CyberData

The IP Endpoint Company

# Administration guide for CyberData RFID Access Control Devices

Document Part # 931724A

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

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 configuration guide 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 configuration guide or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this configuration guide and to any such product, software, firmware, and/or hardware.

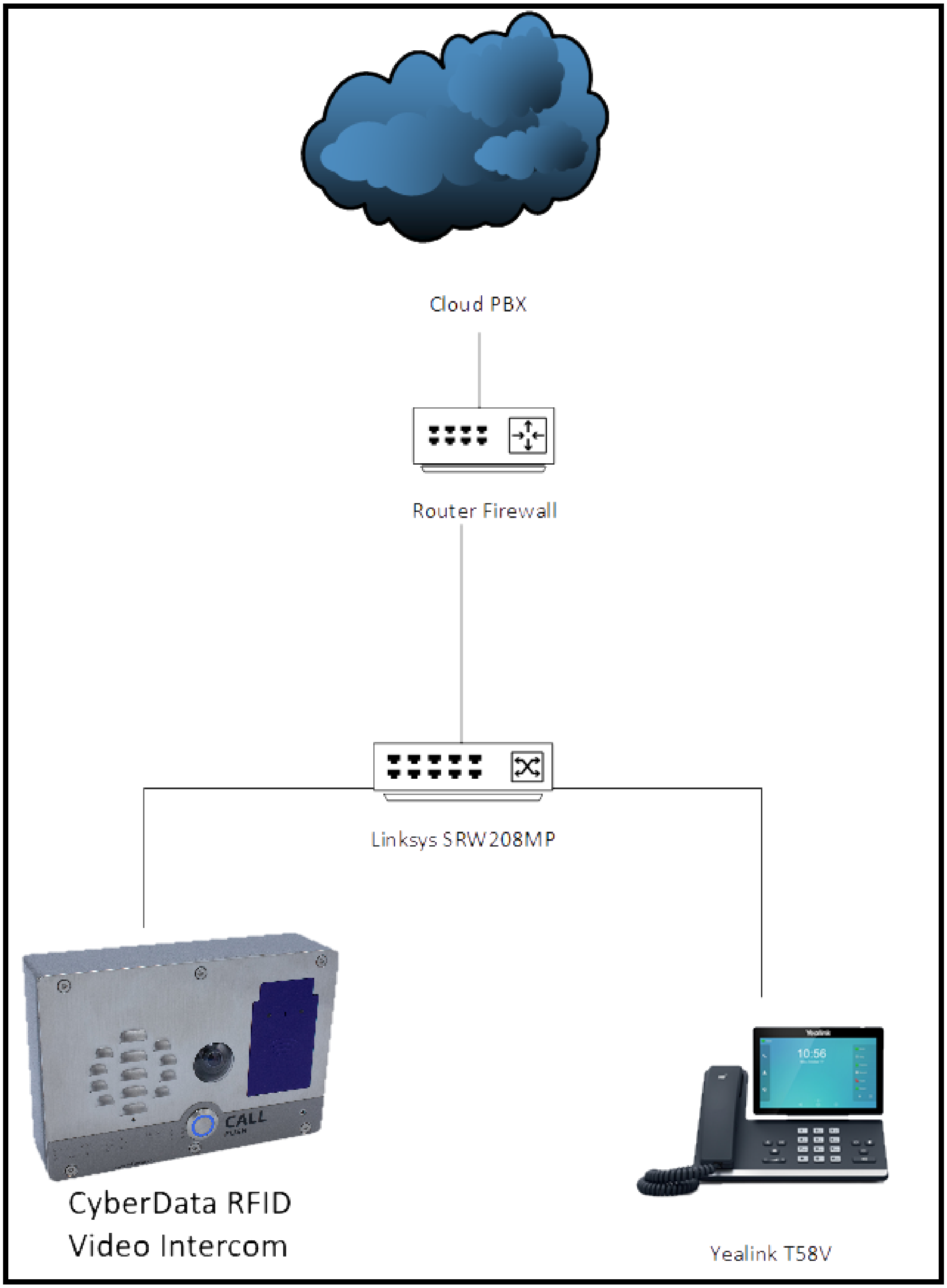
OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software. Software or firmware developed by CyberData that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

# Revision Information

- 931724A Initial release on 2/19/2020

# Table of Contents

# 1.0 Setup Diagram and Test Equipment



## TEST EQUIPMENT USED

| Name of Product | Part Number | Firmware Version |
|---|---|---|
| SIP Outdoor Intercom with RFID | 011477 | 1.1.0 |
| SIP H.264 Video Outdoor Intercom with RFID | 011478 | 1.1.0 |
| RFID Secure Access Control Endpoint | 011425 | 1.2.1 |
| RFID/Keypad Secure Access Control Endpoint | 011426 | 1.2.1 |

# 2.0 Understanding Administration of the products

The CyberData Access control line of products was designed with security in mind. Our devices handle RFID card encryption differently compared to other RFID readers on the market. Most other RFID card readers have cards that are preprogrammed and simply use the ID from the card for authorization; certain card brands print this ID string on the card themselves.

CyberData uses Mifare Plus X 2K or 4K cards with our RFID products. These cards are unprogrammed and will require to be programming to function. Since the cards require programming, to be used with our system, a connection to the web interface of the RFID unit is required. There is no way to program RFID cards **without** access to the unit's web interface.

Since a connection to the unit is required for programming of the cards, CyberData recommends procuring an additional unit for administration purposes when deploying many RFID card readers.

CyberData also offers a two-factor authentication option for extremely secure access situations. The RFID/Keypad Secure Access Control Endpoint (**011426**) can be used in single or two factor authentication mode if desired. When used in two factor mode the unit will require an RFID card (something you have) AND an access code (something you know) to allow access through that door.

# 3.0 Before You Start

### Network Information and Recommendations

CyberData devices can use a Fully Qualified Domain Name (FQDN) for the SIP server and Outbound Proxy addresses. CyberData Devices may need to perform a DNS A query to resolve the IP address of the configured SIP server's FQDN. It is necessary to ensure the configured DNS server(s) have an A record for the Outbound Proxy address.

In addition, be sure to verify the following ports are available for use:

- UDP 5060-5061, 5090 (SIP)
- UDP 10500 (RTP)

SIP ports 5060-5061 and RTP port 10500 are the default values on all noted firmware levels.

Alternatively, SIP ports for the paging and Nightringer extension are configurable on the **SIP** page of the web interface.

The RTP port setting on the **SIP** page is used for both extensions.

### Product Documentation and Utilities

Before you start, download the Operation and Quick Start guides from the product webpage:

RFID Secure Access Control Endpoint (011425)
RFID/Keypad Secure Access Control Endpoint (011426)
SIP Outdoor Intercom with RFID (011477)
SIP h.264 Video Outdoor Intercom with RFID (011478)

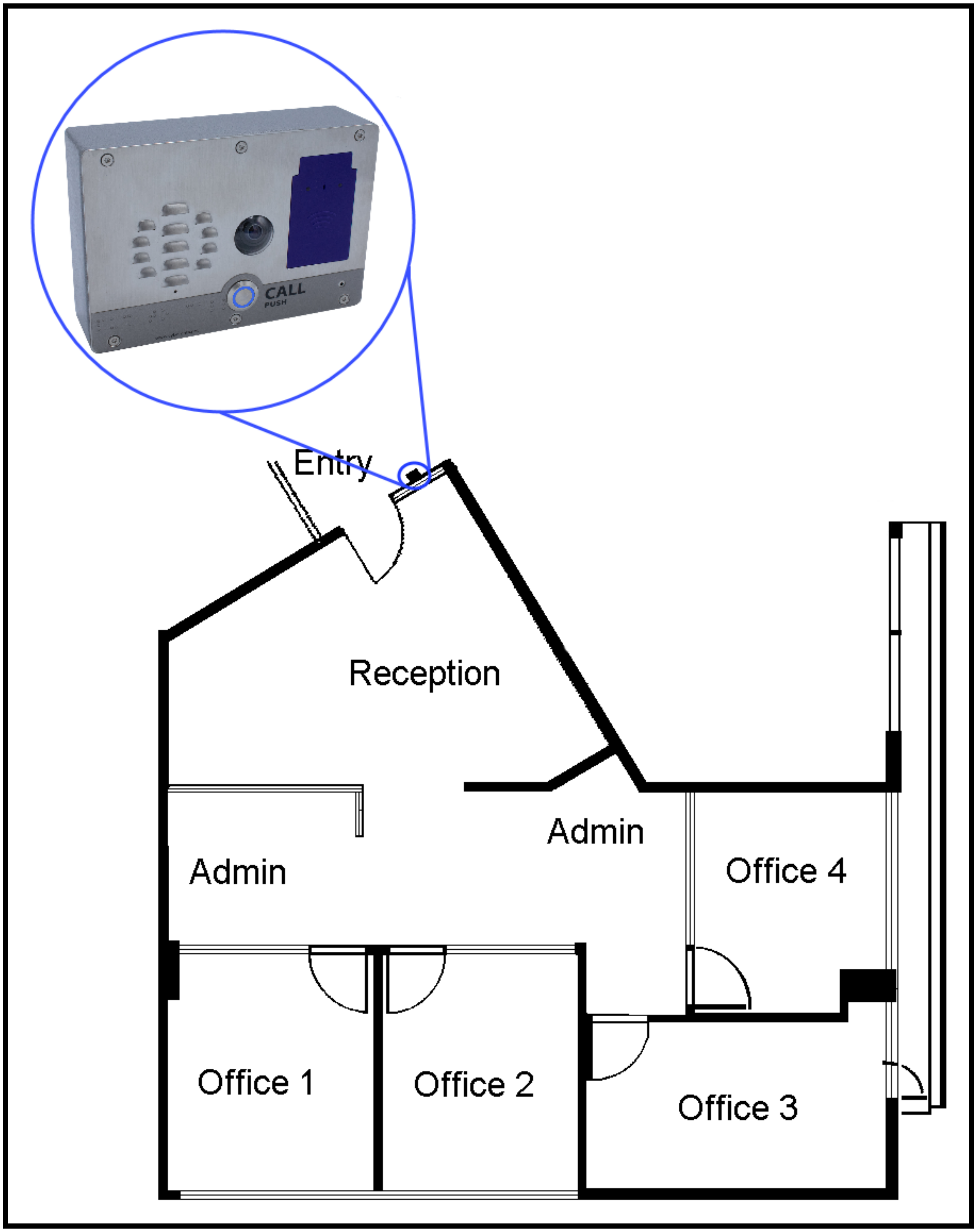
Adding users to the CyberData RFID Access control endpoint will require an active connection to the web interface of the device. This is the main way to manage the unit and will be required for the purposes of this guide.

