CyberData
The IP Endpoint Company

SIP Outdoor Video Intercom with RFID Operations Guide

Part #*011478*

Document Part #*931667A*
for Firmware Version *1.0.0*

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

SIP Outdoor Video Intercom with RFID Operations Guide 931667A
Part # 011478

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

CyberData
The IP Endpoint Company

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
http://support.cyberdata.net/

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

Revision Information

Revision 931667A, which corresponds to firmware version 1.0.0, was released on December 21, 2018.

Browsers Supported

The following browsers have been tested against firmware version 1.0.0:

- Internet Explorer (version: 11)
- Firefox (also called Mozilla Firefox) (version: 62.0)
- Chrome (version: 63.0.3239.132)
- Safari (version: 12)
- Microsoft Edge (version: 42.17134.1.0)

Pictorial Alert Icons

⚠ GENERAL ALERT	**General Alert** This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.
⏚	**Ground** This pictoral alert indicates the Earth grounding connection point.

Hazard Levels

Danger: Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

Warning: Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution: Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

Notice: Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

Important Safety Instructions

1. Read these instructions.

2. Keep these instructions.

3. Heed all warnings.

4. Follow all instructions.

5. Do not use this apparatus near water.

6. Clean only with dry cloth.

7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.

8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.

9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.

10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.

11. Only use attachments/accessories specified by the manufacturer.

12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

13. Prior to installation, consult local building and electrical code requirements.

14. **WARNING: The Intercom enclosure is not rated for any AC voltages!**

⚠ GENERAL ALERT	Warning *Electrical Hazard:* This product should be installed by a licensed electrician according to all local electrical and building codes.

⚠ GENERAL ALERT	Warning *Electrical Hazard:* To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

⚠ GENERAL ALERT	Warning The PoE connector is intended for intra-building connections only and does not route to the outside plant.

Contents

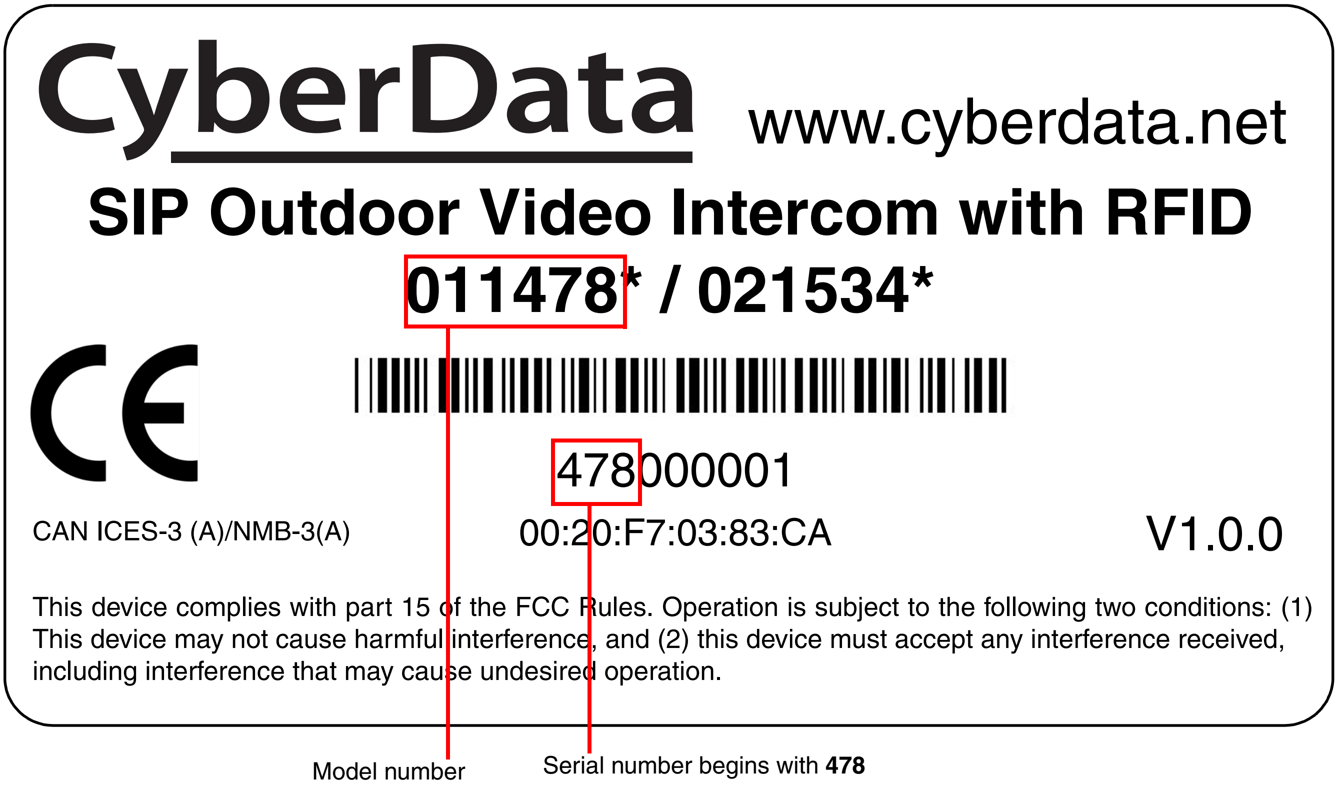
1 Product Overview

1.1 How to Identify This Product

To identify the SIP Outdoor Video Intercom with RFID, look for a model number label similar to the one shown in
Figure 1-1. Confirm the following:

- The model number on the label should be **011478**.
- The serial number on the label should begin with **478**.

Figure 1-1. Model Number Label



CyberData www.cyberdata.net

SIP Outdoor Video Intercom with RFID

011478* / 021534*

478000001

CAN ICES-3 (A)/NMB-3(A)

00:20:F7:03:83:CA

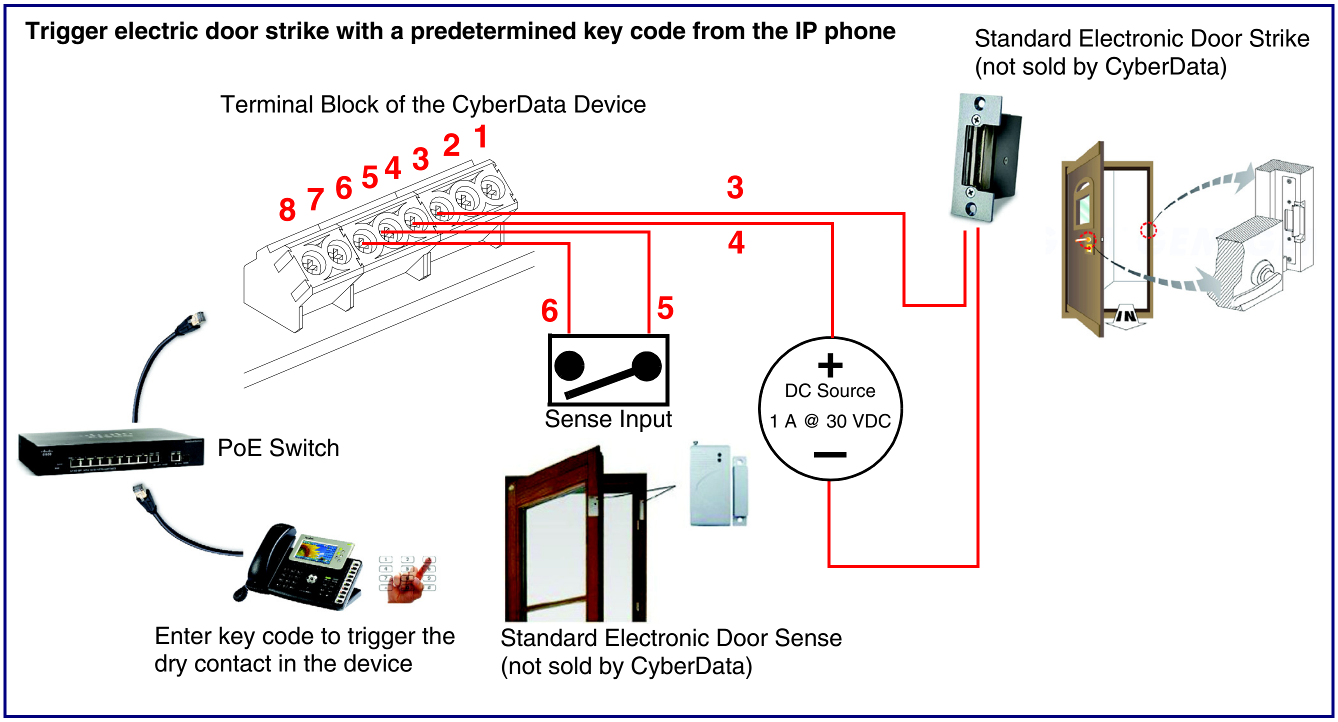
V1.0.0

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

1.2 Typical System Installation

The following figures illustrate how the SIP Outdoor Video Intercom with RFID can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation


Trigger electric door strike with a predetermined key code from the IP phone
Terminal Block of the CyberData Device
8 7 6 5 4 3 2 1
3
4
6
5
Standard Electronic Door Strike
(not sold by CyberData)
+
DC Source
1 A @ 30 VDC
–
Sense Input
PoE Switch
Enter key code to trigger the
dry contact in the device
Standard Electronic Door Sense
(not sold by CyberData)

1.3 Product Features

The SIP Outdoor Video Intercom with RFID has the following features:

- Mifare Plus X 2K/4K cards are supported for a high level of encryption
- Alert buzzer
- Red/Green lock status lights
- Built in time of access scheduler
- Local and remote logging with time stamp
- NTP time support
- Supports 500 Access Cards
- Blacklisted code alert via dialout and multicast stored messages
- Device ships with packet of 5 RFID cards
- PoE 802.3af enabled (Powered-over-Ethernet)
- SIP compliant
- Adjustable camera angle
- Full-duplex voice operation
- Supports SRST in a Cisco environment
- Network web management
- Network adjustable speaker volume and microphone sensitivity
- Network downloadable firmware
- Doubles as a paging speaker
- Downloadable alert, ringtones and callout messages
- Dry relay contact for auxiliary control
- Door closure and tamper alert signal
- Optional Weather Shroud for even greater weather protection
- IP65 rated enclosure
- Security Torx screws with driver kit

1.4 Supported Protocols

The Intercom supports the following protocols:

- SIP (session initiation protocol)
- HTTP Web-based configuration

  Provides an intuitive user interface for easy system configuration and verification of Intercom operations.
- DHCP Client

  Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client

  Facilitates hosting for the Autoprovisioning configuration file.
- RTP
- RTP/AVP - Audio Video Profile
- TLS 1.2
- Facilitates autoprovisioning configuration values on boot
- Audio Encodings

  PCMU (G.711 mu-law)

  PCMA (G.711 A-law)

  G.722

  G.729

1.5 Supported SIP Servers

The following link contains information on how to configure the device for the supported SIP servers:

https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers

1.6 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
RFID Card Protocol	ISO/IEC 14443 Type A - 13.56 MHz Standard
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply (not included)[a]
Speaker Output	2 Watts Peak Power
On-Board Relay	1A @ 30 VDC
Supported RFID cards	Mifare Plus X 2K or 4K
Enrollment Encryption Level	Encrypted to AES 128
Payload Types	G.711 a-law, G.711 µ-law, G.722, and G.729
Video Codec	H.264 Baseline
Camera Resolution	320 x 240
SIP Video Payload	Baseline profile @ 320x240
Video Lens Angle	72 degrees
Network Security	TLS/SSL 1.2
IP Rating	IP65
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
IP Rating	IP65
Dimensions[b]	7.480 inch [190 mm] Length 2.284 inch [58 mm] Width 5.118 inch [130 mm] Height
Weight	2.8 lbs. [1.27 kg]
Boxed Weight	4.0 lbs. [1.81 kg]
Compliance	CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant
Warranty	2 Years Limited
Part Number	011478

[a] Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

[b] Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

1.7 Compliance

1.7.1 CE Testing

CE testing has been performed according to EN ISO/IEC 17050 for Emissions, Immunity, and Safety. The Declaration of Conformity can be supplied upon request.

1.7.2 FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

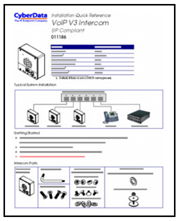
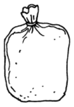
2 Installing the SIP Outdoor Video Intercom with RFID

2.1 Parts List

Table 2-1 illustrates the SIP Outdoor Video Intercom with RFID parts.

Note See Appendix A, "Mounting the SIP Outdoor Video Intercom with RFID" for physical mounting information.

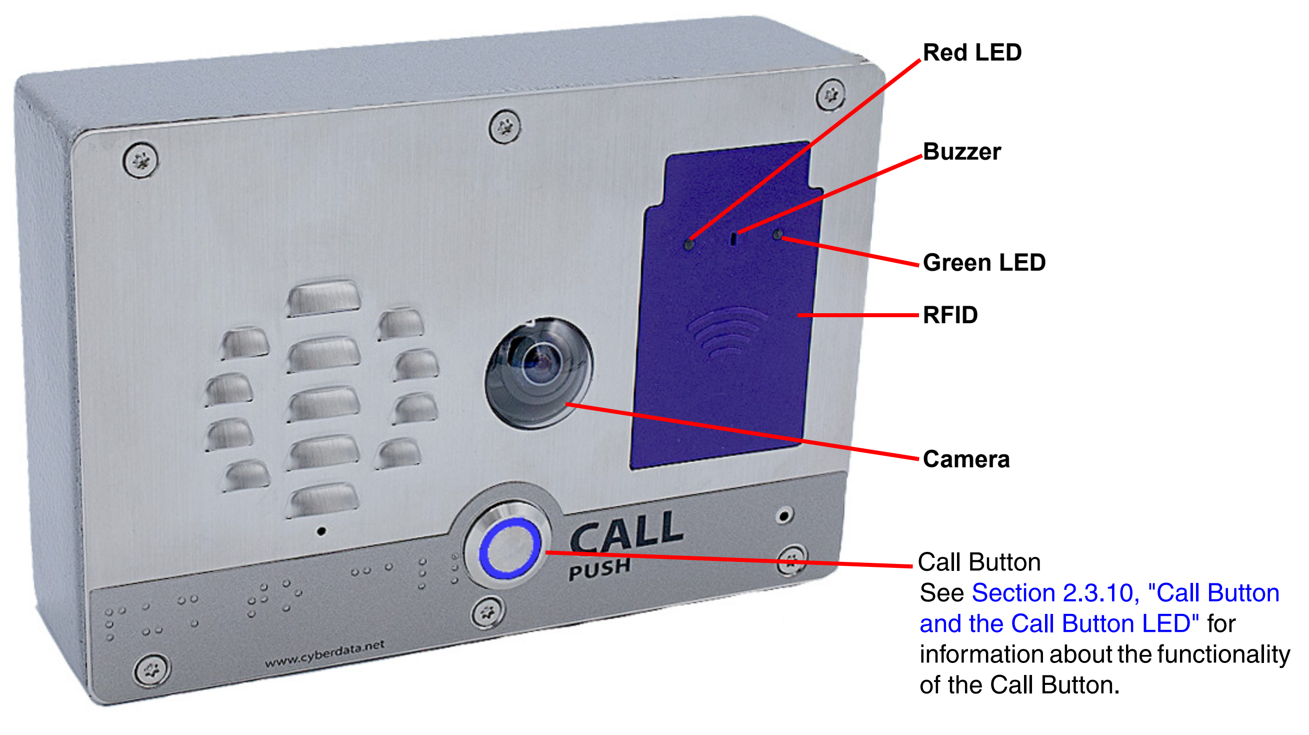
Table 2-1. Parts List

Quantity	Part Name	Illustration
1	Intercom Assembly	
1	Installation Quick Reference Guide	CyberData The IP Endpoint Company Installation Quick Reference VoIP V3 Intercom SIP Compliant 011186 a. Default if there is not a DHCP server present. Typical System Installation Getting Started Intercom Parts
1	Intercom Mounting Accessory Kit	

2.2 Components

Figure 2-1 shows the components of the device.

Figure 2-1. Components



See Section 2.3.10, "Call Button and the Call Button LED" for information about the functionality of the Call Button.

2.3 Intercom Setup

2.3.1 Mechanical Adjustment

The SIP Outdoor Video Intercom with RFID has a mechanical adjustment that ships in the default position of 0 degrees horizontal (Figure 2-2), but it allows you to tilt it 15 degrees down or 15 degrees up as shown in Figure 2-3 and Figure 2-4.

Figure 2-2. Mechanical Adjustment at 0 degrees horizontal

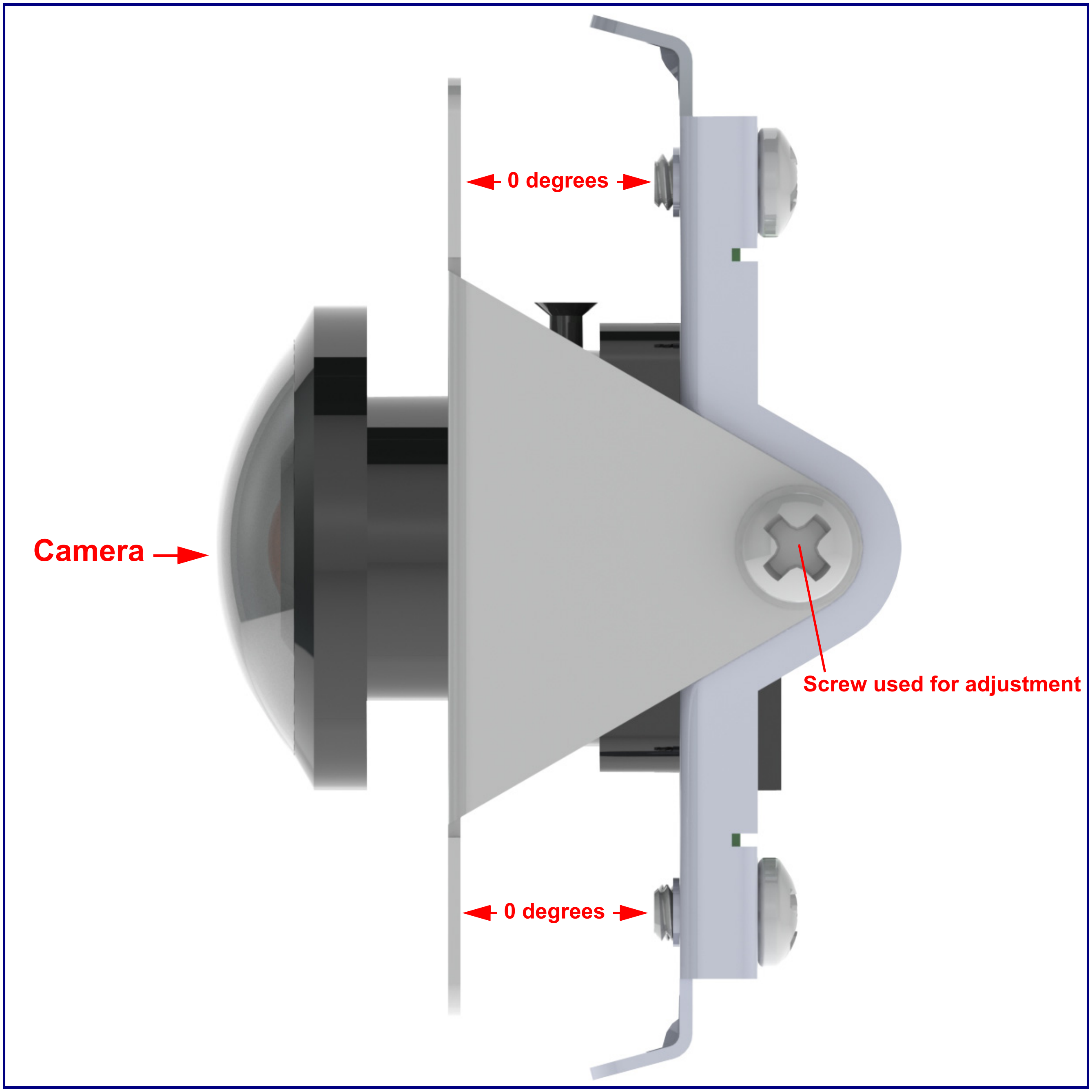


Figure 2-3. Mechanical Adjustment at +15 Degree Angle to - 15 Degree Angle

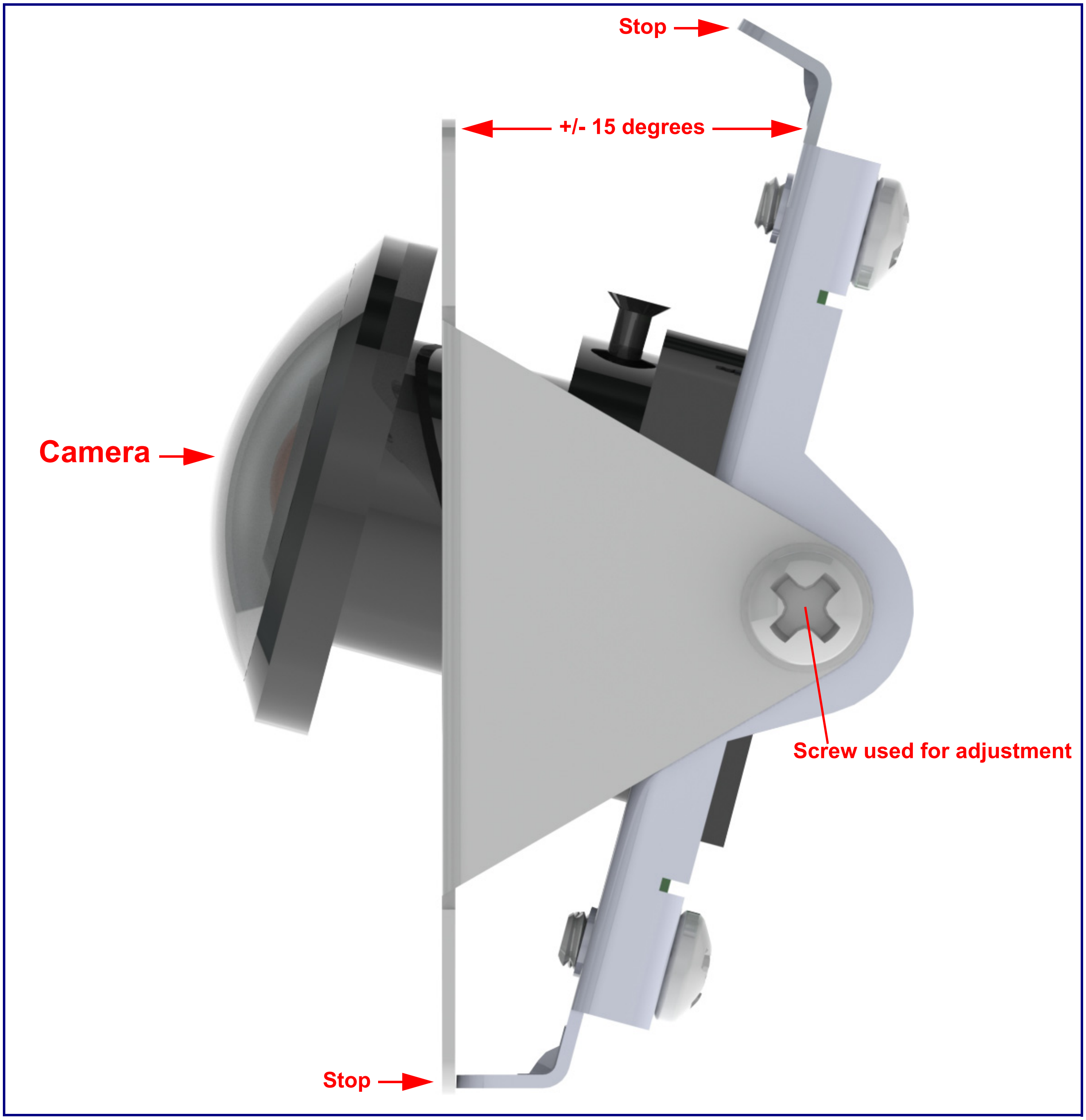
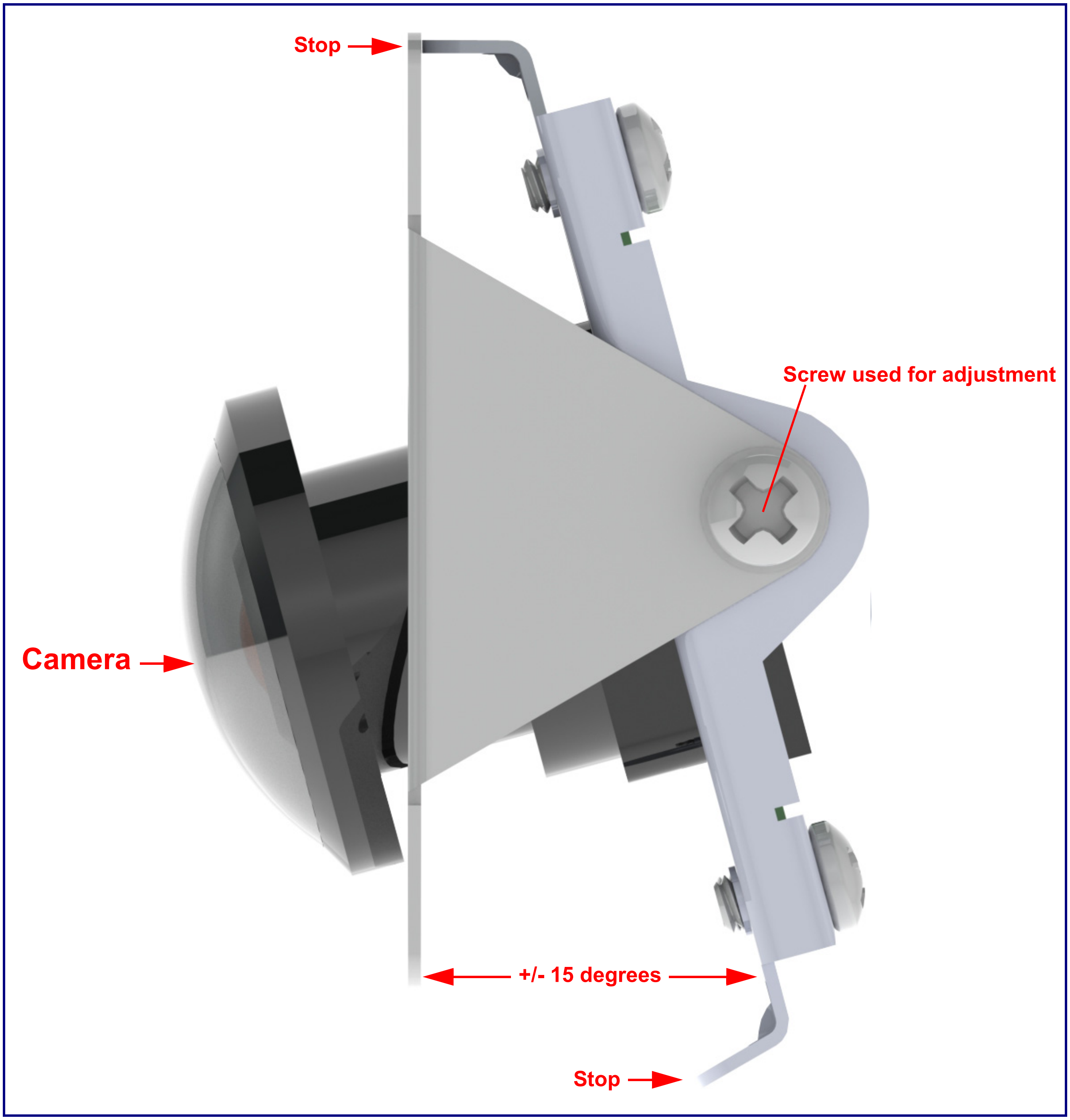


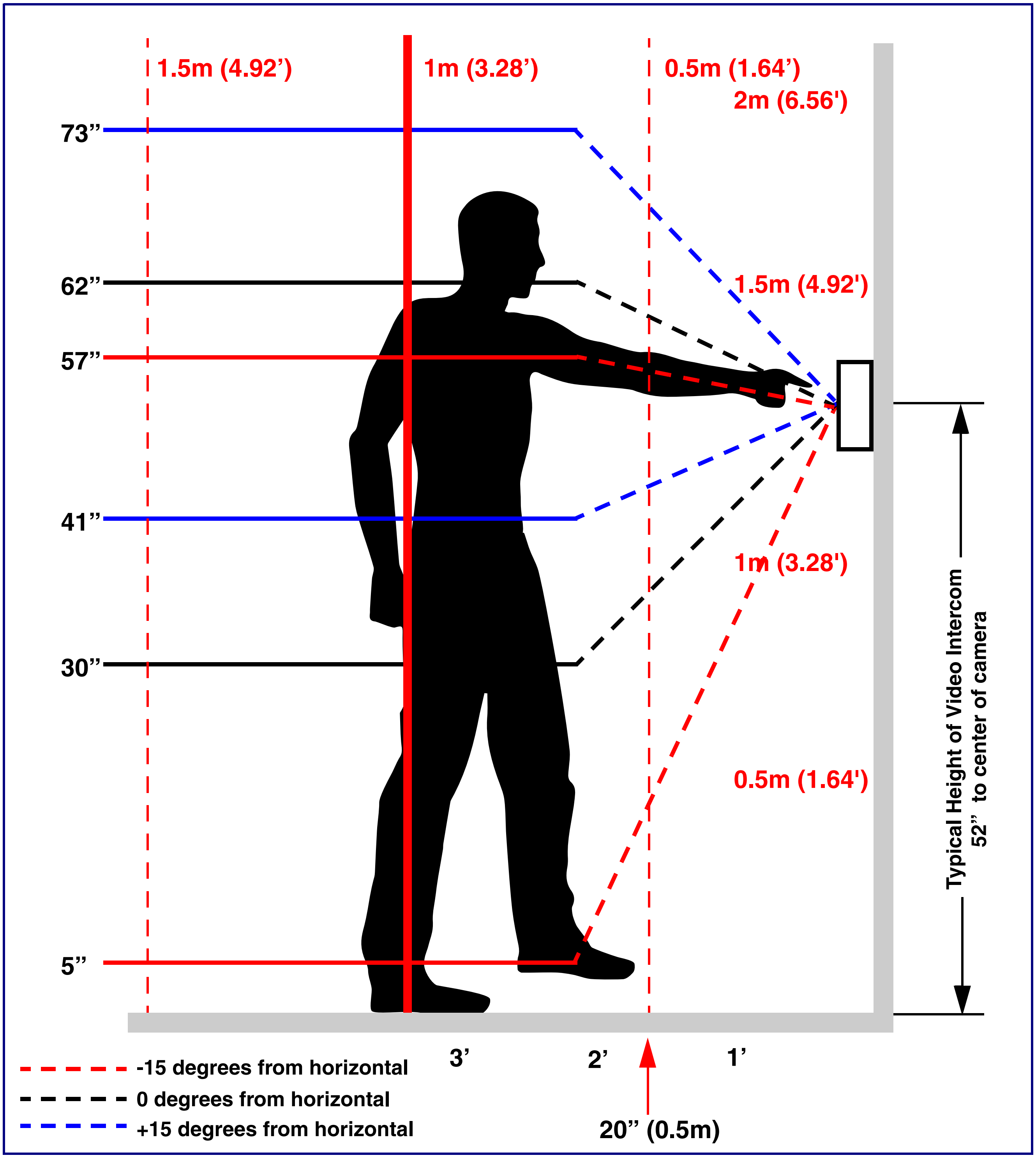
Figure 2-4. Mechanical Adjustment at +15 Degree Angle to - 15 Degree Angle



2.3.2 Field of View

Figure 2-5 shows the field of view of the SIP Outdoor Video Intercom with RFID when it is mounted at the recommended 48 to 52 inches above the ground.

Figure 2-5. Field of View



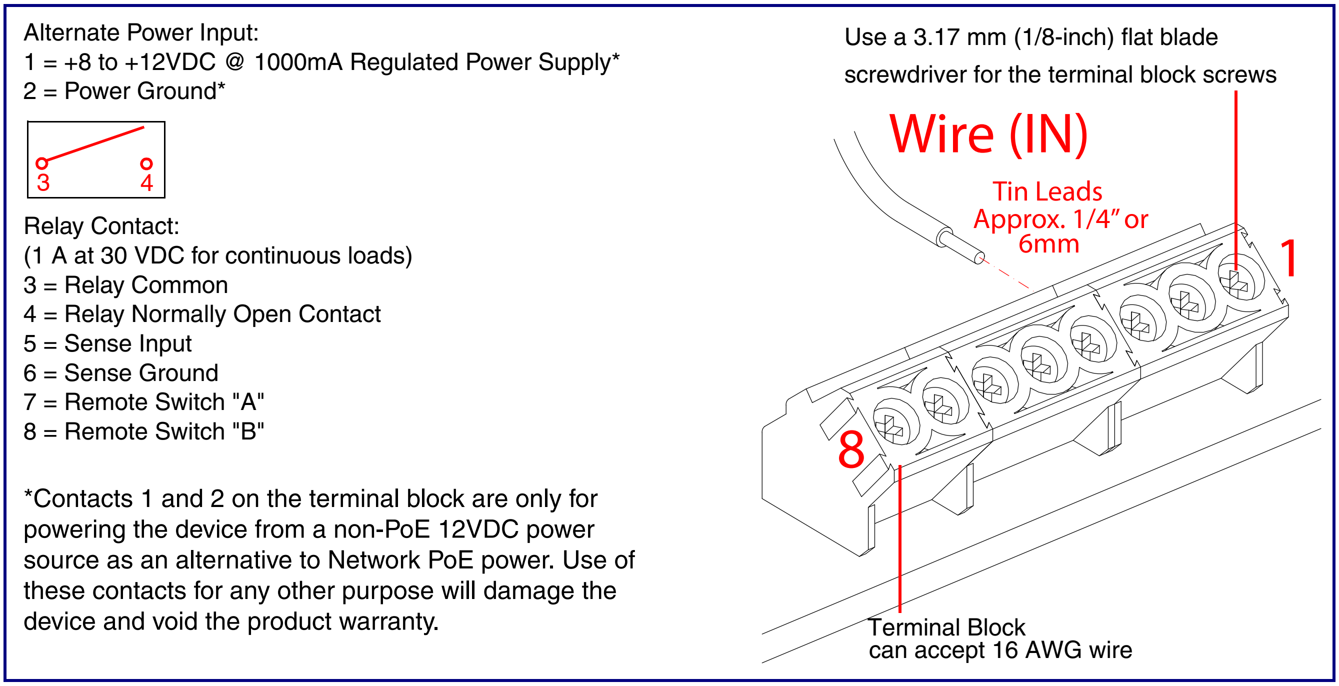
2.3.3 Intercom Connections

Figure 2-6 shows the pin connections on the terminal block. This terminal block can accept 16 AWG gauge wire.

Note As an alternative to using PoE power, you can supply +8 to +12VDC @ 1000mA Regulated Power Supply into the terminal block.

> ⚠ GENERAL ALERT
>
> **Caution**
>
> *Equipment Hazard*: Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

Figure 2-6. Connections and Alternate Power Input



Alternate Power Input:
1 = +8 to +12VDC @ 1000mA Regulated Power Supply*
2 = Power Ground*

Relay Contact:
(1 A at 30 VDC for continuous loads)
3 = Relay Common
4 = Relay Normally Open Contact
5 = Sense Input
6 = Sense Ground
7 = Remote Switch "A"
8 = Remote Switch "B"

*Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

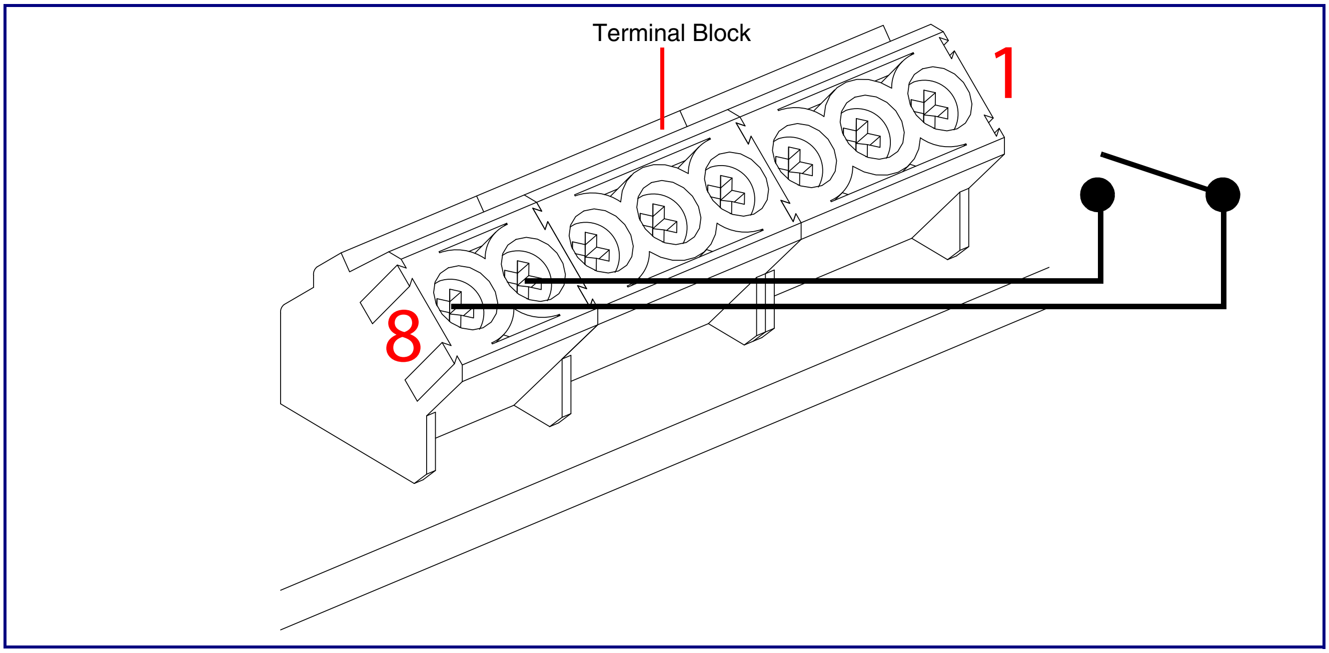
Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws

Terminal Block
can accept 16 AWG wire

2.3.3.1 Remote Switch Connection

Wiring pins 7 and 8 of the terminal block to a switch will initiate a SIP call when the switch is closed. The call will go to the extension specified as the dial out extension on the **SIP** page.

Figure 2-7. Remote Switch Connection



2.3.4 Using the On-Board Relay

⚠ GENERAL ALERT

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

⚠ GENERAL ALERT

Warning

Electrical Hazard: The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

⚠ GENERAL ALERT

Warning

Electrical Hazard: The relay does not support AC powered door strikes.

Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.

