed by the IP address. Otherwise, you may encounter this message:
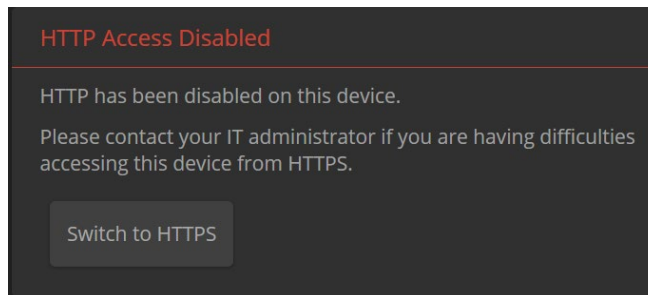
Switch to HTTPS if you see this message.

Expect a security warning from your browser

Different browsers will respond with different messages and options. Your browser will probably present a message indicating one of these things:

- The connection is not private
- The site is not secure
- The site is not trusted
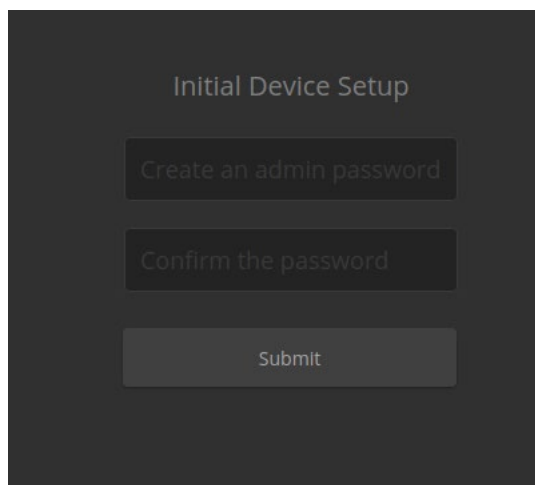- The site poses a security threat

This is because the certificate (the product's website security credential) is self-signed rather than being issued by an external certificate authority.

To proceed to the product's web interface, you will need to make the selections that your browser's security message discourages. The security warning page may present an option to learn more, view details, or go to the "Advanced" page. When you select the applicable option, your browser provides a button or link to continue to the IP address you entered, with a reminder that it may be unsafe. Select this option.

After you have accessed the product's web interface once, your browser remembers its IP address and will not present the security message again.

Device set-up

The first time the product's web interface is accessed, it presents a landing page for initial set-up tasks. You will also encounter this page after restoring factory defaults. After you complete the initial set-up, you will be able to work with the product.

Create and confirm the admin password, and complete any other required tasks such as accepting agreements. Then select Submit. The main administrative web interface opens.

In the administrative web interface, you can configure product security features to conform to the IT policies for your environment. Except where otherwise noted, these settings are on the Security page.

- Choose whether to expire idle sessions – By default, the web interface automatically logs you out after 30 minutes of inactivity.
- Enable HTTP access – Enable connections to the product's web interface using the less-secure HTTP protocol.
- Enable Telnet access – This is disabled by default.
- Enable USB streaming – USB streaming is disabled by default. You can enable it on the Streaming page.

# Firmware Update Instructions – OneLINK Bridge

Requirements

- Network access to the OneLINK Bridge.
- The web interface's admin password.
- The .p7m firmware file for the OneLINK Bridge – download this from https://www.legrandav.com/. It is available on the product page's Resources tab.
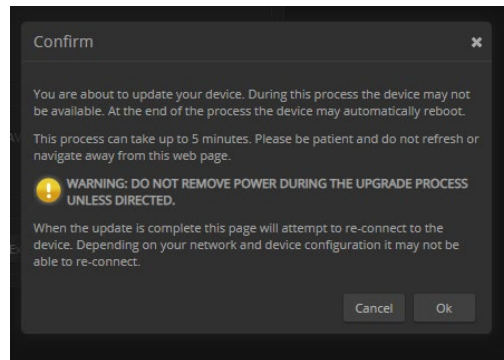
Step-By-Step Process

