

HuddleSHOT All-In-One Conferencing Camera

Current Release

HuddleSHOT 1.1.2

January 13, 2020

Improvements

- In some cases, speaker audio from HuddleSHOT cameras could become distorted. This has been fixed.
- In some cases, firmware updates for HuddleSHOT cameras could fail. This has been fixed.

HuddleSHOT 1.1.0

December 23, 2019

New Features

- If you restore factory defaults, the camera 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 cameras 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.
- When static IP addressing is selected, the administrator can specify a DNS server.
- The camera can now stream video to a PCC Premier camera controller.
- UVC color controls are now available.

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.
 - IP streaming is disabled.
 - Telnet access is disabled.
- The Telnet command `network settings get` now includes the camera's hostname in the information it returns.
- The Telnet command `camera ccu get` now returns all camera ccu settings if no parameter is specified.
- Telnet commands to set hostnames and other user-definable strings now accept hyphens.
- Telnet commands now recognize the appropriate ranges of values for various camera settings, such as iris.
- Improved IP streaming performance.
- Improved zoom performance.
- Improved help text for some Telnet commands.
- When connected to a Mac, USB playback audio could become distorted over time. This has been fixed.
- Exporting data to an Android device now works properly.

Release History

HuddleSHOT 1.0.0

August 15, 2019

Notes

- Initial release.
- Speaker left and right channels are currently labeled from the unit's perspective, not the user's perspective.
- Video artifacts can appear in the USB and IP streaming outputs when the system is in full dewarp at 1x zoom, the IP streaming settings are above 720p and/or 15fps, and the IP stream is being actively consumed.
- Sound Bar Mode currently delivers a mixed left/right signal out of the left channel.
- When connected to a Mac, USB playback audio may become distorted over time.

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.

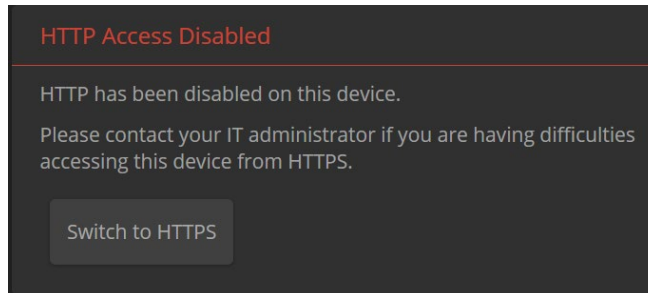
What's new

- 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

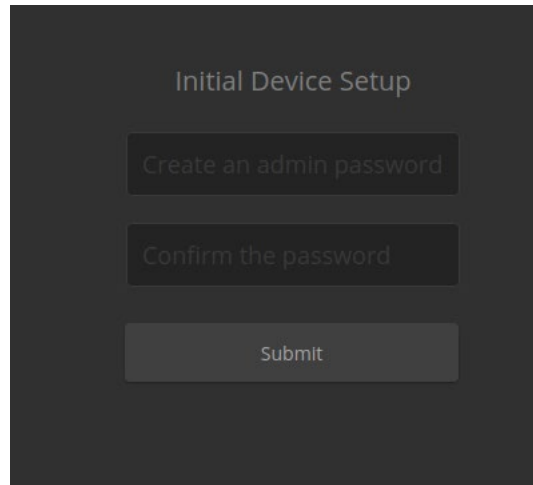
This is because the certificate (the product's website security credential) is self-signed rather than being issued by an external certificate authority.

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: '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.

- Create a user password – Allow password-protected, non-administrative access to the operator's web interface.
- Enable guest access – Allow non-administrative access to the operator's web interface without requiring a login.
- 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 IP streaming – This is disabled by default. You can enable it on the Streaming page.