The device has a built-in relay that can be activated by a web configurable DTMF string that can be received from a VoIP phone supporting out of band (RFC2833) DTMF as well as a number of other triggering events. See the **Device Configuration Page** on the web interface for relay settings.

This relay can be used to trigger low current devices like LED strobes and security camera input signals as long as the load is not an inductive type and the relay is limited to a maximum of 1 Amp @ 30 VDC. Inductive loads can cause excessive “hum” and can interfere with or damage the unit’s electronics.

We highly recommend that inductive load and high current devices use our Networked Dual Door Strike Relay (CD# 011375) (see Section 2.3.5.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source").

This relay interface also has a general purpose input port that can be used to monitor an external switch and generate an event.

For more information on the sensor options, see the **Sensor Configuration Page** on the web interface.

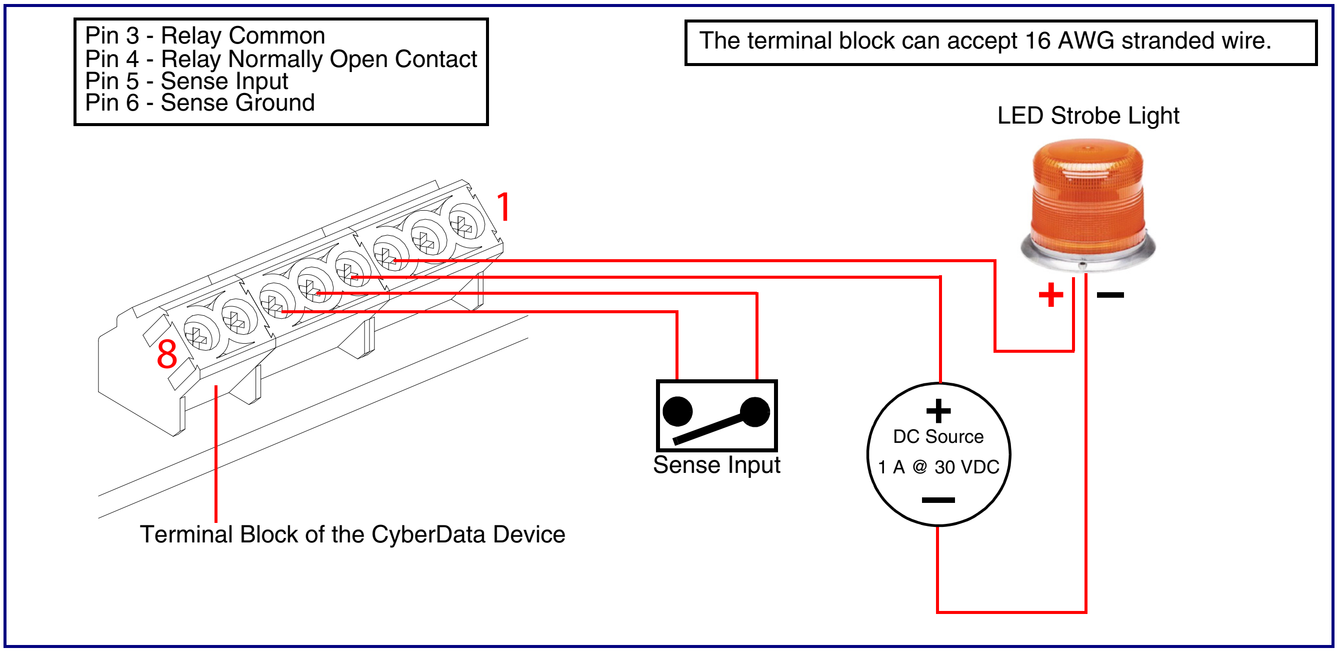
2.3.5 Wiring the Circuit

2.3.5.1 Devices Less than 1A at 30 VDC

If the power for the device is less than 1A at 30 VDC and is not an inductive load, then see Figure 2-8 for the wiring diagram.

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the Network Dual Door Strike Relay (CD# 011375) (see Section 2.3.5.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source").

Figure 2-8. Devices Less than 1A at 30 VDC


Pin 3 - Relay Common
Pin 4 - Relay Normally Open Contact
Pin 5 - Sense Input
Pin 6 - Sense Ground
The terminal block can accept 16 AWG stranded wire.
LED Strobe Light
1
8
+
–
Sense Input
+
DC Source
1 A @ 30 VDC
–
Terminal Block of the CyberData Device

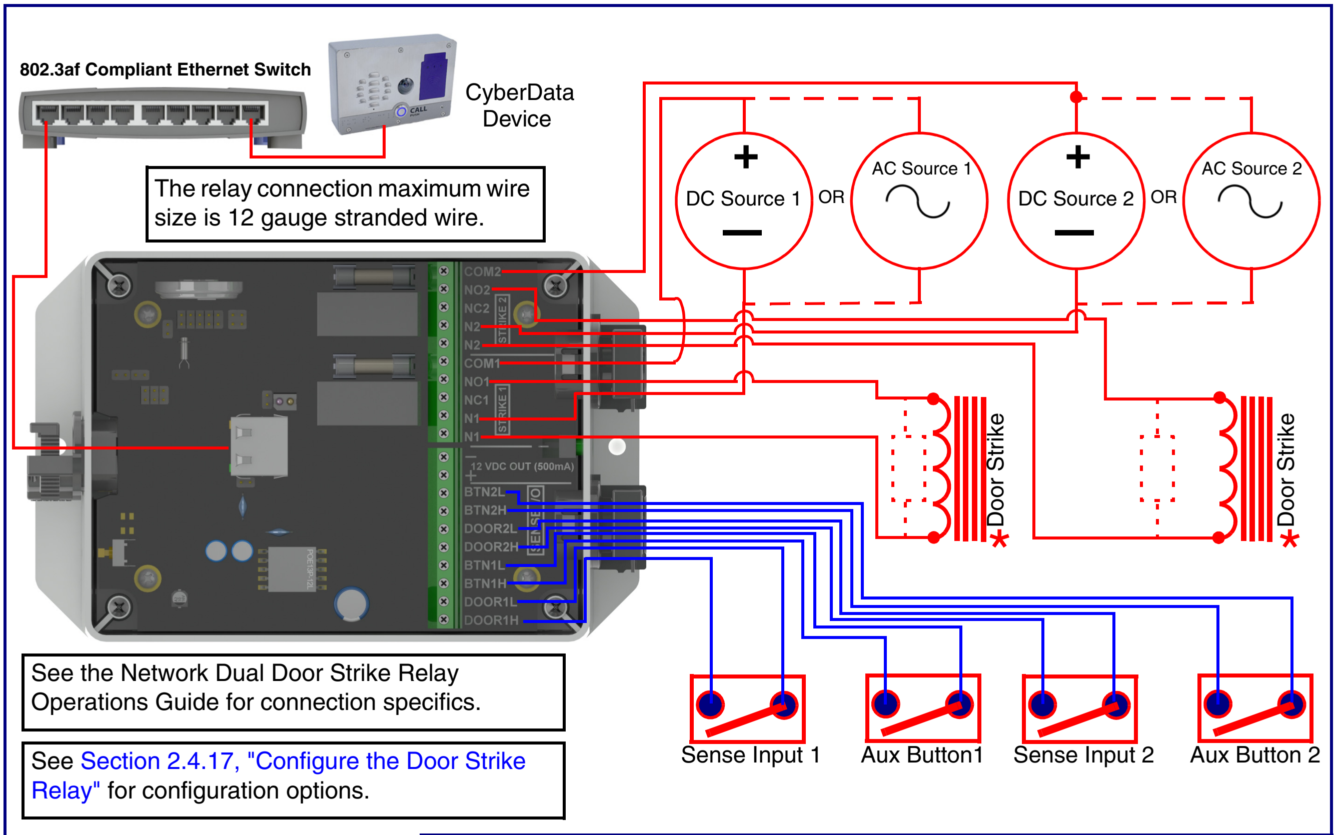
2.3.5.2 Network Dual Door Strike Relay Wiring Diagram with External Power Source

For wiring an electronic door strike to work over a network, we recommend the use of our external Network Dual Door Strike Relay (CD# 011375).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 2-9 and Figure 2-10 for the wiring diagrams.

GENERAL ALERT	**Warning** *Electrical Hazard:* Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

Figure 2-9. Network Dual Door Strike Relay Wiring Diagram with External Power Source



The relay connection maximum wire size is 12 gauge stranded wire.

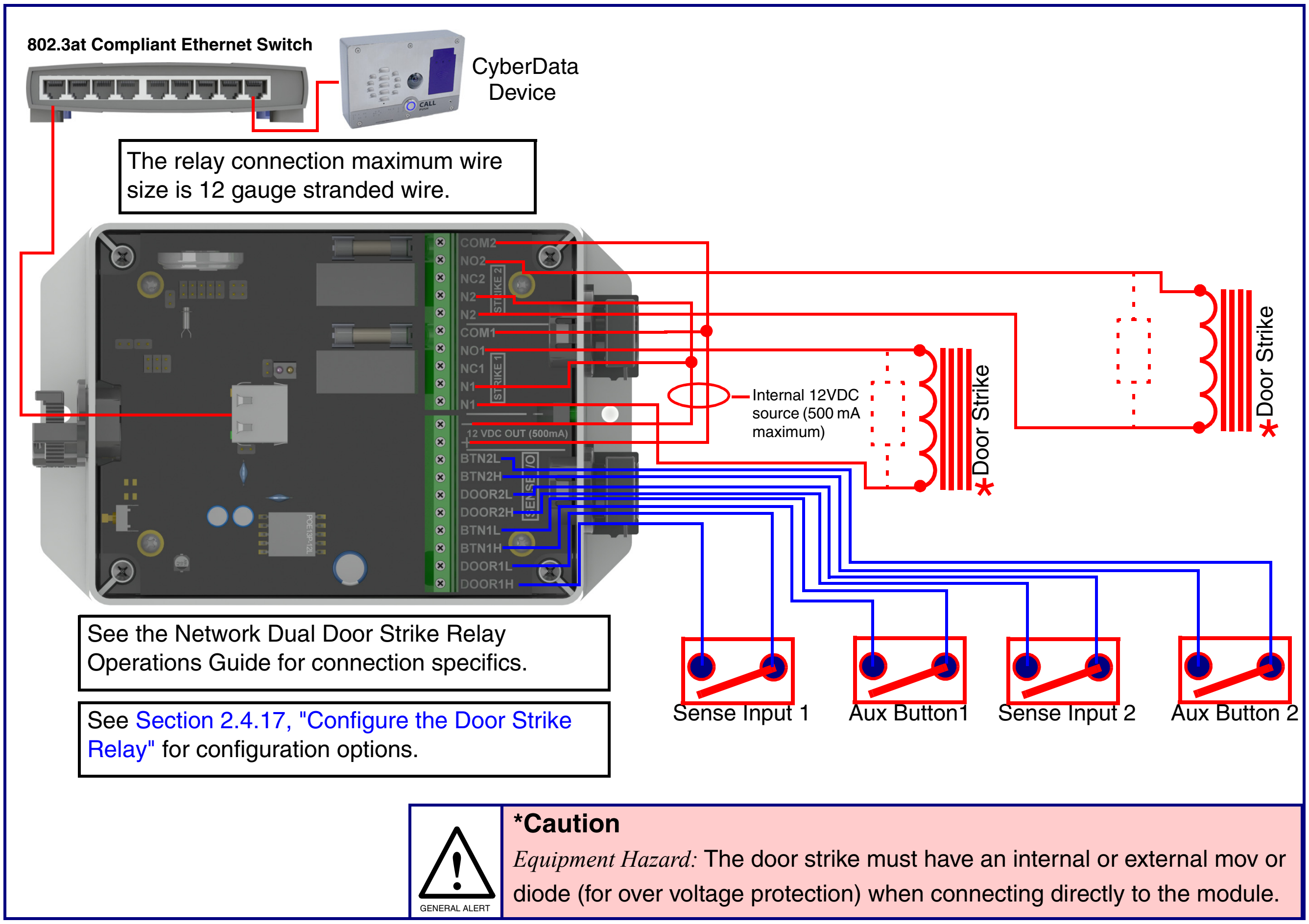
See the Network Dual Door Strike Relay Operations Guide for connection specifics.

See Section 2.4.17, "Configure the Door Strike Relay" for configuration options.

GENERAL ALERT	***Caution** *Equipment Hazard:* The door strike must have an internal or external mov or diode (for over voltage protection) when connecting directly to the module.

2.3.5.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+

Figure 2-10. Network Dual Door Strike Relay Wiring Diagram Using PoE+



The relay connection maximum wire size is 12 gauge stranded wire.

See the Network Dual Door Strike Relay Operations Guide for connection specifics.

See Section 2.4.17, "Configure the Door Strike Relay" for configuration options.

***Caution**

Equipment Hazard: The door strike must have an internal or external mov or diode (for over voltage protection) when connecting directly to the module.

If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

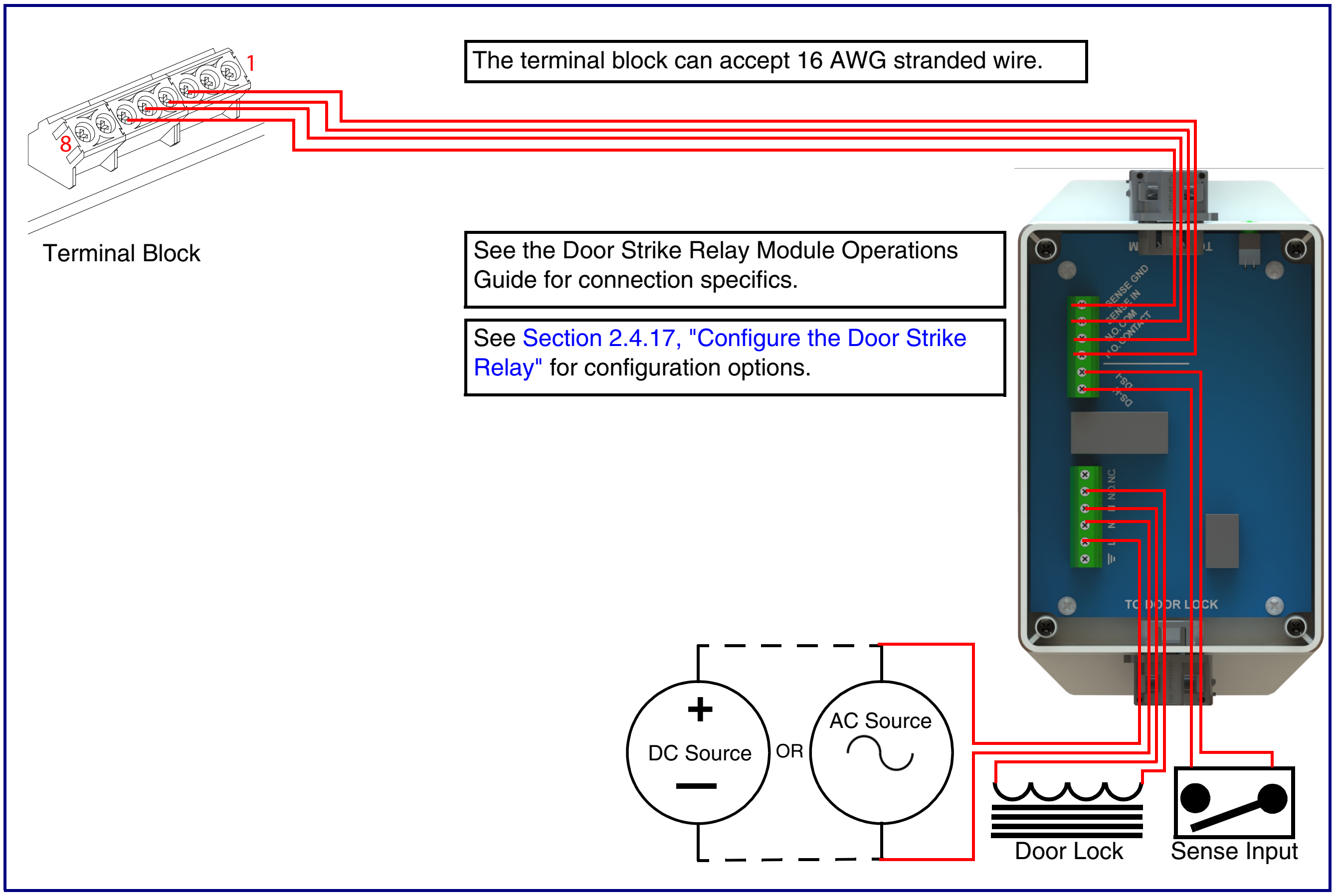
http://support.cyberdata.net/

2.3.5.4 Door Strike Relay Module Wiring Diagram from Intercom

For wiring an electronic door strike, we recommend the use of our external Door Strike Relay Module (CD# 011269).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 2-11 for the wiring diagram.

Figure 2-11. Door Strike Relay Module Wiring Diagram from Intercom



The terminal block can accept 16 AWG stranded wire.

See the Door Strike Relay Module Operations Guide for connection specifics.

See Section 2.4.17, "Configure the Door Strike Relay" for configuration options.

If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

http://support.cyberdata.net/

2.3.6 Intercom Connectors

See the following figures and tables to identify the connectors and functions of the Intercom.

Figure 2-12. Connector Locations—Board Top

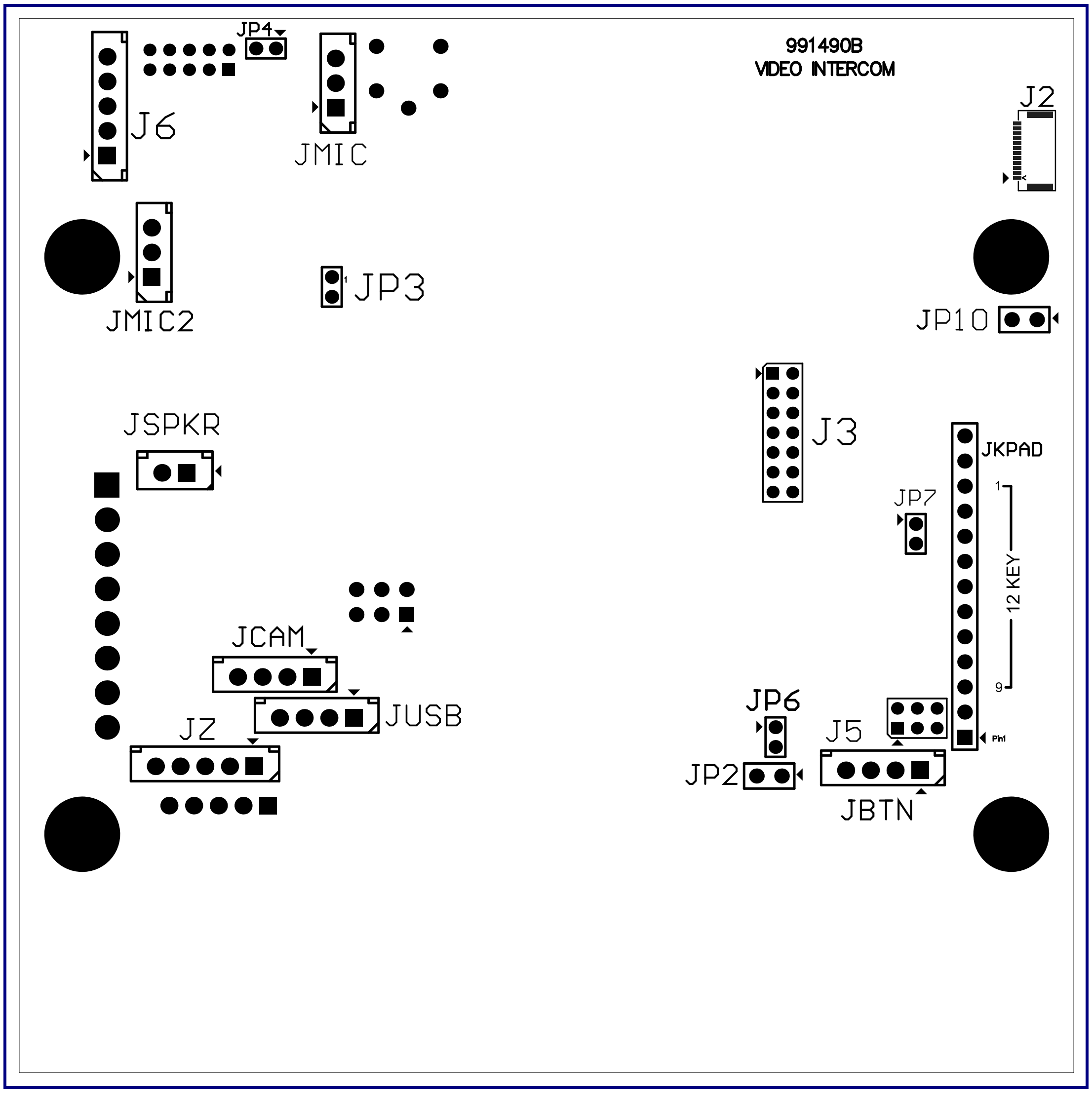


Table 2-2. Connector Functions—Board Top

Connector	Function
JBTN	Call Button LED Interface
JMIC	Microphone Interface
JMIC2	Second Microphone Interface (Not Used)
JSPKR	Speaker Interface
JKPAD	Keypad Interface (Not Used)
JUSB	USB Interface (Not Used)
JZ	I^2C 5V Peripheral Bus
J2	Biometric Interface (Not Used)
J3	JTAG Interface (Not Used)
J5	ISP AT-Tiny Interface (Factory Only)
J6	Digital Microphone Interface (Not Used)
JP3	Mute Disable Jumper—Jumper should be remvoed
JP6	Enable AT-Tiny—Jumper should be installed
JP7	Enable Write to EEPROM—Jumper should be installed
JP10	Disables the intrusion sensor when installed.

Figure 2-13. Connector Locations—Board Bottom

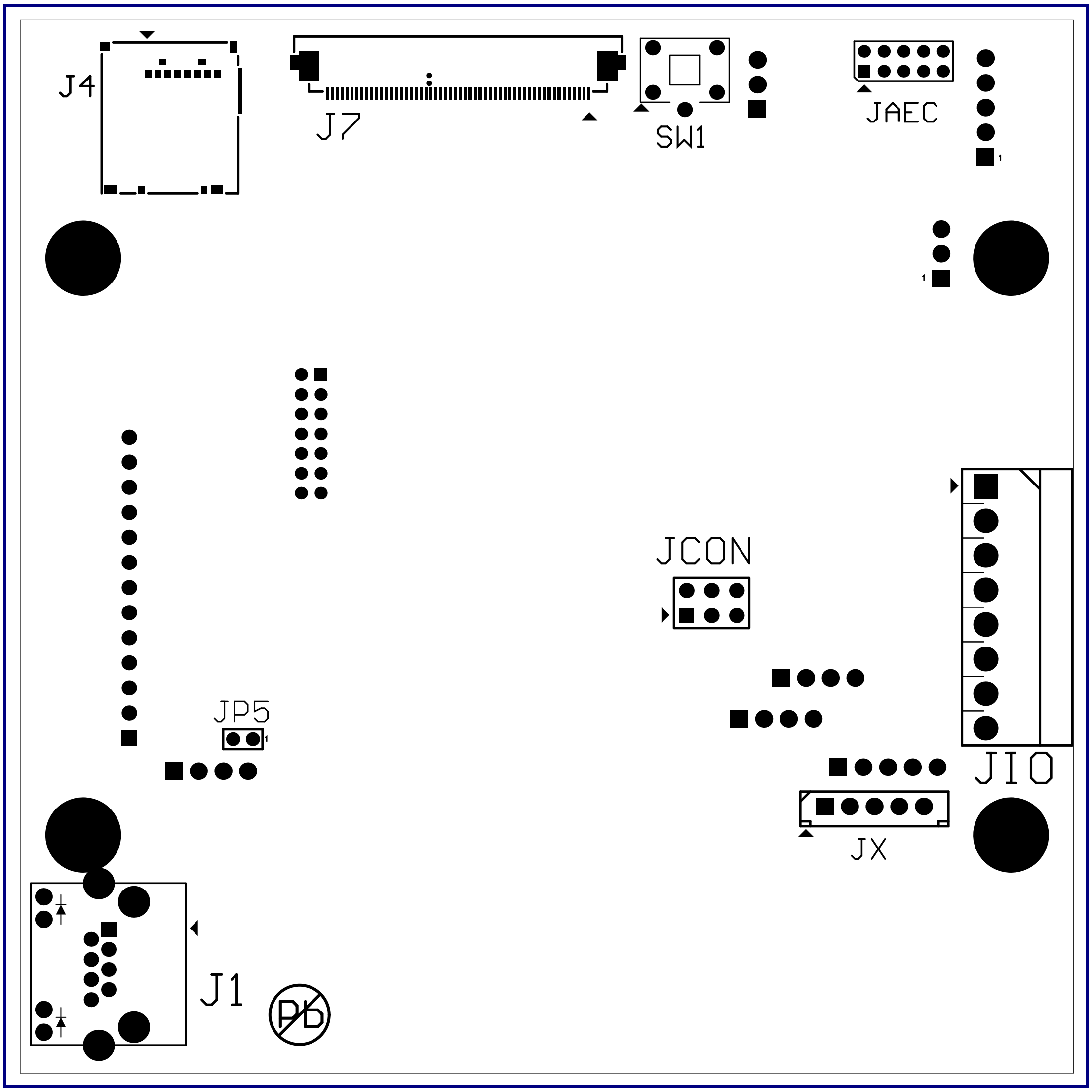


Table 2-3. Connector Functions—Board Bottom

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
J4	SD Card Slot
JAEC	AEC Configuration Interface (Factory Use Only)
JCON	Console Port (Factory Use Only)
JIO	Terminal Block (see Figure 2-6)
JP5	Reset jumper[a]
JX	Auxiliary Strobe Connector
SW1	See Section 2.3.8, "RTFM Button"

[a] Do not install a jumper. Momentary short to reset. Permanent installation of a jumper would prevent the board from running all together.

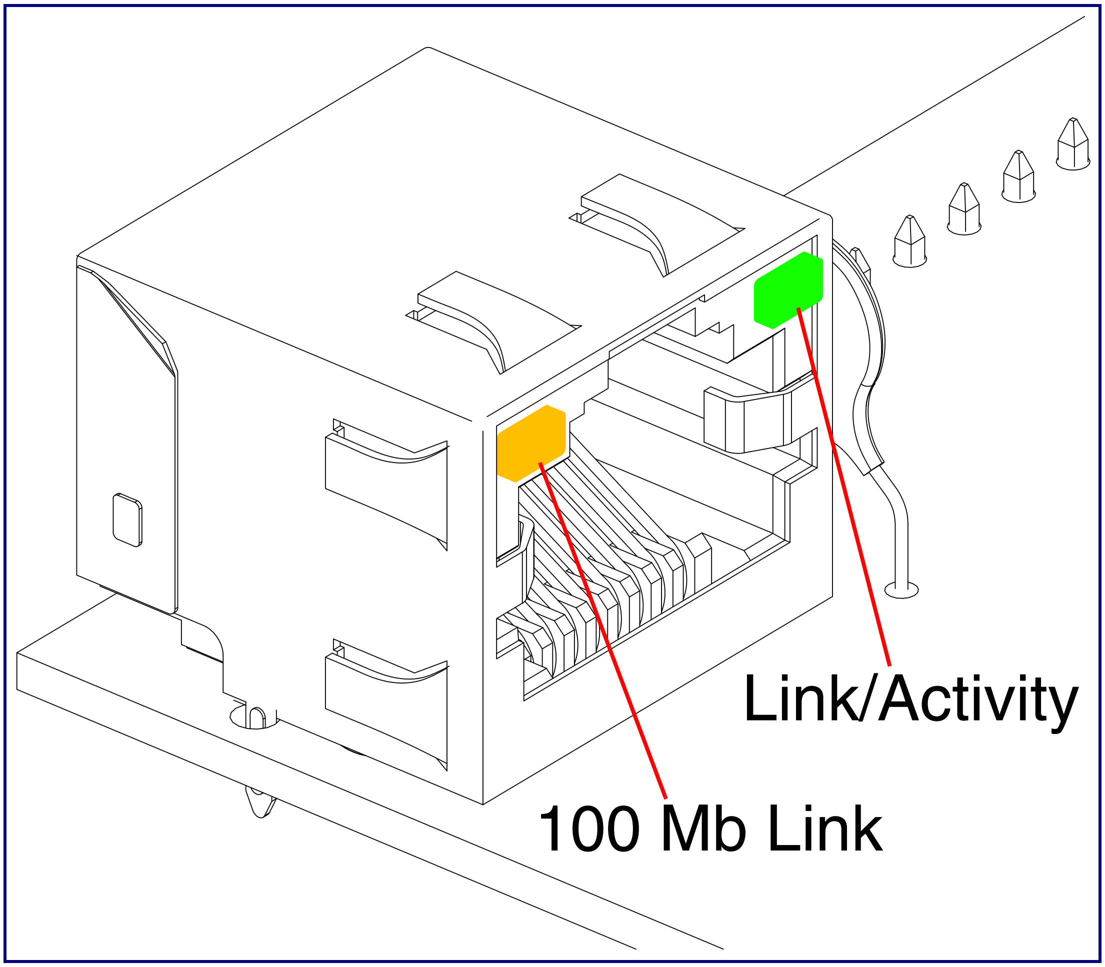
2.3.7 Activity and Link LEDs

2.3.7.1 Verifying the Network Connectivity and Data Rate

When you plug in the Ethernet cable or power supply to the Intercom, the following occurs:

- The square, **GREEN Link/Activity** LED blinks when there is network activity (see Figure 2-14).
- The square, **AMBER 100 Mb Link** LED above the Ethernet port indicates that the network 100 Mb connection has been established (see Figure 2-14).

Figure 2-14. Activity and Link LED

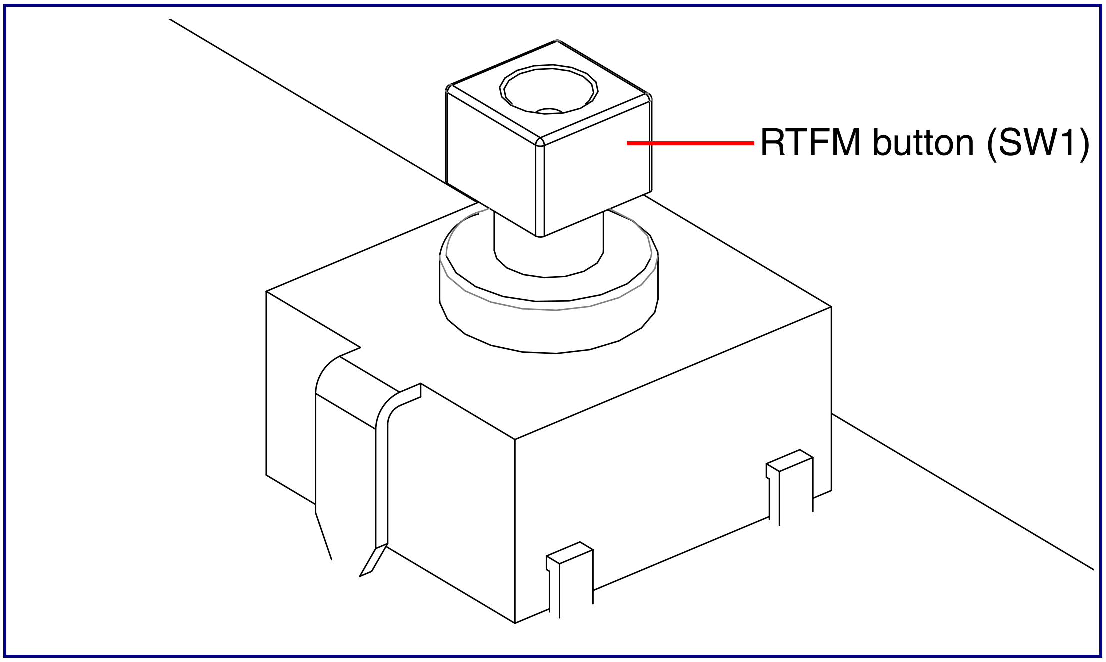


2.3.8 RTFM Button

When the Intercom is operational and linked to the network, you can use the Reset Test Function Management **(RTFM)** button (see **SW1** in Figure 2-15) on the Intercom board to announce and confirm the Intercom's IP Address and test to see if the audio is working.

Note You must do these tests prior to final assembly.

Figure 2-15. RTFM Button (SW1)



2.3.8.1 Announcing the IP Address

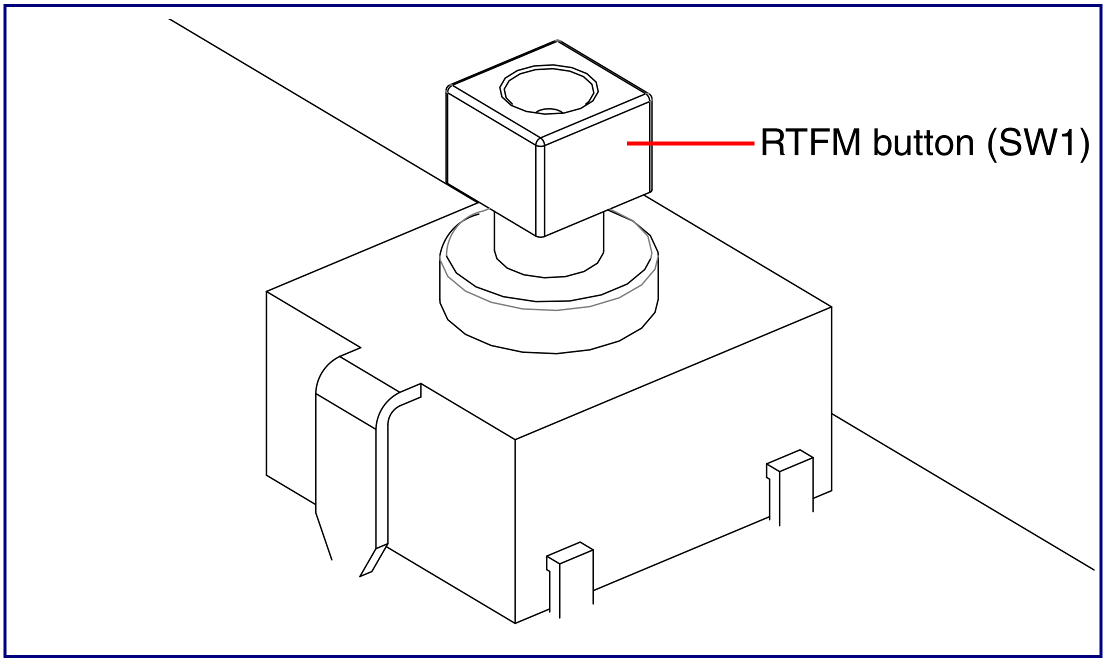
To announce a device's current IP address:

1. Press and release the RTFM button (see **SW1** in Figure 2-16) within a five second window.

Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

Note Pressing and holding the RTFM button for longer than five seconds will restore the device to the factory default settings.

Figure 2-16. RTFM Button (SW1)



2.3.8.2 Restoring the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to a known state.

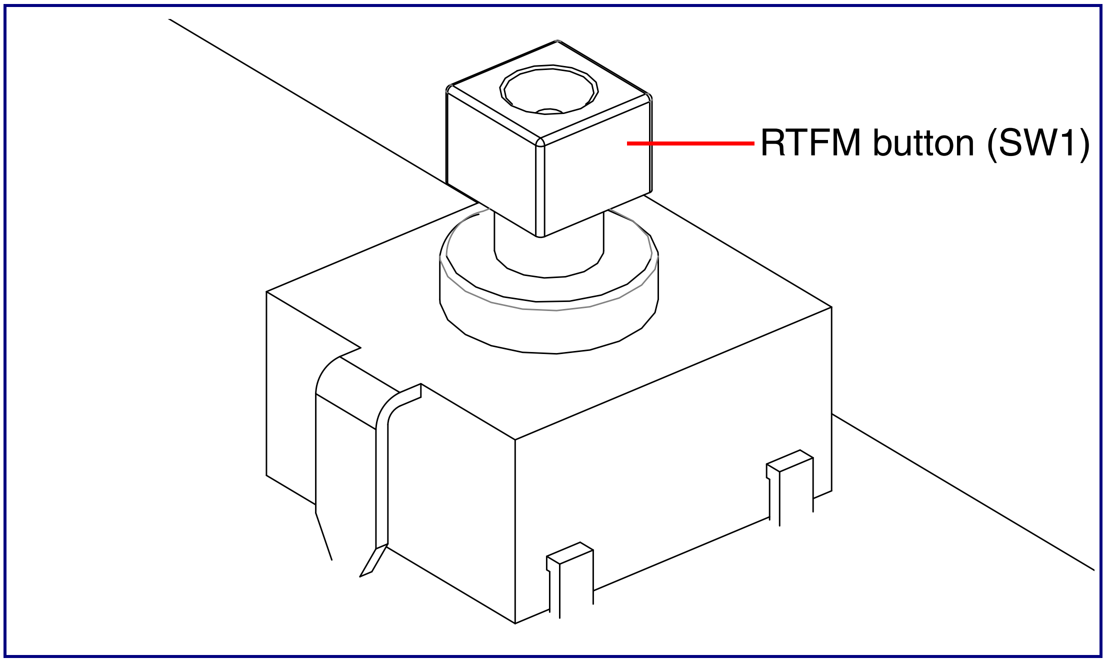
Note Each Intercom is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in Figure 2-17) for more than five seconds.
2. The device announces that it is restoring the factory default settings.

Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

Figure 2-17. RTFM Button (SW1)



2.3.9 Adjusting the Intercom Volume

You can adjust the Intercom volume through the SIP Volume, Multicast Volume, Ring Volume, and Sensor Volume settings on the Device Configuration Page.