The CyberData Discovery Utility can be used to locate CyberData devices on your network. You may download it from the following web address:
http://www.cyberdata.net/assets/common/discovery.zip

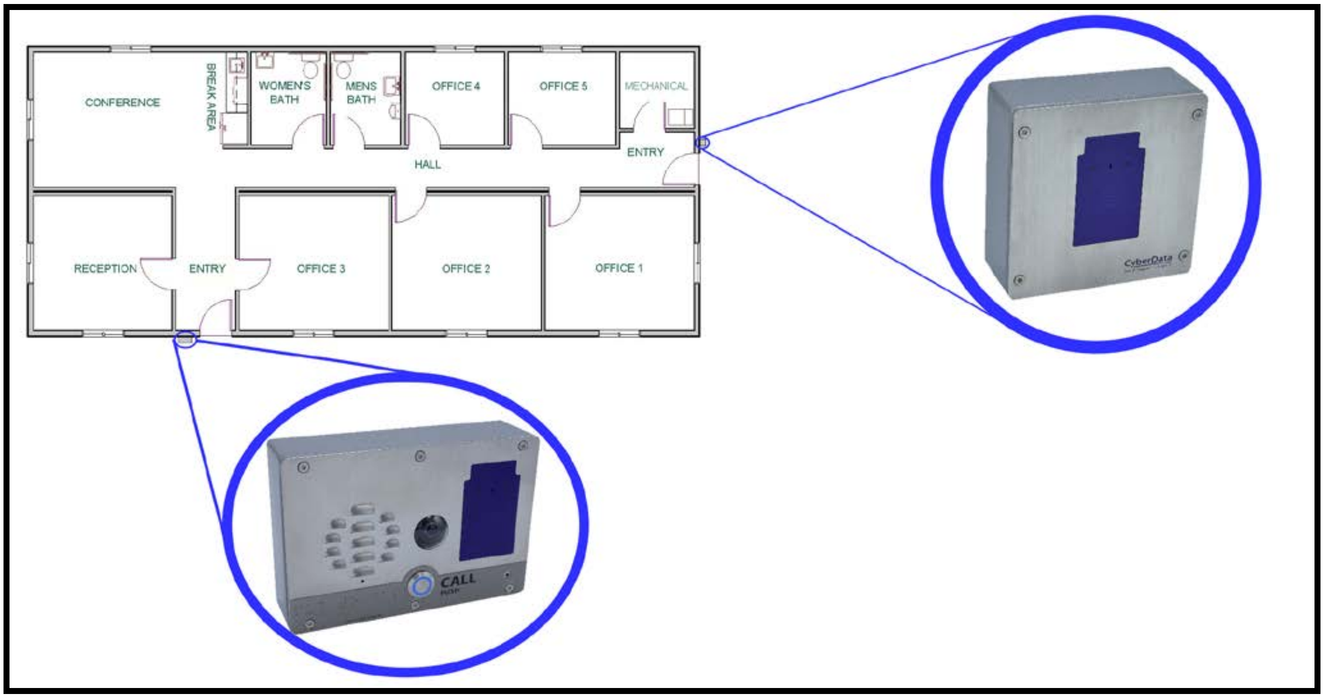
**Note**: DHCP addressing mode is enabled on default on all noted firmware levels.

## 3.1 Typical Deployments

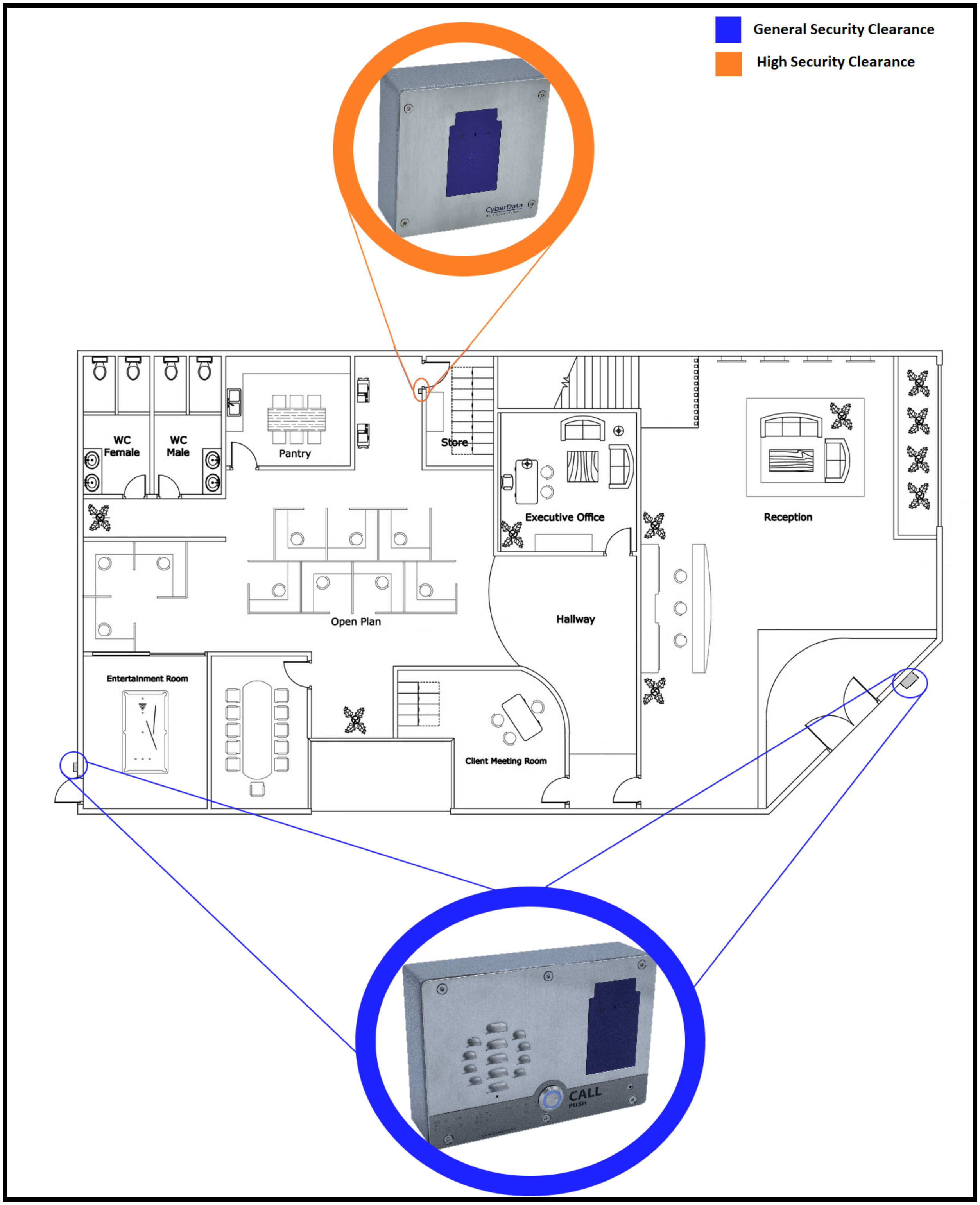
**Single RFID Intercom**



## Two RFID Intercoms, Same Access Level



# Multiple RFID Intercoms, Two Access levels



# 4.0 Configuring an RFID endpoint.

This section applies to the following products:

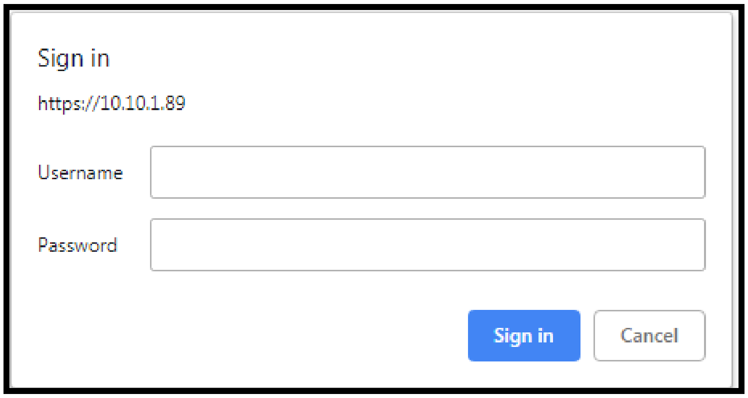
- SIP Outdoor Intercom with RFID - 011477
- SIP H.264 Video Outdoor Intercom with RFID - 011478
- RFID Secure Access Control Endpoint - 011425

**1.** Click **Launch Browser** from the CyberData Discovery Utility or point your browser to the CyberData device's IP address to access the Home Page of the web interface.

**2**. Enter the default credentials when prompted and click the **Sign In** button.

Username: admin
Password: admin

**Figure 4-1. Web Interface Login**



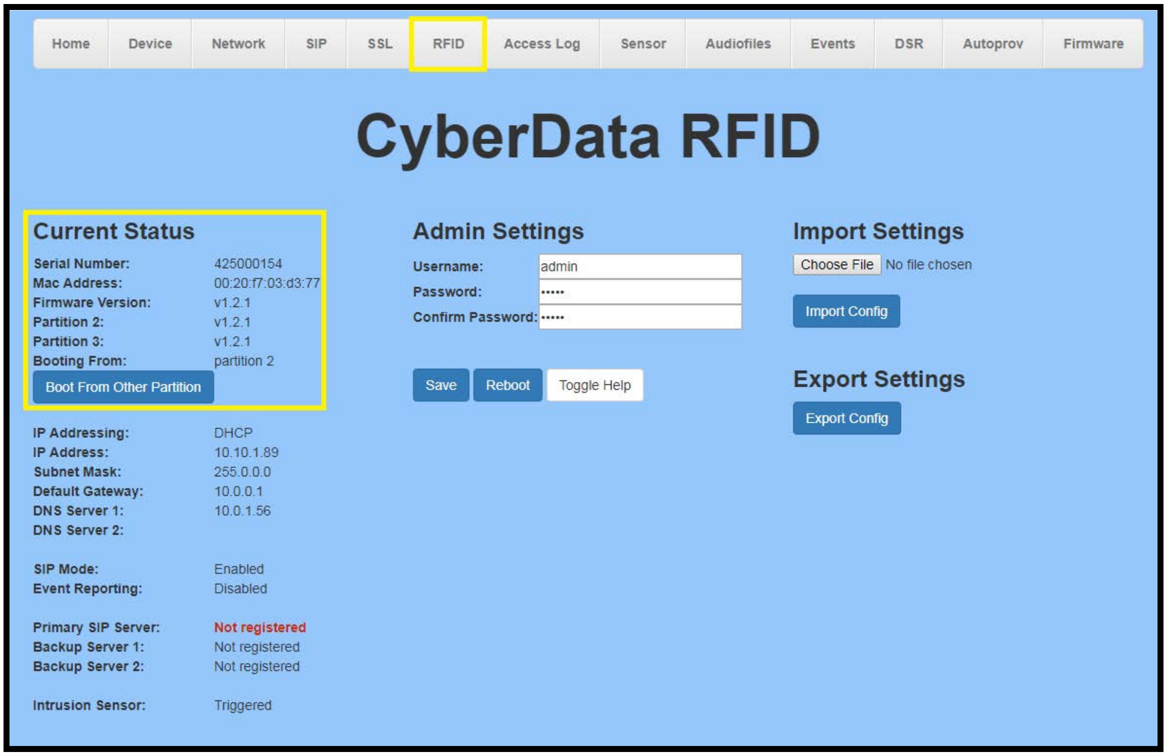
Sign in

https://10.10.1.89

Username

Password

**Figure 4-2. RFID Home Tab**



CyberData RFID

Current Status

Serial Number: 425000154
Mac Address: 00:20:f7:03:d3:77
Firmware Version: v1.2.1
Partition 2: v1.2.1
Partition 3: v1.2.1
Booting From: partition 2

