

# OneLINK HDMI Camera Extension

---

## Current Release

### OneLINK HDMI 1.2.0

December 16, 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.
- Added support for long press right-clicking on iOS devices.
- Vaddio cameras that support DNS Service Discovery can now be discovered from the web interface.
- When static IP addressing is selected, the administrator can specify a DNS server.
- If a Vaddio HDBaseT camera is connected directly to the OneLINK device, the new Pairing page in the web interface displays information about the camera and provides a link to its web interface.

#### Improvements

- Security improvements include changes to the default settings for:
  - 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.
  - 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 camera's hostname in the information it returns.
- Telnet commands to set hostnames and other user-definable strings now accept hyphens.
- On receiving a reboot instruction, the OneLINK device now performs a check to ensure your most recent configuration changes were successfully saved.
- Exporting data to an Android device now works properly.
- 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.
- Improved HDBaseT link negotiation behavior with Vaddio HDBaseT cameras.

## Release History

### OneLINK HDMI 1.1.0

June 26, 2018

#### Improvements

- Various security updates:
  - 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.
  - Improved internal firewall settings.
  - Disabled TLS v1.0 protocol.
- Fix for hostname changes not being properly handled for DHCP.
- Allow import of configuration exported from previous versions of software.
- Updated web UI look and feel.
- Updated system time zone data.
- Interoperability improvements with Internet Explorer 9 through IE11.
- Fix for web UI not rendering in Chrome when fonts.googleapis.com was unreachable.
- Improved several items relating to increased HDBaseT performance.
- Various other minor updates.

### OneLINK HDMI 1.0.1

June 6, 2016

#### Improvements

- Update to work with RoboSHOT 20 UHD camera.
- Update to enable configuration data to be exported and imported when importing to the same firmware version as the exported file.

### OneLINK HDMI 1.0.0

March 31, 2016

#### 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.

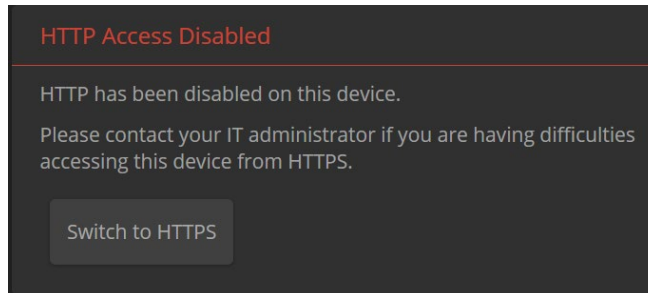
### What's new

- 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

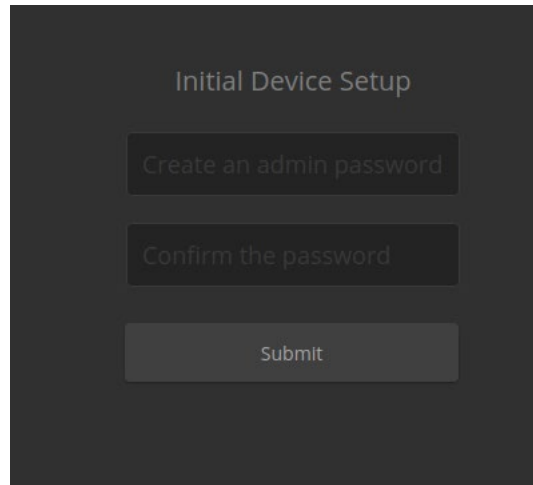
This is because the certificate (the product's website security credential) is self-signed rather than being issued by an external certificate authority.

*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.



The image shows a dark-themed web interface for 'Initial Device Setup'. It contains three input fields stacked vertically: 'Create an admin password', 'Confirm the password', and a 'Submit' button.

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.