2.3.10 Call Button and the Call Button LED

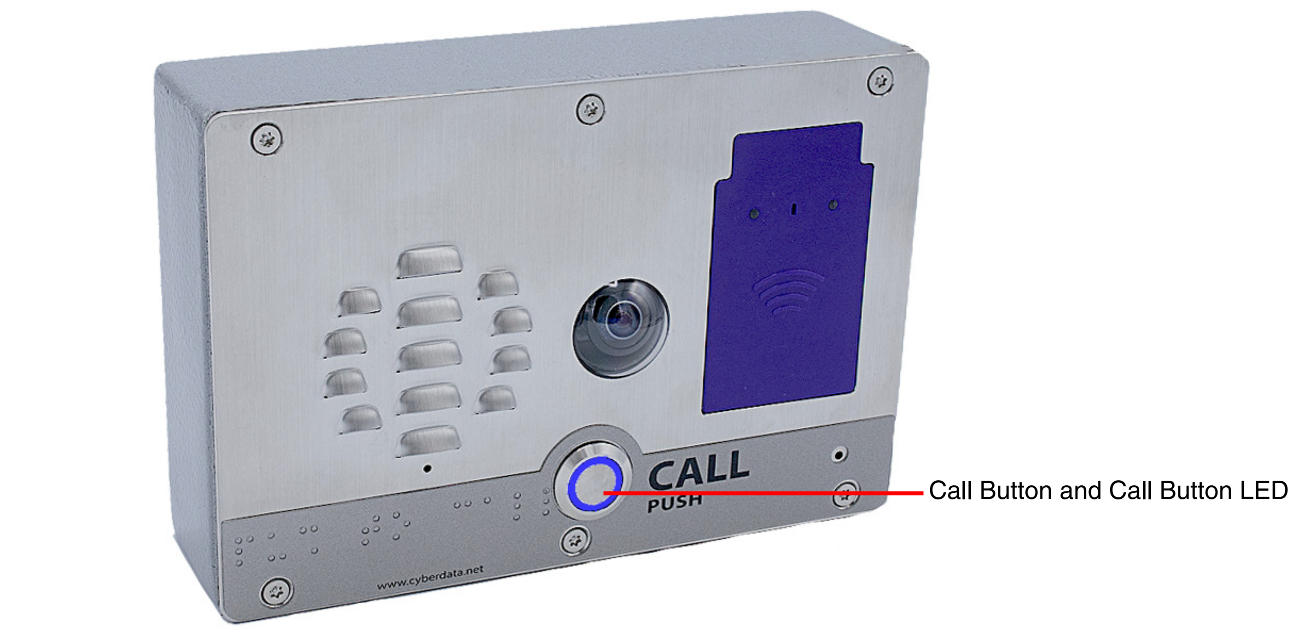
2.3.10.1 Calling with the The Call Button

- You may initiate a call by pressing the **Call** button.
- An active call is indicated by the Call Button LED blinking at one second intervals.
- The Intercom can automatically answer an incoming call.
- You can press the Call Button to terminate an active call.

2.3.10.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- On boot, the Call Button LED will flash ten times a second while setting up the network and downloading autoprovisioning files.
- The device "autoprovisions" by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking. This process will take longer if there are many audio files downloading.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the **Device Configuration Page** (see Section 2.4.5, "Configure the Device"), there is an option called **Button Lit When Idle**. This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 2-18. Call Button and Call Button LED



2.4 Configure the Intercom Parameters

To configure the Intercom online, use a standard web browser.

Configure each Intercom and verify its operation *before* you mount it. When you are ready to mount an Intercom, refer to Appendix A, "Mounting the SIP Outdoor Video Intercom with RFID" for instructions.

2.4.1 Factory Default Settings

All Intercoms are initially configured with the following default IP settings:

When configuring more than one Intercom, attach the Intercoms to the network and configure one at a time to avoid IP address conflicts.

Table 2-4. Factory Default Settings

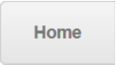
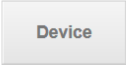
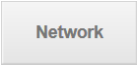
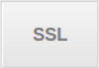
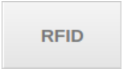
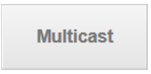
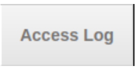
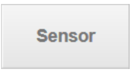
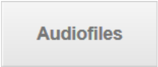
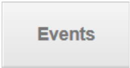
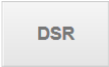
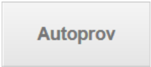
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

[a] Default if there is not a DHCP server present.

2.4.2 Intercom Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every Intercom web page.

Table 2-5. Web Page Navigation

Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device** page.
	Link to the **Video** page.
	Link to the **Network** page.
	Link to go to the **SIP** page.
	Link to the **SSL** page.
	Link to the **RFID** page.
	Link to the **Multicast** page.
	Link to the **Access Log** page.
	Link to the **Sensor** page.
	Link to the **Audiofiles** page.
	Link to the **Events** page.
	Link to the **Door Strike Relay** page.
	Link to the **Autoprovisioning** page.
	Link to the **Firmware** page.

2.4.3 Using the Toggle Help Button

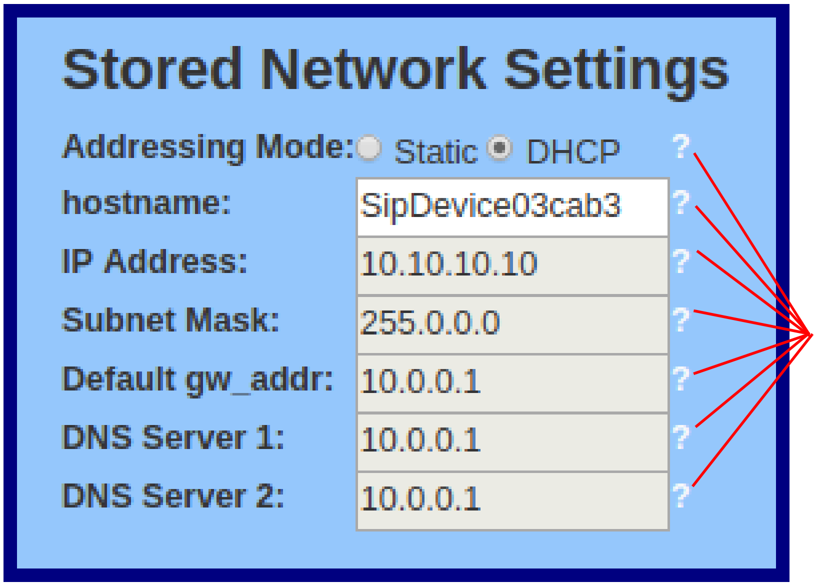
The **Toggle Help** button allows you to see a short description of some of the settings on the webpage. To use the **Toggle Help** button, do the following:

1. Click on the **Toggle Help** button that is on the UI webpage. See Figure 2-19 and Figure 2-20.

Figure 2-19. Toggle/Help Button

2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See Figure 2-20.

Figure 2-20. Toggle Help Button and Question Marks



Stored Network Settings

Addressing Mode: ○ Static ● DHCP ?

hostname: SipDevice03cab3 ?

IP Address: 10.10.10.10 ?

Subnet Mask: 255.0.0.0 ?

Default gw_addr: 10.0.0.1 ?

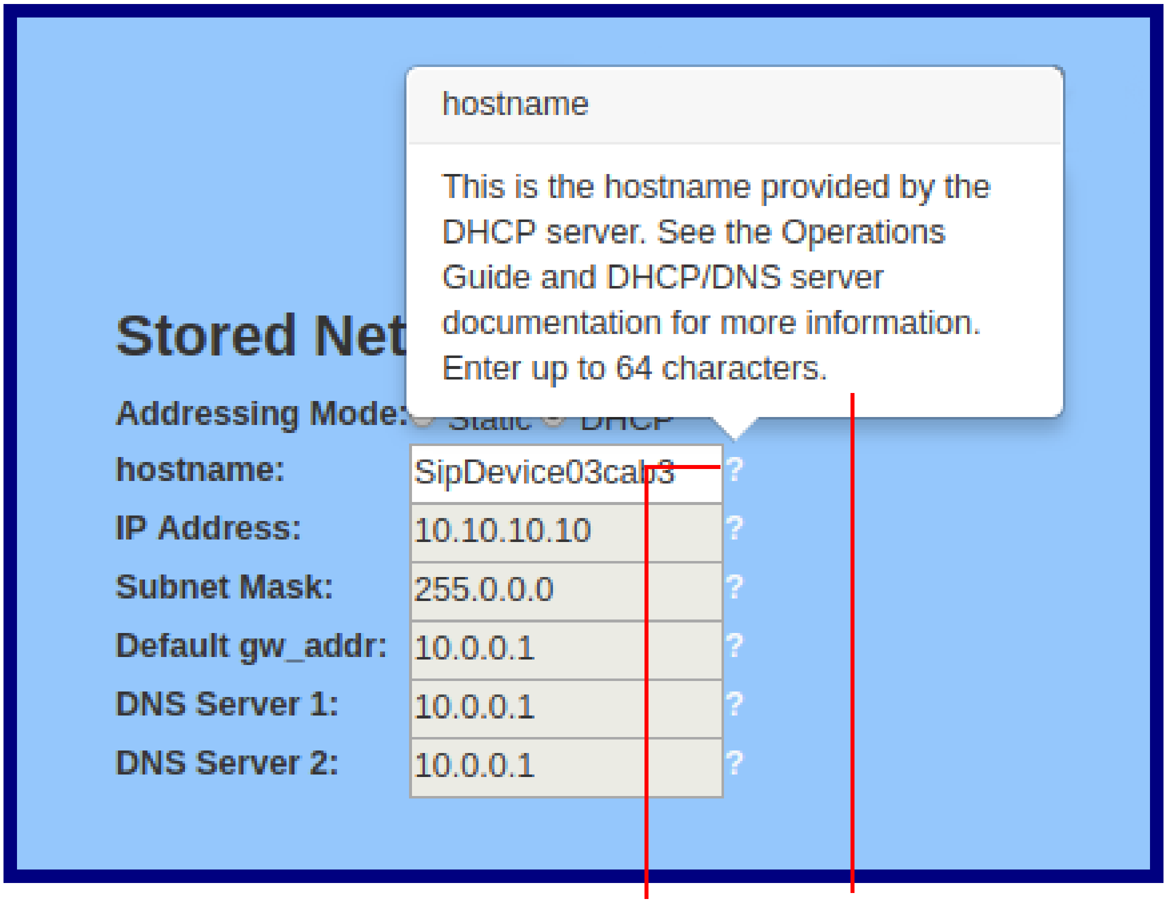
DNS Server 1: 10.0.0.1 ?

DNS Server 2: 10.0.0.1 ?

Question mark appears next to the web page items

3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-21.

Figure 2-21. Short Description Provided by the Help Feature



hostname

This is the hostname provided by the DHCP server. See the Operations Guide and DHCP/DNS server documentation for more information. Enter up to 64 characters.

Stored Net

Addressing Mode:	○ Static ○ DHCP
hostname:	SipDevice03cab3 ?
IP Address:	10.10.10.10 ?
Subnet Mask:	255.0.0.0 ?
Default gw_addr:	10.0.0.1 ?
DNS Server 1:	10.0.0.1 ?
DNS Server 2:	10.0.0.1 ?

Question mark

A short description of the web page item will appear

2.4.4 Log in to the Configuration Home Page

1. Open your browser to the Intercom IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the Intercom.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

https://www.cyberdata.net/pages/discovery

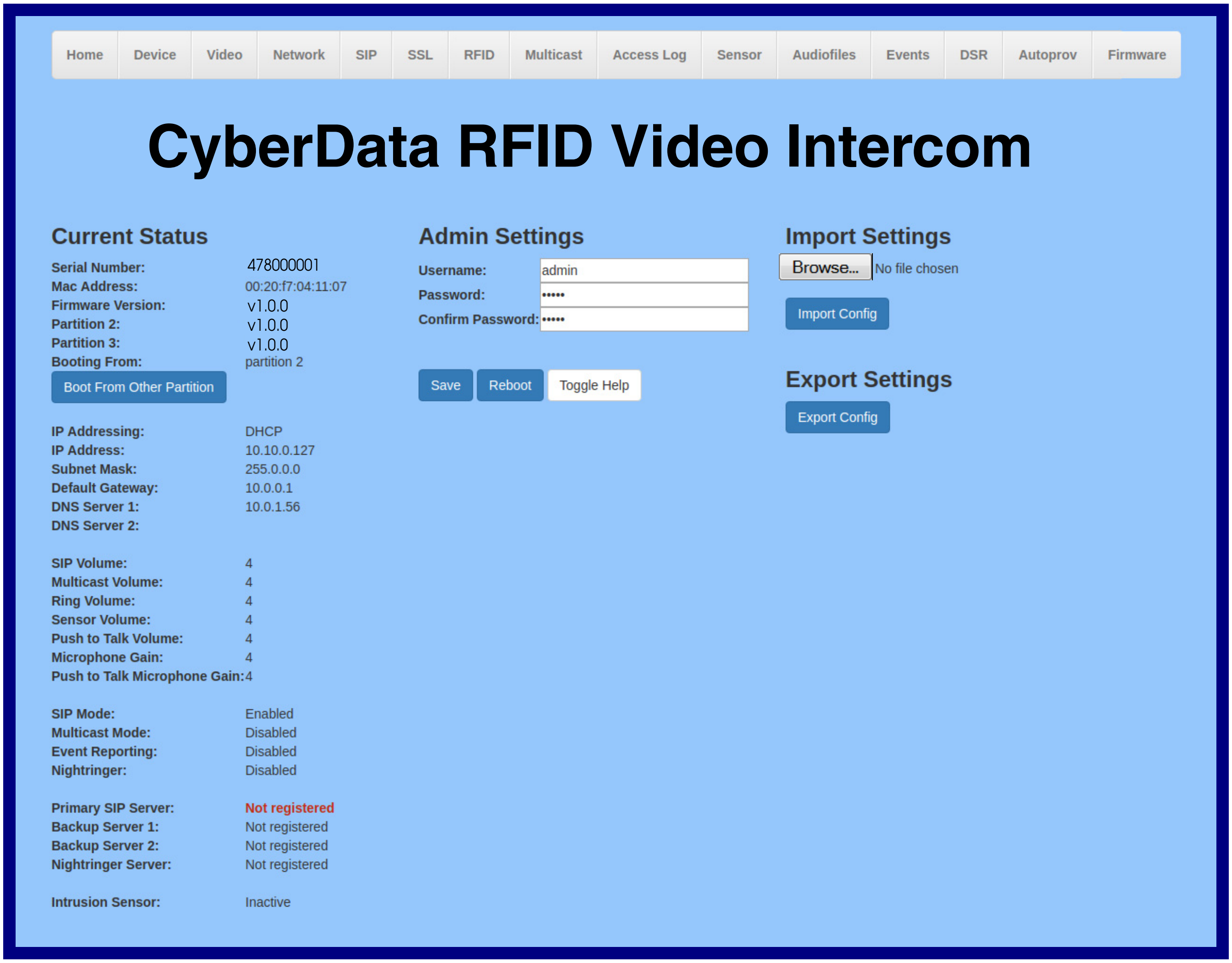
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-22):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 2-22. Home Page



CyberData RFID Video Intercom

Current Status

Serial Number: 478000001
Mac Address: 00:20:f7:04:11:07
Firmware Version: v1.0.0
Partition 2: v1.0.0
Partition 3: v1.0.0
Booting From: partition 2

IP Addressing: DHCP
IP Address: 10.10.0.127
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

SIP Volume: 4
Multicast Volume: 4
Ring Volume: 4
Sensor Volume: 4
Push to Talk Volume: 4
Microphone Gain: 4
Push to Talk Microphone Gain: 4

SIP Mode: Enabled
Multicast Mode: Disabled
Event Reporting: Disabled
Nightringer: Disabled

Primary SIP Server: Not registered
Backup Server 1: Not registered
Backup Server 2: Not registered
Nightringer Server: Not registered

Intrusion Sensor: Inactive

Admin Settings

Username: admin
Password: •••••
Confirm Password: •••••

Import Settings

No file chosen

Export Settings

3. On the **Home** page, review the setup details and navigation buttons described in Table 2-6.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-6. Home Page Overview

Web Page Item	**Description**
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
Partition 2	Contains a complete copy of bootable software.
Partition 3	Contains an alternate, complete copy of bootable software.
Booting From	Indicates the partition currently used for boot.
	Allows the user to boot from the alternate partition.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Volume	Shows the current SIP volume level.
Multicast Volume	Shows the current Multicast volume level.
Ring Volume	Shows the current Ring volume level.
Sensor Volume	Shows the current Sensor volume level.
Push to Talk Volume	Shows the current push to talk volume
Microphone Gain	Shows the current microphone gain level.
Push to Talk Microphone Gain	Shows the current push to talk microphone gain level.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.

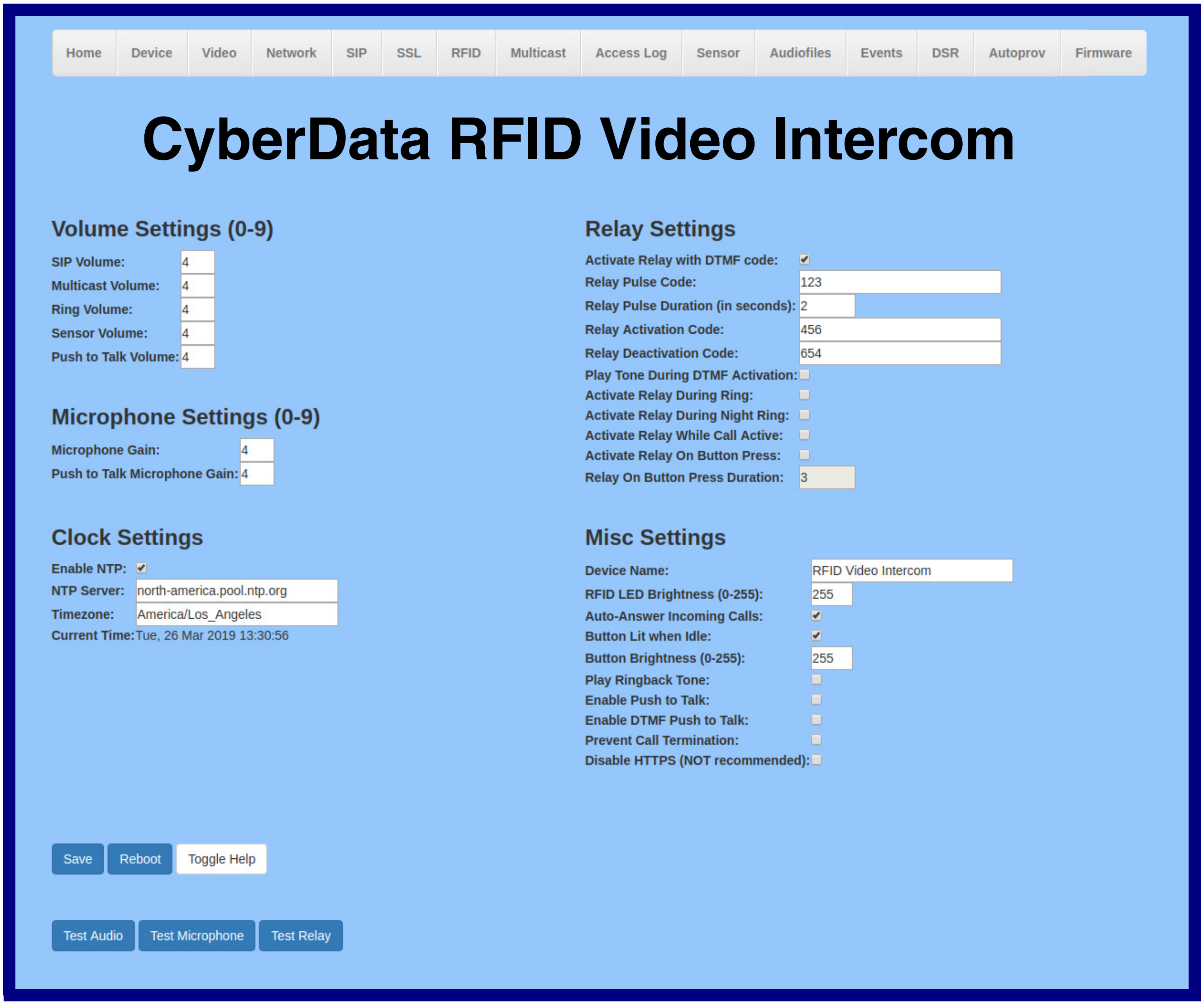
Table 2-6. Home Page Overview (continued)

Web Page Item	Description
Nightringer Server	Shows the current status of Nightringer Server.
Intrusion Sensor	Shows the current status of the intrusion sensor when the Home Page is refreshed.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the **Save** button to save your configuration settings.
	Click on the **Reboot** button to reboot the system.
	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.4.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See Figure 2-23.

Figure 2-23. Device Configuration Page



CyberData RFID Video Intercom

Volume Settings (0-9)

SIP Volume:	4
Multicast Volume:	4
Ring Volume:	4
Sensor Volume:	4
Push to Talk Volume:	4

Microphone Settings (0-9)

Microphone Gain:	4
Push to Talk Microphone Gain:	4

Clock Settings

Enable NTP:	☑
NTP Server:	north-america.pool.ntp.org
Timezone:	America/Los_Angeles
Current Time:	Tue, 26 Mar 2019 13:30:56

Relay Settings

Activate Relay with DTMF code:	☑
Relay Pulse Code:	123
Relay Pulse Duration (in seconds):	2
Relay Activation Code:	456
Relay Deactivation Code:	654
Play Tone During DTMF Activation:	□
Activate Relay During Ring:	□
Activate Relay During Night Ring:	□
Activate Relay While Call Active:	□
Activate Relay On Button Press:	□
Relay On Button Press Duration:	3

Misc Settings

Device Name:	RFID Video Intercom
RFID LED Brightness (0-255):	255
Auto-Answer Incoming Calls:	☑
Button Lit when Idle:	☑
Button Brightness (0-255):	255
Play Ringback Tone:	□
Enable Push to Talk:	□
Enable DTMF Push to Talk:	□
Prevent Call Termination:	□
Disable HTTPS (NOT recommended):	□

2. On the **Device** page, you may enter values for the parameters indicated in Table 2-7.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-7. Device Configuration Parameters

Web Page Item	Description
Volume Settings (0-9)	
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.
Ring Volume ?	Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when Auto-Answer Incoming Calls is disabled.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.
Push to Talk Volume ?	Set the speaker volume for Push to Talk operation. A value of 0 will mute the speaker in Push to Talk mode.
Microphone Settings	
Microphone Gain ?	Set the microphone gain level.
Push to Talk Microphone Gain ?	Set the microphone gain level for Push to Talk operation.
Clock Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See **https://en.wikipedia.org/wiki/List_of_tz_database_time_zones** for a full list of valid strings.
Current Time	Displays the current time.
Relay Settings	
Activate Relay with DTMF Code ?	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
Relay Pulse Code ?	DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).

Table 2-7. Device Configuration Parameters (continued)

Web Page Item	**Description**
Relay Pulse Duration (in seconds) ?	The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.
Relay Activation Code ?	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Deactivation Code ?	Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Play tone during DTMF Activation ?	When selected, the device will play a tone out of the speaker upon DTMF relay activation. The tone plays for the DTMF Activation Duration (in seconds).
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.
Activate Relay While Call Active ?	When selected, the relay will be activated as long as the SIP call is active.
Activate Relay on Button Press ?	When selected, the relay will be activated when the Call button is pressed.
Relay on Button Press Duration ?	The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A **Relay on Button Press Duration** value of 0 will pulse the relay once when the Call button is pressed.
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
RFID LED Brightness (0-255) ?	The desired brightness of the leds on the rfid reader. Acceptable values are 0-255, where 0 is off and 255 is max brightness. Enter up to 3 digits.
Auto-Answer Incoming Calls ?	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until someone presses the Call button to answer the call or the caller disconnects before the call can be answered.
Button Lit When Idle ?	When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).
Button Brightness (0-255) ?	The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to three digits.
Play Ringback Tone ?	When selected, the device will play a ringback tone (corresponds to Ringback Tone on the Audiofiles page) out of the speaker while placing an outbound call. The Ringback Tone will play until the call is answered.
Enable Push to Talk ?	This option is for noisy environments. When enabled, the microphone will be muted normally. When the Call button is pressed and held, it will unmute the microphone and allow the operator to send audio back. Using Push to Talk prevents the operator from terminating a call by pressing the Call button. The call must be terminated by the phone user.

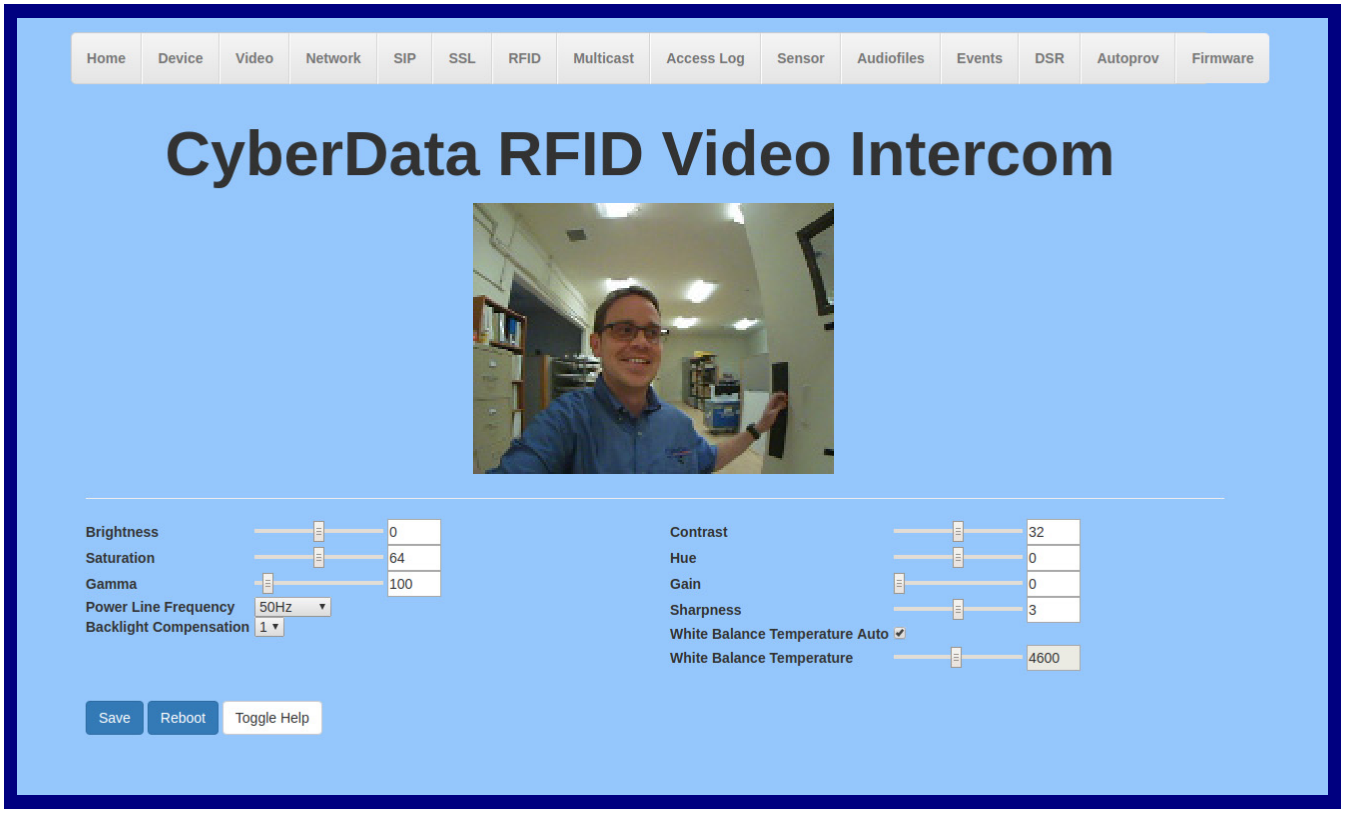
Table 2-7. Device Configuration Parameters (continued)

Web Page Item	Description
Enable DTMF Push to Talk ?	This option is for noisy environments. When enabled, in an active call, the remote phone can force receive only audio (setting the mic gain to max and muting the speaker) by pressing the ***** key. Pressing the **#** key will force send only audio (setting the max speaker volume and muting the mic). Pressing the **0** key will restore full duplex operation with the normal microphone and speaker volume.
Prevent Call Termination ?	When this option is enabled, a call cannot be terminated using the call button.
Disable HTTPS (NOT recommended) ?	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons. **Note** This setting requires a reboot for the changes to take effect.
Test Audio	Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.
Test Microphone	Click on the **Test Microphone** button to do a microphone test. When the **Test Microphone** button is pressed, the following occurs: 1. The device will immediately start recording 3 seconds of audio. 2. The device will beep (indicating the end of recording). 3. The device will play back the recorded audio.
Test Relay	Click on the **Test Relay** button to do a relay test.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.4.6 Configure the Video Parameters

1. Click the **Video** menu button to open the **Video** page (Figure 2-25).

Figure 2-24. Video Page



CyberData RFID Video Intercom

Brightness 0
Saturation 64
Gamma 100
Power Line Frequency 50Hz
Backlight Compensation 1

Contrast 32
Hue 0
Gain 0
Sharpness 3
White Balance Temperature Auto ☑
White Balance Temperature 4600

2. On the **Video** page, enter values for the parameters indicated in Table 2-9.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-8. Video Page Parameters

Web Page Item	Description
Brightness ?	The Brightness parameter brightens the entire image equally. Enter a value between -64 and 64. The default value is 0.
Saturation ?	Saturation increases the separation between colors, and has a more noticeable effect on vibrant colors, less on neutral colors, and no effect on black and white images. Enter a value between 0 and 128. The default value is 64.
Gamma ?	Gamma controls the image's grayscale. Increasing gamma can make the image look brighter, because it increases the brightness of the shadows and midtones without affecting the highlights. Enter a value between 72 and 500. The default value is 100.
Power Line Frequency ?	The Power line Frequency option allows the user to select 50Hz, 60Hz, or disabled for the frequency of the power line. Adjust this value if you're seeing flickering from fluorescent light sources. The default value is 50Hz.
Backlight Compensation ?	Backlight Compensation allows the camera to adjust the exposure of the entire image to properly expose the subject in the foreground, to avoid silhouettes where there is a bright light source. Select 0, 1, or 2. The default value is 1.
White Balance Temperature Auto ?	White balance temperature auto allows the device to automatically compensate for cast in lighting. Select "On" or "Off." The default value is "On."
Contrast ?	Contrast is the separation between the darkest and brightest areas of the image. Increasing contrast will make an image look more vibrant; decreasing can make it look duller. Enter a value between 0 and 64. The default value is 32.
Hue ?	Also referred to as "tint," hue affects the red/green balance of the image. Enter a value between -40 and 40. The default value is 0.
Gain ?	Gain controls the amplification of the signal from the camera, including background noise. Enter a value between 0 and 100. The default value is 0.
Sharpness ?	Sharpness controls the contrast along and near the edges in the image. Enter a value between 0 and 6. The default value is 3.
White Balance Temperature ?	White balance temperature compensates for cast in lighting, keeping white and gray neutral. This setting is only applicable if "White Balance Temperature Auto" is set to "off." Enter a value between 2800 and 6500. The default value is 4600.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

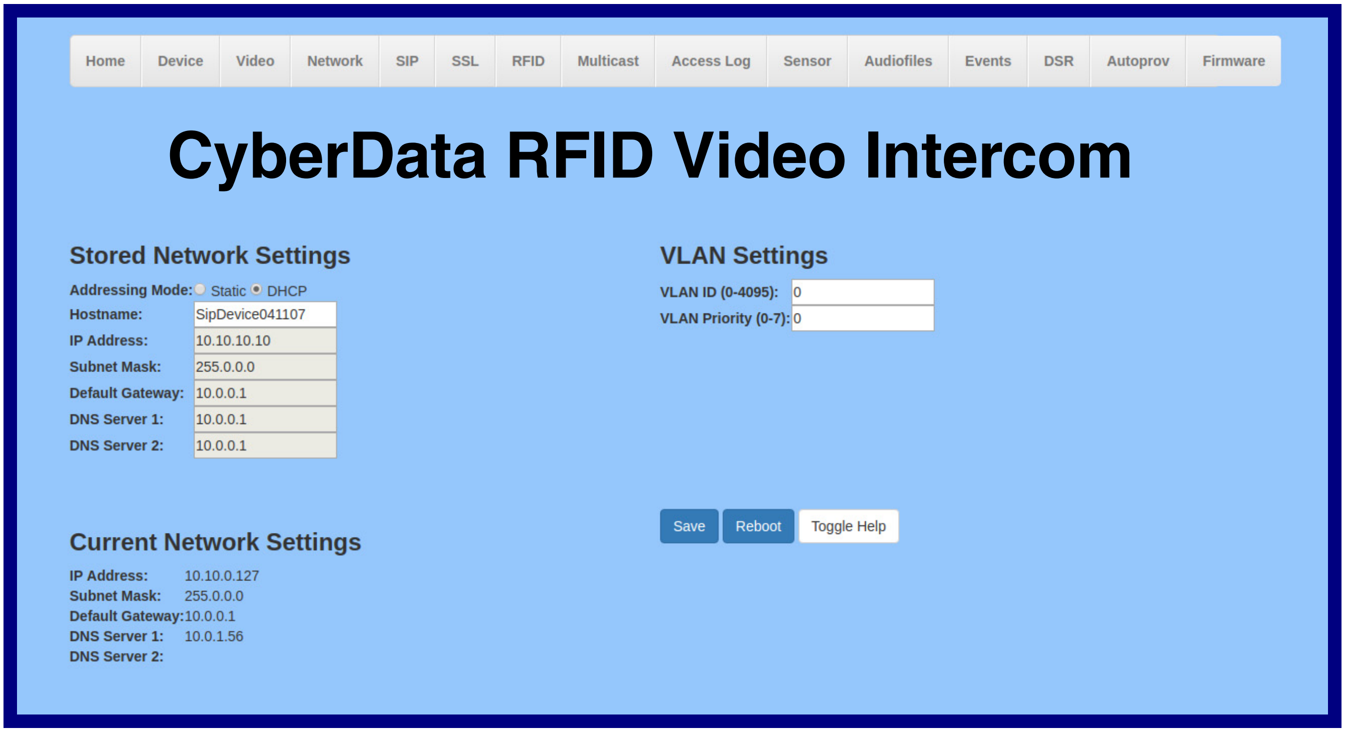
Table 2-8. Video Page Parameters (continued)

Web Page Item	Description
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.4.7 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-25).

Figure 2-25. Network Configuration Page



CyberData RFID Video Intercom

Stored Network Settings

Addressing Mode: ○ Static ● DHCP
Hostname: SipDevice041107
IP Address: 10.10.10.10
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.0.1
DNS Server 2: 10.0.0.1

VLAN Settings

VLAN ID (0-4095): 0
VLAN Priority (0-7): 0

Current Network Settings

IP Address: 10.10.0.127
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

2. On the **Network** page, enter values for the parameters indicated in Table 2-9.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-9. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.4.1, "Factory Default Settings" for factory default settings. Be sure to click **Save** and **Reboot** to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/ DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. A value of 0 disables vlan. **Note**: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in “trunking mode” for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.

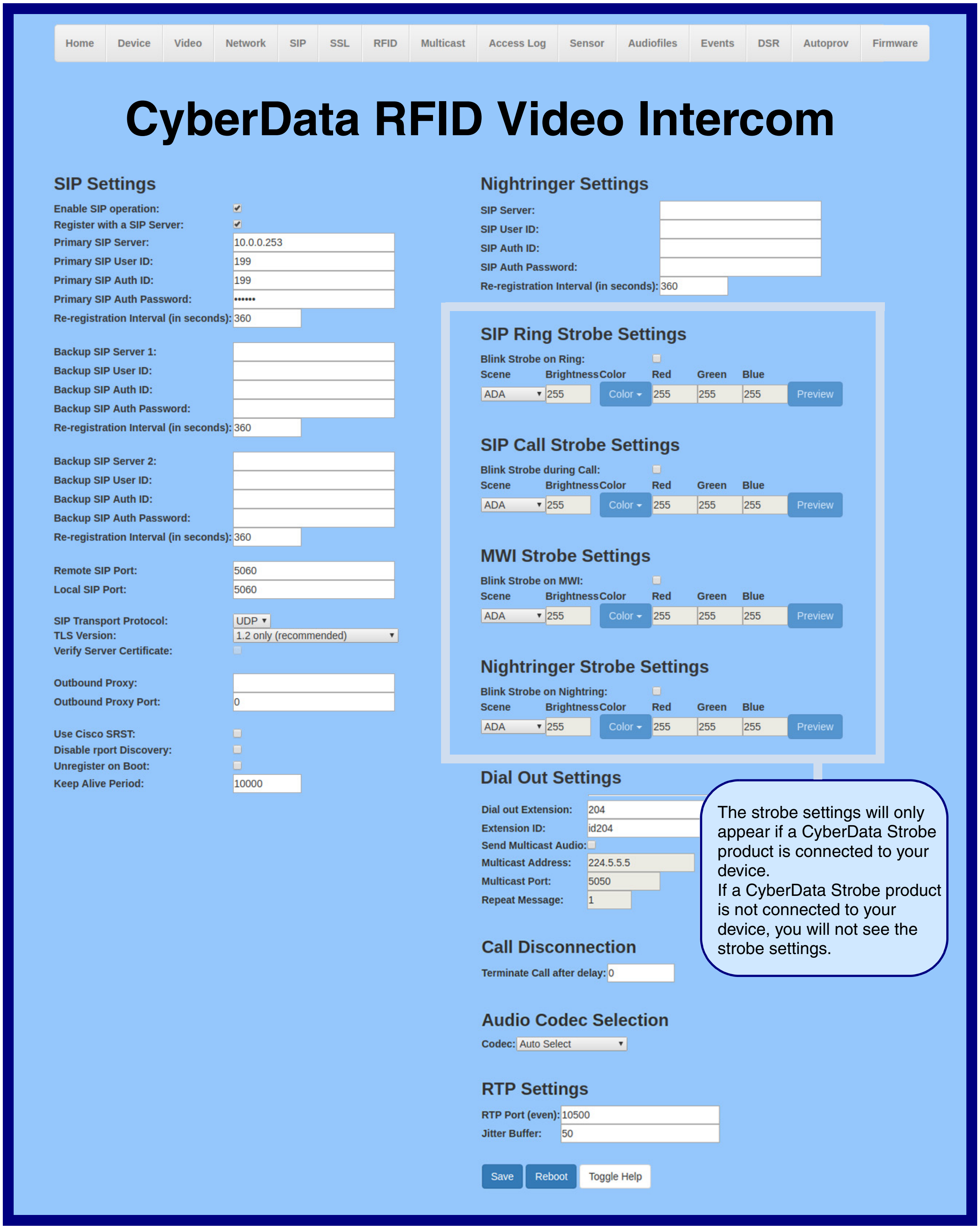
Table 2-9. Network Configuration Parameters (continued)

Web Page Item	Description
	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.4.8 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-26).