IP Addressing: DHCP
IP Address: 10.10.1.89
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

SIP Mode: Enabled
Event Reporting: Disabled

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

Intrusion Sensor: Triggered

Admin Settings

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

Import Settings

No file chosen

Export Settings

**3.** On the Home tab, click on RFID on the top toolbar of your screen to access the RFID tab.

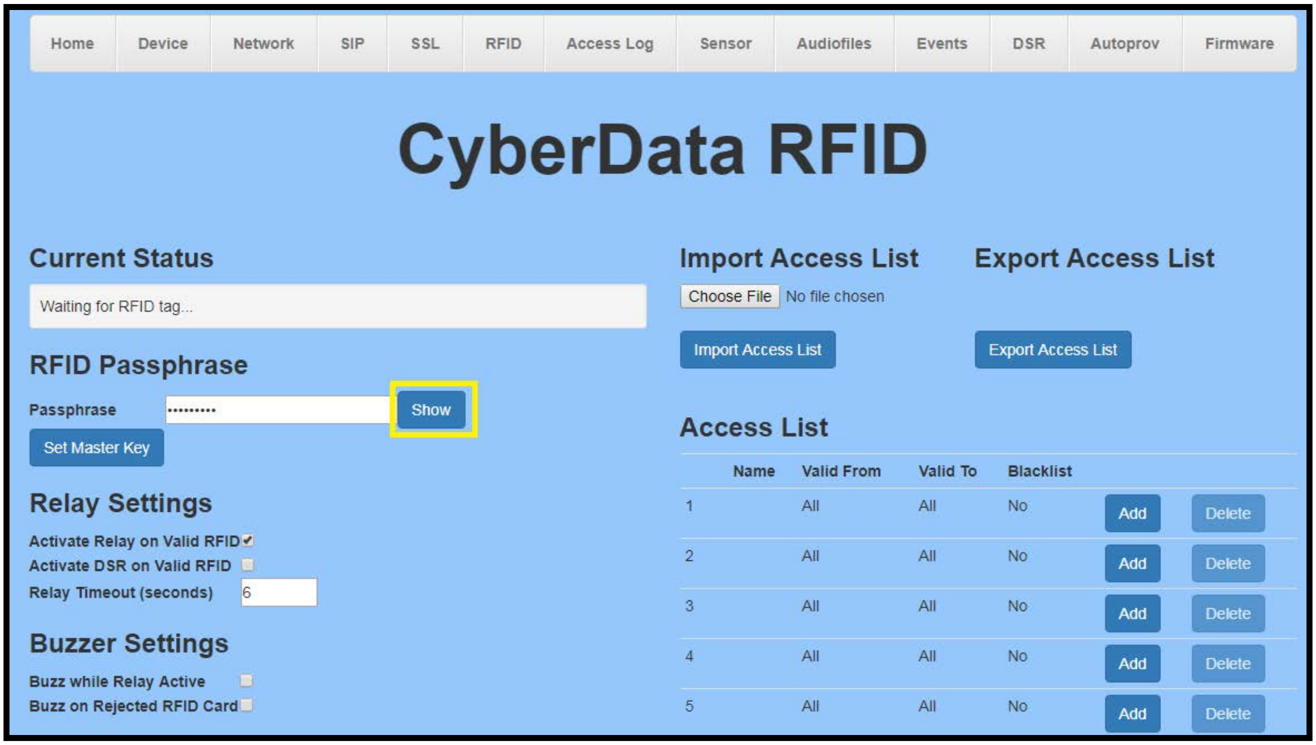
***Note****: The firmware version, network information and registration status are shown on the home tab.*

**4.** The passphrase for the unit must be changed before cards are programmed.

**Note:** The passphrase is a word or phrase that is used in the programming in the RFID cards. This passphrase makes the cards more secure and unique since it is required for programming.

**Important Note: The Passphrase is extremely important in creating new cards and managing multiple RFID endpoints. Make sure to retain the Passphrase in a safe location.**

## 4-3. RFID Passphrase



# CyberData RFID

## Current Status

Waiting for RFID tag...

## RFID Passphrase

Passphrase ••••••••• Show

Set Master Key

## 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 □

## Import Access List

Choose File No file chosen

Import Access List

## Export Access List

Export Access List

## Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | | All | All | No | Add | Delete |
| 2 | | All | All | No | Add | Delete |
| 3 | | All | All | No | Add | Delete |
| 4 | | All | All | No | Add | Delete |
| 5 | | All | All | No | Add | Delete |

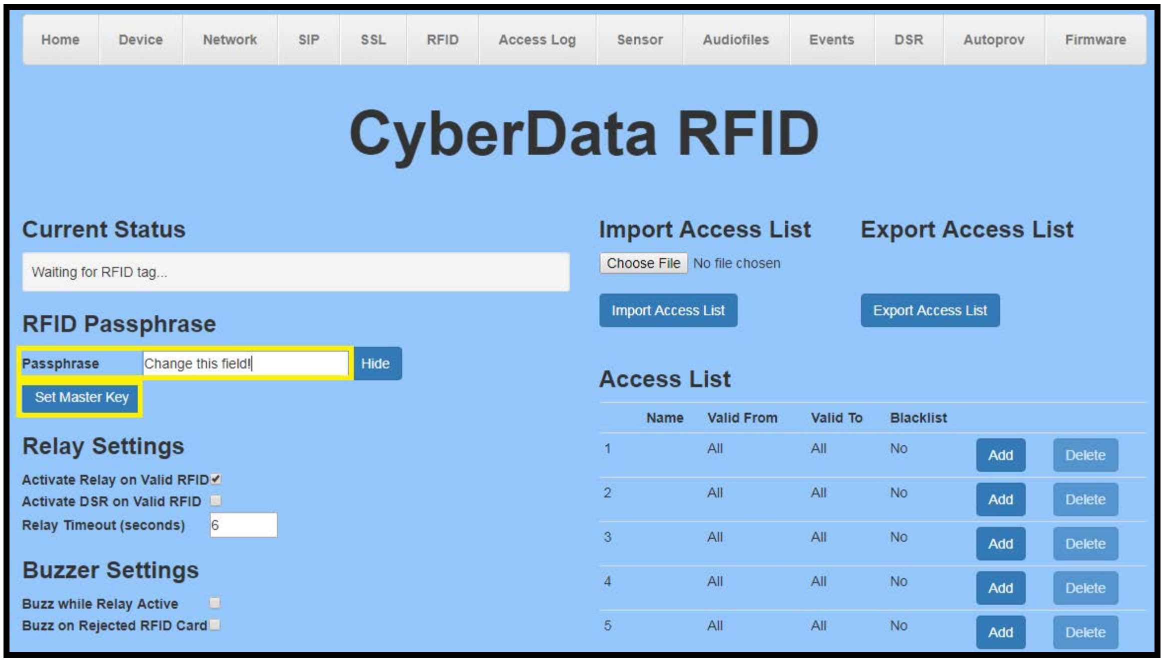
**5.** Press the Show button to see the passphrase as you set it.

***Note:*** *The passphrase can be between 1-255 characters. The longer the passphrase the stronger the encryption.*

**6.** Set the RFID passphrase.

**7.** Press the Set Master Key button.

### 4-4. Set the Passphrase



CyberData RFID

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase: Change this field!

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 ☐

Import Access List

No file chosen

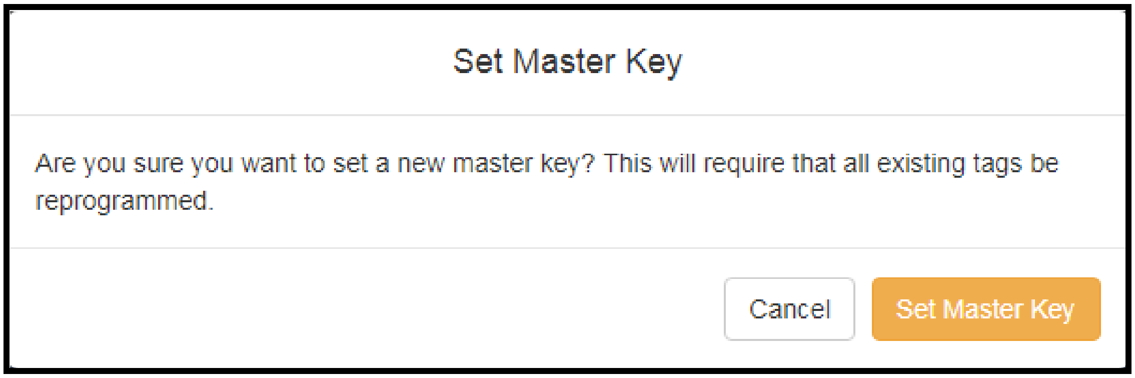
Export Access List

Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | | All | All | No | Add | Delete |
| 2 | | All | All | No | Add | Delete |
| 3 | | All | All | No | Add | Delete |
| 4 | | All | All | No | Add | Delete |
| 5 | | All | All | No | Add | Delete |