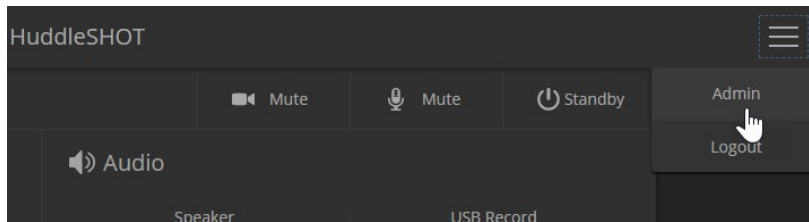
Firmware Update Instructions – HuddleSHOT

Requirements

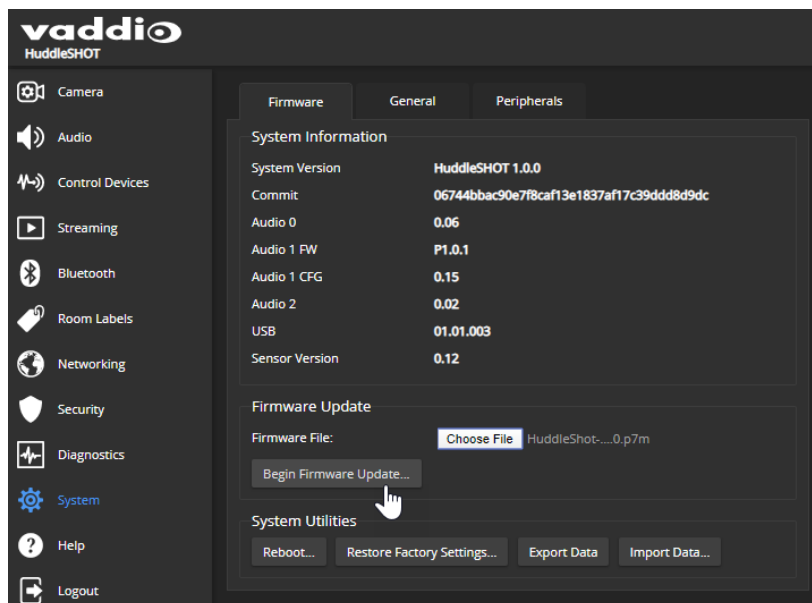
- Network access to the camera.
- The web interface's admin password.
- The .p7m firmware file for the camera – download this from <https://www.legrandav.com/>. It is available on the product page's Resources tab.

Step-By-Step Process

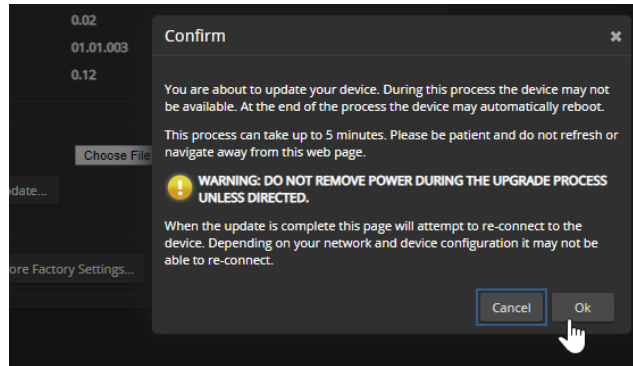
1. Enter the IP address or hostname for the camera into the address bar of a web browser.
2. Log in as admin.



3. Navigate to the System page. Your camera'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 OK. A progress message box opens and the indicator light on the front of the camera turns yellow/green. If the update process presents warnings or error messages, read them carefully.
8. The camera reboots when the update is complete.

Caution

The camera 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:

- Ponder the fact that most of the world's water is south of the equator.
- Think back: When you were eight years old, what did you consider to be the coolest technological innovation of all time? Has that opinion withstood the test of time?
- Think of ways to look legitimately busy while avoiding work. (Our technical expert Scott refers to all such activities as "changing the oil in the lawn mower.")

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 · Phone 800.572.2011 / +1.763.971.4400 · Fax +1.763.971.4464
Email – Europe, Middle East, Africa: av.emea.vaddio.support@legrand.com | All other regions: av.vaddio.support@legrand.com

Visit us at 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**