Figure 2-26. SIP Configuration Page



CyberData RFID Video Intercom

SIP Settings

Enable SIP operation: ☑
Register with a SIP Server: ☑
Primary SIP Server: 10.0.0.253
Primary SIP User ID: 199
Primary SIP Auth ID: 199
Primary SIP Auth Password: ••••••
Re-registration Interval (in seconds): 360

Backup SIP Server 1:
Backup SIP User ID:
Backup SIP Auth ID:
Backup SIP Auth Password:
Re-registration Interval (in seconds): 360

Backup SIP Server 2:
Backup SIP User ID:
Backup SIP Auth ID:
Backup SIP Auth Password:
Re-registration Interval (in seconds): 360

Remote SIP Port: 5060
Local SIP Port: 5060

SIP Transport Protocol: UDP
TLS Version: 1.2 only (recommended)
Verify Server Certificate: □

Outbound Proxy:
Outbound Proxy Port: 0

Use Cisco SRST: □
Disable rport Discovery: □
Unregister on Boot: □
Keep Alive Period: 10000

Nightringer Settings

SIP Server:
SIP User ID:
SIP Auth ID:
SIP Auth Password:
Re-registration Interval (in seconds): 360

SIP Ring Strobe Settings

Blink Strobe on Ring: □

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

SIP Call Strobe Settings

Blink Strobe during Call: □

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

MWI Strobe Settings

Blink Strobe on MWI: □

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

Nightringer Strobe Settings

Blink Strobe on Nightring: □

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

Dial Out Settings

Dial out Extension: 204
Extension ID: id204
Send Multicast Audio: □
Multicast Address: 224.5.5.5
Multicast Port: 5050
Repeat Message: 1

Call Disconnection

Terminate Call after delay: 0

Audio Codec Selection

Codec: Auto Select

RTP Settings

RTP Port (even): 10500
Jitter Buffer: 50

Save Reboot Toggle Help

The strobe settings will only appear if a CyberData Strobe product is connected to your device.
If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.

2. On the **SIP** page, enter values for the parameters indicated in Table 2-10.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-10. SIP Configuration Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable **SIP Operation** and disable **Register with a SIP Server** (see Section 2.4.8.2, "Point-to-Point Configuration").
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-10. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Auth Password	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds)	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Remote SIP Port	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP Transport Protocol	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Outbound Proxy	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Use Cisco SRST	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Disable rport Discovery	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Unregister on Boot	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
SIP Ring Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Ring	When selected, the Strobe will blink a scene when ringing.
Scene	Select desired scene (only one may be chosen).
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.

Table 2-10. SIP Configuration Parameters (continued)

Web Page Item	Description
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Ring. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for SIP Ring.
Green ?	The green LED value for SIP Ring.
Blue ?	The blue LED value for SIP Ring.
Preview	Use this button to preview the strobe flashing behavior for the **SIP Ring Strobe Settings**.
SIP Call Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe during Call ?	When selected, the Strobe will blink a scene during a call.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Call. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for SIP Call.
Green ?	The green LED value for SIP Call.
Blue ?	The blue LED value for SIP Call.
Preview	Use this button to preview the strobe flashing behavior for the **SIP Call Strobe Settings**.
MWI Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**

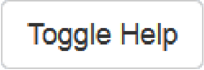
Table 2-10. SIP Configuration Parameters (continued)

Web Page Item	Description
Blink Strobe on MWI ?	When selected, the strobe will blink a scene when a voicemail is waiting for its extension.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
MWI Call Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a message waiting. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for MWI.
Green ?	The green LED value for MWI.
Blue ?	The blue LED value for MWI.
	Use this button to preview the strobe flashing behavior for the **MWI Strobe Settings**.
Nightringer Settings	
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
SIP User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
SIP Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
SIP Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Nightringer Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Nightring ?	When selected, the Strobe will blink a scene when the Nightringer is ringing.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.

Table 2-10. SIP Configuration Parameters (continued)

Web Page Item	Description
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for Nightringer.
Green	The green LED value for Nightringer.
Blue	The blue LED value for Nightringer.
	Use this button to preview the strobe flashing behavior for the **Nightringer Strobe Settings**.
Dial Out Settings	
Dial Out Extension	Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters. **Note**: For information about dial-out extension strings and DTMF tones, see Section 2.4.8.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".
Extension ID	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Send Multicast Audio	When selected, the device will play an audio file to the specified multicast address and port.
Multicast Address	The multicast address used for multicasting an audio file.
Multicast Port	The multicast port used for multicasting an audio file.
Repeat Message	The number of times to repeat the audio message to the remote endpoint. Enter a value from 1-65536.
Call Disconnection	
Terminate Call After Delay	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Audio Codec Selection	
Codec	Select the desired codec (only one may be chosen).
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Jitter Buffer	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.

Table 2-10. SIP Configuration Parameters (continued)

Web Page Item	Description
	Click the **Save** button to save your configuration settings.
	Click on the **Reboot** button to reboot the system.
	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note For specific server configurations, go to the following website address:

https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers

2.4.8.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

On the **SIP Configuration Page**, dial out extensions support the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-11. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 64.

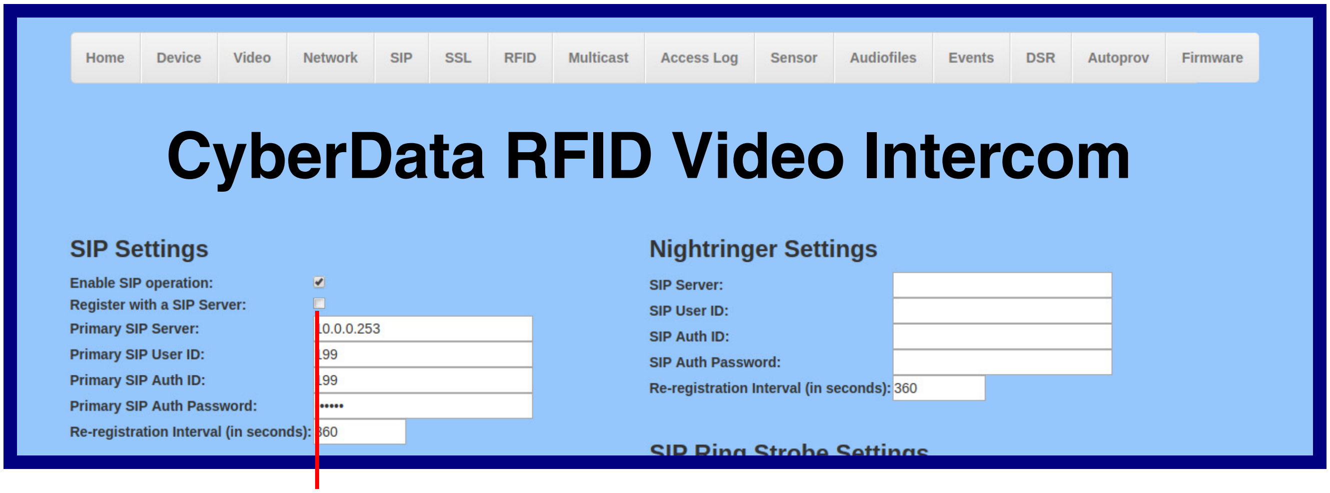
2.4.8.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see Figure 2-27), it is possible to set the device to dial out to a single endpoint.

In this case, the dial-out extension should be the IP address of the remote device. The device can also receive Point-to-Point calls. The delayed DTMF functionality is available in the Point-to-Point Mode.

Note Receiving point-to-point SiP calls may not work with all phones.

Figure 2-27. SIP Page Set to Point-to-Point Mode



SIP Settings

Enable SIP operation: ☑
Register with a SIP Server: ☐
Primary SIP Server: 10.0.0.253
Primary SIP User ID: 199
Primary SIP Auth ID: 199
Primary SIP Auth Password: •••••
Re-registration Interval (in seconds): 360

Nightringer Settings

SIP Server:
SIP User ID:
SIP Auth ID:
SIP Auth Password:
Re-registration Interval (in seconds): 360

SIP Ring Strobe Settings

Device is set to NOT register with a SIP server

2.4.8.3 Delayed DTMF

On the **SIP Configuration** page the dial out extension supports the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-12. Examples of Dial-Out Extension Strings

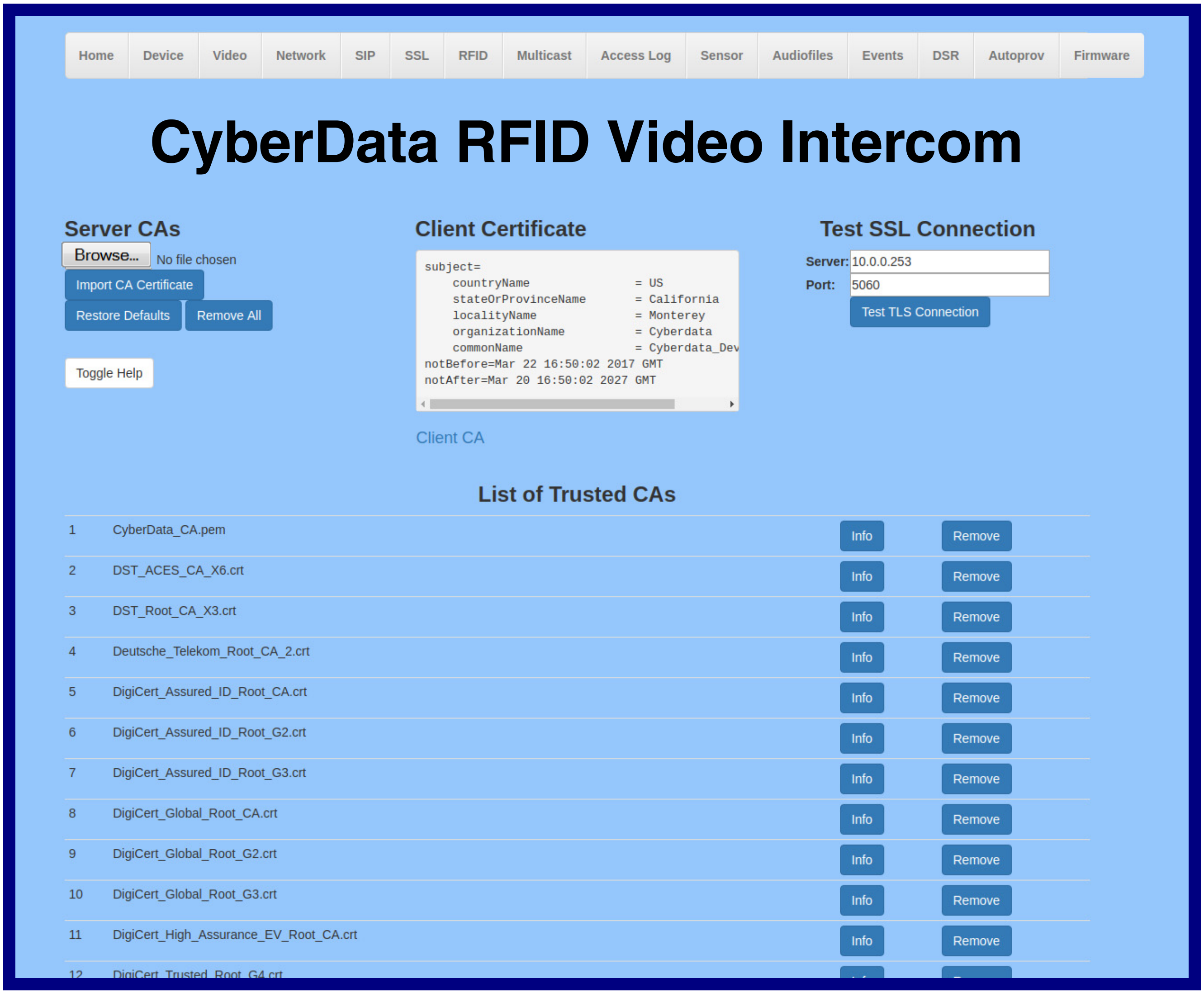
Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 25.

2.4.9 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-59).

Figure 2-28. SSL Configuration Page



CyberData RFID Video Intercom

Server CAs

Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = Cyberdata_Dev
notBefore=Mar 22 16:50:02 2017 GMT
notAfter=Mar 20 16:50:02 2027 GMT
```

Test SSL Connection

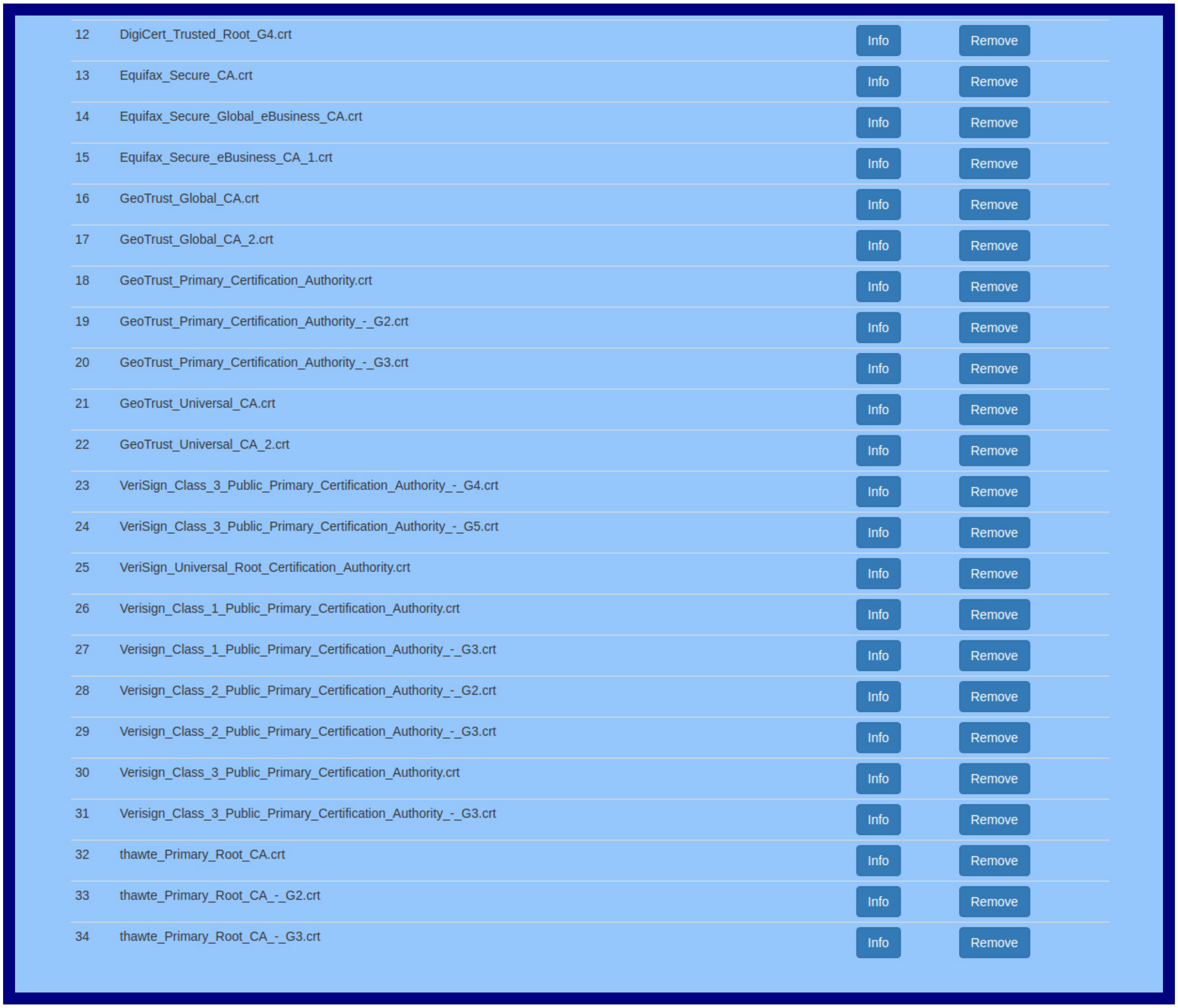
Server: 10.0.0.253

Port: 5060

List of Trusted CAs

1	CyberData_CA.pem
2	DST_ACES_CA_X6.crt
3	DST_Root_CA_X3.crt
4	Deutsche_Telekom_Root_CA_2.crt
5	DigiCert_Assured_ID_Root_CA.crt
6	DigiCert_Assured_ID_Root_G2.crt
7	DigiCert_Assured_ID_Root_G3.crt
8	DigiCert_Global_Root_CA.crt
9	DigiCert_Global_Root_G2.crt
10	DigiCert_Global_Root_G3.crt
11	DigiCert_High_Assurance_EV_Root_CA.crt
12	DigiCert_Trusted_Root_G4.crt

Figure 2-29. SSL Configuration Page



12	DigiCert_Trusted_Root_G4.crt	Info	Remove
13	Equifax_Secure_CA.crt	Info	Remove
14	Equifax_Secure_Global_eBusiness_CA.crt	Info	Remove
15	Equifax_Secure_eBusiness_CA_1.crt	Info	Remove
16	GeoTrust_Global_CA.crt	Info	Remove
17	GeoTrust_Global_CA_2.crt	Info	Remove
18	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
19	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
20	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
21	GeoTrust_Universal_CA.crt	Info	Remove
22	GeoTrust_Universal_CA_2.crt	Info	Remove
23	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
24	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
25	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
26	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
27	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
28	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
29	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
30	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
31	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
32	thawte_Primary_Root_CA.crt	Info	Remove
33	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
34	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

2. On the **SSL** page, enter values for the parameters indicated in Table 2-13.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

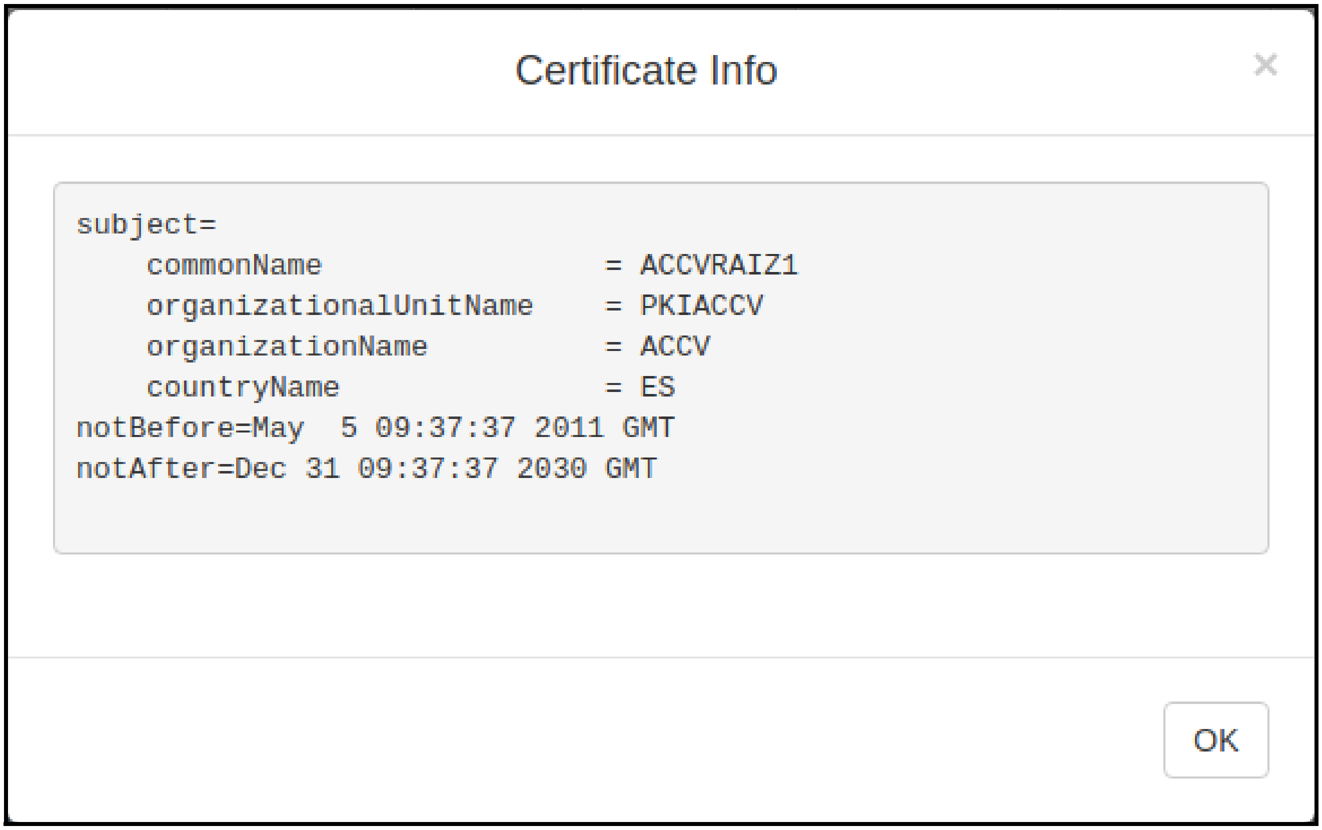
Table 2-13. SSL Configuration Parameters

Web Page Item	Description
Server CAs	
	Use this button to select a configuration file to import.
	Click **Browse** to select a CA certificate to import. After selecting a server certificate authority (CA), click **Import CA Certificate** to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	Restore Defaults will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
	Restore Defaults will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
Client CA ?	Right click and **Save Link As...** to get the Cyberdata CA used to sign this client certificate.
Test SSL Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The ssl test server port. The supported range is 0-65536. SIP connections over TLS to port 5060 will do the same.
	Use this button to test a TLS connection to a remote server. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
List of Trusted CAs	
	Provides details of the certificate. After clicking on this button, the **Certificate Info Window** appears. See Section 2.4.9.1, "Certificate Info Window".
	Removes this certificate from the list of trusted certificates. After clicking on this button, the **Remove Server Certificate Window** appears. See Section 2.4.9.2, "Remove Server Certificate Window".

2.4.9.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See Figure 2-30.

Figure 2-30. Certificate Info Window

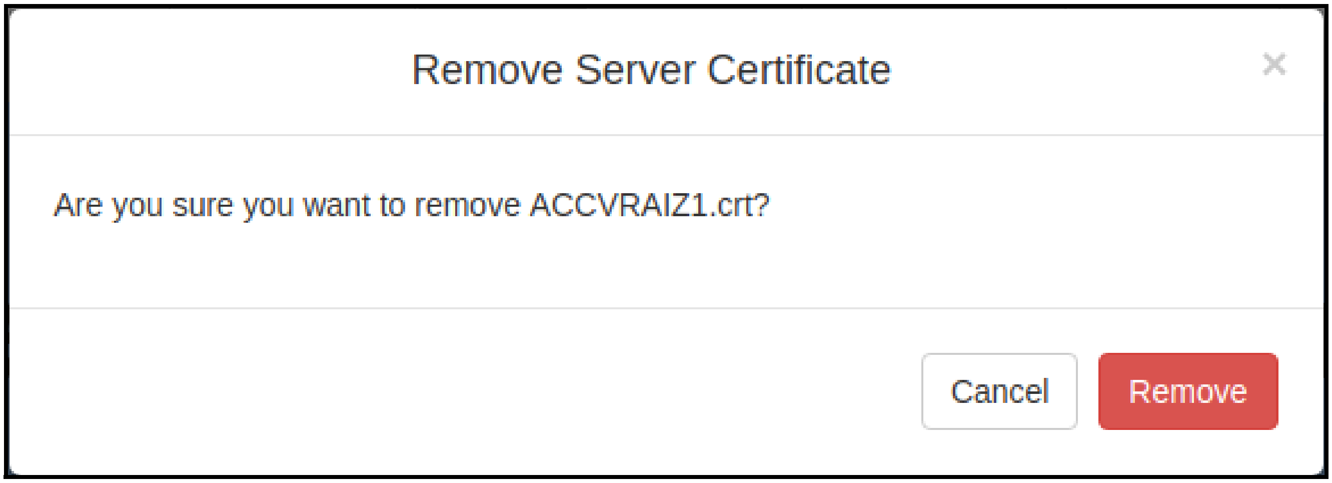