**8.** Accept the popup.

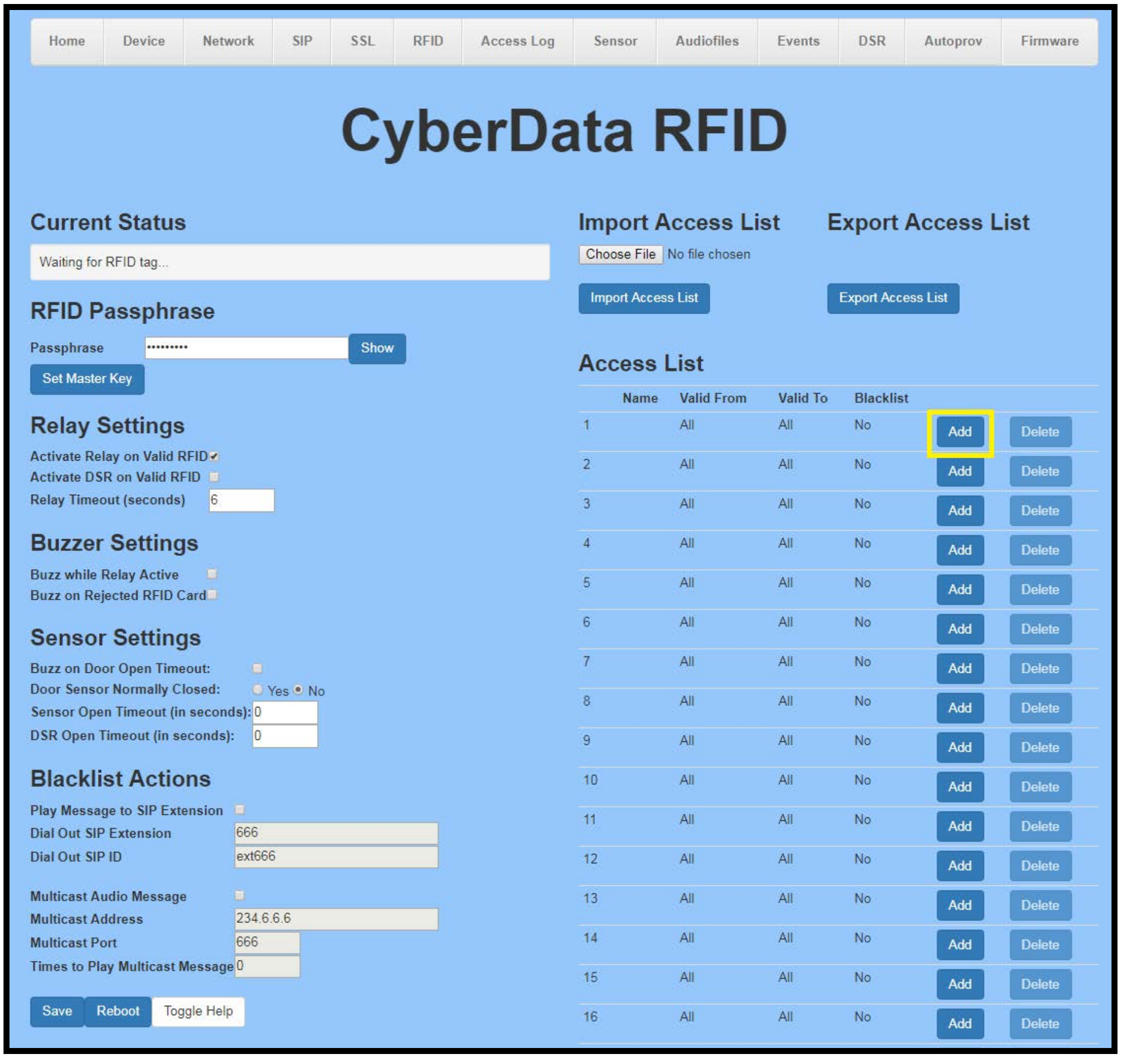
### 4-5. Set the Master Key



Set Master Key

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

## Figure 4-6. RFID Tab



Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase: •••••••• [Show]

[Set Master Key]

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

[Save] [Reboot] [Toggle Help]

Import Access List

[Choose File] No file chosen

[Import Access List]

Export Access List

[Export Access List]

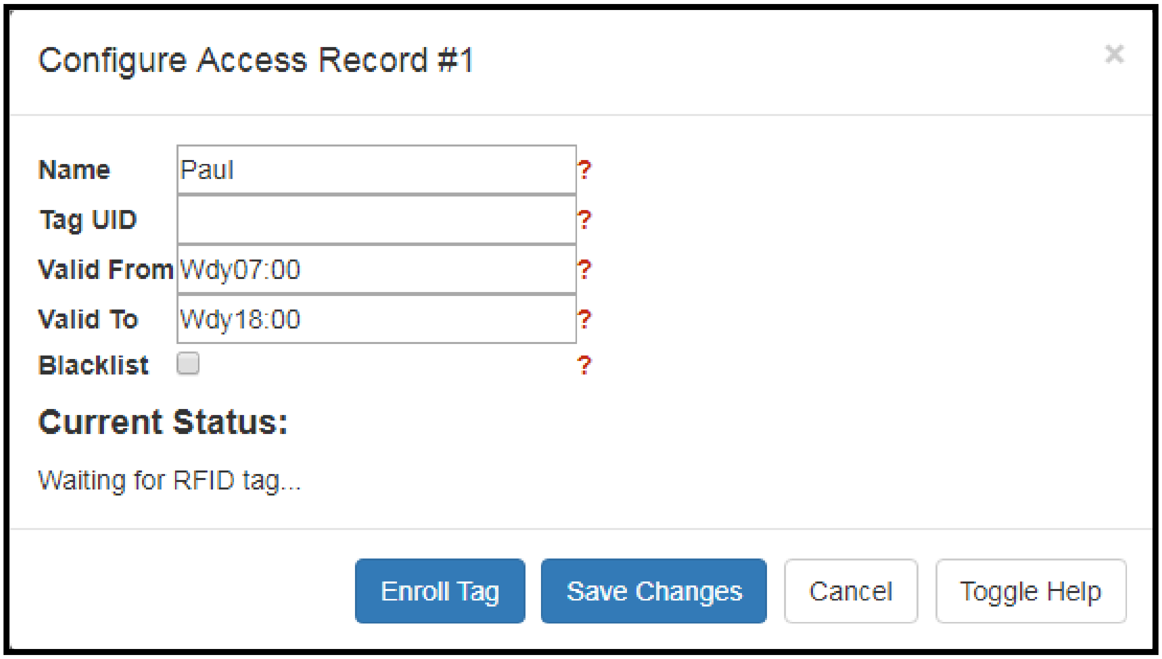
Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | | All | All | No | Add | Delete |
| 2 | | All | All | No | Add | Delete |
| 3 | | All | All | No | Add | Delete |
| 4 | | All | All | No | Add | Delete |
| 5 | | All | All | No | Add | Delete |
| 6 | | All | All | No | Add | Delete |
| 7 | | All | All | No | Add | Delete |
| 8 | | All | All | No | Add | Delete |
| 9 | | All | All | No | Add | Delete |
| 10 | | All | All | No | Add | Delete |
| 11 | | All | All | No | Add | Delete |
| 12 | | All | All | No | Add | Delete |
| 13 | | All | All | No | Add | Delete |
| 14 | | All | All | No | Add | Delete |
| 15 | | All | All | No | Add | Delete |
| 16 | | All | All | No | Add | Delete |

***Note:*** *The RFID tab is used to enroll new RFID tags and change settings that involve the use of RFID cards. This page is used to setup the blacklisted card actions taken by the device when a blacklisted card is used.*

**9.** Press the Add button to enroll a new card.

## 4-7. Configure Access Record



Configure Access Record #1

Name: Paul

Tag UID:

Valid From: Wdy07:00

Valid To: Wdy18:00

Blacklist: □

**Current Status:**

Waiting for RFID tag...

***Note**: The toggle help function will give information about the specific requirements for the valid to and valid from fields.*

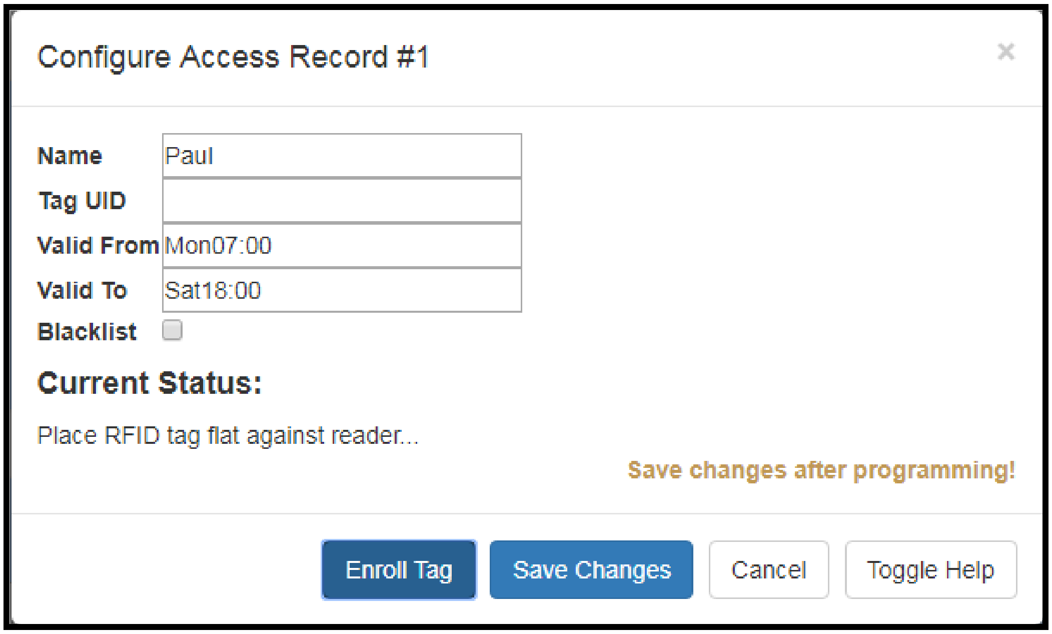
**10.** Set the Name of the user for the RFID card.

**11.** Set the Valid from and Valid to times.

***Note:** The valid times must have a three-letter code and can have a time as well. In the screenshot Paul's card is set to be valid for Weekdays (Wdy) from 7:00am to 6:00pm. Other three-letter codes are Mon-Sun for days of the week.*

**12.** Press Enroll Tag to begin the tag programming process.

## 4-8. Card Programming


Configure Access Record #1

Name: Paul
Tag UID:
Valid From: Mon07:00
Valid To: Sat18:00
Blacklist: □

**Current Status:**

Place RFID tag flat against reader...

Save changes after programming!