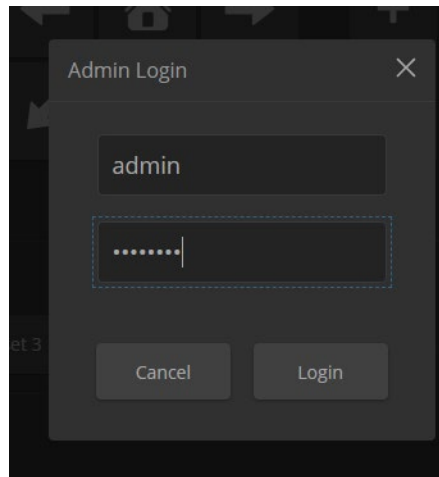
## Firmware Update Instructions – OneLINK HDMI

### Requirements

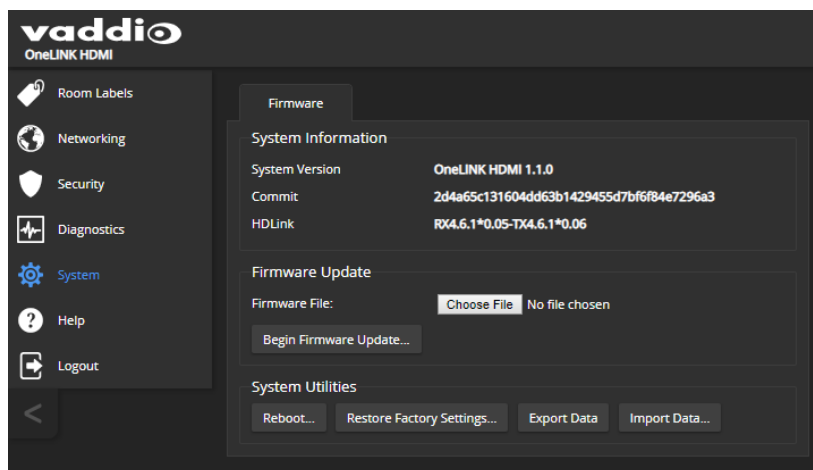
- Network access to the OneLINK device.
- The web interface's admin password.
- The .p7m firmware file for the OneLINK device – download this from <https://www.legrandav.com/>. It is available on the product page's Resources tab.

### Step-By-Step Process

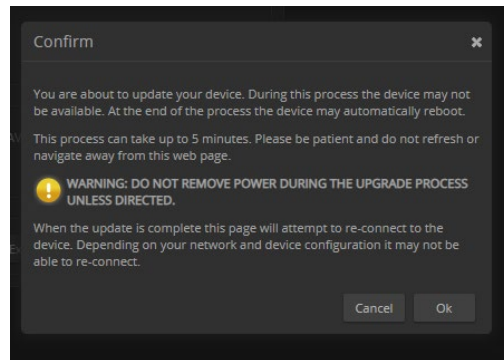
1. Enter the IP address for the OneLINK device into the address bar of a web browser. The front panel display shows the OneLINK device's IP address.
2. Log in as admin.



3. Navigate to the System page. Your OneLINK device's System page 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.



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 device must remain connected to power and to the network during the update. Interrupting the update could make the camera 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:

- Consider the lilies of the field.
- Consider a spherical cow.
- Consider the relative benefits of pens and pencils.

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**

Vaddio is a brand of Legrand AV Inc. · [www.legrandav.com](http://www.legrandav.com) · Phone 800.572.2011 / +1.763.971.4400 · Fax +1.763.971.4464  
Email – Europe, Middle East, Africa: [av.emea.vaddio.support@legrand.com](mailto:av.emea.vaddio.support@legrand.com) | All other regions: [av.vaddio.support@legrand.com](mailto:av.vaddio.support@legrand.com)

Visit us at [www.legrandav.com](http://www.legrandav.com) for firmware updates, specifications, drawings, manuals, and technical support information, and more.

Vaddio is a registered trademark of Legrand AV Inc. All other brand names or marks are used for identification purposes and are trademarks of their respective owners. All patents are protected under existing designations. Other patents pending.

©2019 Legrand AV Inc.  
A brand of  **legrand**