```
subject=
    commonName                   = ACCVRAIZ1
    organizationalUnitName       = PKIACCV
    organizationName             = ACCV
    countryName                  = ES
notBefore=May  5 09:37:37 2011 GMT
notAfter=Dec 31 09:37:37 2030 GMT
```

2.4.9.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See Figure 2-31.

Figure 2-31. Remove Server Certificate Window



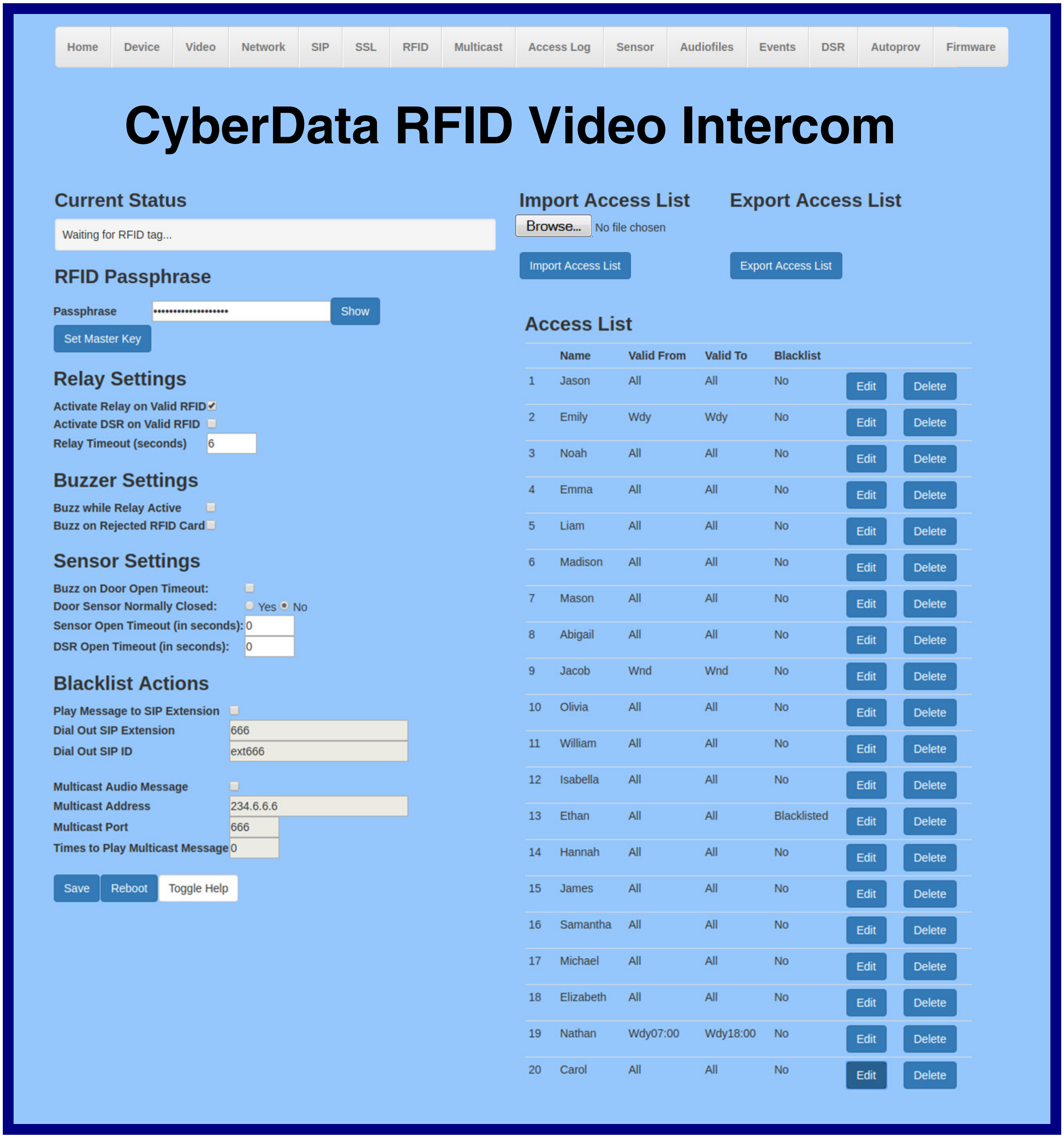
Remove Server Certificate

Are you sure you want to remove ACCVRAIZ1.crt?

2.4.10 Configure the RFID Configuration Parameters

1. Click the **RFID** menu button to open the **RFID** page (Figure 2-59).

Figure 2-32. RFID Configuration Page



CyberData RFID Video Intercom

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase ••••••••••••••••••

Relay Settings

Activate Relay on Valid RFID ☑
Activate DSR on Valid RFID ☐
Relay Timeout (seconds) 6

Buzzer Settings

Buzz while Relay Active ☐
Buzz on Rejected RFID Card ☐

Sensor Settings

Buzz on Door Open Timeout: ☐
Door Sensor Normally Closed: ○ Yes ● No
Sensor Open Timeout (in seconds): 0
DSR Open Timeout (in seconds): 0

Blacklist Actions

Play Message to SIP Extension ☐
Dial Out SIP Extension 666
Dial Out SIP ID ext666

Multicast Audio Message ☐
Multicast Address 234.6.6.6
Multicast Port 666
Times to Play Multicast Message 0

Import Access List

No file chosen

Export Access List

Access List

	Name	Valid From	Valid To	Blacklist
1	Jason	All	All	No
2	Emily	Wdy	Wdy	No
3	Noah	All	All	No
4	Emma	All	All	No
5	Liam	All	All	No
6	Madison	All	All	No
7	Mason	All	All	No
8	Abigail	All	All	No
9	Jacob	Wnd	Wnd	No
10	Olivia	All	All	No
11	William	All	All	No
12	Isabella	All	All	No
13	Ethan	All	All	Blacklisted
14	Hannah	All	All	No
15	James	All	All	No
16	Samantha	All	All	No
17	Michael	All	All	No
18	Elizabeth	All	All	No
19	Nathan	Wdy07:00	Wdy18:00	No
20	Carol	All	All	No

2. On the **RFID** page, enter values for the parameters indicated in Table 2-17.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-14. RFID Page Parameters

Web Page Item	Description
Current Status	Display the current status of the RFID reader."
RFID Passphrase	
Passphrase ?	The master password or phrase used to setup the authentication tokens for your RFID tags. Make sure to write this down!
	Shows the Master Key.
	Launches the **Set Master Key** dialog box, allowing the user to set the master key. Please note that when a master key is set, all cards programmed with the old key will be invalidated.
Relay Settings	
Activate Relay on Valid RFID ?	Activates the relay when a valid code is entered. This would likely be used to open a door.
Activate DSR on Valid RFID ?	Activates the remote relay when a valid code is entered. This would likely be used to open a door.
Relay Timeout (seconds) ?	Specifies how many seconds the relay will be activated after a valid code entry. In a typical use case, this would specify how long the door is unlocked.
Buzzer Settings	
Buzz while Relay Active ?	When selected, an audible buzz will indicate the relay is active.
Buzz on Rejected RFID Card ?	When selected, a pattern will play on the buzzer to indicate an invalid code was entered.
Sensor Settings	
Buzz on Door Open Timeout ?	When selected, the buzzer will beep until the on-board door sensor is deactivated.
Door Sensor Normally Closed ?	Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block. See the Operations Guide for more information.
Sensor Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits.
DSR Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the remote (DSR) door sensor is activated. The action(s) performed are based on the configured Remote Door Sensor Settings below.
Blacklist Settings	
Play Message to SIP Extension ?	When selected, the device will make a SIP call and play the "blacklist" audio file when a blacklisted code is entered.

Table 2-14. RFID Page Parameters (continued)

Web Page Item	**Description**
Dial Out SIP Extension ?	The extension that will be dialed if "Play Mesage to SIP Extension" is selected above. Enter up to 64 alphanumeric characters.
Dial Out SIP ID ?	Additional caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Multicast Audio Message ?	When selected, the device will multicast the "blacklist" audio file to the specified address and port.
Multicast Address ?	The multicast address that the "blacklist" audio file will be played to.
Multicast Port ?	The multicast port that the "blacklist" audio file will be played to.
Times to Play Multicast Message ?	The number of times the "blacklist" audio file will be played via multicast. Enter a value between 1 and 65535.
Import Access List ?	After selecting an access list file, click on the **Import Access List** button to import the access list from the selected file.
	Use this button to select a file to import.
	This button imports an access list that it is in .xml format.
Export Access List ?	Click on the **Export Access List** button to export the current access list to a file.
	Use this button to select a file to export.
	This button exports the list of access records in xml format.
Access List	List of Access records.
Name ?	Tag user's name.
Valid From ?	Date and time in the form "DOWHH:MM". The field must contain a three-letter string indicating the day of week, Weekday (Wdy), Weekend (Wnd), or "All". The optional time is in 24 hour format and the range is inclusive.
Valid To ?	Date and time in the form "DOWHH:MM". The field must contain a three-letter string indicating the day of week, Weekday (Wdy), Weekend (Wnd), or "All". The optional time is in 24 hour format and the range is inclusive.
Blacklist ?	Mark this tag for immediate rejection and optional blacklist alerts.
	Launches the **Configure Access Record** edit box, allowing the user to add a new record.
	Launches the **Configure Access Record** edit box, allowing the user to make changes to an existing record.
	Deletes a record.

Table 2-14. RFID Page Parameters (continued)

Web Page Item	Description
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

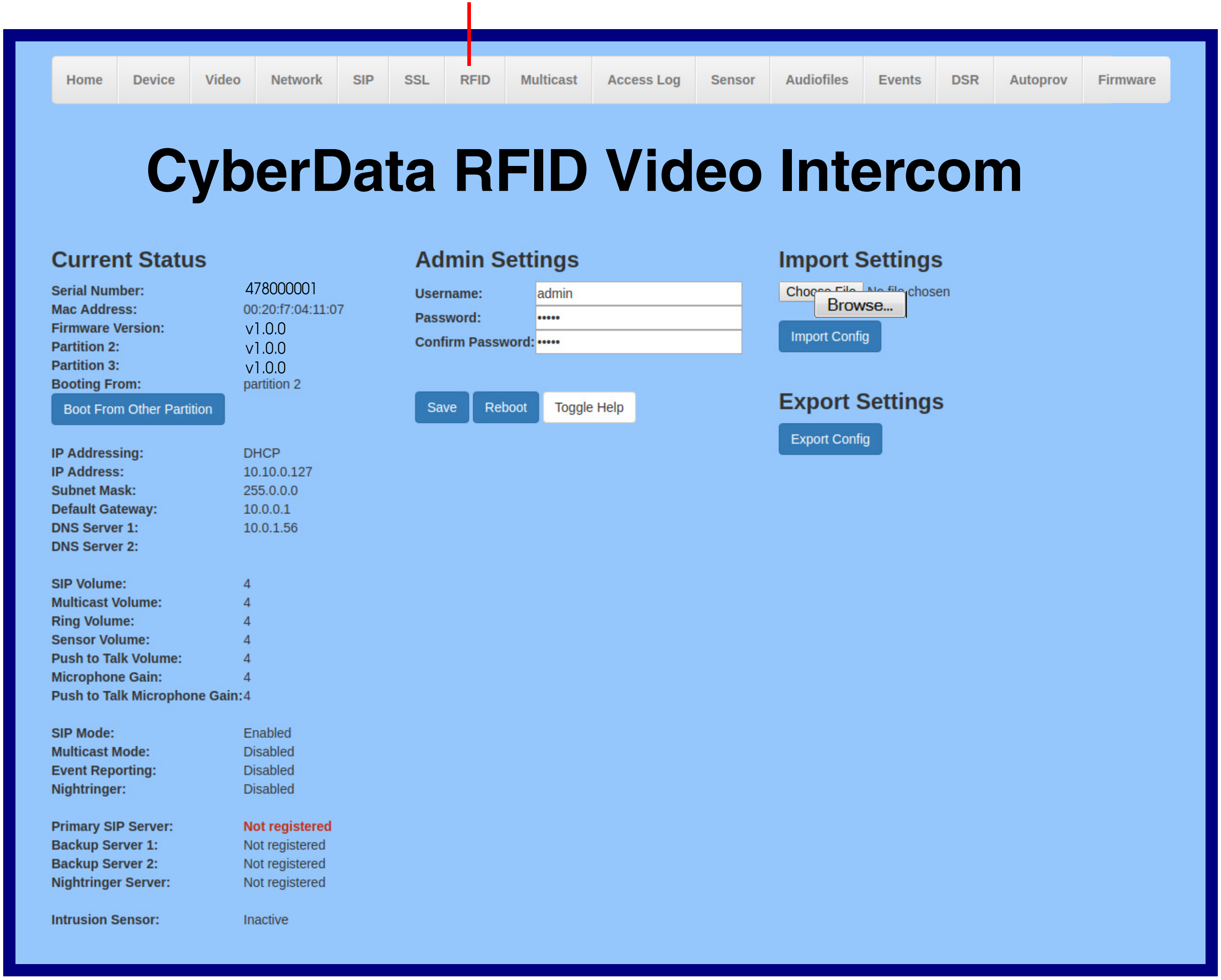
2.4.11 Enrollment Procedure

Welcome to the CyberData Keypad RFID, featuring two-factor authentication. This document illustrates the user friendly, intuitive process you will use to enroll your RFID cards and set keypad codes to enhance your security.

1. From the **Home Page** (Figure 2-33), click on the **RFID** menu button (Figure 2-33) to navigate to the **RFID** page (Figure 2-34).

Figure 2-33. From the Home Page, navigate to the RFID page

Click on the **RFID** menu button to navigate to the **RFID** page



CyberData RFID Video Intercom

Current Status

Serial Number: 478000001
Mac Address: 00:20:f7:04:11:07
Firmware Version: v1.0.0
Partition 2: v1.0.0
Partition 3: v1.0.0
Booting From: partition 2

IP Addressing: DHCP
IP Address: 10.10.0.127
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

SIP Volume: 4
Multicast Volume: 4
Ring Volume: 4
Sensor Volume: 4
Push to Talk Volume: 4
Microphone Gain: 4
Push to Talk Microphone Gain: 4

SIP Mode: Enabled
Multicast Mode: Disabled
Event Reporting: Disabled
Nightringer: Disabled

Primary SIP Server: Not registered
Backup Server 1: Not registered
Backup Server 2: Not registered
Nightringer Server: Not registered

Intrusion Sensor: Inactive

Admin Settings

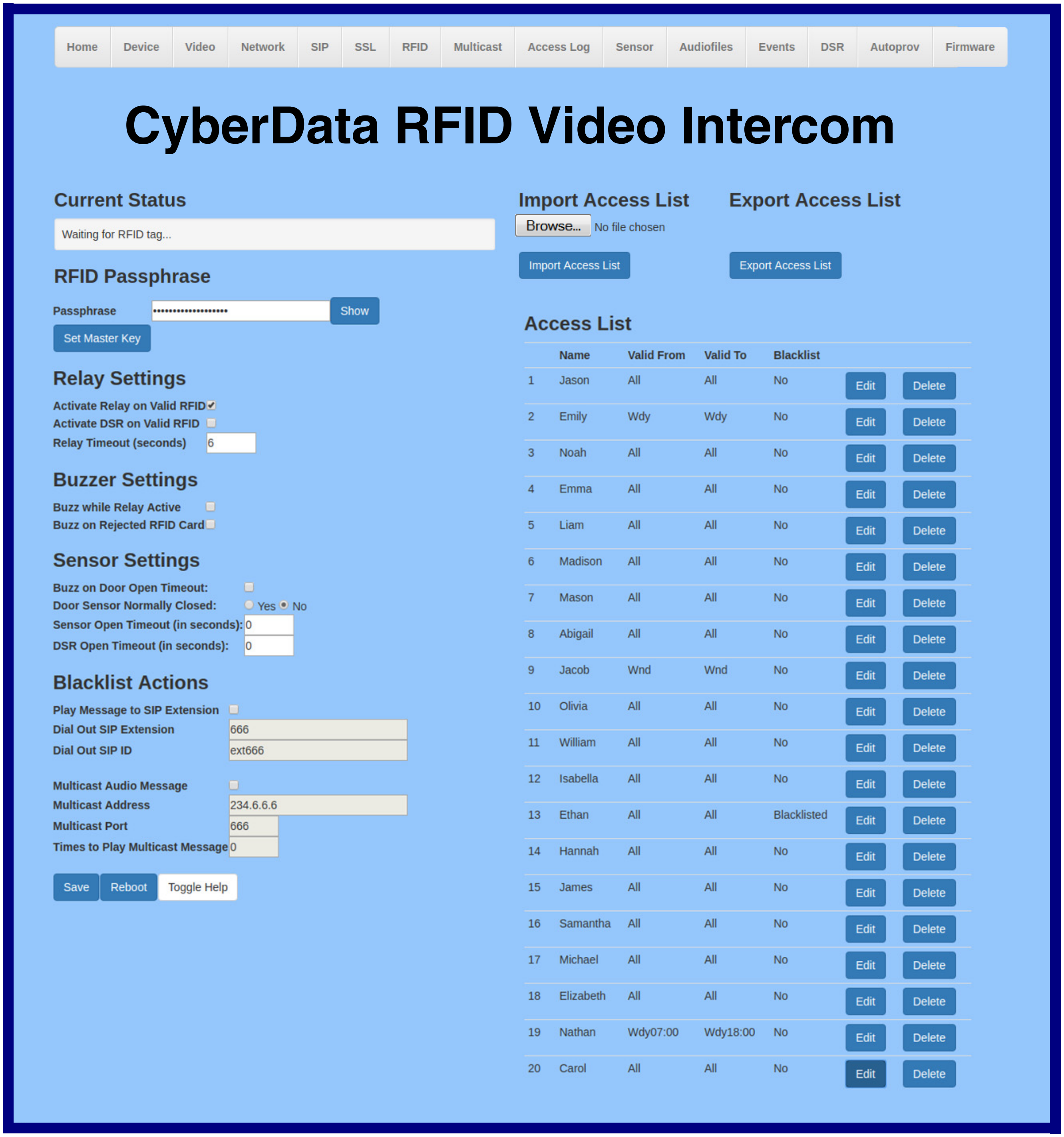
Username: admin
Password: •••••
Confirm Password: •••••

Import Settings

No file chosen

Export Settings

Figure 2-34. RFID Page



CyberData RFID Video Intercom

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase: ••••••••••••••••••

Relay Settings

Activate Relay on Valid RFID ☑
Activate DSR on Valid RFID □
Relay Timeout (seconds): 6

Buzzer Settings

Buzz while Relay Active □
Buzz on Rejected RFID Card □

Sensor Settings

Buzz on Door Open Timeout: □
Door Sensor Normally Closed: ○ Yes ● No
Sensor Open Timeout (in seconds): 0
DSR Open Timeout (in seconds): 0

Blacklist Actions

Play Message to SIP Extension □
Dial Out SIP Extension: 666
Dial Out SIP ID: ext666

Multicast Audio Message □
Multicast Address: 234.6.6.6
Multicast Port: 666
Times to Play Multicast Message: 0

Import Access List

No file chosen

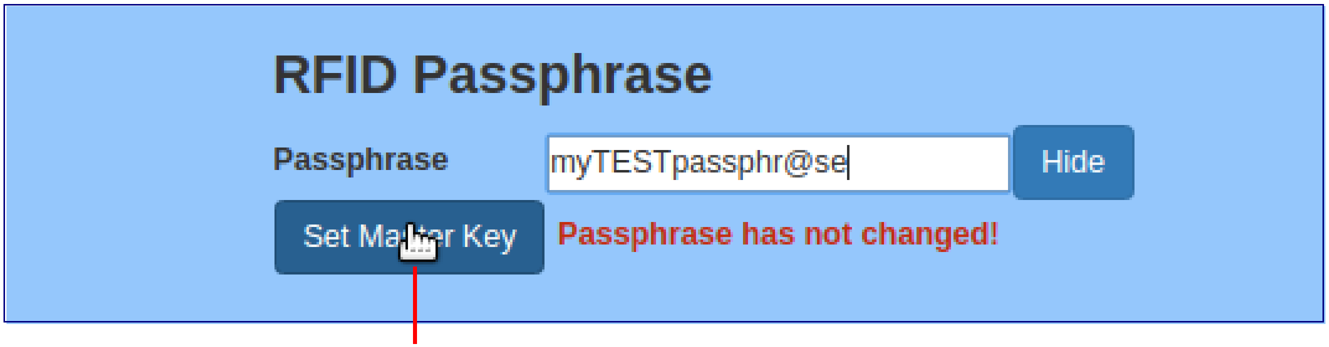
Export Access List

Access List

	Name	Valid From	Valid To	Blacklist		
1	Jason	All	All	No	Edit	Delete
2	Emily	Wdy	Wdy	No	Edit	Delete
3	Noah	All	All	No	Edit	Delete
4	Emma	All	All	No	Edit	Delete
5	Liam	All	All	No	Edit	Delete
6	Madison	All	All	No	Edit	Delete
7	Mason	All	All	No	Edit	Delete
8	Abigail	All	All	No	Edit	Delete
9	Jacob	Wnd	Wnd	No	Edit	Delete
10	Olivia	All	All	No	Edit	Delete
11	William	All	All	No	Edit	Delete
12	Isabella	All	All	No	Edit	Delete
13	Ethan	All	All	Blacklisted	Edit	Delete
14	Hannah	All	All	No	Edit	Delete
15	James	All	All	No	Edit	Delete
16	Samantha	All	All	No	Edit	Delete
17	Michael	All	All	No	Edit	Delete
18	Elizabeth	All	All	No	Edit	Delete
19	Nathan	Wdy07:00	Wdy18:00	No	Edit	Delete
20	Carol	All	All	No	Edit	Delete

2. From the **RFID** page (Figure 2-34), the user will be prompted for a Passphrase that will serve as the Master Key. Enter a passphrase (Figure 2-35), and copy it to a secure location.

Figure 2-35. Enter a passphrase



RFID Passphrase

Passphrase: myTESTpassphr@se

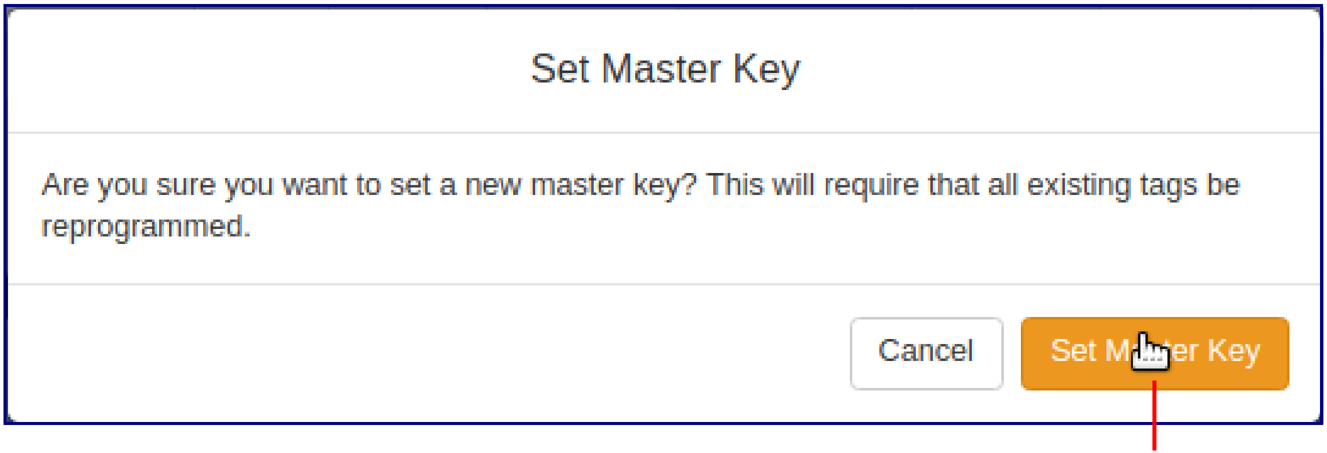
Passphrase has not changed!

Click on the **Set Master Key** button

3. When the user clicks on the **Set Master Key** button (Figure 2-35), a **Set Master Key** dialog box will appear. See Figure 2-36.

4. In the dialog box, click on the **Set Master Key** button. See Figure 2-36.

Figure 2-36. Set Master Key dialog box will appear



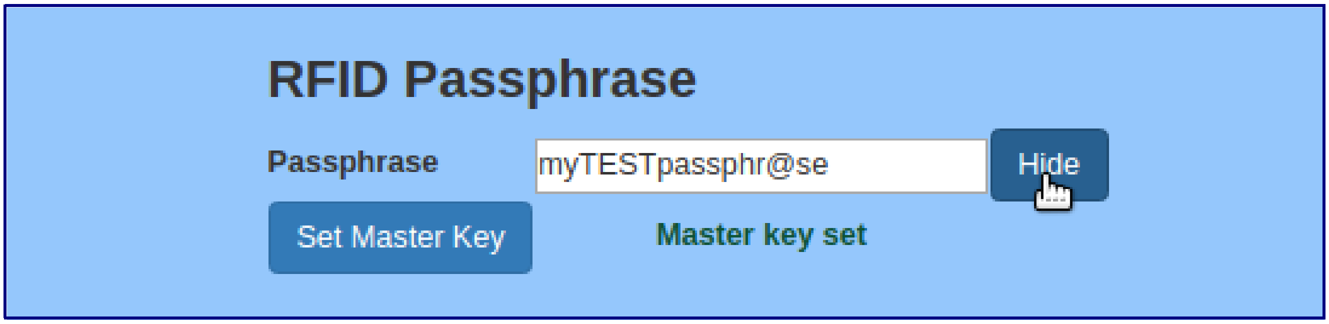
Set Master Key

Are you sure you want to set a new master key? This will require that all existing tags be reprogrammed.

Click on the **Set Master Key** button

5. The Master Key will be set. See Figure 2-37.

Figure 2-37. The Master Key will be set



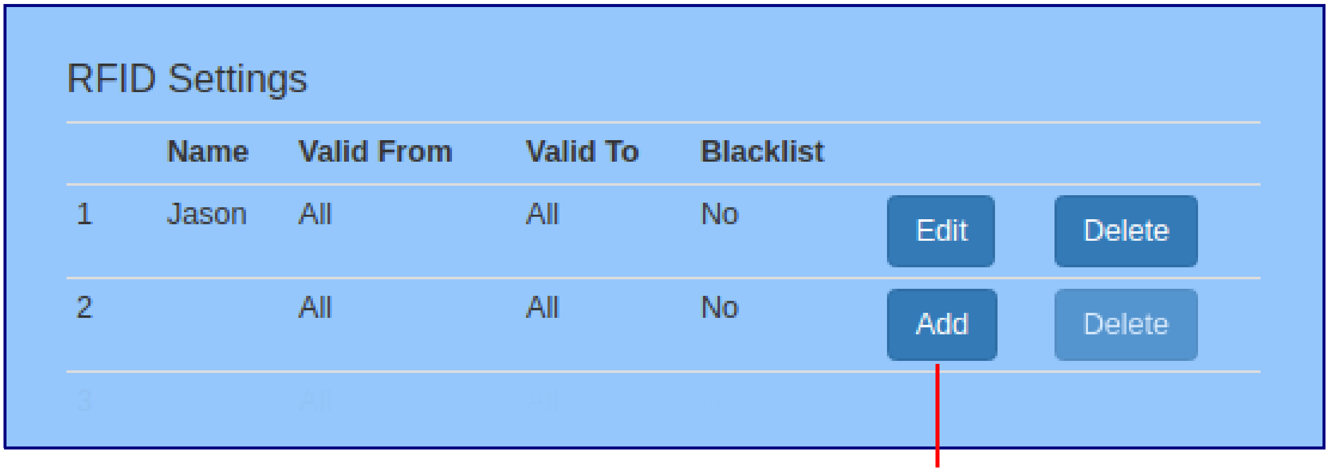
RFID Passphrase

Passphrase: myTESTpassphr@se

Master key set

6. To enroll a user, select an empty record and click on the **Add** button. See Figure 2-38.

Figure 2-38. Select an empty record and click on the Add button



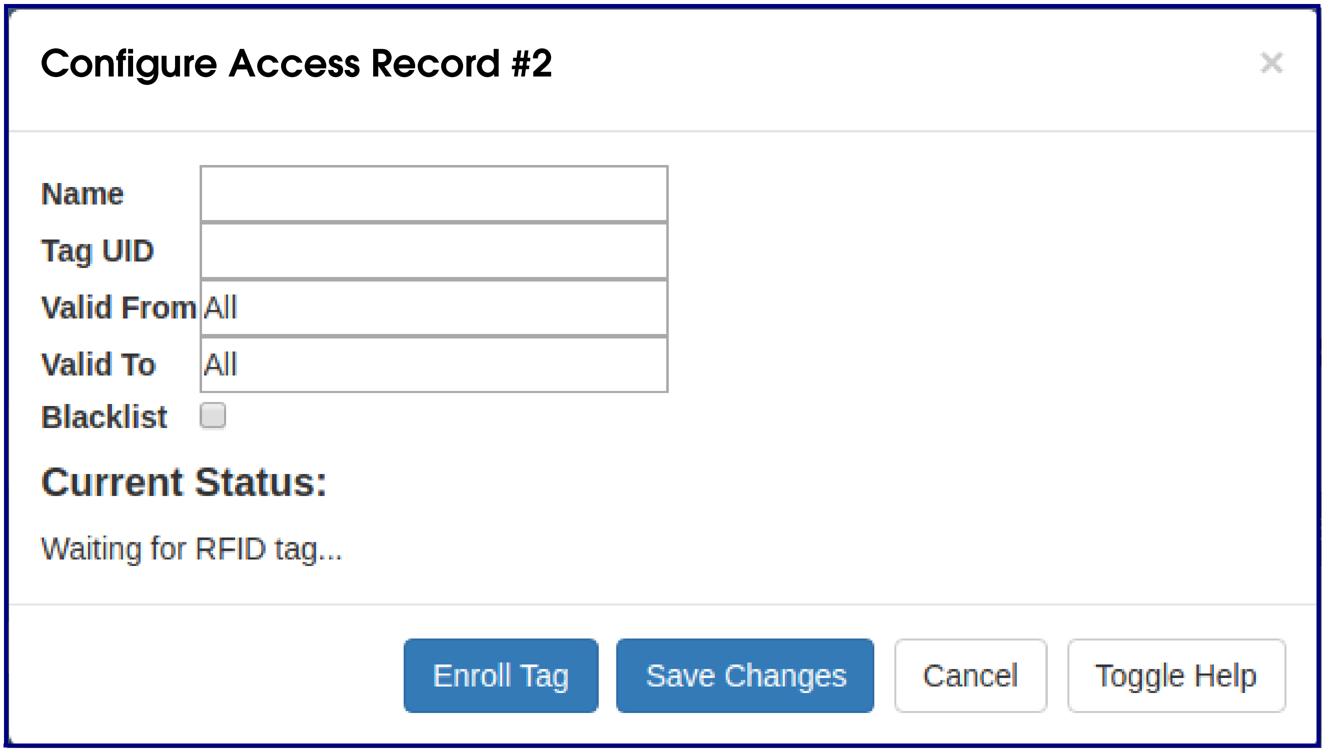
RFID Settings

	Name	Valid From	Valid To	Blacklist		
1	Jason	All	All	No	Edit	Delete
2		All	All	No	Add	Delete

Select an empty record and click on **Add** button

7. This is action will launch an edit box named **Configure Access Record #2**. See Figure 2-39.

Figure 2-39. An edit box named Configure Access Record #2



Configure Access Record #2

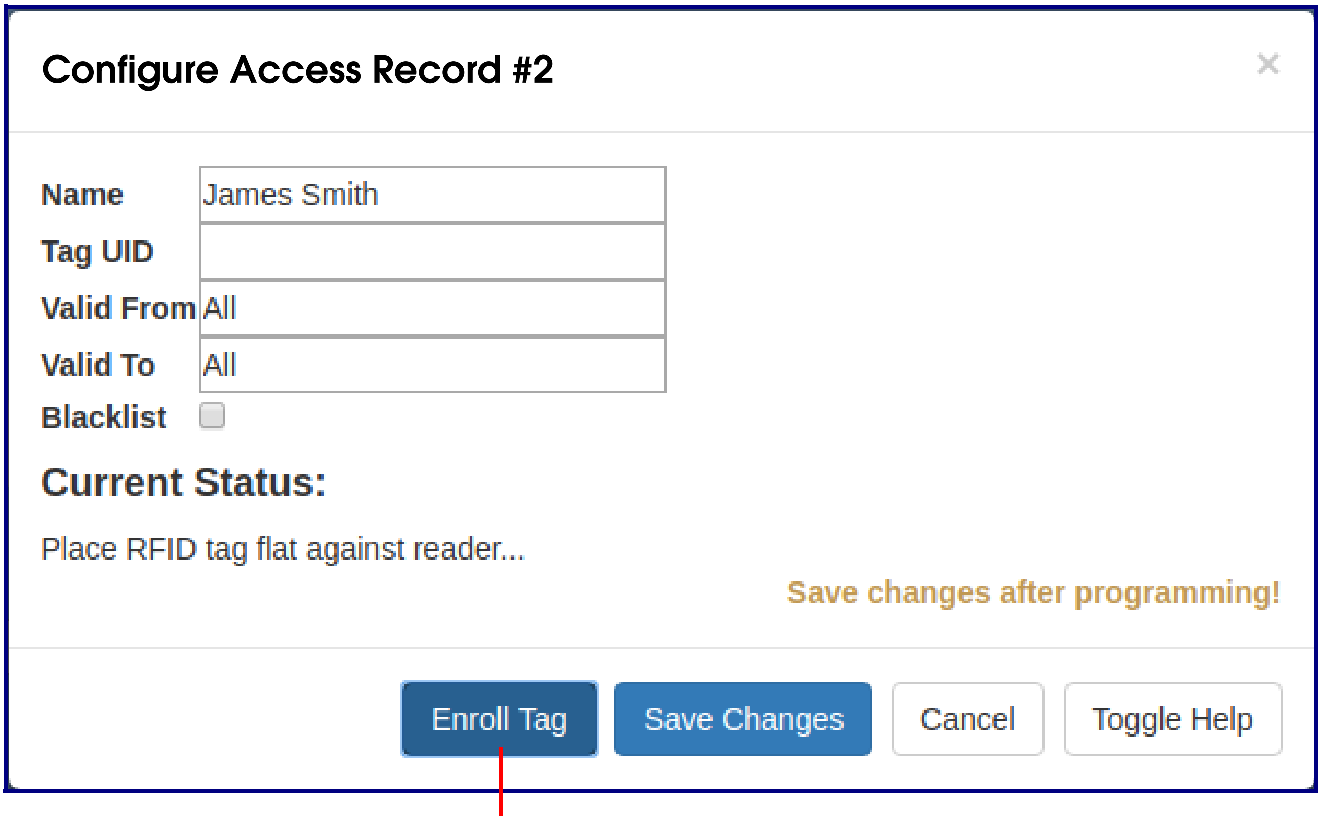
Name	
Tag UID	
Valid From	All
Valid To	All
Blacklist	□

Current Status:

Waiting for RFID tag...

8. Click on the **Enroll Tag** button, and place the card flat against the RFID reader. See Figure 2-40.

Figure 2-40. Click on the Enroll Tag button



Configure Access Record #2

Name: James Smith

Tag UID:

Valid From: All

Valid To: All

Blacklist ☐

Current Status:

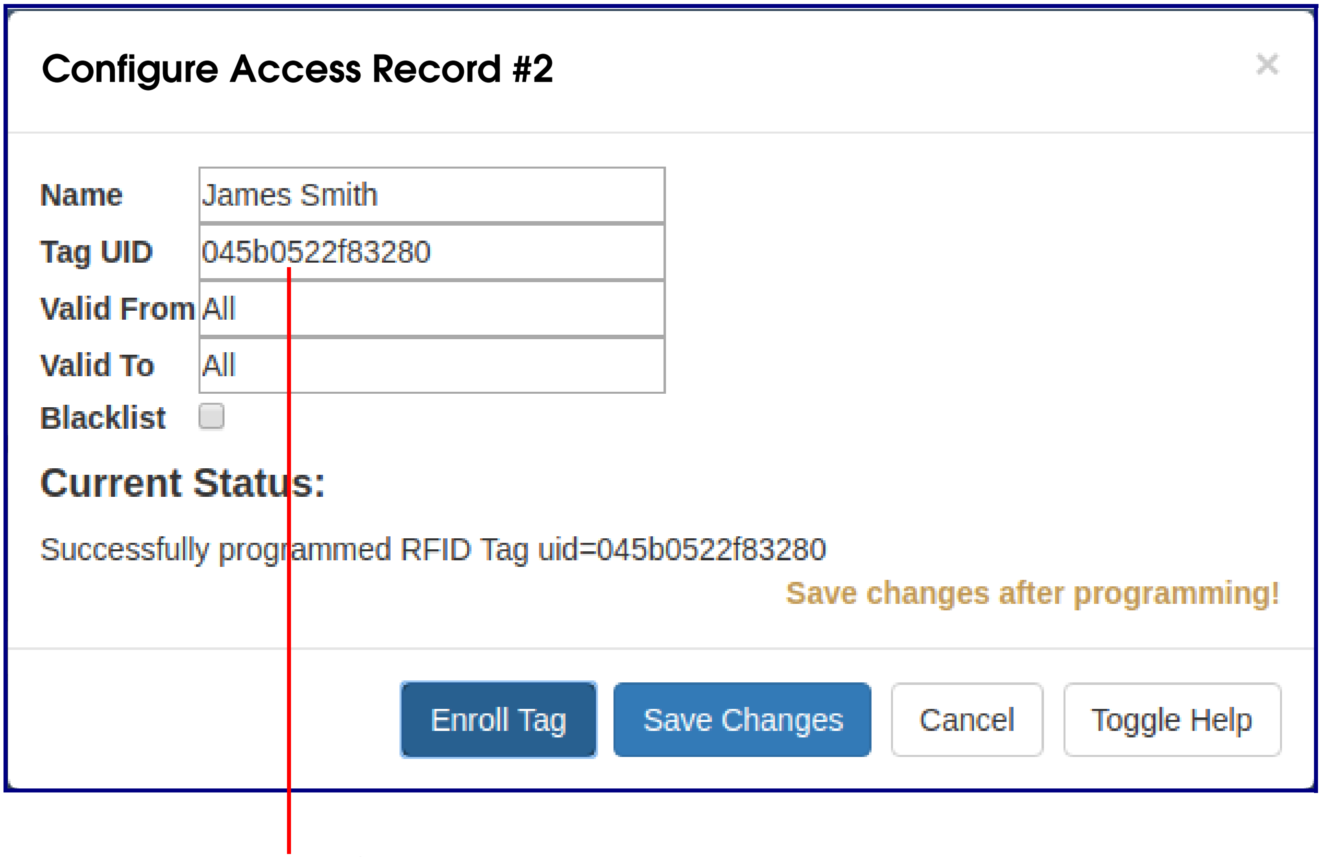
Place RFID tag flat against reader...

Save changes after programming!

Click on the **Enroll Tag** button, and place the card flat against the RFID reader.

9. The **Tag UID** field will be populated. See Figure 2-41 and Figure 2-42.

Figure 2-41. The Tag UID field will be populated



Configure Access Record #2

Name	James Smith
Tag UID	045b0522f83280
Valid From	All
Valid To	All
Blacklist	□

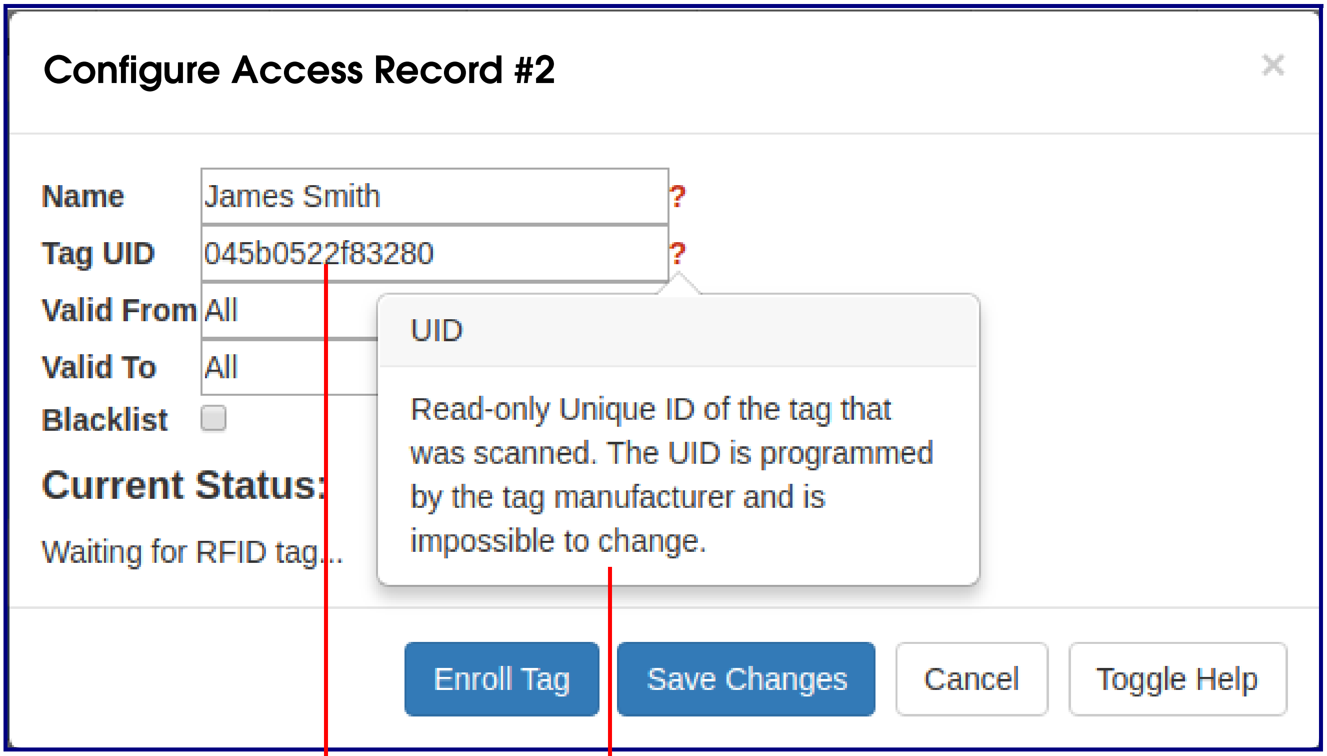
Current Status:

Successfully programmed RFID Tag uid=045b0522f83280

Save changes after programming!

The **Tag UID** field will be populated

Figure 2-42. The Tag UID field will be populated



Configure Access Record #2

Name: James Smith

Tag UID: 045b0522f83280

Valid From: All

Valid To: All

Blacklist: □

Current Status:

Waiting for RFID tag...

UID

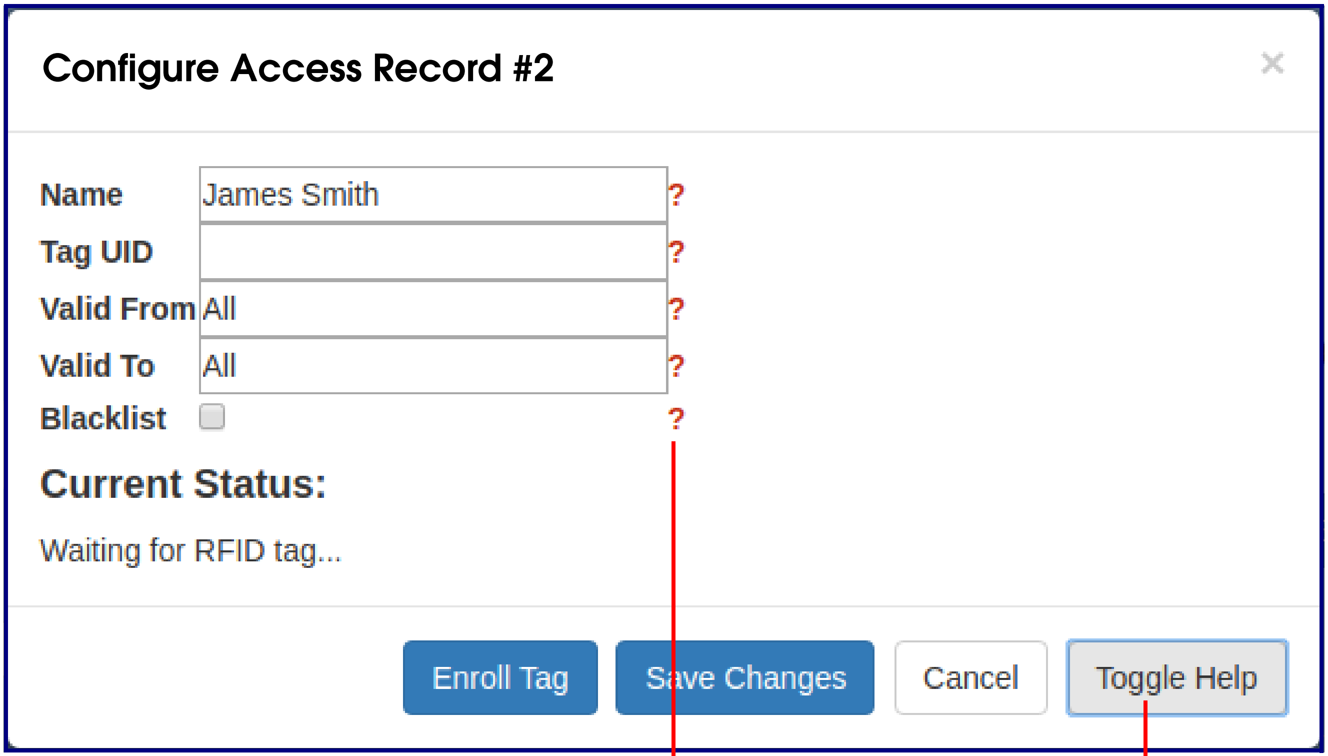
Read-only Unique ID of the tag that was scanned. The UID is programmed by the tag manufacturer and is impossible to change.

The **Tag UID** field will be populated

10. Click on the **Toggle Help** button for assistance in populating the other fields. See Figure 2-43.

11. Move the mouse pointer to hover over the question mark, and a short description of the web page item will appear.

Figure 2-43. Use the Toggle Help button for assistance in populating the other fields



Configure Access Record #2

Name	James Smith
Tag UID	
Valid From	All
Valid To	All
Blacklist	□

Current Status:

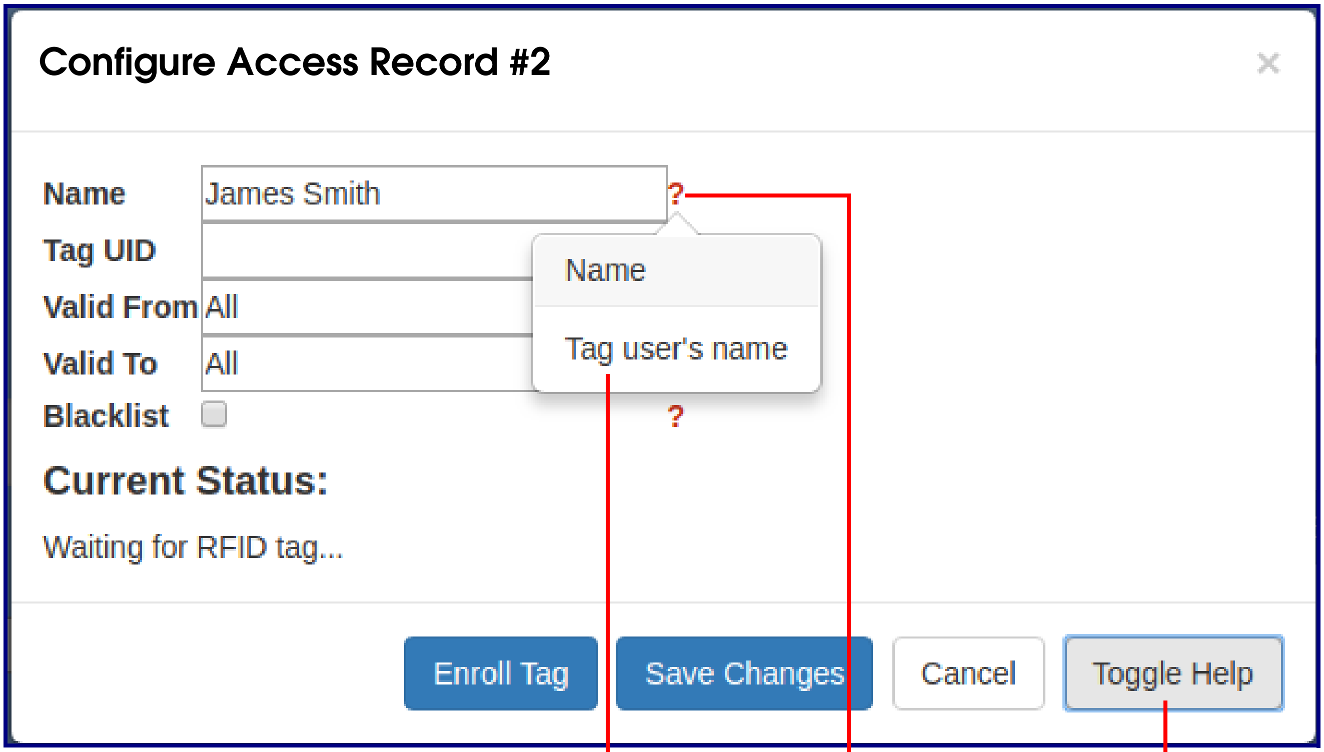
Waiting for RFID tag...

Move the mouse pointer to hover over the question mark, and a short description of the web page item will appear.

Use the **Toggle Help** button for assistance in populating the other fields.

12. Click on the **Toggle Help** button for assistance in populating the **Name** field. See Figure 2-44.

Figure 2-44. Click on the Toggle Help button for assistance in populating the Name fields



Configure Access Record #2

Name: James Smith

Tag UID:

Valid From: All

Valid To: All

Blacklist: □

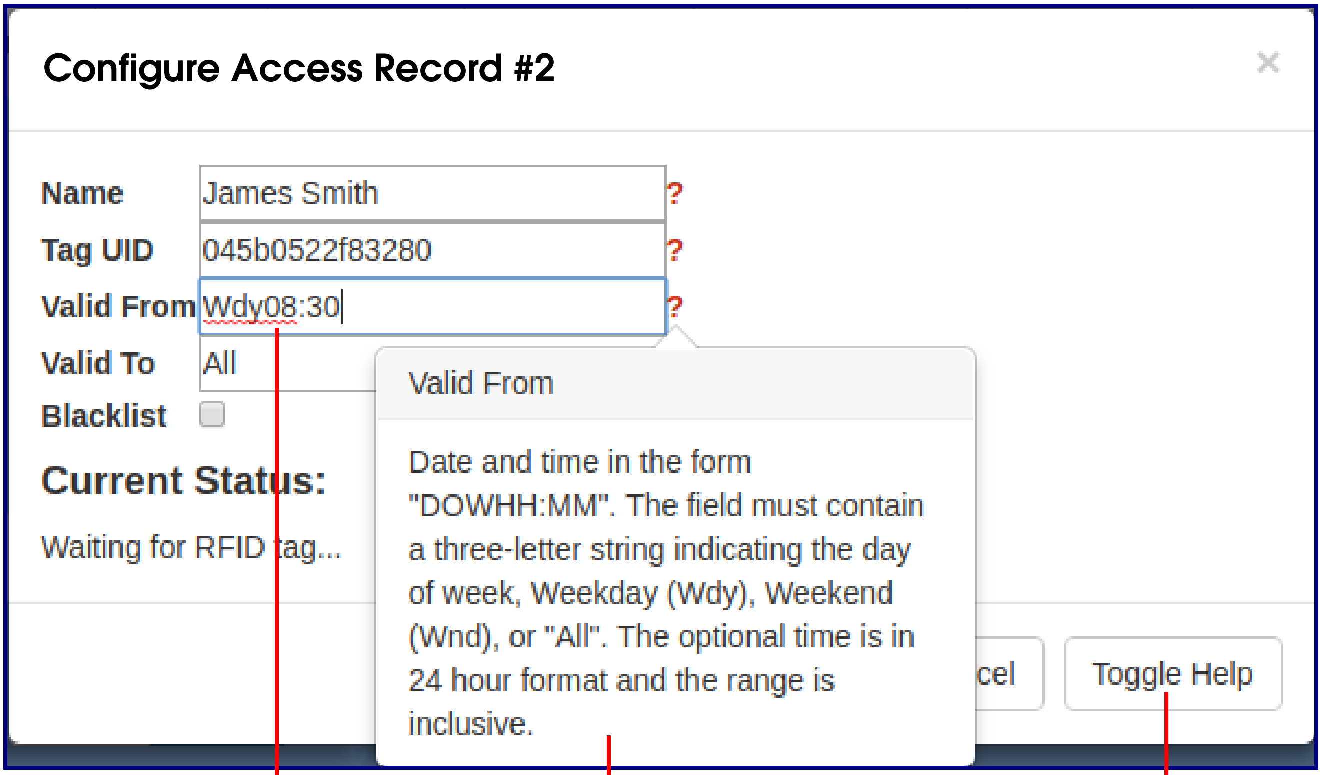
Current Status:

Waiting for RFID tag...

For assistance in populating the **Name** field, click on the **Toggle Help** button.

13. Use the **Toggle Help** button for assistance in populating the **Valid From** field. See Figure 2-45.

Figure 2-45. Use the Toggle Help button for assistance in populating the Valid From field



Configure Access Record #2

Name	James Smith
Tag UID	045b0522f83280
Valid From	Wdy08:30
Valid To	All
Blacklist	□

Current Status:

Waiting for RFID tag...

Valid From

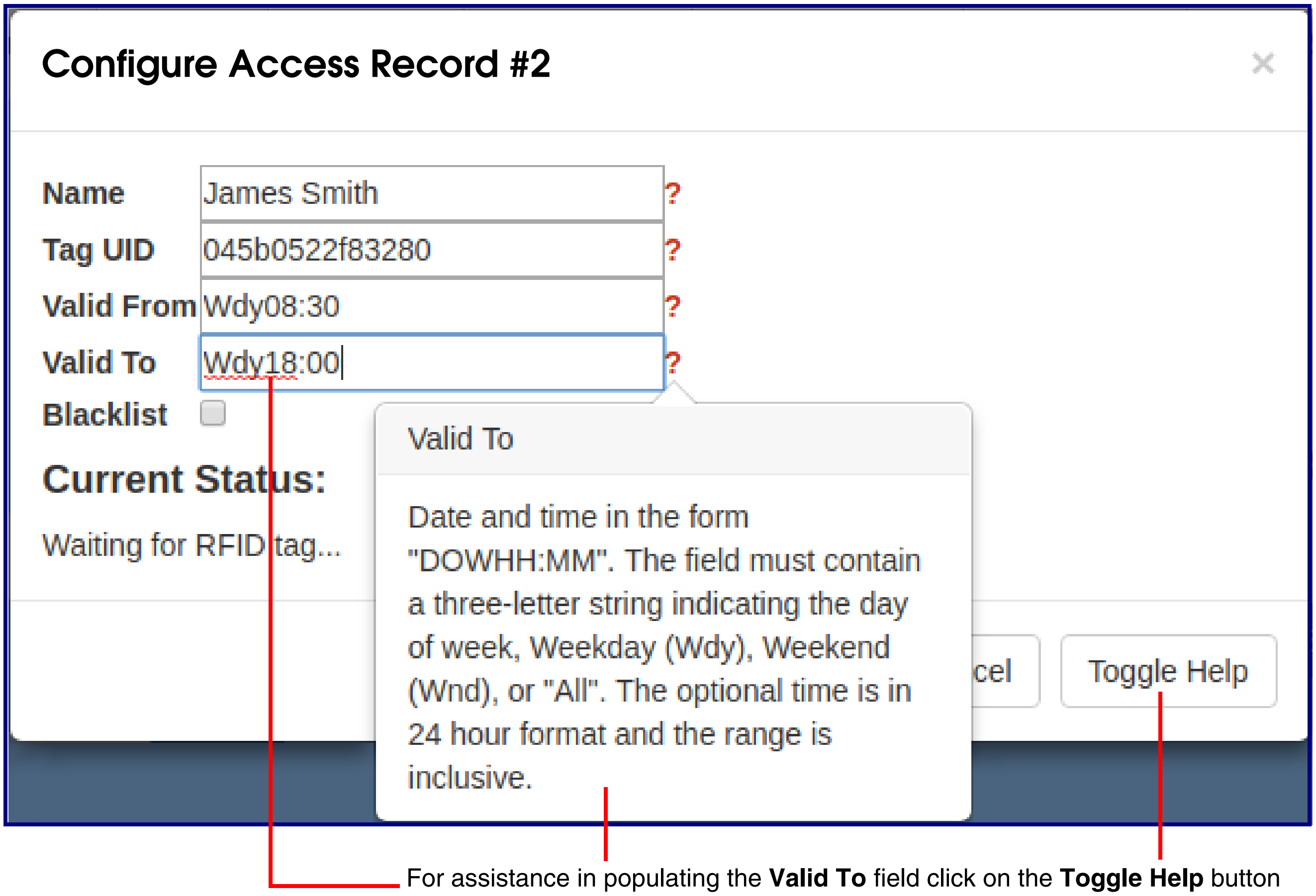
Date and time in the form "DOWHH:MM". The field must contain a three-letter string indicating the day of week, Weekday (Wdy), Weekend (Wnd), or "All". The optional time is in 24 hour format and the range is inclusive.

For assistance in populating the **Valid From** field, click on the **Toggle Help** button

14. Use the **Toggle Help** button for assistance in populating the **Valid To** field. See Figure 2-46.

Note The **Enable NTP** setting on the **Device** page must be selected to limit the times valid for the RFID tags.

Figure 2-46. Use the Toggle Help button for assistance in populating the Valid To field



Configure Access Record #2

Name: James Smith

Tag UID: 045b0522f83280

Valid From: Wdy08:30

Valid To: Wdy18:00

Blacklist: □

Current Status:

Waiting for RFID tag...

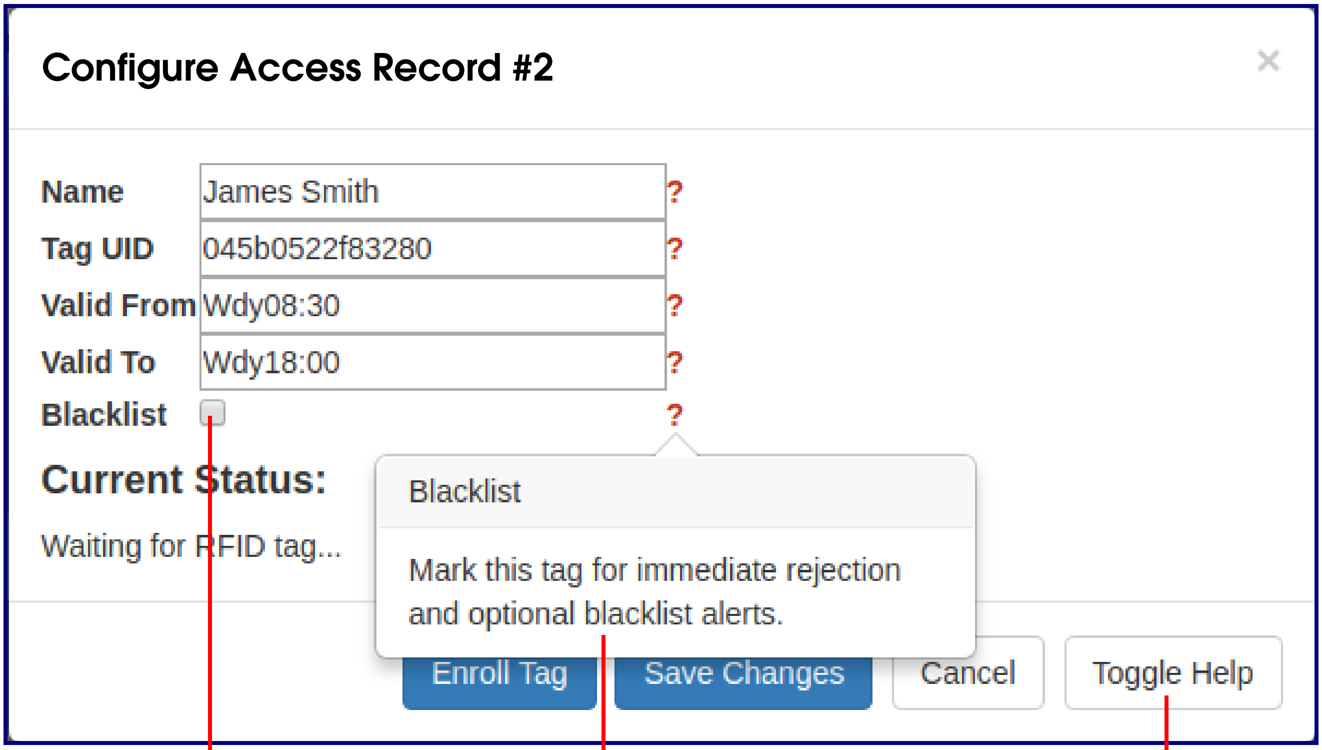
Valid To

Date and time in the form "DOWHH:MM". The field must contain a three-letter string indicating the day of week, Weekday (Wdy), Weekend (Wnd), or "All". The optional time is in 24 hour format and the range is inclusive.

For assistance in populating the **Valid To** field click on the **Toggle Help** button

15. Click on the **Toggle Help** button for assistance in populating the **Blacklist** check box. See Figure 2-47.

Figure 2-47. Click on the Toggle Help button for assistance in populating the Blacklist check box



Configure Access Record #2

Name: James Smith

Tag UID: 045b0522f83280

Valid From: Wdy08:30

Valid To: Wdy18:00

Blacklist □

Current Status:

Waiting for RFID tag...

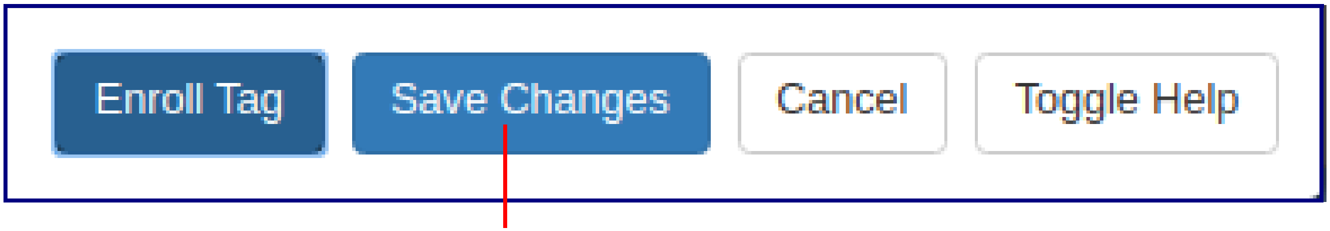
Blacklist

Mark this tag for immediate rejection and optional blacklist alerts.

For assistance in populating the **Blacklist** check box, click on the **Toggle Help** button

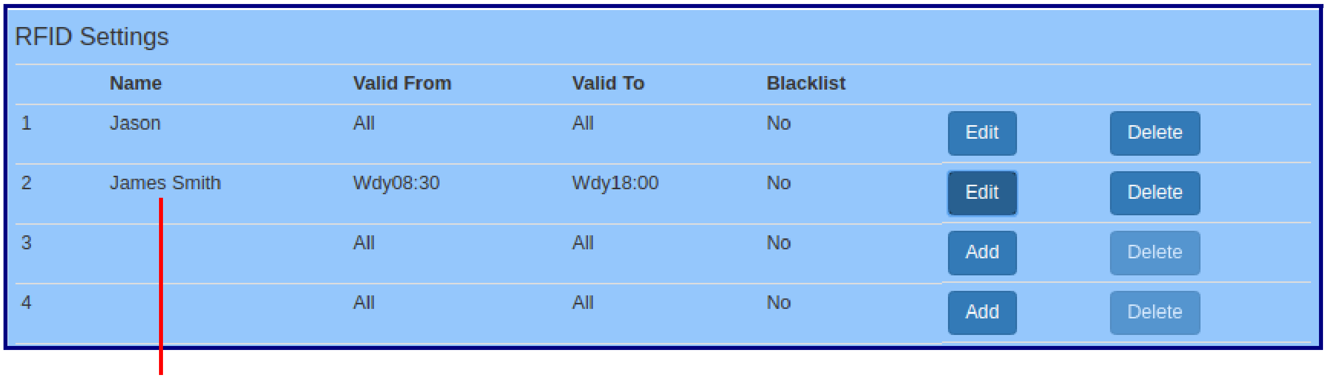
16. Click on the **Save Changes** button (Figure 2-48), and your record will appear in the web page list. See Figure 2-49.

Figure 2-48. Click on the Save Changes button



Click on the **Save Changes** button

Figure 2-49. Your record will appear in the web page list



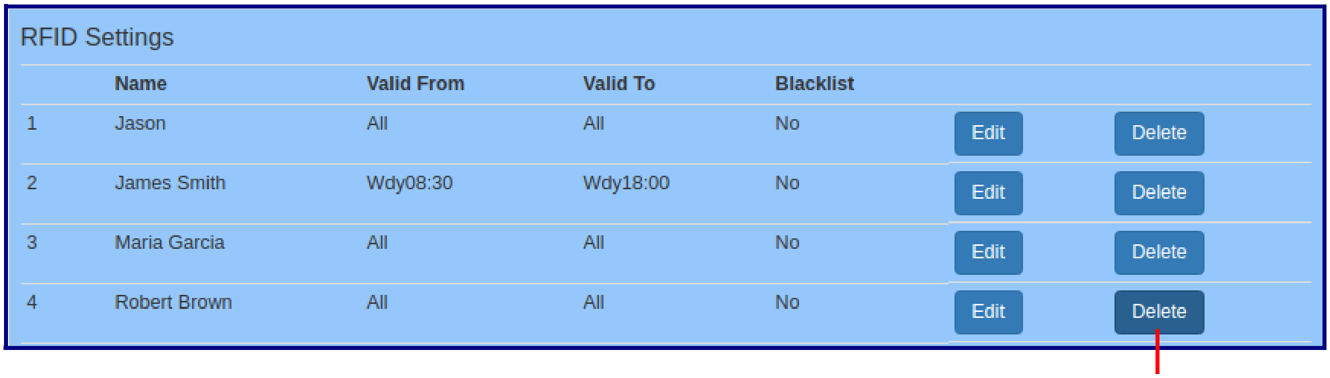
RFID Settings

	Name	Valid From	Valid To	Blacklist		
1	Jason	All	All	No	Edit	Delete
2	James Smith	Wdy08:30	Wdy18:00	No	Edit	Delete
3		All	All	No	Add	Delete
4		All	All	No	Add	Delete

Your record will appear in the web page list

17. To delete a record, click on the **Delete** button. See Figure 2-50.

Figure 2-50. To delete a record, select the Delete button



RFID Settings

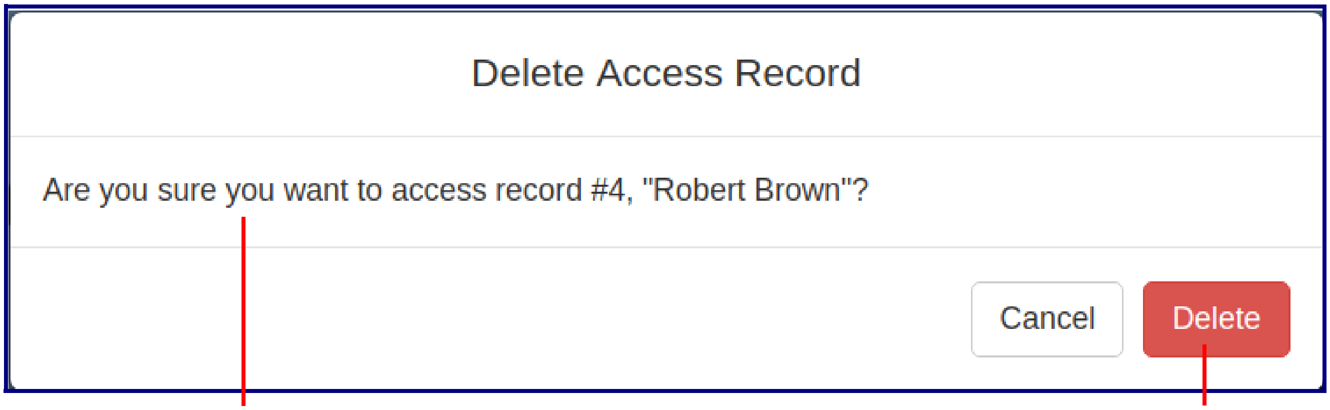
	Name	Valid From	Valid To	Blacklist		
1	Jason	All	All	No	Edit	Delete
2	James Smith	Wdy08:30	Wdy18:00	No	Edit	Delete
3	Maria Garcia	All	All	No	Edit	Delete
4	Robert Brown	All	All	No	Edit	Delete

To delete a record, click on the **Delete** button.

18. You will be prompted to delete the record. See Figure 2-51.

19. Click on the **Delete** button to confirm the deletion. See Figure 2-51.

Figure 2-51. You will be prompted to delete the record



Delete Access Record

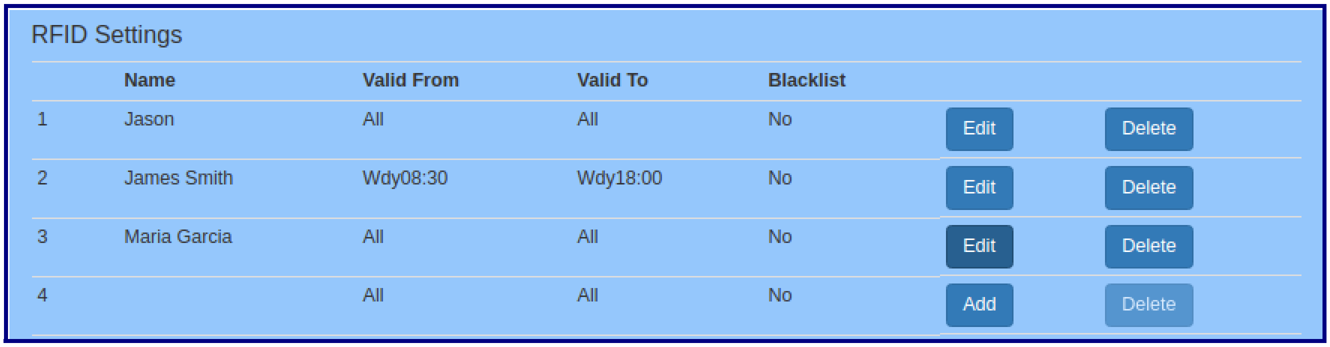
Are you sure you want to access record #4, "Robert Brown"?

You will be prompted to delete the record.

Click on the **Delete** button to confirm the deletion

20. The record will no longer appear in your settings. See Figure 2-52.

Figure 2-52. The record will no longer appear in your settings

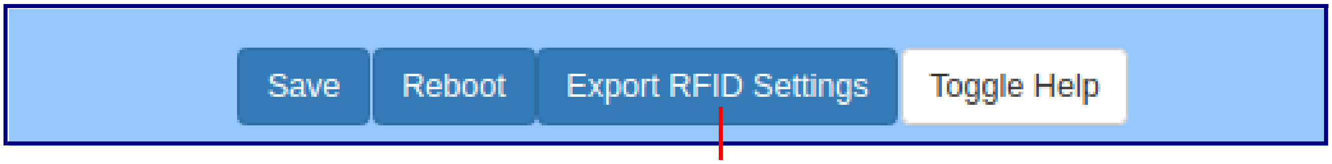


RFID Settings

	Name	Valid From	Valid To	Blacklist		
1	Jason	All	All	No	Edit	Delete
2	James Smith	Wdy08:30	Wdy18:00	No	Edit	Delete
3	Maria Garcia	All	All	No	Edit	Delete
4		All	All	No	Add	Delete

21. To export the RFID records, to provide a backup copy, or to share the enrolled tags with another device, click on the **Export RFID Settings** button. See Figure 2-53.

Figure 2-53. Click on the Export RFID Settings button

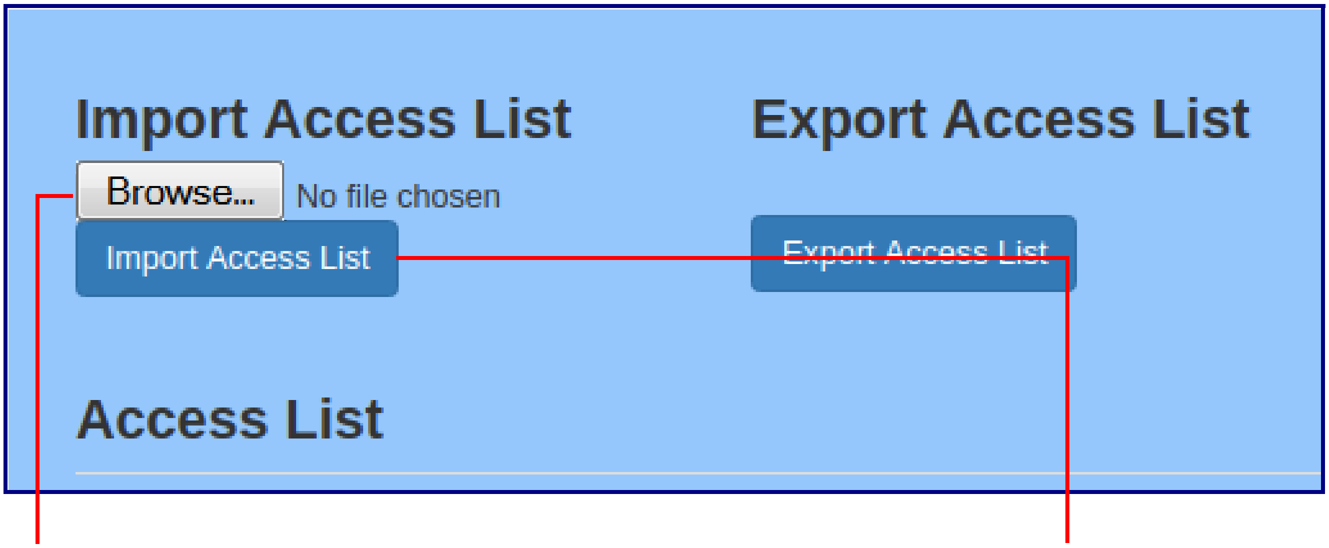


Click on the **Export RFID Settings** button

Exporting RFID will create an xml file in the directory specified in your browser's **Downloads** location. Devices that require this file may use **Import Config** setting on the **Home Page**, or use Autoprovisioning (see the Operations Guide.)

22. To share the configuration via **Import Config**, navigate to the **RFID** page of the second device, and click on the **Browse** (or **Choose File**) button to choose the Access List file. See Figure 2-54.

Figure 2-54. Click on the Browse button to choose the Access List file

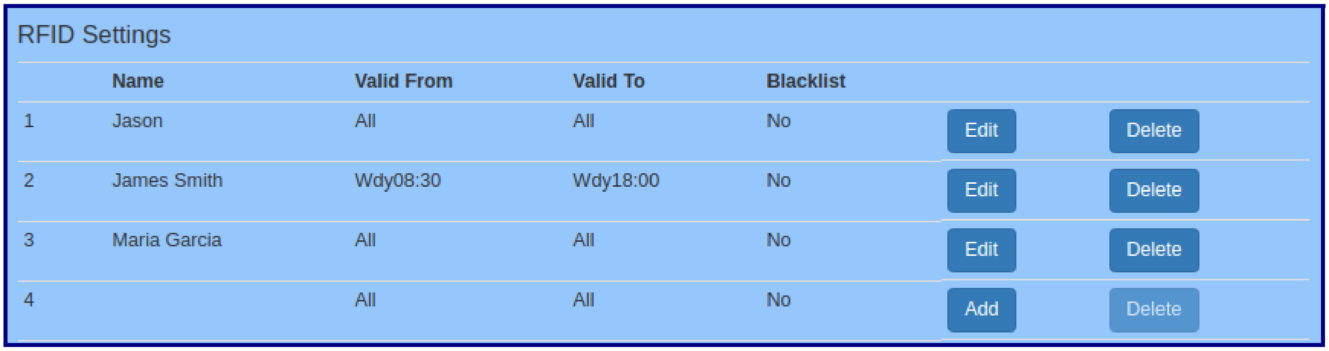


Click on the **Browse** button to choose the Access list file

Click on the **Import Access List** button to import the records

23. Click on the **Import Config** button (Figure 2-54) to import the records, and they will be added to the RFID page. See Figure 2-55.

Figure 2-55. The imported records will be added to the RFID page



RFID Settings

	Name	Valid From	Valid To	Blacklist		
1	Jason	All	All	No	Edit	Delete
2	James Smith	Wdy08:30	Wdy18:00	No	Edit	Delete
3	Maria Garcia	All	All	No	Edit	Delete
4		All	All	No	Add	Delete

2.4.12 Configure the Multicast Parameters

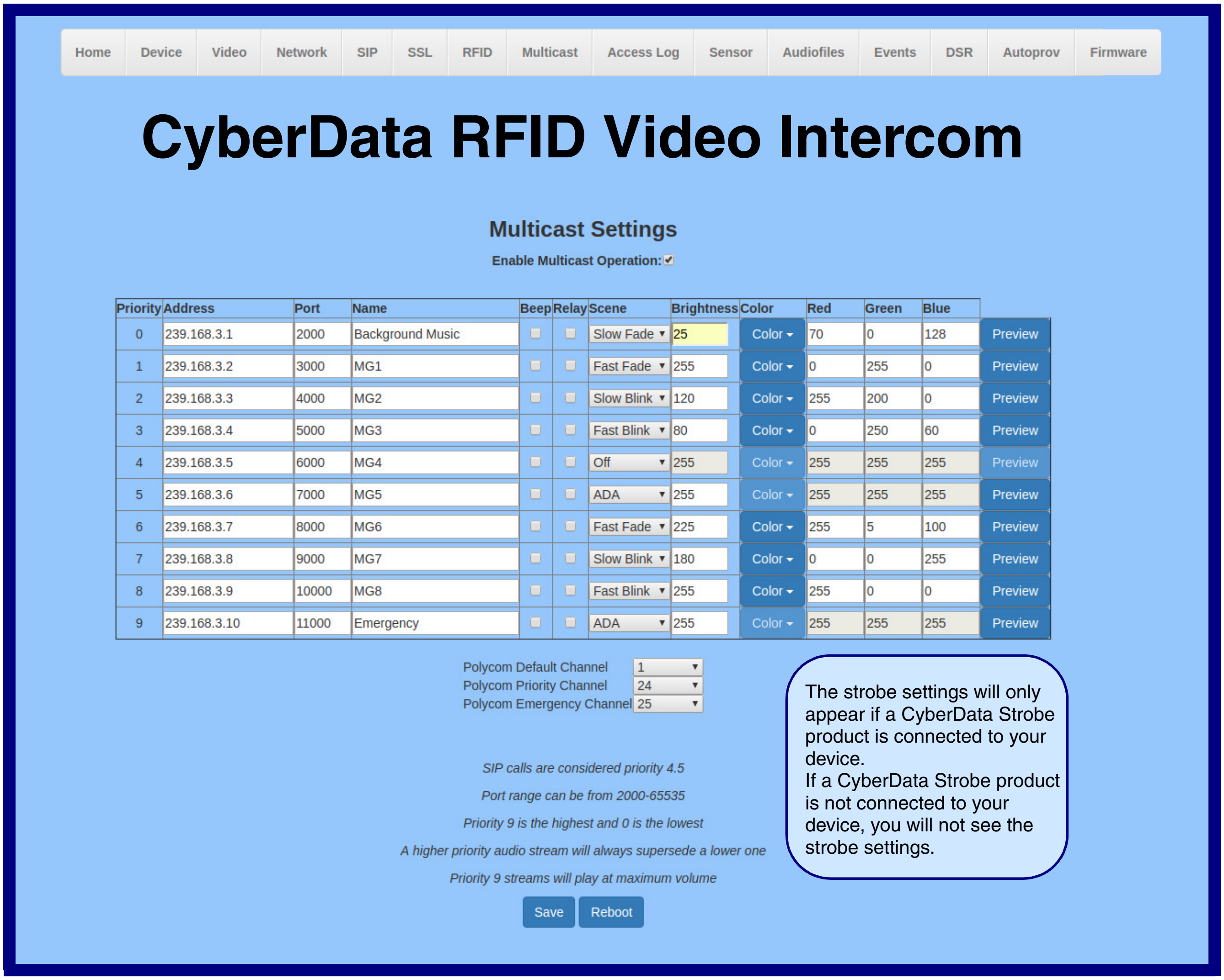
The Multicast Configuration page allows the device to join up to ten paging zones for receiving ulaw/alaw encoded RTP audio streams.

A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can be in a given paging zone. Each multicast group is defined by a multicast address and port number.

Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3. The device supports simultaneous SIP and Multicast.

1. Click on the **Multicast** menu button to open the **Multicast** page. See Figure 2-56.

Figure 2-56. Multicast Configuration Page



CyberData RFID Video Intercom

Multicast Settings

Enable Multicast Operation: ☑

Priority	Address	Port	Name	Beep	Relay	Scene	Brightness	Color	Red	Green	Blue	
0	239.168.3.1	2000	Background Music	□	□	Slow Fade	25	Color	70	0	128	Preview
1	239.168.3.2	3000	MG1	□	□	Fast Fade	255	Color	0	255	0	Preview
2	239.168.3.3	4000	MG2	□	□	Slow Blink	120	Color	255	200	0	Preview
3	239.168.3.4	5000	MG3	□	□	Fast Blink	80	Color	0	250	60	Preview
4	239.168.3.5	6000	MG4	□	□	Off	255	Color	255	255	255	Preview
5	239.168.3.6	7000	MG5	□	□	ADA	255	Color	255	255	255	Preview
6	239.168.3.7	8000	MG6	□	□	Fast Fade	225	Color	255	5	100	Preview
7	239.168.3.8	9000	MG7	□	□	Slow Blink	180	Color	0	0	255	Preview
8	239.168.3.9	10000	MG8	□	□	Fast Blink	255	Color	255	0	0	Preview
9	239.168.3.10	11000	Emergency	□	□	ADA	255	Color	255	255	255	Preview

Polycom Default Channel 1
Polycom Priority Channel 24
Polycom Emergency Channel 25

SIP calls are considered priority 4.5

Port range can be from 2000-65535

Priority 9 is the highest and 0 is the lowest

A higher priority audio stream will always supersede a lower one