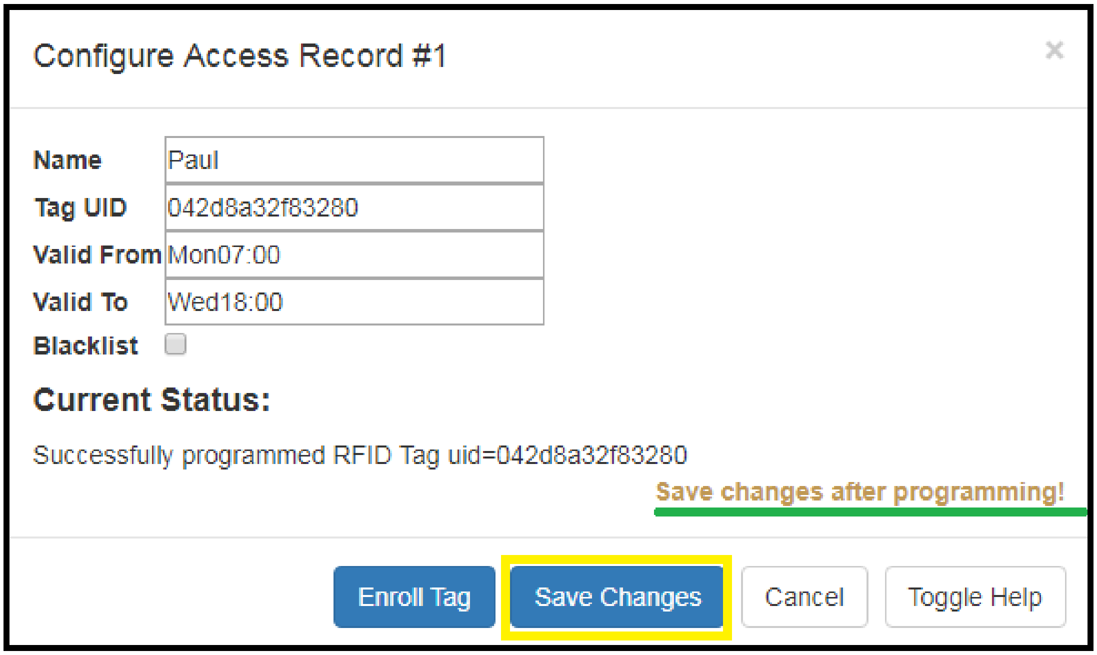
***Note:*** *The unit is now in programming mode and any card held in the field will be programmed. There will be onscreen instructions to walk through the programming process. Only one card can be associated with a user.*

**13.** Hold the RFID card flat against the reader to program the card. The card will be programmed, which only takes a few seconds.

**14.** During the programming status the Current Status field will show the current action of the reader.

**15.** Once programmed the popup will show the UID of the card. Make sure to save changes.

4-9. Card Programmed



Configure Access Record #1

Name: Paul

Tag UID: 042d8a32f83280

Valid From: Mon07:00

Valid To: Wed18:00

Blacklist: □

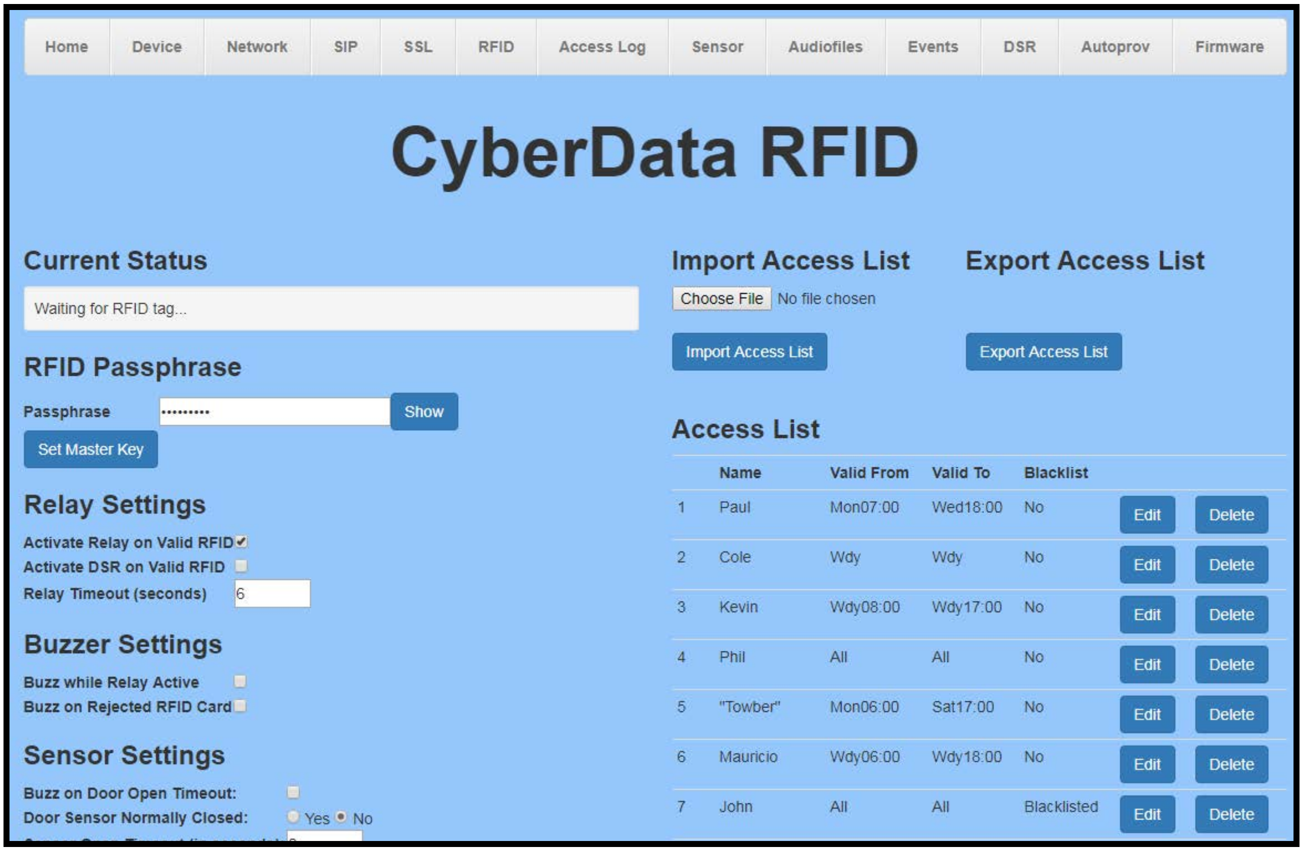
**Current Status:**

Successfully programmed RFID Tag uid=042d8a32f83280

Save changes after programming!

**16.** Repeat these steps to enroll multiple users of the RFID reader.

Figure 4-10. Populated list of access users



## Current Status

Waiting for RFID tag...

## RFID Passphrase

Passphrase ••••••••• Show

Set Master Key

## 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

## Import Access List

Choose File No file chosen

Import Access List

## Export Access List

Export Access List

## Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | Paul | Mon07:00 | Wed18:00 | No | Edit | Delete |
| 2 | Cole | Wdy | Wdy | No | Edit | Delete |
| 3 | Kevin | Wdy08:00 | Wdy17:00 | No | Edit | Delete |
| 4 | Phil | All | All | No | Edit | Delete |
| 5 | "Towber" | Mon06:00 | Sat17:00 | No | Edit | Delete |
| 6 | Mauricio | Wdy06:00 | Wdy18:00 | No | Edit | Delete |
| 7 | John | All | All | Blacklisted | Edit | Delete |

**17.** Once the list of users is created press the Export Access List button to export a file containing the newly created users.

**18.** Simply import the exported list to any new RFID access control devices to configure them.

# 5.0 Configuring a Keypad/RFID Endpoint

This section applies to the following product:

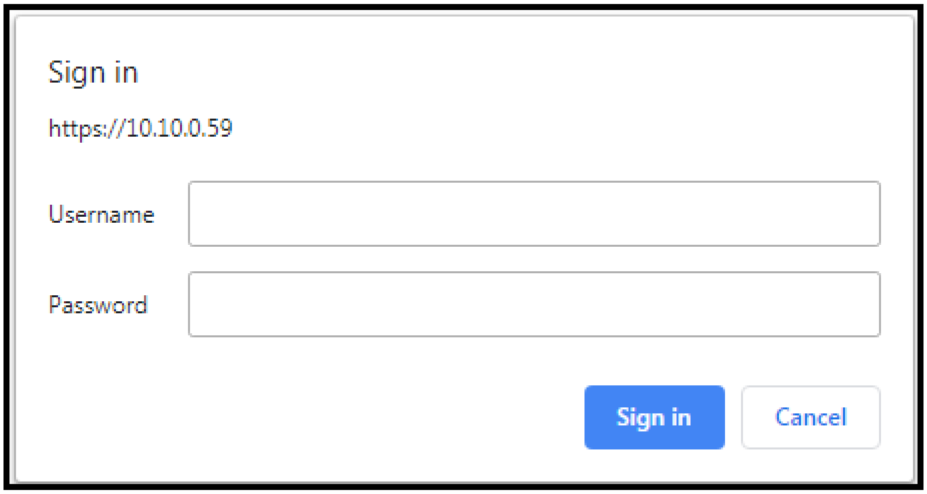
- RFID/Keypad Secure Access Control Endpoint - 011426

**1.** Click **Launch Browser** from the CyberData Discovery Utility or point your browser to the CyberData device's IP address to access the Home Page of the web interface.