1. Enter the IP address for the OneLINK Bridge into the address bar of a web browser.
   You can obtain the IP address by pressing the Display IP Address button. The connected display shows the OneLINK device's IP address.
2. Log in as admin.
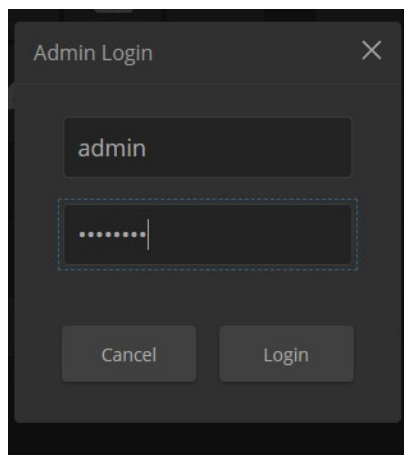
3. Navigate to the System page. Your OneLINK Bridge may present different information than shown in the screen shot.
4. Select Choose File, then browse to the downloaded firmware and select it. The filename ends with .p7m.
5. Select Begin Firmware Update.
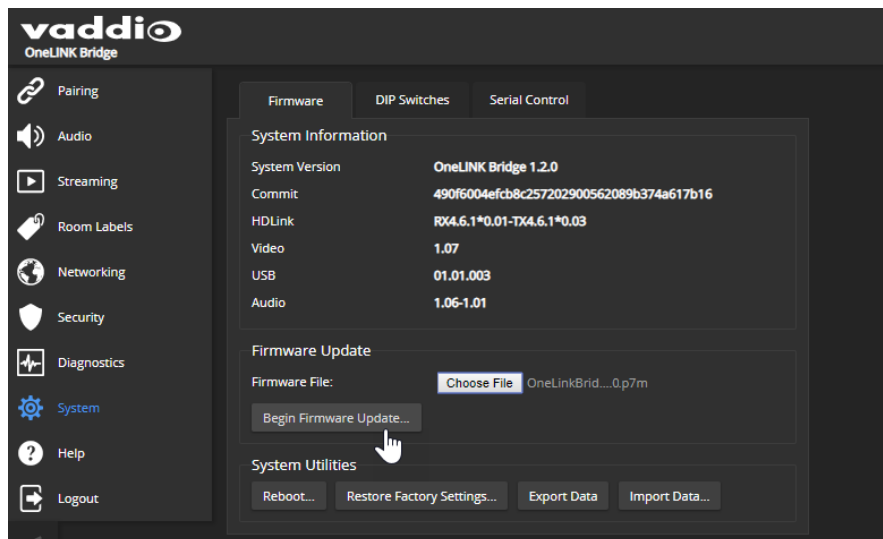
6. Read and understand the information in the Confirm dialog box. It's dull, but it could save you some time and aggravation.

Confirm

You are about to update your device. During this process the device may not be available. At the end of the process the device may automatically reboot.

This process can take up to 5 minutes. Please be patient and do not refresh or navigate away from this web page.

⚠ WARNING: DO NOT REMOVE POWER DURING THE UPGRADE PROCESS UNLESS DIRECTED.

When the update is complete this page will attempt to re-connect to the device. Depending on your network and device configuration it may not be able to re-connect.

Cancel   Ok

7. Select Continue. A progress message box opens. If the update process presents warnings or error messages, read them carefully.
8. The device reboots when the update is complete.

Caution
The OneLINK device must remain connected to power and to the network during the update. Interrupting the update could make the OneLINK device unusable.

This update can take up to 5 minutes to complete; the pop-up message window will identify the progress of the update.

While you're waiting, you could try the following:

- How many anagrams of "OneLINK Bridge" can you make?
- Ponder why children ask for puppies but not armadillos.
- Calculate how many tennis balls it would take to fill a city bus.

After the update is complete, the System page will display the new firmware version under System Information. Enjoy that 'New Firmware Smell'!

If the update procedure is interrupted for any reason the product may need to be returned to Vaddio for updating. If the update does not seem to run, DO NOT TURN OFF THE PRODUCT OR UNPLUG IT. CALL TECH SUPPORT IMMEDIATELY.

If you have any questions, call Vaddio Technical Support: (+1) 763-971-4428 or 1-800-572-2011