Priority 9 streams will play at maximum volume

The strobe settings will only appear if a CyberData Strobe product is connected to your device.
If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.

2. On the **Multicast** page, enter values for the parameters indicated in Table 2-15.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-15. Multicast Page Parameters

Web Page Item	**Description**
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). SIP calls are considered priority **4.5**. See Section 2.4.12.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Beep	When selected, the device will play a beep before multicast audio is sent.
Relay	When selected, the device will activate a relay before multicast audio is sent.
Scene ?	Select desired scene (only one may be chosen). **Note: The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.**
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.

Table 2-15. Multicast Page Parameters (continued)

Web Page Item	Description
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
	Use this button to preview the strobe flashing behavior for the **Multicast Strobe Settings**.
	Click the **Save** button to save your configuration settings.
	Click on the **Reboot** button to reboot the system.

2.4.12.1 Assigning Priority

The device will prioritize simultaneous audio streams according to their priority in the list.

If both SIP and Multicast is enabled, SIP audio streams are considered priority **4.5**. SIP audio will interrupt multicast streams with priority **0** through **4** and will be interrupted by multicast streams with priority **5** through **9**.

During priority **9** multicast streams, the volume is set to maximum.

Note SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

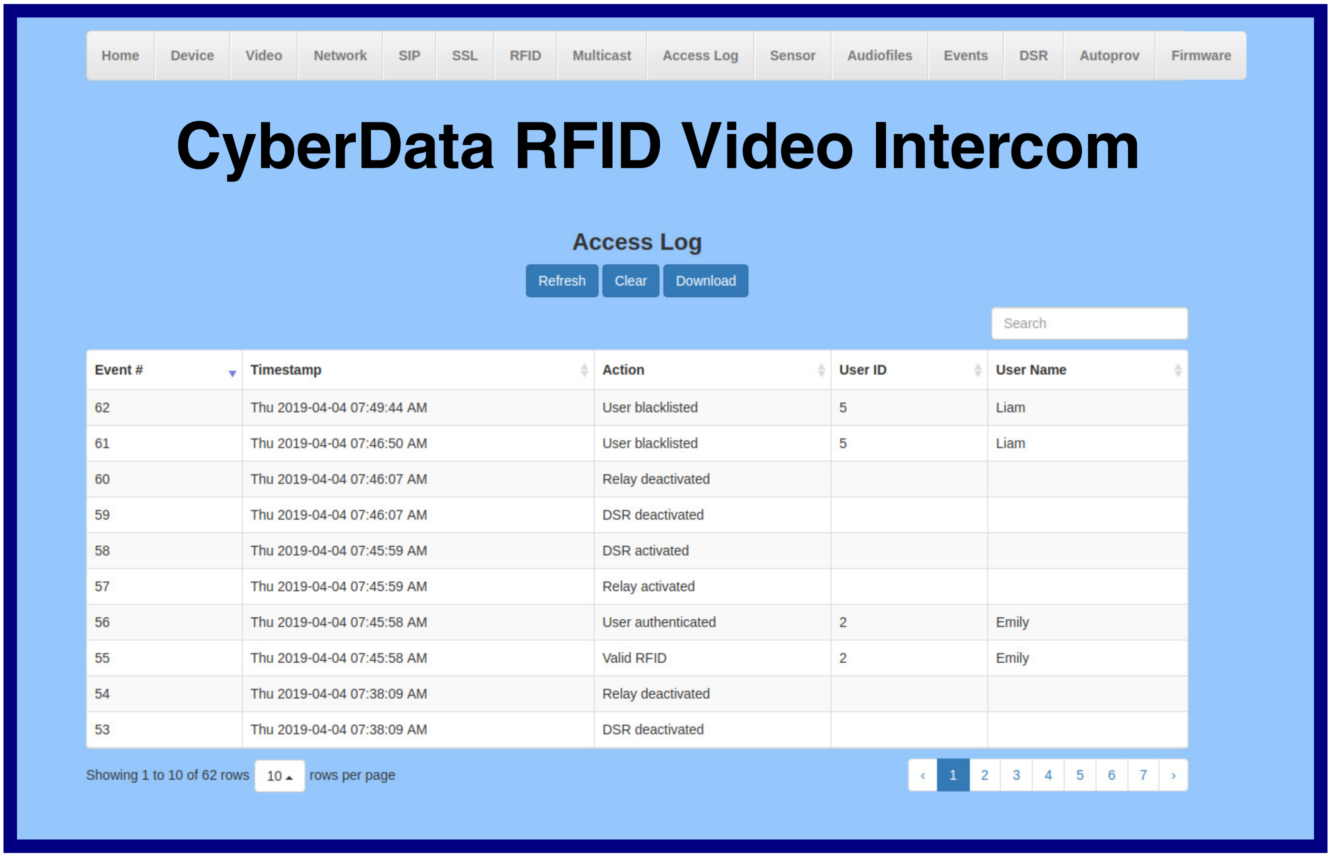
Ringtones and Nightringtones

Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

2.4.13 Configure the Access Log Parameters

1. Click the **Access Log** menu button to open the **Access Log** page (Figure 2-59).

Figure 2-57. Access Log Page



CyberData RFID Video Intercom

Access Log

Event #	Timestamp	Action	User ID	User Name
62	Thu 2019-04-04 07:49:44 AM	User blacklisted	5	Liam
61	Thu 2019-04-04 07:46:50 AM	User blacklisted	5	Liam
60	Thu 2019-04-04 07:46:07 AM	Relay deactivated		
59	Thu 2019-04-04 07:46:07 AM	DSR deactivated		
58	Thu 2019-04-04 07:45:59 AM	DSR activated		
57	Thu 2019-04-04 07:45:59 AM	Relay activated		
56	Thu 2019-04-04 07:45:58 AM	User authenticated	2	Emily
55	Thu 2019-04-04 07:45:58 AM	Valid RFID	2	Emily
54	Thu 2019-04-04 07:38:09 AM	Relay deactivated		
53	Thu 2019-04-04 07:38:09 AM	DSR deactivated		

Showing 1 to 10 of 62 rows 10 rows per page

2. On the **Access Log** page, enter values for the parameters indicated in Table 2-13.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

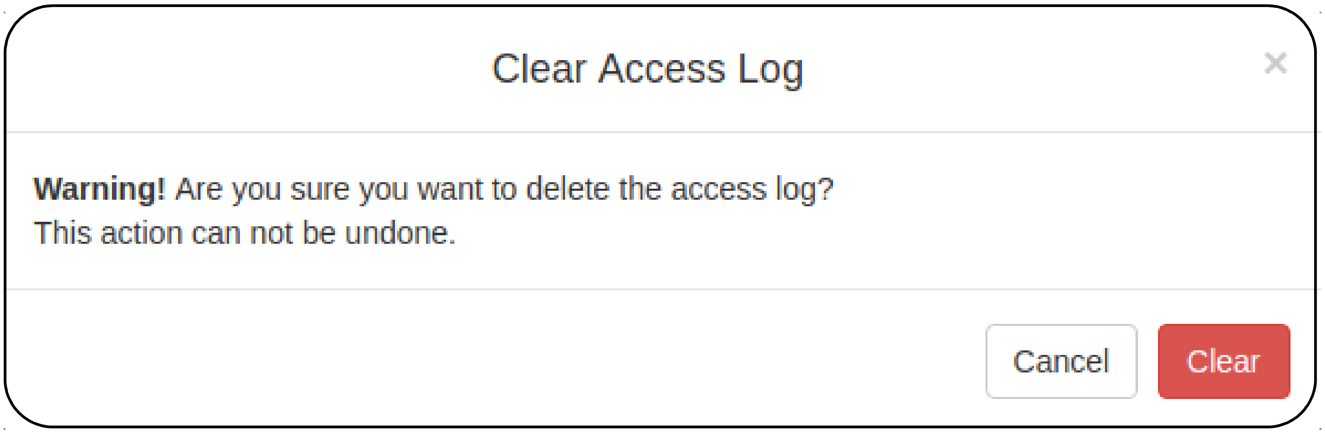
Table 2-16. Access Log Configuration Parameters

Web Page Item	Description
Access Log	
Refresh	Refresh the web page view new log entries.
Clear	Erases the log. When pressed, the **Clear Access Log Confirmation Window** appears. See Section 2.4.13.1, "Clear Access Log Confirmation Window".
Download	Downloads the access log.
Search ?	Search the access log.
Event # ?	System generated number to identify the event.
Timestamp ?	Displays the time of the event (**Day of week Year-Month-Day Hour:Minute:Seconds AM/PM**).
Action ?	Describes the event.
User ID ?	Displays the ID number of the user.
User Name ?	Displays the name of the user.

2.4.13.1 Clear Access Log Confirmation Window

The **Clear Access Log Confirmation Window** will ask if the user wants to delete the access log. This window appears after clicking on the **Clear** button. See Figure 2-58.

Figure 2-58. Clear Access Log Confirmation Window



Clear Access Log

Warning! Are you sure you want to delete the access log?
This action can not be undone.

2.4.14 Configure the Sensor Configuration Parameters

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor** page to trigger on an open or short condition on these pins. The door sensor alarm will be activated when the **Door Open Timeout** parameter has been met.

The intrusion sensor is an optical sensor installed on the Intercom board and will be activated when the Intercom is removed from the case.

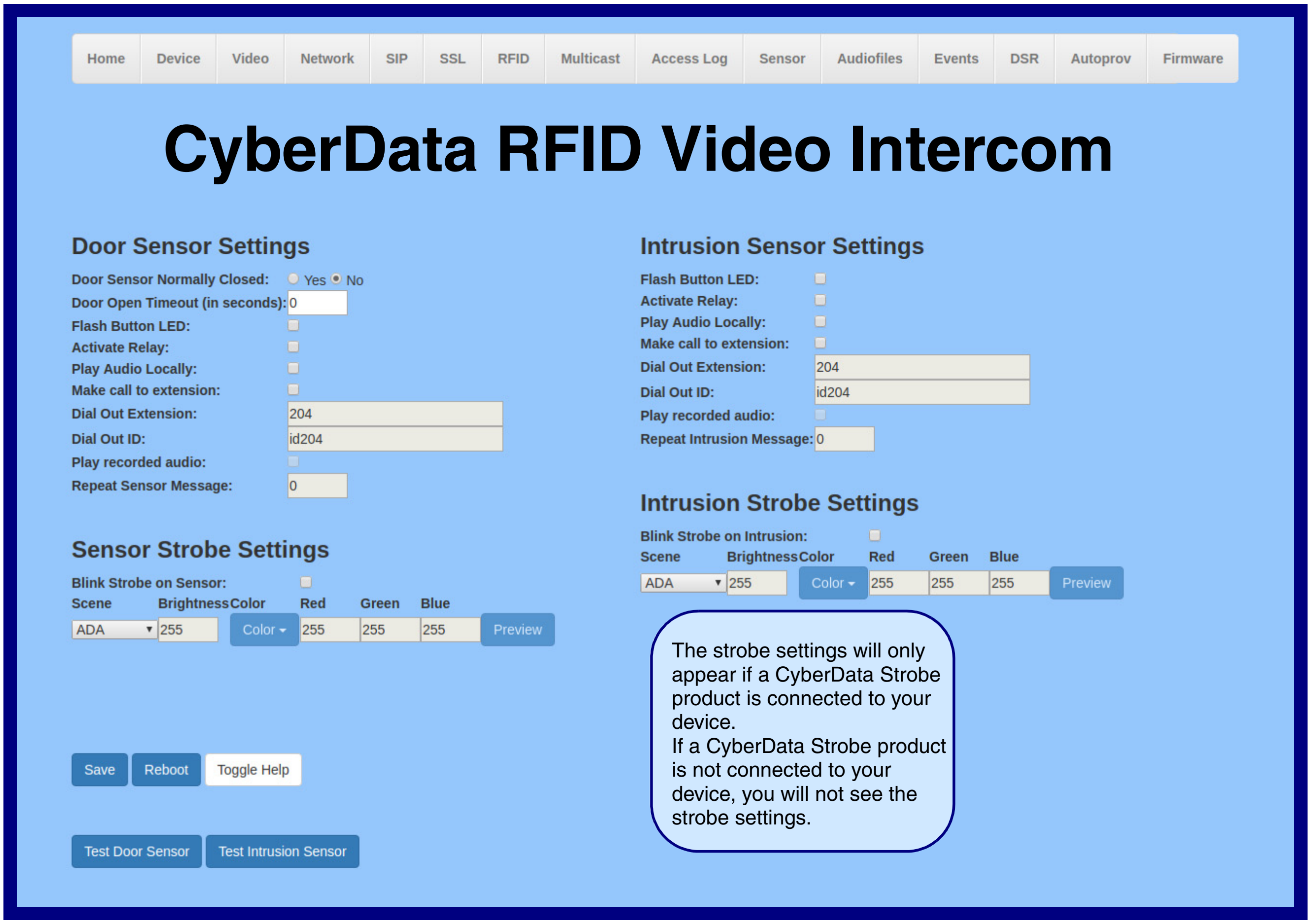
Each sensor can trigger up to five different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Loop an audio file out of the Intercom speaker until the sensor is deactivated
- Call an extension and establish two way audio
- Call an extension and play a pre-recorded audio file

Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

1. Click **Sensor** menu button to open the **Sensor** page (Figure 2-59).

Figure 2-59. Sensor Configuration Page



CyberData RFID Video Intercom

Door Sensor Settings

Door Sensor Normally Closed: ○ Yes ● No
Door Open Timeout (in seconds): 0
Flash Button LED: □
Activate Relay: □
Play Audio Locally: □
Make call to extension: □
Dial Out Extension: 204
Dial Out ID: id204
Play recorded audio: □
Repeat Sensor Message: 0

Sensor Strobe Settings

Blink Strobe on Sensor: □

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color ▾	255	255	255

Intrusion Sensor Settings

Flash Button LED: □
Activate Relay: □
Play Audio Locally: □
Make call to extension: □
Dial Out Extension: 204
Dial Out ID: id204
Play recorded audio: □
Repeat Intrusion Message: 0

Intrusion Strobe Settings

Blink Strobe on Intrusion: □

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color ▾	255	255	255

The strobe settings will only appear if a CyberData Strobe product is connected to your device.
If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.

2. On the **Sensor** page, enter values for the parameters indicated in Table 2-17.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-17. Sensor Configuration Parameters

Web Page Item	**Description**
Door Sensor Settings	
Door Sensor Normally Closed ?	Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.
Door Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits.
Flash Button LED ?	When selected, the Call button LED will flash until the on-board door sensor is deactivated (roughly 10 times/second).
Activate Relay ?	When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the door sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the on-board door sensor is activated. Use the **Dial Out Extension** field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio ?	When selected, the device will call the **Dial Out Extension** and play an audio file to the phone answering the SIP call (corresponds to **Door Ajar** on the **Audiofiles** page).
Repeat Sensor Message ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Sensor Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Sensor ?	When selected, the Strobe will blink a scene when the sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.

Table 2-17. Sensor Configuration Parameters (continued)

Web Page Item	Description
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for the Sensor.
Green ?	The green LED value for the Sensor.
Blue ?	The blue LED value for the Sensor.
	Use this button to preview the strobe flashing behavior for the **Sensor Strobe Settings**.
Intrusion Sensor Settings	
Flash Button LED ?	When selected, the Call button LED will flash until the intrusion sensor is deactivated (roughly 10 times/second).
Activate Relay ?	When selected, the device's on-board relay will be activated until the intrusion sensor is deactivated.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the intrusion sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the intrusion sensor is activated. Use the **Dial Out Extension** field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the intrusion sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio ?	When selected, the device will call the **Dial Out Extension** and play an audio file (corresponds to **Intrusion Sensor Triggered** on the **Audiofiles** page) to the phone answering the SIP call when the intrusion sensor is activated.
Repeat Intrusion Message ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Intrusion Sensor Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Intrusion Sensor ?	When selected, the Strobe will blink a scene when the intrusion sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.

Table 2-17. Sensor Configuration Parameters (continued)

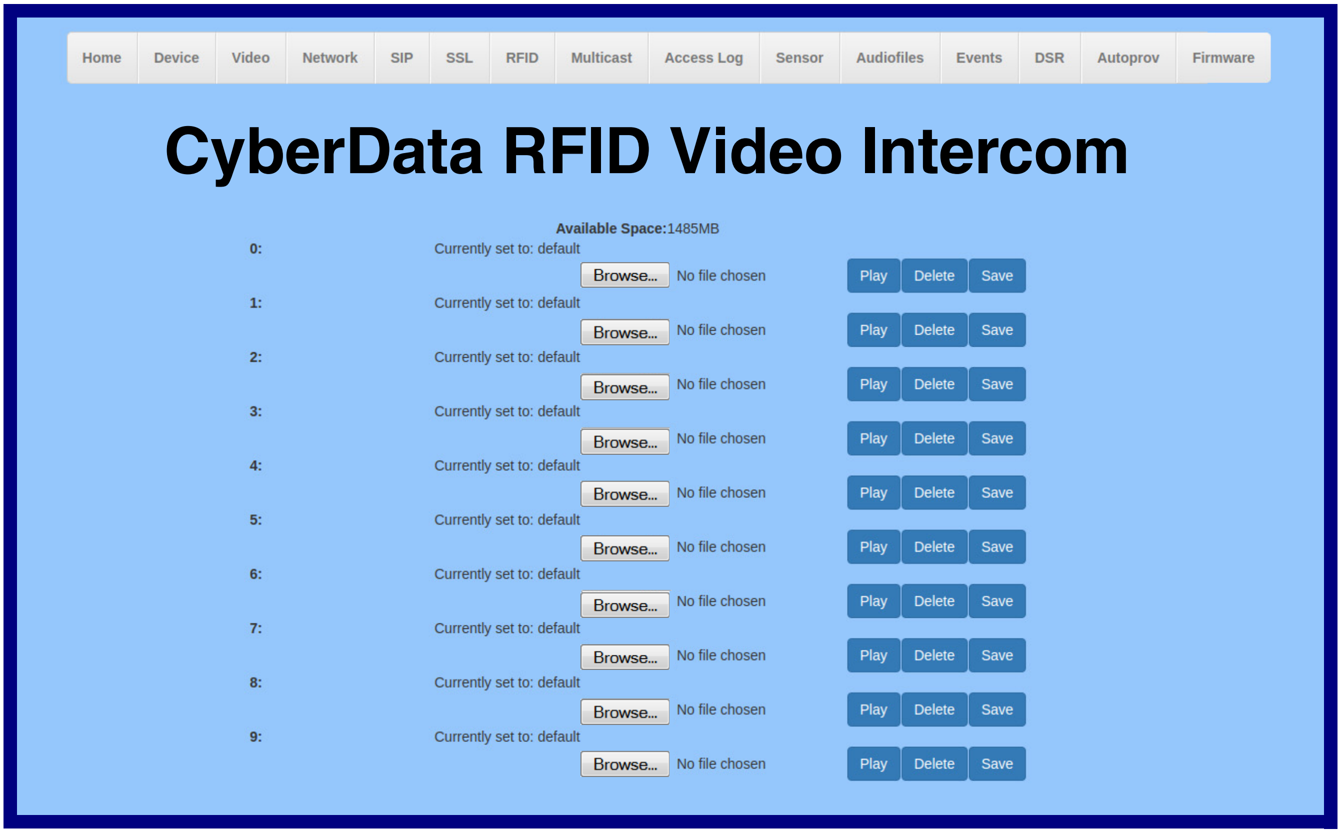
Web Page Item	Description
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the intrusion sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for the Intrusion Sensor.
Green ?	The green LED value for the Intrusion Sensor.
Blue ?	The blue LED value for the Intrusion Sensor.
Preview	Use this button to preview the strobe flashing behavior for the **Intrusion Sensor Strobe Settings**.
Test Door Sensor	Click the **Test Door Sensor** button to test the door sensor.
Test Intrusion Sensor	Click the **Test Intrusion Sensor** button to test the Intrusion sensor.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.4.15 Configure the Audio Configuration Parameters

The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the Intercom.

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-60).

Figure 2-60. Audiofiles Configuration Page



CyberData RFID Video Intercom

Available Space:1485MB

0: Currently set to: default
No file chosen

1: Currently set to: default
No file chosen

2: Currently set to: default
No file chosen

3: Currently set to: default
No file chosen

4: Currently set to: default
No file chosen

5: Currently set to: default
No file chosen

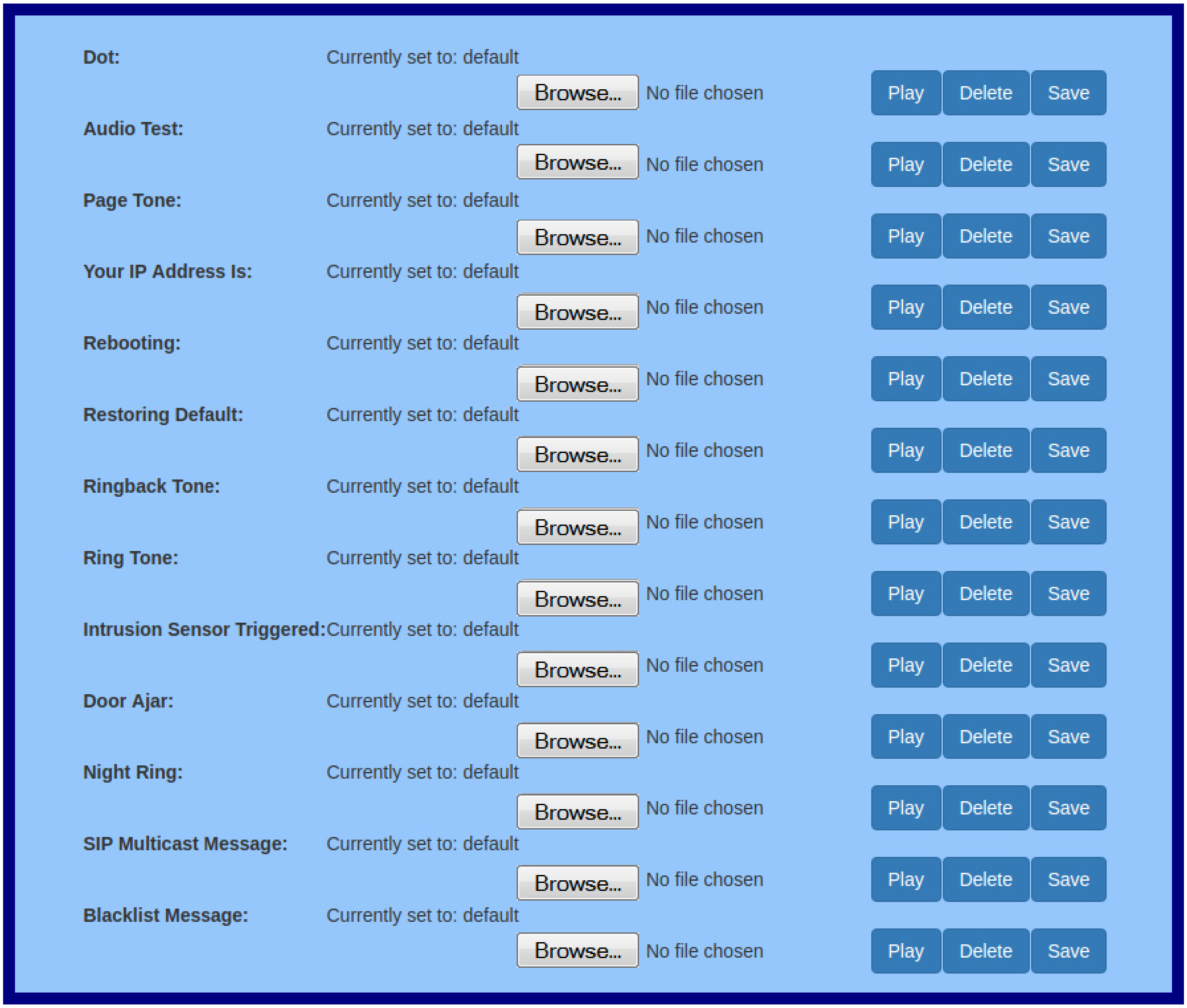
6: Currently set to: default
No file chosen

7: Currently set to: default
No file chosen

8: Currently set to: default
No file chosen

9: Currently set to: default
No file chosen

Figure 2-61. Audiofiles Page



Dot: Currently set to: default
No file chosen

Audio Test: Currently set to: default
No file chosen

Page Tone: Currently set to: default
No file chosen

Your IP Address Is: Currently set to: default
No file chosen

Rebooting: Currently set to: default
No file chosen

Restoring Default: Currently set to: default
No file chosen

Ringback Tone: Currently set to: default
No file chosen

Ring Tone: Currently set to: default
No file chosen

Intrusion Sensor Triggered: Currently set to: default
No file chosen

Door Ajar: Currently set to: default
No file chosen

Night Ring: Currently set to: default
No file chosen

SIP Multicast Message: Currently set to: default
No file chosen

Blacklist Message: Currently set to: default
No file chosen

2. On the **Audiofiles** page, enter values for the parameters indicated in Table 2-18.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-18. Audiofiles Configuration Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word “zero.” '1' corresponds to the spoken word “one.” '2' corresponds to the spoken word “two.” '3' corresponds to the spoken word “three.” '4' corresponds to the spoken word “four.” '5' corresponds to the spoken word “five.” '6' corresponds to the spoken word “six.” '7' corresponds to the spoken word “seven.” '8' corresponds to the spoken word “eight.” '9' corresponds to the spoken word “nine.”
Dot	Corresponds to the spoken word “dot.” (24 character limit)
Audio Test	Corresponds to the message ***“This is the CyberData IP speaker test message...”*** (24 character limit)
Page Tone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address Is	Corresponds to the message “Your IP address is...” (24 character limit).
Rebooting	Corresponds to the spoken word “Rebooting” (24 character limit).
Restoring Default	Corresponds to the message “Restoring default” (24 character limit).
Ringback Tone	This is the ringback tone that plays when calling a remote extension (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Intrusion Sensor Triggered	Corresponds to the message “Intrusion Sensor Triggered” (24 character limit).
Door Ajar	Corresponds to the message “Door Ajar” (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the **Ring Tone** parameter.
SIP Multicast Message	This is the message that plays when multicast audio is initiated by the call button.
Browse...	Click on the **Browse** button to navigate to and select an audio file.
Play	The **Play** button will play that audio file.

Table 2-18. Audiofiles Configuration Parameters (continued)

Web Page Item	Description
	The **Delete** button will delete any user uploaded audio and restore the stock audio file.
	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

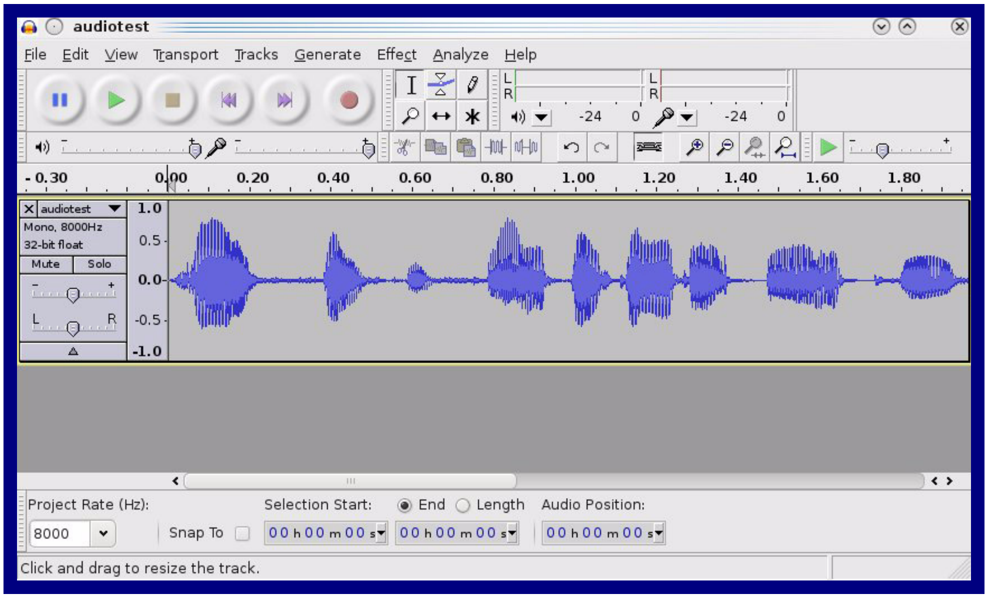
2.4.15.1 User-created Audio Files

User created audio files should be saved in the following format:

RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-62 through Figure 2-64.

Figure 2-62. Audacity 1



Mono, 8000Hz
32-bit float

Project Rate (Hz): 8000

Snap To □

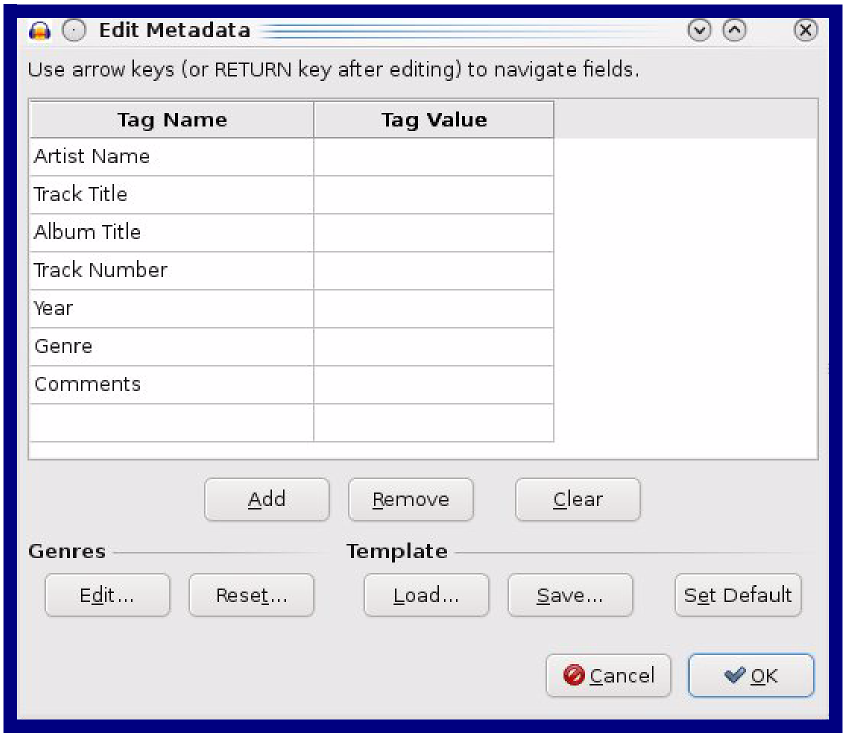
Selection Start: 00 h 00 m 00 s

● End ○ Length 00 h 00 m 00 s

Audio Position: 00 h 00 m 00 s

Click and drag to resize the track.

Figure 2-63. Audacity 2



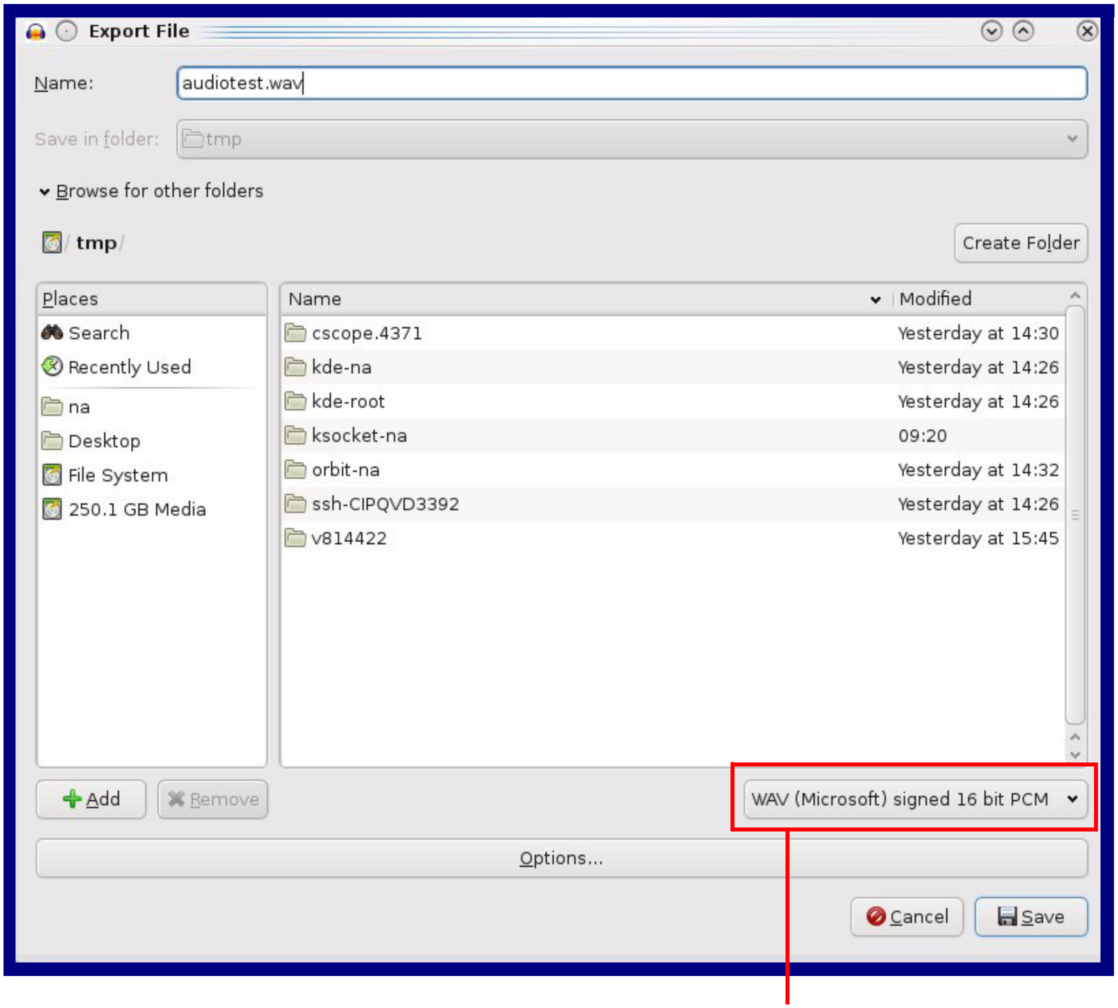
Use arrow keys (or RETURN key after editing) to navigate fields.

Tag Name	Tag Value
Artist Name	
Track Title	
Album Title	
Track Number	
Year	
Genre	
Comments	

When you export an audio file with Audacity, save the output as:

- **WAV (Microsoft) signed 16 bit PCM**.

Figure 2-64. WAV (Microsoft) signed 16 bit PCM



Export File

Name: audiotest.wav

Save in folder: tmp

tmp /

Name	Modified
cscope.4371	Yesterday at 14:30
kde-na	Yesterday at 14:26
kde-root	Yesterday at 14:26
ksocket-na	09:20
orbit-na	Yesterday at 14:32
ssh-CIPQVD3392	Yesterday at 14:26
v814422	Yesterday at 15:45

WAV (Microsoft) signed 16 bit PCM

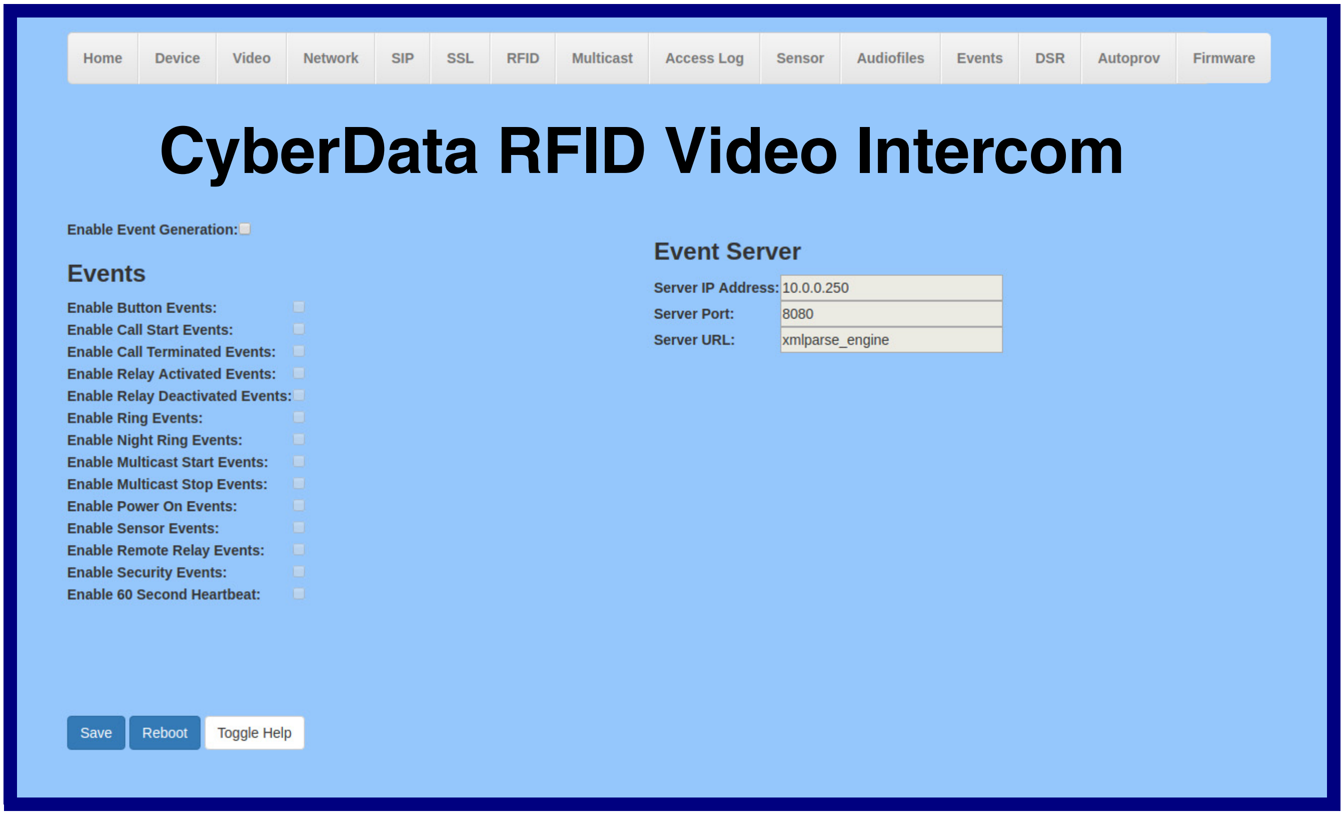
WAV (Microsoft) signed 16 bit PCM

2.4.16 Configure the Events Parameters

The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

1. Click on the **Events** menu button to open the **Events** page (Figure 2-65).

Figure 2-65. Event Configuration Page



CyberData RFID Video Intercom

Enable Event Generation: □

Events

Enable Button Events: □
Enable Call Start Events: □
Enable Call Terminated Events: □
Enable Relay Activated Events: □
Enable Relay Deactivated Events: □
Enable Ring Events: □
Enable Night Ring Events: □
Enable Multicast Start Events: □
Enable Multicast Stop Events: □
Enable Power On Events: □
Enable Sensor Events: □
Enable Remote Relay Events: □
Enable Security Events: □
Enable 60 Second Heartbeat: □

Event Server

Server IP Address: 10.0.0.250
Server Port: 8080
Server URL: xmlparse_engine

2. On the **Events** page, enter values for the parameters indicated in Table 2-19.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-19. Events Configuration Parameters

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Button Events ?	When selected, the device will report Call button presses.
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call. A Ring Event will not be generated when **Auto-Answer Incoming Calls** is enabled on the **Device** page.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Sensor Events ?	When selected, the device will report when the on-board sensor is activated.
Enable Remote Relay Events ?	When selected, the device will report when the remote relay (DSR) is activated.
Enable Security Events ?	When enabled, the device will report when the intrusion sensor is activated.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Check All	Click on **Check All** to select all of the events on the page.
Uncheck All	Click on **Uncheck All** to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.

Table 2-19. Events Configuration Parameters(continued)

Web Page Item	Description
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.4.16.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.4.17 Configure the Door Strike Relay

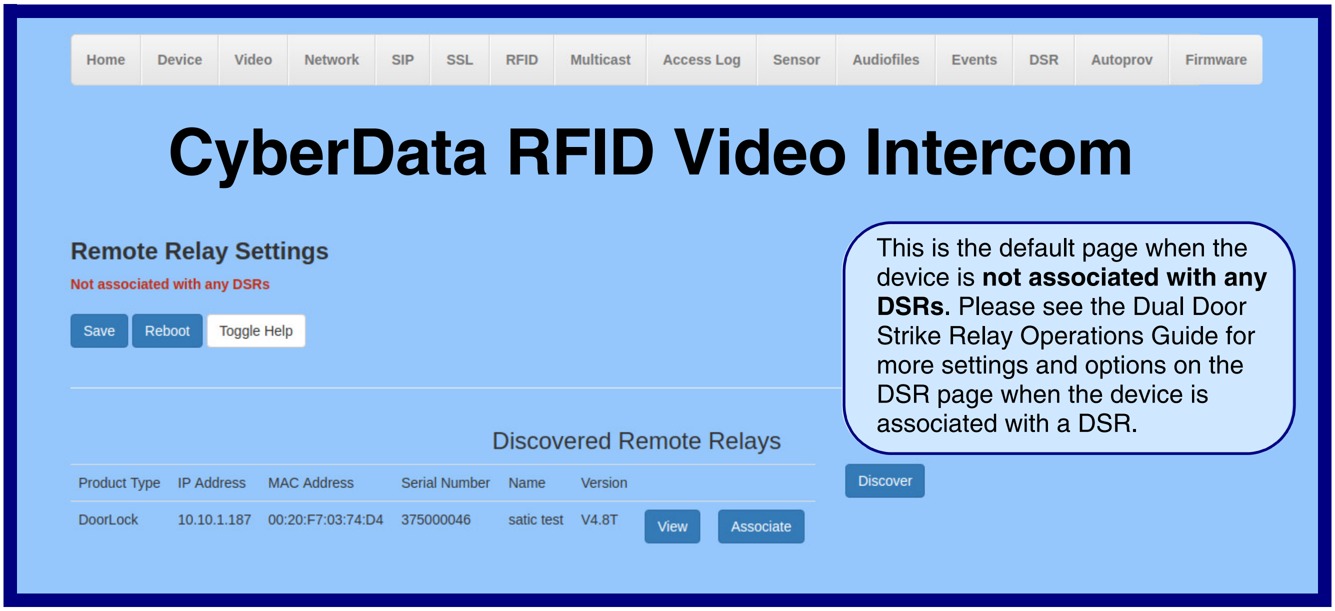
The Door Strike Relay (DSR) is a network device designed to control an electronic door strike. The DSR is meant to be used as a replacement for (or an addition to) the on-board relay. In addition to being a drop-in 12 Amp relay, the DSR can monitor and record when the door is open or closed.

The DSR can be configured to trigger in the following ways: on the entry of a DTMF code, manually through the web interface, or by using a Windows application.

This section describes operations for running firmware version 4.8 or later of the Dual Door Strike Relay. If you have an older version of the firmware, then please contact CyberData Technical Support. The version number appears in the **Discovered Remote Relays** section on the **DSR** page (Figure 2-66).

1. Click on the **DSR** menu button to open the **DSR** page (Figure 2-66).

Figure 2-66. DSR Page (not associated with any DSRs)



CyberData RFID Video Intercom

Remote Relay Settings

Not associated with any DSRs

Discovered Remote Relays

Product Type	IP Address	MAC Address	Serial Number	Name	Version		
DoorLock	10.10.1.187	00:20:F7:03:74:D4	375000046	satic test	V4.8T	View	Associate

This is the default page when the device is **not associated with any DSRs.** Please see the Dual Door Strike Relay Operations Guide for more settings and options on the DSR page when the device is associated with a DSR.

2. On the **DSR** page, enter values for the parameters indicated in Table 2-20.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-20. DSR Configuration Parameters (not associated with any DSRs)

Web Page Item	Description
Remote Relay Settings	The settings in this section will activate an associated door strike relay. If a door strike relay is not associated with the device, then you will only see the words **Not associated with any DSRs**.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Discovered Remote Relays	The **Discovered Remote Relays** section lists all of the networked door strike relays on the network. To associate your device with a door strike relay, click on the **Associate** button. This action allows the user to configure the door strike relay. Keep in mind that a device may only be associated with one door strike relay.
Product Type	Displays the product type of the remote relay.
IP Address	Displays the IP address of the remote relay.
MAC Address	Displays the MAC address of the remote relay.
Serial Number	Displays the serial number of the remote relay.
Name	Displays the name of the remote relay.
Version	Displays the version of the remote relay.
Discover	Use this button to search for and find any remote relays that are available on the network.
View	Use this button to view the settings of a remote relay that has been “discovered” after pressing the **Discover** button.
Associate	Use this button to associate the remote relay with the device. Only one relay may be associated with a device.
Disassociate	Use this button to disassociate the remote relay from the device. Only one relay may be associated with a device. This button is only available when a relay is associated with a device.

Note Associating a DSR does not require a reboot. However, you should reboot the device after disassociating a DSR.

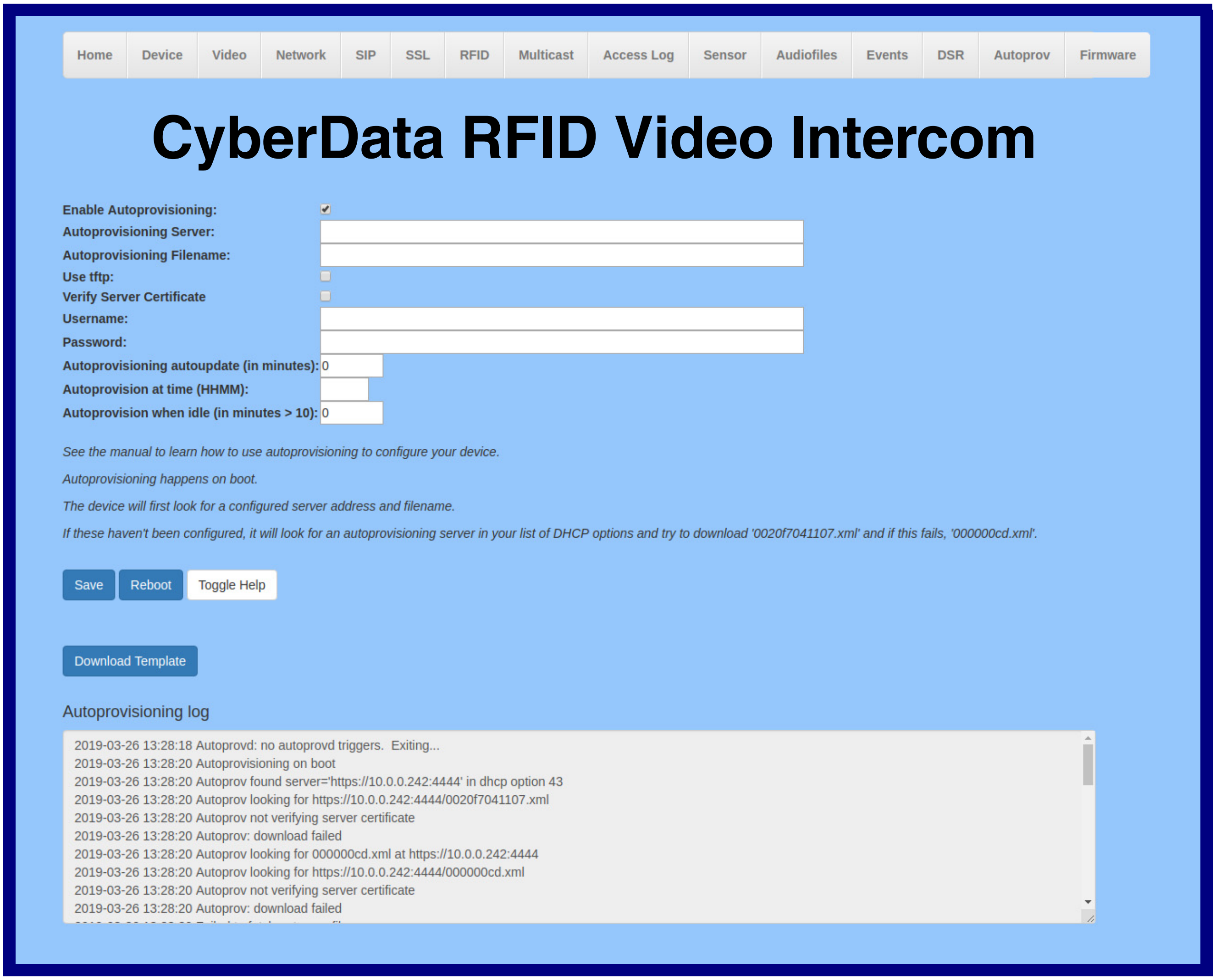
2.4.18 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to automatically configure your device. The autoprovisioning file is an xml file with the device configuration. Values found in this file will override values stored in on-board memory.

Note By default, the device will try to set up its configuration with autoprovisioning.

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See Figure 2-67.

Figure 2-67. Autoprovisioning Page



CyberData RFID Video Intercom

Enable Autoprovisioning: ☑
Autoprovisioning Server:
Autoprovisioning Filename:
Use tftp: □
Verify Server Certificate □
Username:
Password:
Autoprovisioning autoupdate (in minutes): 0
Autoprovision at time (HHMM):
Autoprovision when idle (in minutes > 10): 0

See the manual to learn how to use autoprovisioning to configure your device.

Autoprovisioning happens on boot.

The device will first look for a configured server address and filename.

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f7041107.xml' and if this fails, '000000cd.xml'.

Autoprovisioning log