**2.** Enter the default credentials when prompted and click the **Sign In** button.

Username: admin
Password: admin

**Figure 5-1. Web Interface Login**



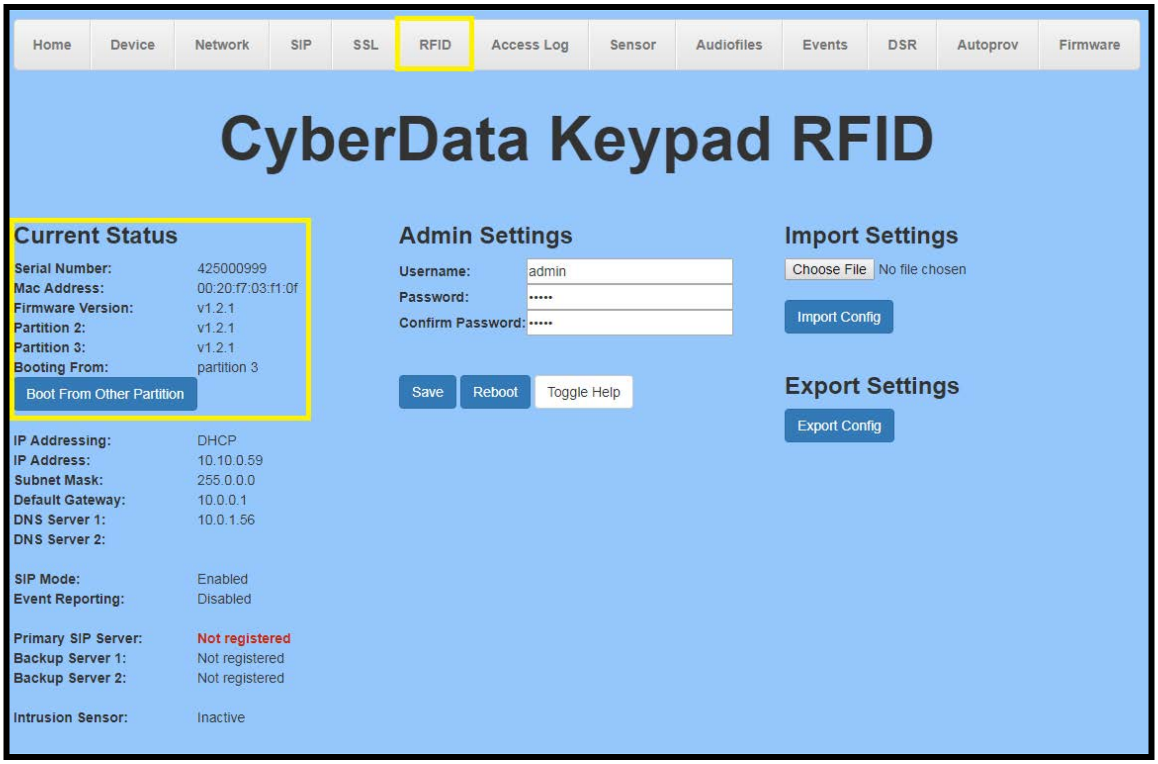
Sign in

https://10.10.0.59

Username

Password

Figure 5-2. RFID Home Tab



CyberData Keypad RFID

Current Status

| | |
|---|---|
| Serial Number: | 425000999 |
| Mac Address: | 00:20:f7:03:f1:0f |
| Firmware Version: | v1.2.1 |
| Partition 2: | v1.2.1 |
| Partition 3: | v1.2.1 |
| Booting From: | partition 3 |
| IP Addressing: | DHCP |
| IP Address: | 10.10.0.59 |
| Subnet Mask: | 255.0.0.0 |
| Default Gateway: | 10.0.0.1 |
| DNS Server 1: | 10.0.1.56 |
| DNS Server 2: | |
| SIP Mode: | Enabled |
| Event Reporting: | Disabled |
| Primary SIP Server: | Not registered |
| Backup Server 1: | Not registered |
| Backup Server 2: | Not registered |
| Intrusion Sensor: | Inactive |

Admin Settings

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

Import Settings

No file chosen

Export Settings

**3.** On the Home tab, click on RFID on the top toolbar of your screen to access the RFID tab.

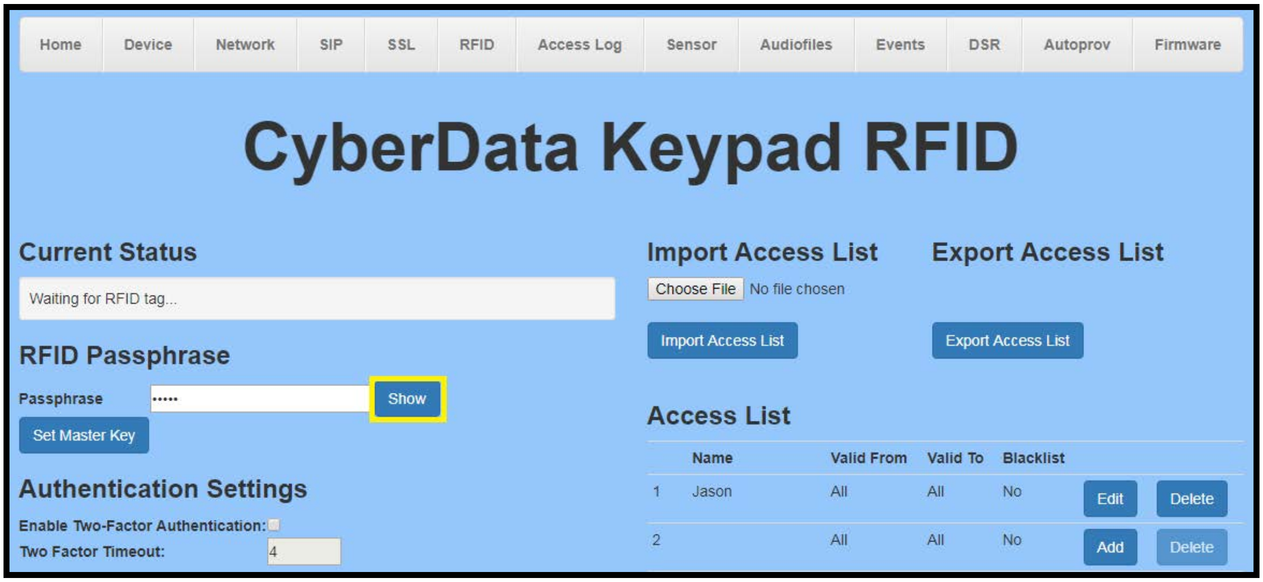
***Note****: The firmware version, network information and registration status are shown on the home tab.*

**4.** The passphrase for the unit must be changed before cards are programmed.

***Note:** The passphrase is a word or phrase that is used in the programming in the RFID cards. This passphrase makes the cards more secure and unique since it is required for programming.*

**Important Note: The Passphrase is extremely important in creating new cards and managing multiple RFID endpoints. Make sure to retain the Passphrase in a safe location.**

## 5-3. RFID Passphrase



CyberData Keypad RFID

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase: •••••

Authentication Settings

Enable Two-Factor Authentication: □

Two Factor Timeout: 4

Import Access List

No file chosen

Export Access List

Access List

| | Name | Valid From | Valid To | Blacklist |
|---|---|---|---|---|
| 1 | Jason | All | All | No |
| 2 | | All | All | No |

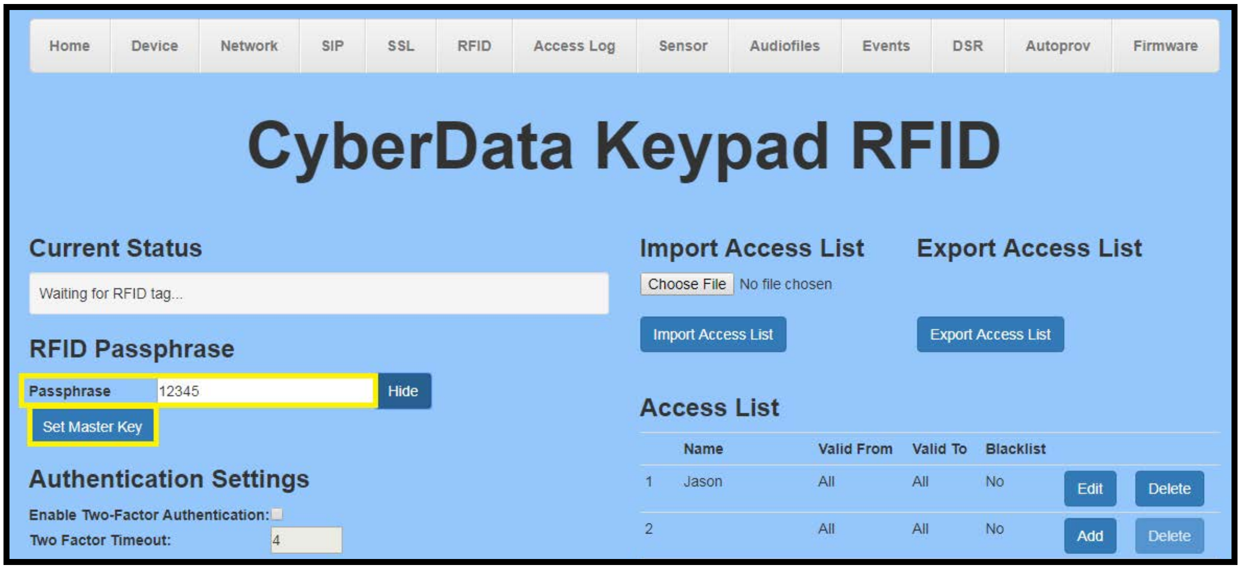
**5.** Press the Show button to see the passphrase as you set it.

***Note:*** *The passphrase can be between 1-255 characters. The longer the passphrase the stronger the encryption.*

**6.** Set the RFID passphrase.

**7.** Press the Set Master Key button.

### 5-4. Set the Passphrase



CyberData Keypad RFID

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase: 12345

Authentication Settings

Enable Two-Factor Authentication: □

Two Factor Timeout: 4

Import Access List

Choose File No file chosen

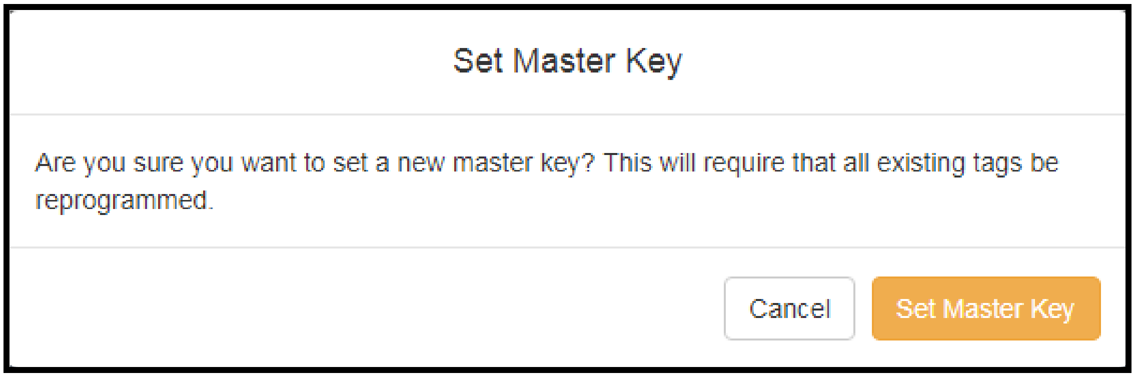
Export Access List

Access List

|  | Name | Valid From | Valid To | Blacklist |
|---|---|---|---|---|
| 1 | Jason | All | All | No |
| 2 |  | All | All | No |

**8.** Accept the popup.

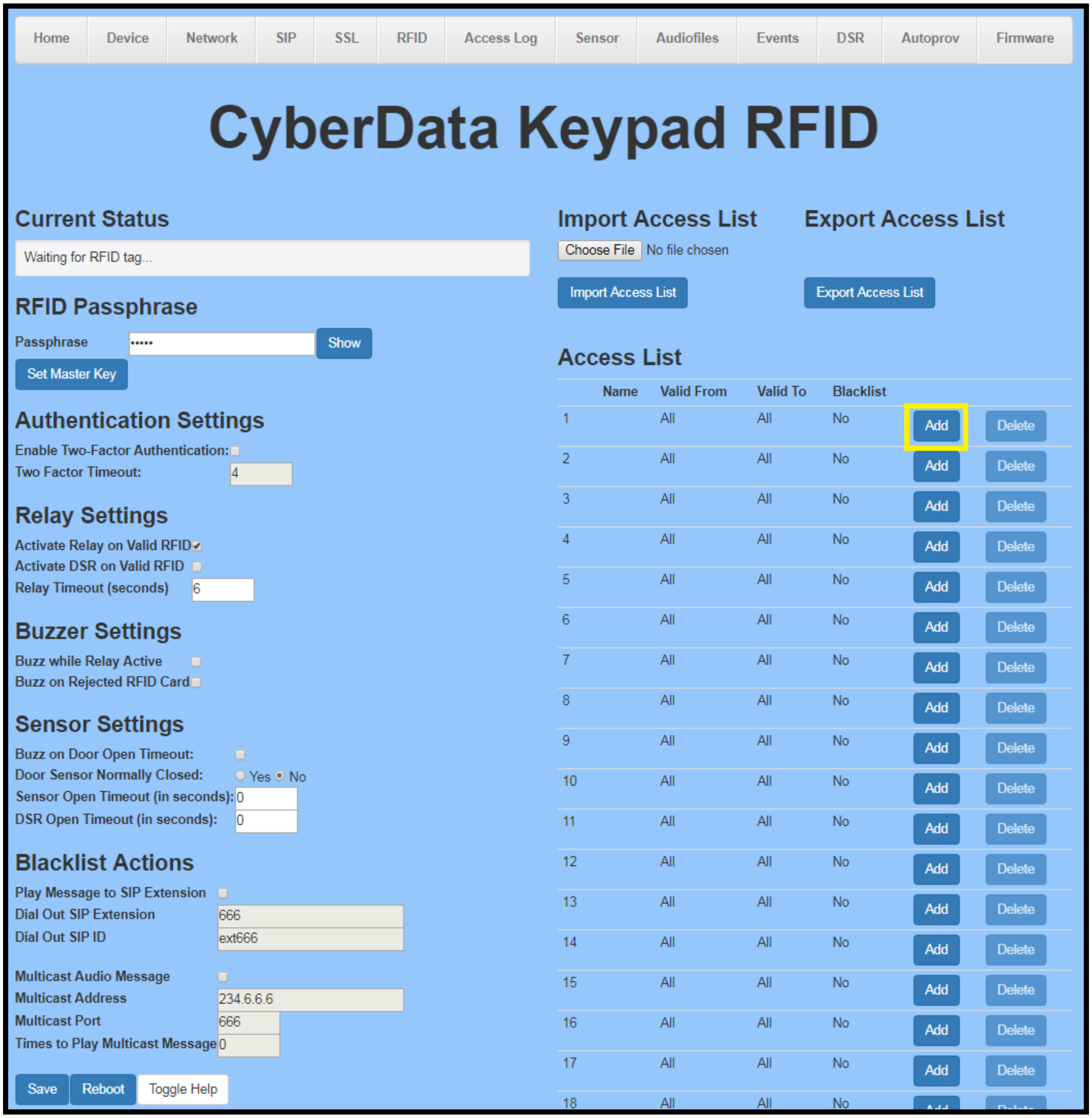
### 5-5. Set the Master Key



Set Master Key

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

**Figure 5-6. RFID Tab**



CyberData Keypad RFID

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase •••••

Authentication Settings

Enable Two-Factor Authentication: □
Two Factor Timeout: 4

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

Choose File No file chosen

Export Access List

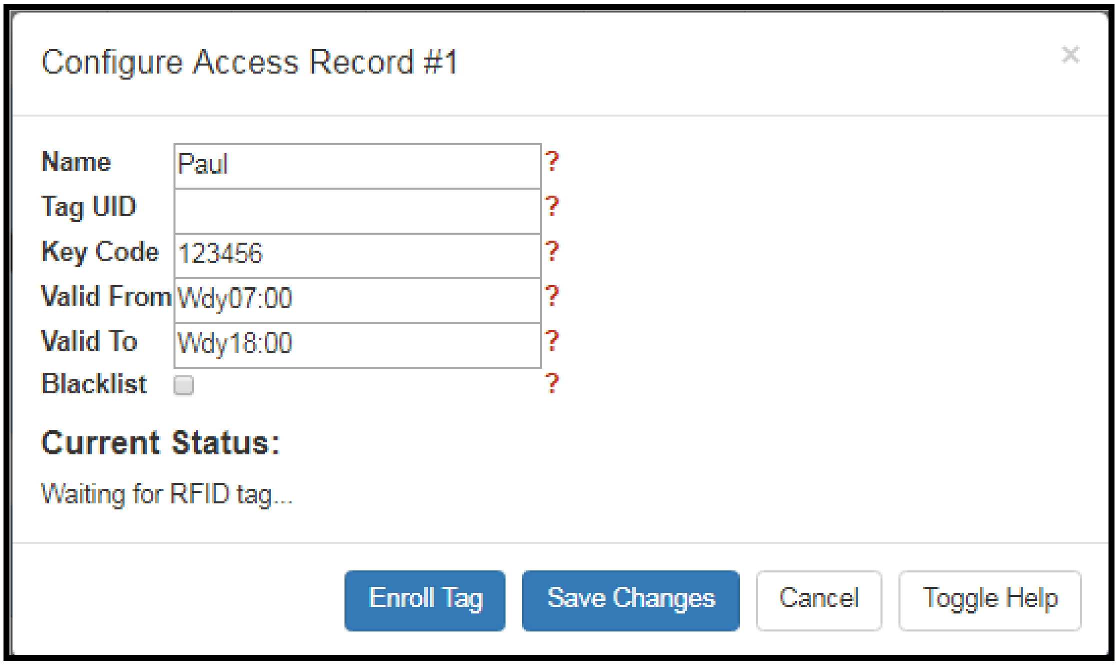
Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | | All | All | No | Add | Delete |
| 2 | | All | All | No | Add | Delete |
| 3 | | All | All | No | Add | Delete |
| 4 | | All | All | No | Add | Delete |
| 5 | | All | All | No | Add | Delete |
| 6 | | All | All | No | Add | Delete |
| 7 | | All | All | No | Add | Delete |
| 8 | | All | All | No | Add | Delete |
| 9 | | All | All | No | Add | Delete |
| 10 | | All | All | No | Add | Delete |
| 11 | | All | All | No | Add | Delete |
| 12 | | All | All | No | Add | Delete |
| 13 | | All | All | No | Add | Delete |
| 14 | | All | All | No | Add | Delete |
| 15 | | All | All | No | Add | Delete |
| 16 | | All | All | No | Add | Delete |
| 17 | | All | All | No | Add | Delete |
| 18 | | All | All | No | | |

***Note:** The RFID tab is used to enroll new RFID tags and change settings that involve the use of RFID cards. This page is used to setup the blacklisted card actions taken by the device when a blacklisted card is used.*

**9.** Press the Add button to enroll a new card.

## 5-7. Configure Access Record



Configure Access Record #1

| | |
|---|---|
| Name | Paul |
| Tag UID | |
| Key Code | 123456 |
| Valid From | Wdy07:00 |
| Valid To | Wdy18:00 |
| Blacklist | □ |

**Current Status:**

Waiting for RFID tag...

***Note****: The toggle help function will give information about the specific requirements for the valid to and valid from fields.*

**10.** Set the Name of the user for the RFID card.

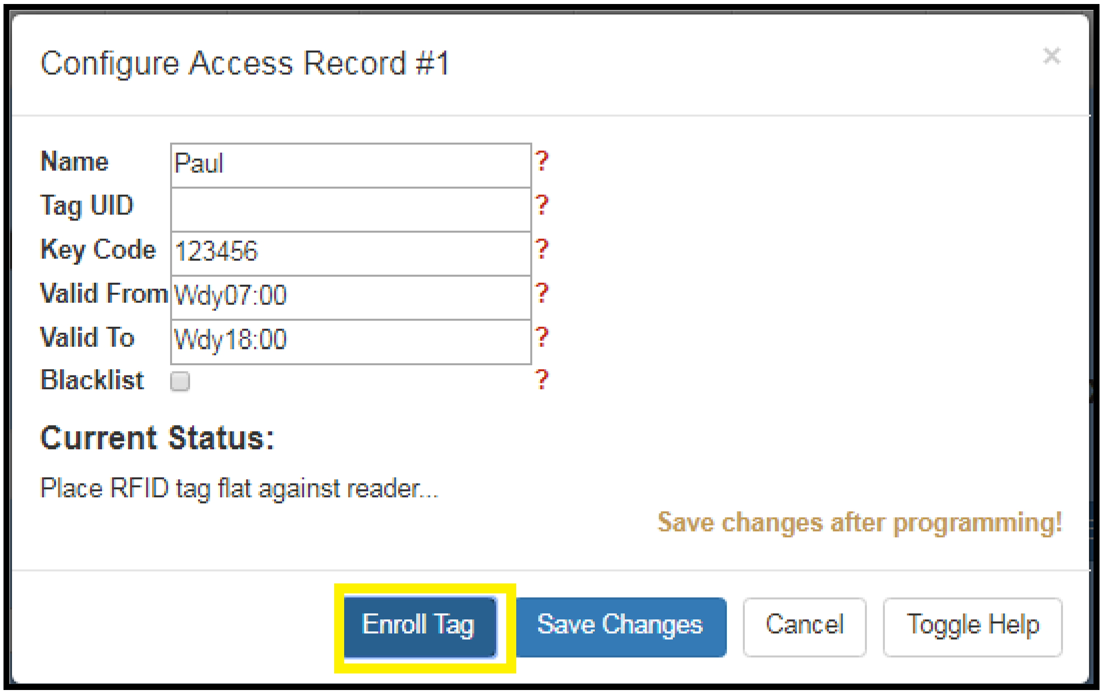
**11.** Set the Keycode for the user.

**12.** Set the Valid from and Valid to times.

***Note:*** *The valid times must have a three-letter code and can have a time as well. In the screenshot Paul's card is set to be valid for Weekdays (Wdy) from 7:00am to 6:00pm. Other three-letter codes are Mon-Sun for days of the week.*

**13.** Press Enroll Tag to begin the tag programming process.

**5-8. Card Programming**



Configure Access Record #1

| | |
|---|---|
| Name | Paul |
| Tag UID | |
| Key Code | 123456 |
| Valid From | Wdy07:00 |
| Valid To | Wdy18:00 |
| Blacklist | □ |

**Current Status:**

Place RFID tag flat against reader...

Save changes after programming!