```
2019-03-26 13:28:18 Autoprovd: no autoprovd triggers.  Exiting...
2019-03-26 13:28:20 Autoprovisioning on boot
2019-03-26 13:28:20 Autoprov found server='https://10.0.0.242:4444' in dhcp option 43
2019-03-26 13:28:20 Autoprov looking for https://10.0.0.242:4444/0020f7041107.xml
2019-03-26 13:28:20 Autoprov not verifying server certificate
2019-03-26 13:28:20 Autoprov: download failed
2019-03-26 13:28:20 Autoprov looking for 000000cd.xml at https://10.0.0.242:4444
2019-03-26 13:28:20 Autoprov looking for https://10.0.0.242:4444/000000cd.xml
2019-03-26 13:28:20 Autoprov not verifying server certificate
2019-03-26 13:28:20 Autoprov: download failed
```

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-21.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed..

Table 2-21. Autoprovisioning Page Parameters

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of **<mac address>.xml**. Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the **Autoprovisioning Page**. Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Download Template	Press the **Download Template** button to create an autoprovisioning file for the device. See Section 2.4.18.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

Note You must click on the **Save** button for the changes to take effect.

2.4.18.1 Autoprovisioning

On boot, the device will look for an autoprovisioning server configured on the Autoprovisioning Page or specified as a DHCP option. When it finds a server, it will try to download the following (in order of preference):

1. The file configured on the autoprovisioning page.
2. A file named according to it's mac address (for example: 0020f7350058.xml).
3. The file 000000cd.xml

The file can be hosted using a standard web server (like apache, IIS, or nginx), and the device can download over SSL. The file server can be an ipv4 address in dotted decimal notation or a fully qualified domain name.

By default, the device will get its autoprovisioning server from the DHCP options. See Section 2.4.18.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

The DHCP option determines the protocol used to download the autoprovisioning file. The device looks for DHCP options in the following order:

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.

You can download an autoprovisioning template file from the Autoprovisioning Page using the **Download Template** button (see Table 2-21). This file contains every configuration option that can be set on the board.

Autoprovisioning files can contain the whole configuration or a subset of this file. The first autoprovisioning file can also contain links to other autoprovisioning files.

The <MiscSettings> section contains some examples of additional autoprovisioning files:

```
    <MiscSettings>
        <DeviceName>CyberData VoIP Device</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
    </MiscSettings>
```

After downloading the first autoprovisioning file, the device will step through up to twenty additional <AutoprovFile> entries and try to download these files from the same server.

When the device finds a filename with the string **[macaddress]**, it will replace this string with the mac address.

As an example, the user has configured option 43 on their DHCP server to “http://example.com,” and on their server, they have a file named **0020f7123456.xml** (the same as the mac address of the device).

The file 0020f7123456.xml contains:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
         <MiscSettings>
                <DeviceName>Newname</DeviceName>
                <AutoprovFile>common.xml</AutoprovFile>
                <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>
                <AutoprovFile>audio[macaddress]</AutoprovFile>
                <AutoprovFile>device.xml</AutoprovFile>
         </MiscSettings>
</specific>
```

1. The device will first set it's name to 'Newname'.
2. It will try to download http://example.com/common.xml.
3. It will try to download http://example.com/sip_reg0020f7123456.xml.
4. It will try to download http://example.com/audio0020f7123456.
5. It will try to download http://example.com/device.xml.

The device is reconfigured every time it downloads a new file so if two files configure the same option the last one will be the one that is saved.

It is possible to autoprovision autoprovisioning values (for example, to disable autoprovisioning or to configure a time to check for new files).

Checking for New Autoprovisioning Files after Boot

The device will always check for an autoprovisioning files on boot but it can be configured to also check after a periodic delay, when idle, or at a specified time. When one of these options is set, the device will download its autoprovisioning files again, and if it finds any differences from the files it downloaded on boot, it will force a reboot and reconfigure.

The Autoprovisioning Filename

The autoprovisioning filename can contain a file, a file path, or a directory.

Table 2-22. Autoprovisioning File Name

Autoprovisioning Filename	Autoprovisioning Server	File Downloaded
config.xml	10.0.1.3	10.0.1.3/config.xml
/path/to/config.xml	10.0.1.3	10.0.1.3/path/to/config.xml
subdirectory/path/	10.0.1.3	10.0.1.3/subdirectory/path/0020f7020002.xml

TFTP options may not support subdirectories. If a directory is set in the filename field, firmware and audio files will also be downloaded from this subdirectory.

If the filename ends with a forward slash "/," the device will treat it as a subdirectory.

For example:

> The autoprovisioning server is set to "https://www.example.com"
>
> The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

https://www.example.com/cyberdata/0020f7123456.xml

...and if this fails:

https://www.example.com/cyberdata/000000cd.xml

Audio files and firmware files will also add "cyberdata" to the URL before downloading.

Autoprovisioning Firmware Updates

```
<FirmwareSettings>
  <FirmwareFile>505-uImage-ceilingspeaker</FirmwareFile>
  <FirmwareServer>10.0.1.3</FirmwareServer>
  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
  <CallButton31>firmware_file_v10.3.0</CallButton31>
</FirmwareSettings>
```

In the <FirmwareSettings> section, the <FirmwareServer> element can be used to specify a different server for hosting firmware files. When this element is not available, the device will try to download the file from the autoprovisioning server.

The device will use the filename to determine when to autoprovision firmware updates. The default configuration is blank, so the first time you set a value in your autoprovisioning file, it may force a firmware update even if the firmware version has not changed.

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-uImage-[device_file_name]).

The device also supports product strings for downloading firmware. If the <FirmwareFile> option is not set, the device will look for its particular product string for a firmware filename. In this way, a generic autoprovisioning file can specify unique firmware for a range of products.

The list of valid product strings:

```
<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>
```

Autoprovisioning Example 1

Here's a simple example using four autoprovisioning files to configure two devices:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2).

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is “https://autoprovtest.server.net.” The files on this server are as follows:

000000cd.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
<AutoprovFile>sip_common.xml</AutoprovFile>
<AutoprovFile>sip_[macaddress].xml</AutoprovFile>
</MiscSettings>
```

sip_common.xml

```
<SIPSettings>
<SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

sip_0020f7020001.xml

```
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

sip_0020f7020002.xml

```
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

On boot, Device1 tries to fetch the file **0020f7023614.xml** from “https://autoprovtest.server.net”. This file is not available, so device1 then tries to fetch the file **000000cd.xml**. This file exists, and Device1 parses the three elements.

1. Device1 changes its device name to **CyberData Autoprovisioned**.

2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from “https://autoprovtest.server.net,” and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.

3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from “https://autoprovtest.server.net,” and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from “https://autoprovtest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2) and boot them on a network with a DHCP server configured with an autoprovisioning server at **10.0.1.3** on option **150**. Our TFTP server has three files:

0020f7020001.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

0020f7020002.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

common_settings.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
</MiscSettings>
<SIPSettings> <SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

1. On boot, Device1 downloads **0020f7020001.xml** from **10.0.1.3** and imports these values. The SIP User ID is **198**, the password is **ext198**, and the dialout extension is **204**.

2. Device1 then gets the filename **common_settings.xml** from the AutoprovFile element and downloads this file from the TFTP server at **10.0.1.3**. and imports these settings. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

XML Files

XML files can contain <AutoprovFile> elements. If multiple DHCP options are specified, the device will try to download autoprovisioning files from each in turn. The device will only look for <AutoprovFile> elements in the first file downloaded from each server. You can specify up to 20 <AutoprovFile> elements in the first autoprovisioning file.

There are numerous ways to change an element of the **configuration(xml)** file. Using **sip ext** as an example, the extension can be changed:

Within the device-specific xml, i.e. **[macaddress].xml**, via the AutoprovFile element:<SIPSettings>/<SIPExt>

From the device specific xml, a pointer to a sip_common file

From the device specific xml, a pointer to the device specific sip_[macaddress].xml

From the common file, a pointer to sip_common.xml

From the common file, a pointer to the device specific (sip_[macaddress].xml)

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used autoprovisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if autoprovisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio** page or by changing the autoprovisioning file with “**default**” set as the file name.

2.4.18.2 Sample dhcpd.conf

```
#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
    default-lease-time 3600;

    option routers                  10.0.0.1;
    option subnet-mask              255.0.0.0;

    option domain-name              "voiplab";
    option domain-name-servers      10.0.0.252;

    option time-offset              -8;             # Pacific Standard Time

#     option www-server               99.99.99.99;                    # OPTION 72

#     option tftp-server-name          "10.0.1.52";                   # OPTION 66
#     option tftp-server-name          "http://test.cyberdata.net";   # OPTION 66

#     option option-150                10.0.0.252;                    # OPTION 150

# These two lines are needed for option 43
#     vendor-option-space VendorInfo;                                  # OPTION 43
#     option VendorInfo.text "http://test.cyberdata.net";             # OPTION 43

    range 10.10.0.1 10.10.2.1; }
```

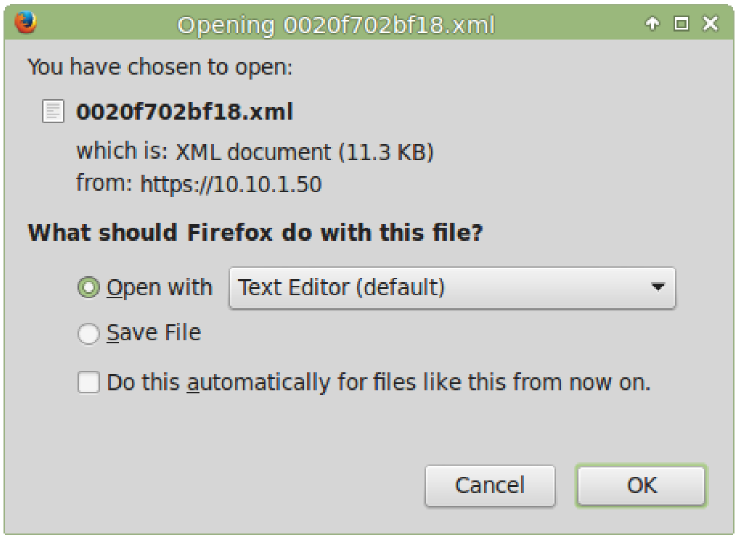
2.4.18.3 Download Template Button

The **Download Template** button allows the user to generate, download, edit, and then store an autoprovisioning template on the server that serves the autoprovisioning files for devices.

To generate an autoprovisioning template directly from the device, complete the following steps:

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-68). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See Figure 2-68.

Figure 2-68. Configuration File



Opening 0020f702bf18.xml

You have chosen to open:

0020f702bf18.xml

which is: XML document (11.3 KB)
from: https://10.10.1.50

What should Firefox do with this file?

● Open with Text Editor (default)

○ Save File

□ Do this automatically for files like this from now on.

4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.
5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.5 Upgrade the Firmware

Note CyberData strongly recommends that you do not upgrade the firmware when the device is likely to be in use.

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:

   https://www.cyberdata.net/products/011478

2. Unzip the firmware version file. This file may contain the following:

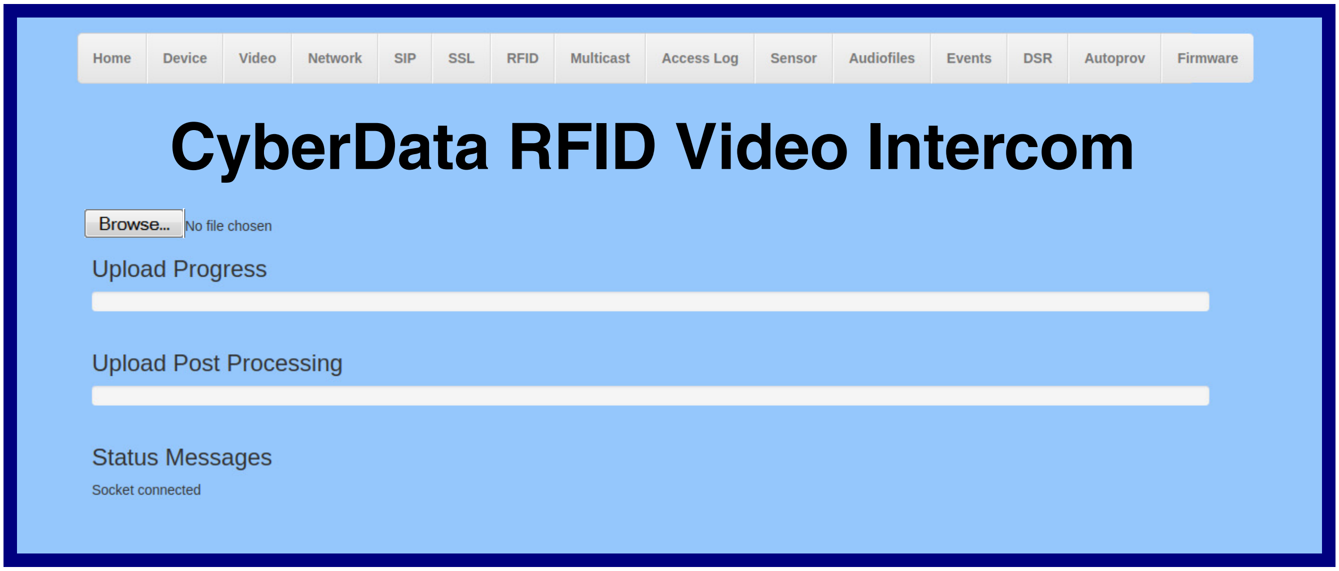
- Firmware file
- Release notes
- Autoprovisioning template

3. Log in to the **Home** page as instructed in Section 2.4.4, "Log in to the Configuration Home Page".

4. Click on the **Firmware** menu button to open the **Firmware** page (Figure 2-69).

GENERAL ALERT	**Caution** ***Equipment Hazard***: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.5, "Upgrade the Firmware".

Figure 2-69. Firmware Page

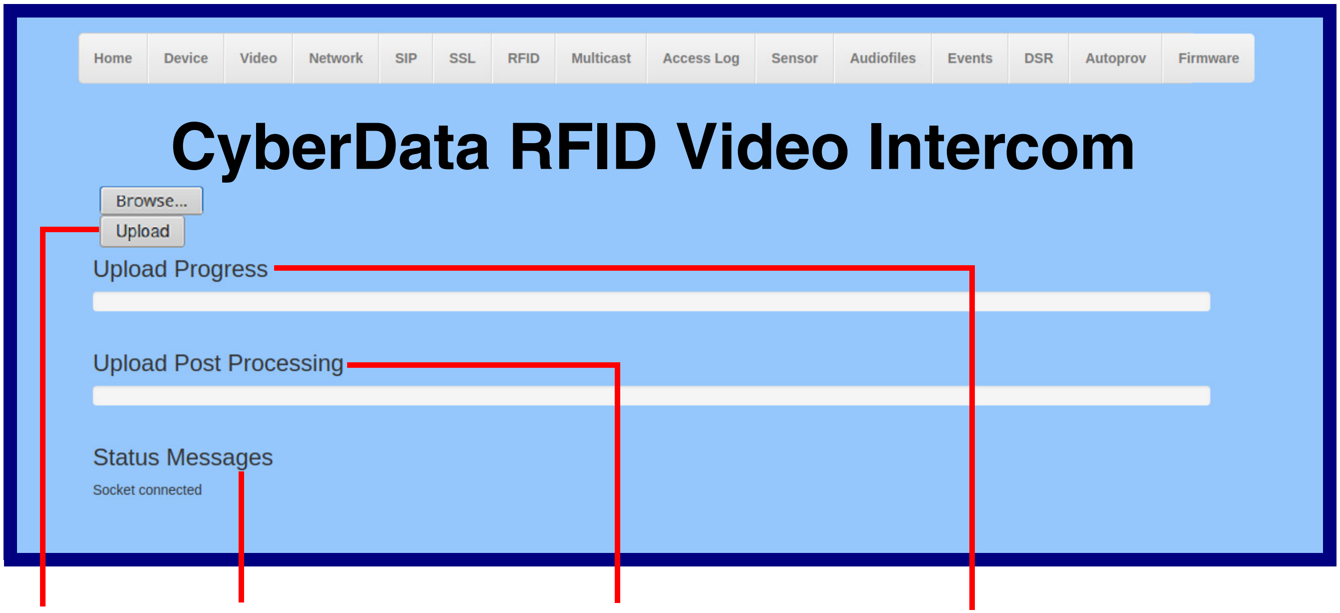


Socket connected

5. Click on the **Browse** button, and then navigate to the location of the firmware file.

6. Select the firmware file. This reveals the **Upload** button (Figure 2-70).

Figure 2-70. Upload Button



Upload button **Status Messages** **Upload Post Processing** bar **Upload Progress** bar

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.

8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.

9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

Note Do not reboot the device before the upgrading process is complete.

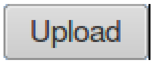
10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.

11. The device will reboot automatically.

12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

Table 2-23 shows the web page items on the **Firmware** page.

Table 2-23. Firmware Page Parameters

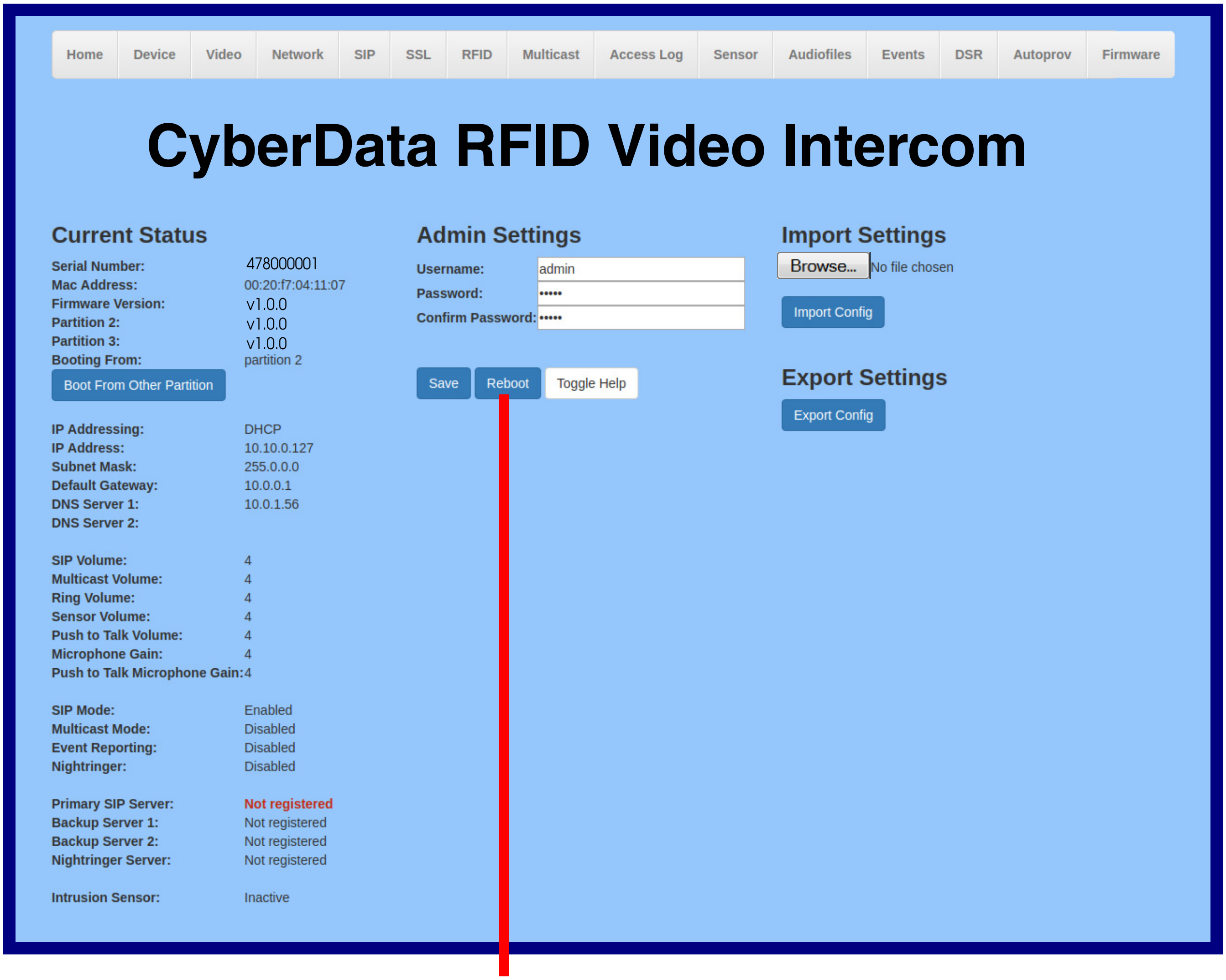
Web Page Item	Description
	Use the **Browse** button to navigate to the location of the firmware file that you want to upload.
	Click on the **Upload** button to automatically upload the selected firmware and reboot the system. **Note**: This button only appears after the user has selected a firmware file.
Upload progress	Status bar indicates the progress in uploading the file.
Upload Post Processing	Status bar indicates the progress of the software installation.
Status Messages	Messages relevant to the firmware update process appear here.

2.6 Reboot the Device

To reboot the device, complete the following steps:

1. Log in to the **Home** page as instructed in Section 2.4.4, "Log in to the Configuration Home Page".
2. Click on the **Reboot** button on the **Home** page (Figure 2-71). A normal restart will occur.

Figure 2-71. Home Page



CyberData RFID Video Intercom

Current Status

Serial Number:	478000001
Mac Address:	00:20:f7:04:11:07
Firmware Version:	v1.0.0
Partition 2:	v1.0.0
Partition 3:	v1.0.0
Booting From:	partition 2
IP Addressing:	DHCP
IP Address:	10.10.0.127
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.1.56
DNS Server 2:	
SIP Volume:	4
Multicast Volume:	4
Ring Volume:	4
Sensor Volume:	4
Push to Talk Volume:	4
Microphone Gain:	4
Push to Talk Microphone Gain:	4
SIP Mode:	Enabled
Multicast Mode:	Disabled
Event Reporting:	Disabled
Nightringer:	Disabled
Primary SIP Server:	Not registered
Backup Server 1:	Not registered
Backup Server 2:	Not registered
Nightringer Server:	Not registered
Intrusion Sensor:	Inactive

Admin Settings

Username:	admin
Password:	•••••
Confirm Password:	•••••

Import Settings

Export Settings

Reboot

2.7 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-24 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.7.1 Command Interface Post Commands

These commands require an authenticated session (a valid username and password to work).

Table 2-24. Command Interface Post Commands

Device Action	**HTTP Post Command**[a]
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=reboot"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=call&extension=600"
Test Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_relay"
Test Audio	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_audio"
Speak IP Address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=speak_ip_address"
Test Mic	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_mic"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "0=Play"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "1=Play"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "2=Play"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "3=Play"
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "4=Play"

Table 2-24. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "5=Play"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "6=Play"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "7=Play"
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "8=Play"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "9=Play"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "d=Play"
Play the Audio Test	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "audiotest=Play"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "pagetone=Play"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "youripaddressis=Play"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "rebooting=Play"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "restoringdefault=Play"
Play the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "ringback=Play"
Play the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "ringtone=Play"
Play the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "intrusionsensortriggered=Play"
Play the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "doorajar=Play"
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "nightring=Play"

Table 2-24. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Swap boot partitions	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=swap_boot_partition"

[a] Type and enter all of each http POST command on one line.

Appendix A: Mounting the SIP Outdoor Video Intercom with RFID

A.1 Mount the Intercom

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to Table A-1. See Table A-2 and Table A-3 for optional accessories.

Table A-1. Mounting Components (Part of the Accessory Kit)

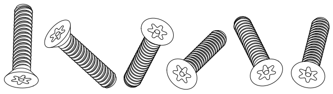
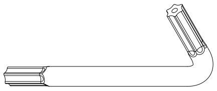
Quantity	Part Name	Illustration
6	Accessory Kit Security Torx MS	
1	Mounting Component Security Torx Key	

Table A-2. Optional Accessories (for gooseneck mounting)

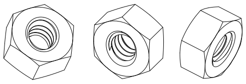
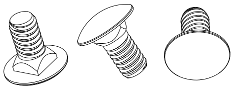
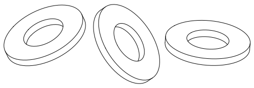
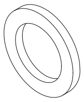
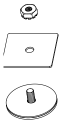
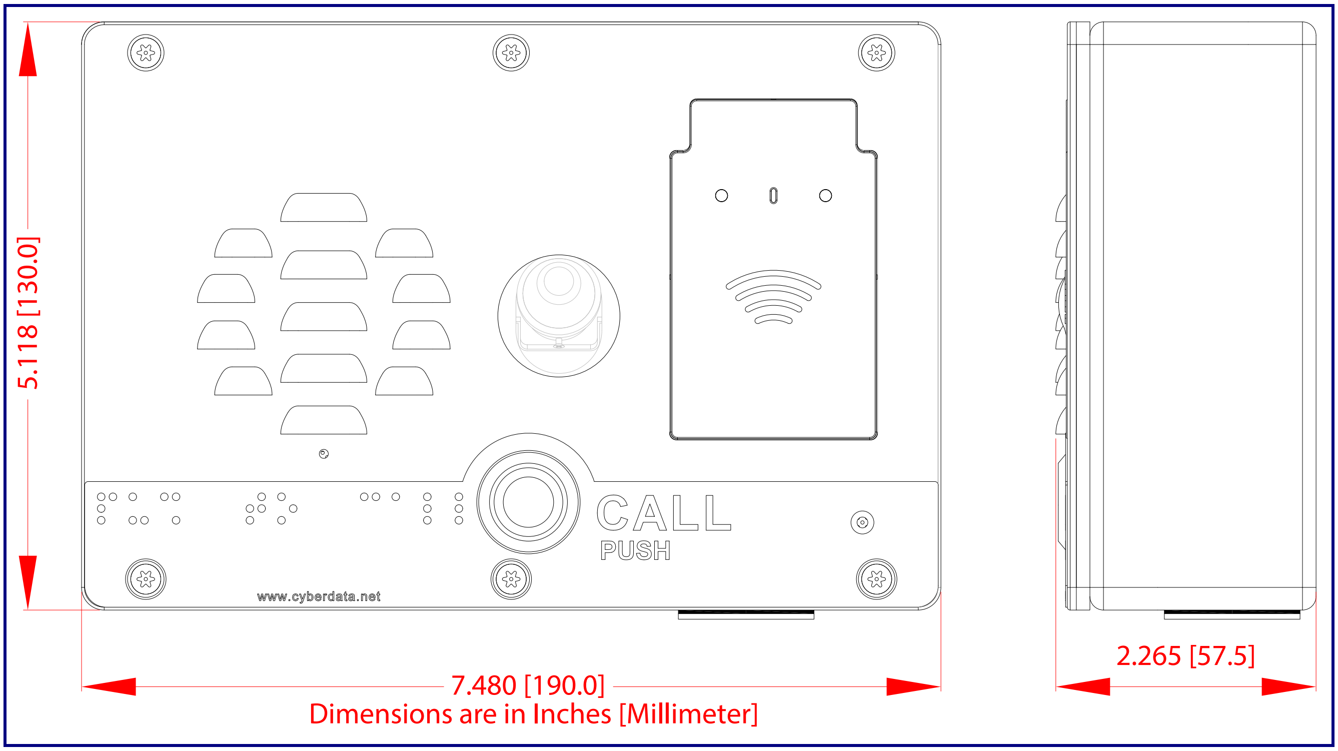
Quantity	Part Name	Illustration
3	Carriage bolt nuts	
3	Carriage bolts	
3	Carriage bolt washers	

Table A-3. Optional Accessories

Quantity	Part Name	Illustration
1	Spacer for Half-inch Set Screw Connector	
1	531085* Hole Plug Assembly	

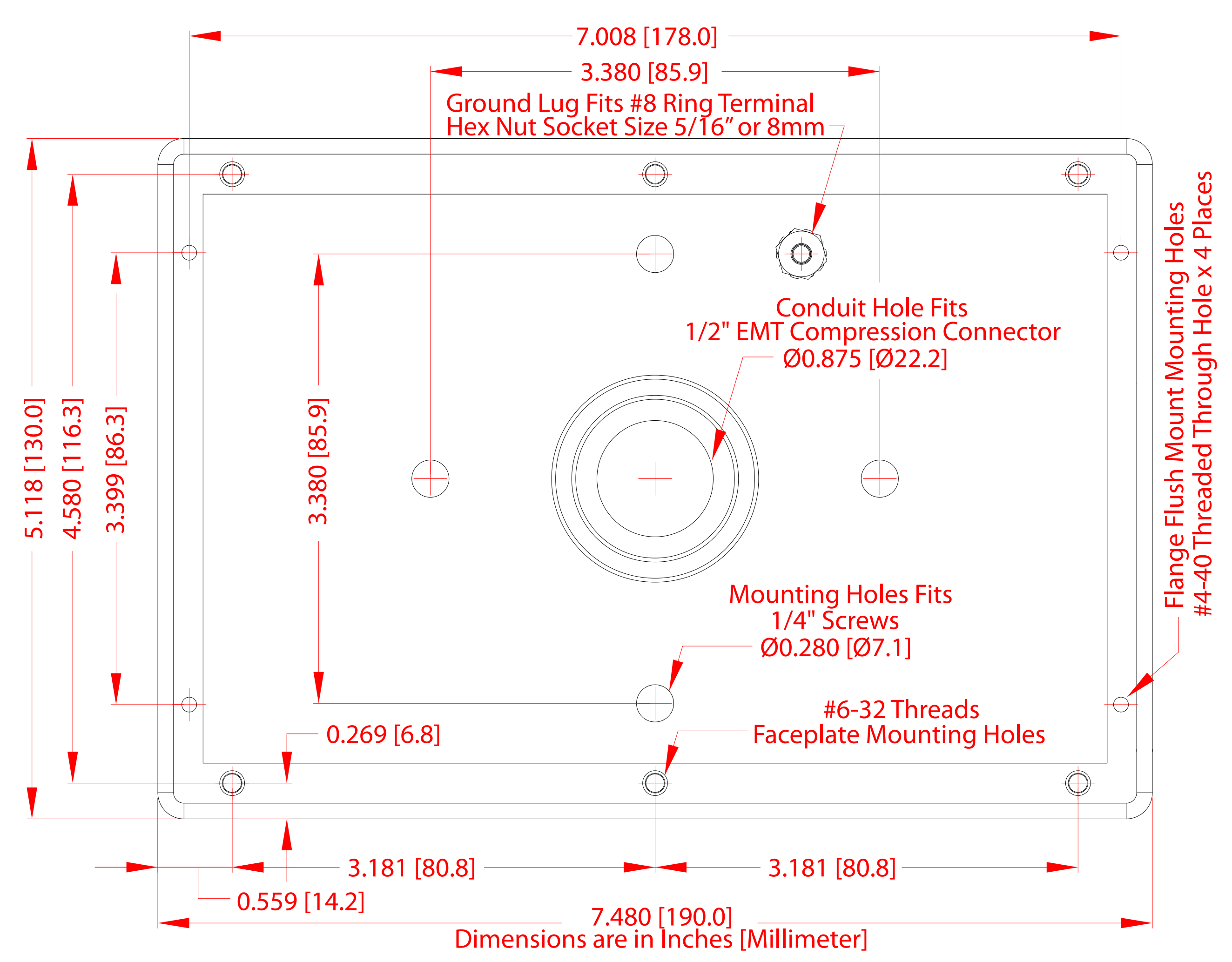
A.2 Dimensions (Front and Side View)

Figure A-1. Unit Dimensions—Front and Side View



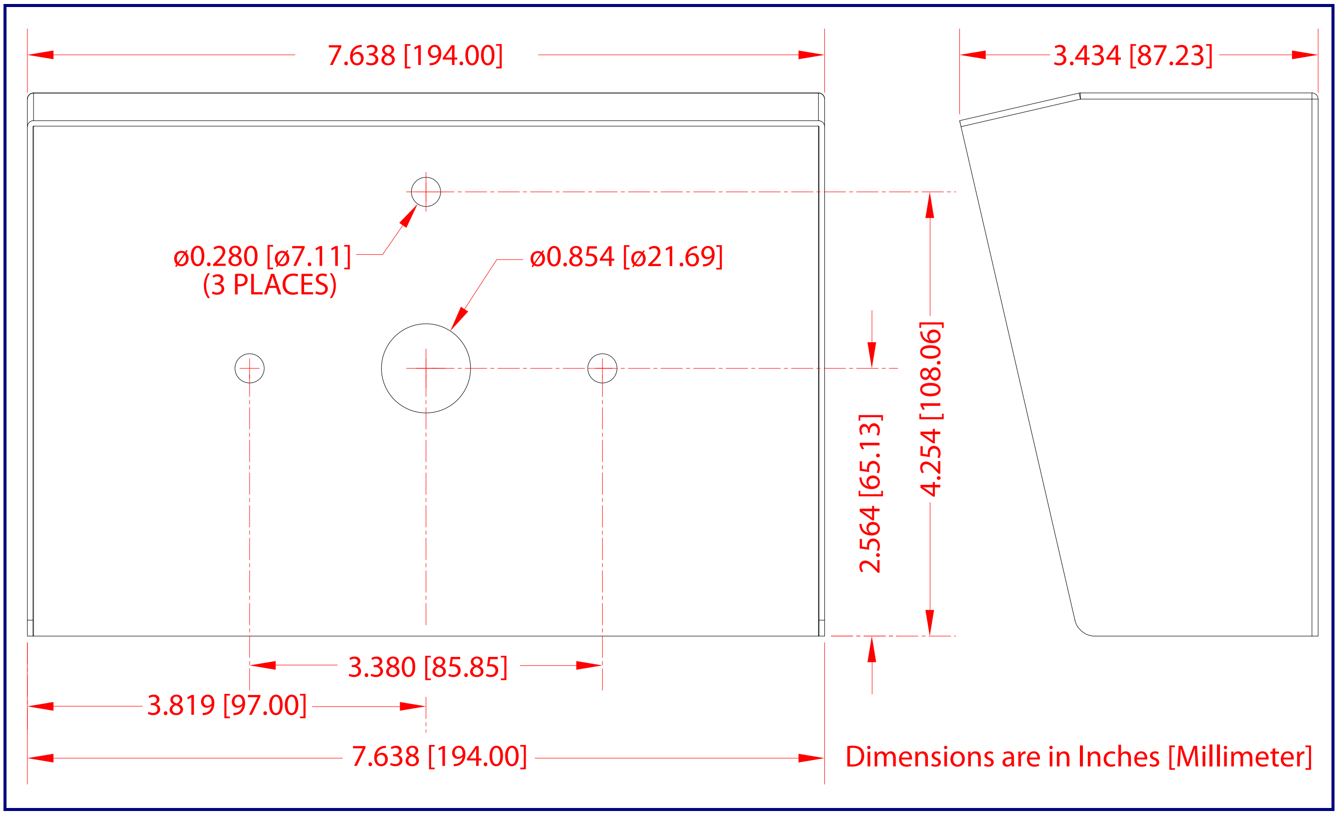
A.3 Unit Dimensions (Rear View with Mounting Hole Locations)

Figure A-2. Unit Dimensions—Rear View with Mounting Hole Locations



A.4 Shroud Dimensions and Mounting Hole Locations

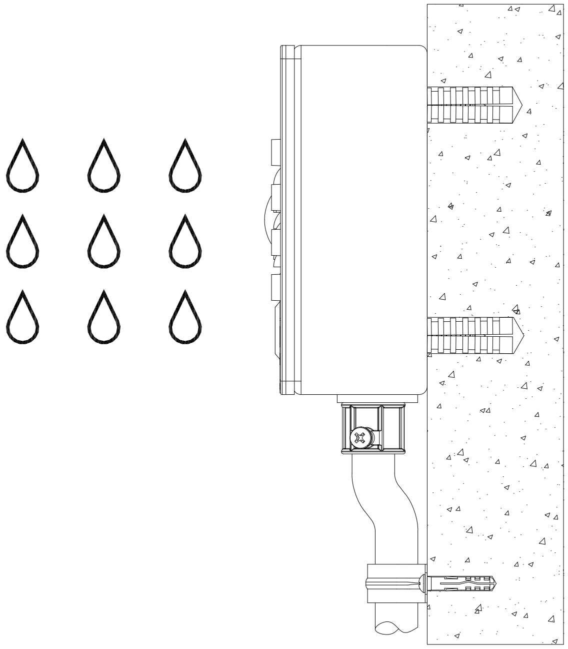
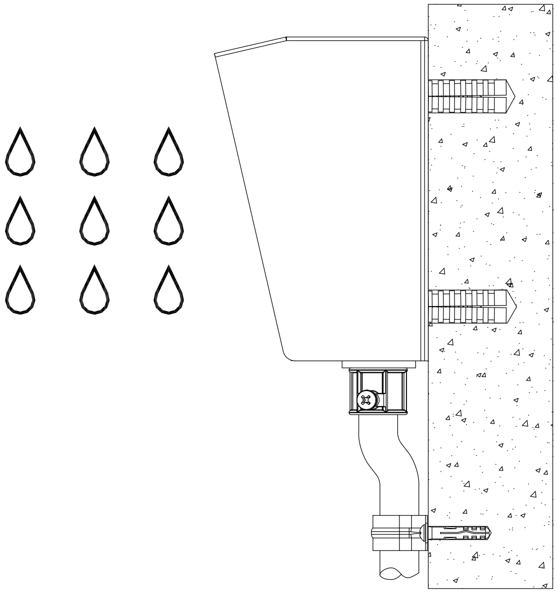
Figure A-3. Shroud Dimensions and Mounting Hole Locations



A.5 Overview of Installation Types

An overview of the installation types and the required components are provided in Table A-4.

Table A-4. Overview of Installation Types

Installation Type	What You Need
Outdoor, on surface	
	011478 Intercom only
Outdoor, on surface with shroud (increased resistance)	
	011478 Intercom 011215 Weather Shroud (sold separately)

Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

```
in.tftpd -l -s /tftpboot/your_directory_name
```

B.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download from the following website address:

https://www.cyberdata.net/pages/solarwinds

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File**/**Configure**/**Security** tab/**Transmit Only**.
3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, click on the **FAQs** tab at the following webpage:

https://www.cyberdata.net/products/011478

C.2 Documentation

The documentation for this product is released in an English language version only.

To download PDF copies of CyberData product documentation, click on the **Downloads** tab at the following webpage:

https://www.cyberdata.net/products/011478

C.3 Contact Information

Contact

CyberData Corporation
3 Justin Court
Monterey, CA 93940 USA
www.CyberData.net
Phone: 800-CYBERDATA (800-292-3732)
Fax: 831-373-4193

Sales

Sales 831-373-2601, Extension 334

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

http://support.cyberdata.net/

The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the **Comments** section of the Support Form.

Phone: (831) 373-2601, Extension 333

C.4 Warranty and RMA Information

The most recent warranty and RMA information is available at the following website address:

http://support.cyberdata.net/

Index