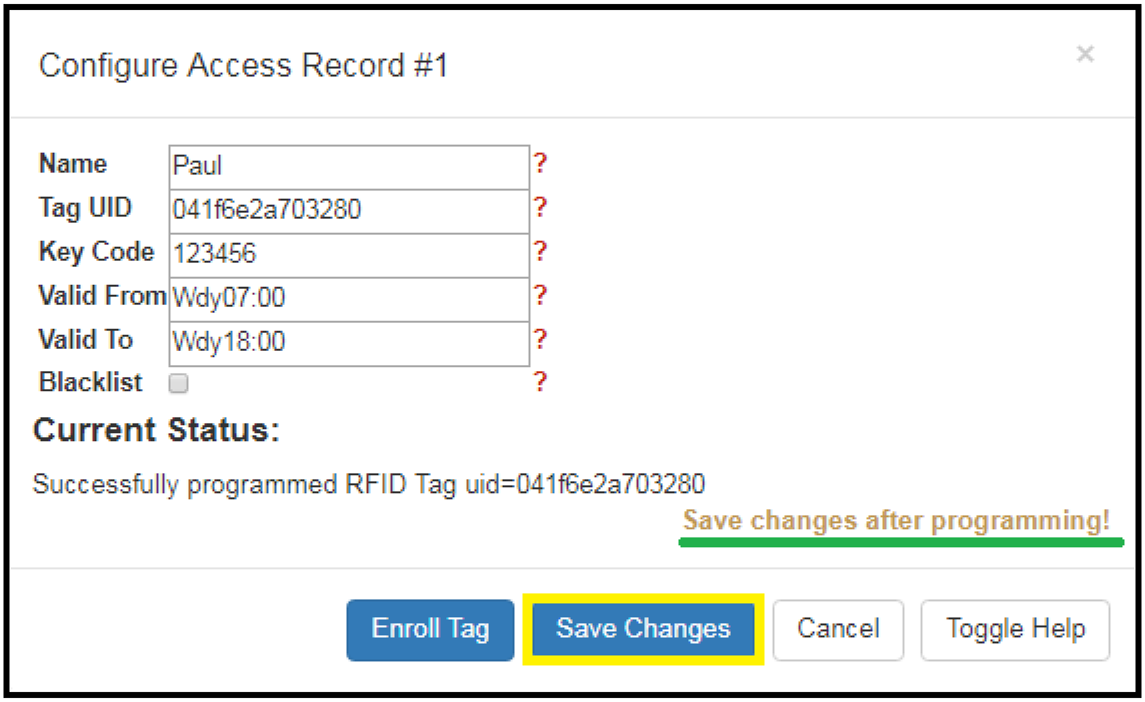
***Note:*** *The unit is now in programming mode and any card held in the field will be programmed. There will be onscreen instructions to walk through the programming process. Only one card can be associated with a user.*

**14.** Hold the RFID card flat against the reader to program the card. The card will be programmed, which only takes a few seconds.

**15.** During the programming status the Current Status field will show the current action of the reader.

**16.** Once programmed the popup will show the UID of the card. Make sure to save changes.

**5-9. Card Programmed**



Configure Access Record #1

| | |
|---|---|
| Name | Paul |
| Tag UID | 041f6e2a703280 |
| Key Code | 123456 |
| Valid From | Wdy07:00 |
| Valid To | Wdy18:00 |
| Blacklist | □ |

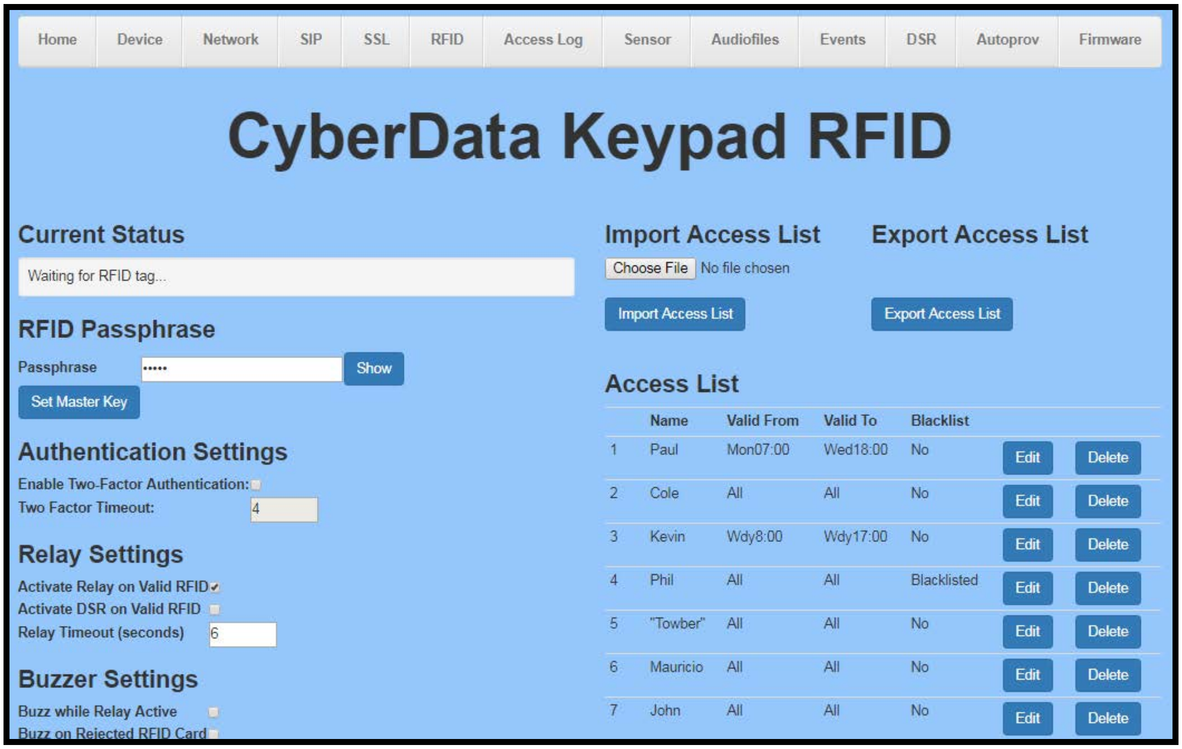
Current Status:

Successfully programmed RFID Tag uid=041f6e2a703280

Save changes after programming!

**16.** Repeat these steps to enroll multiple users of the RFID reader.

**Figure 5-10. Populated list of access users**



CyberData Keypad RFID

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase •••••

Authentication Settings

Enable Two-Factor Authentication: ☐
Two Factor Timeout: 4

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 ☐

Import Access List

No file chosen

Export Access List

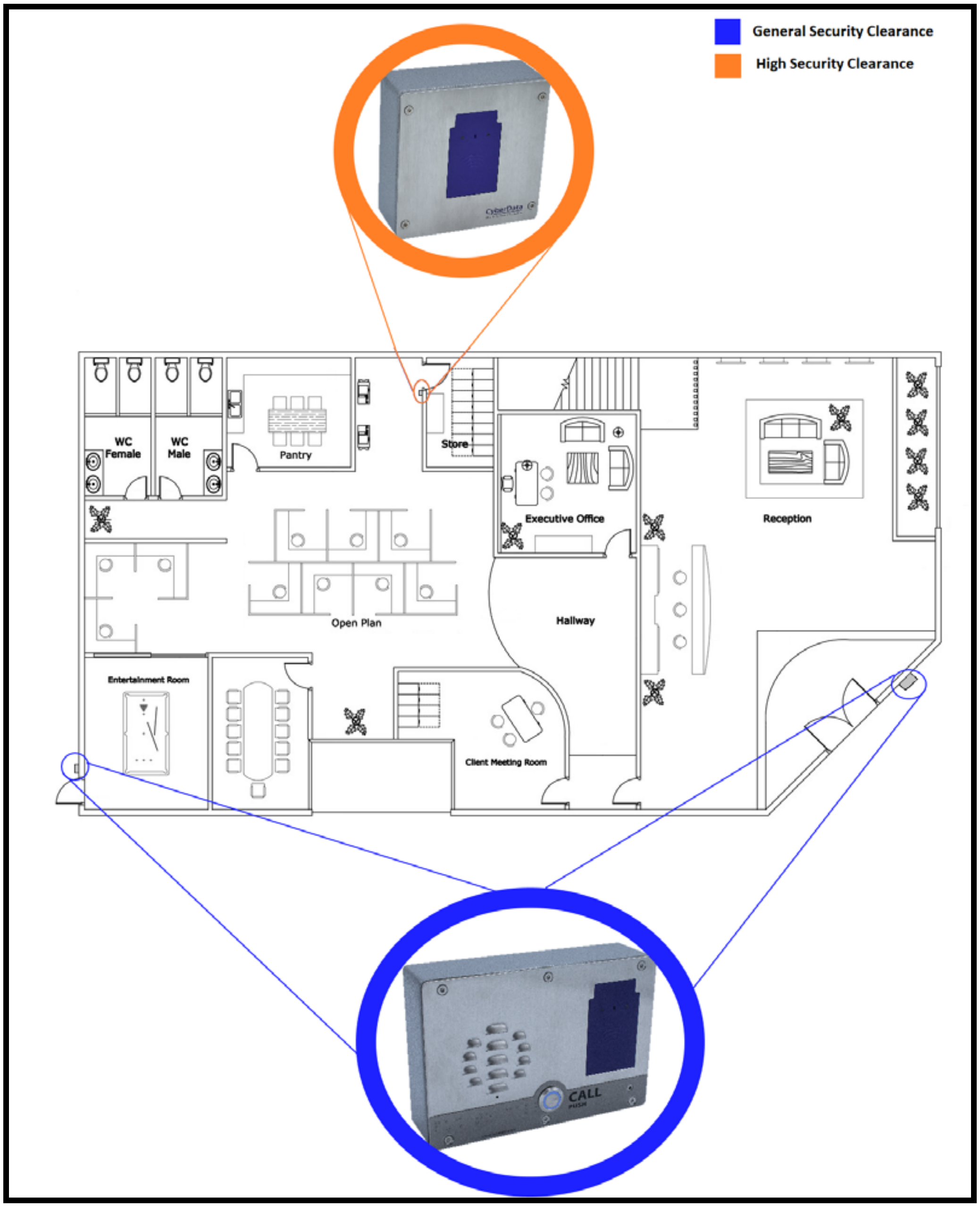
Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | Paul | Mon07:00 | Wed18:00 | No | Edit | Delete |
| 2 | Cole | All | All | No | Edit | Delete |
| 3 | Kevin | Wdy8:00 | Wdy17:00 | No | Edit | Delete |
| 4 | Phil | All | All | Blacklisted | Edit | Delete |
| 5 | "Towber" | All | All | No | Edit | Delete |
| 6 | Mauricio | All | All | No | Edit | Delete |
| 7 | John | All | All | No | Edit | Delete |

# 6.0 Creating Different Security Levels

There are going to be situations where not every user can have access to a door. There are multiple ways to achieve a different security level or access list for an endpoint. CyberData recommends creating a master list of users and removing users from that list that do not need access to create a different security level.

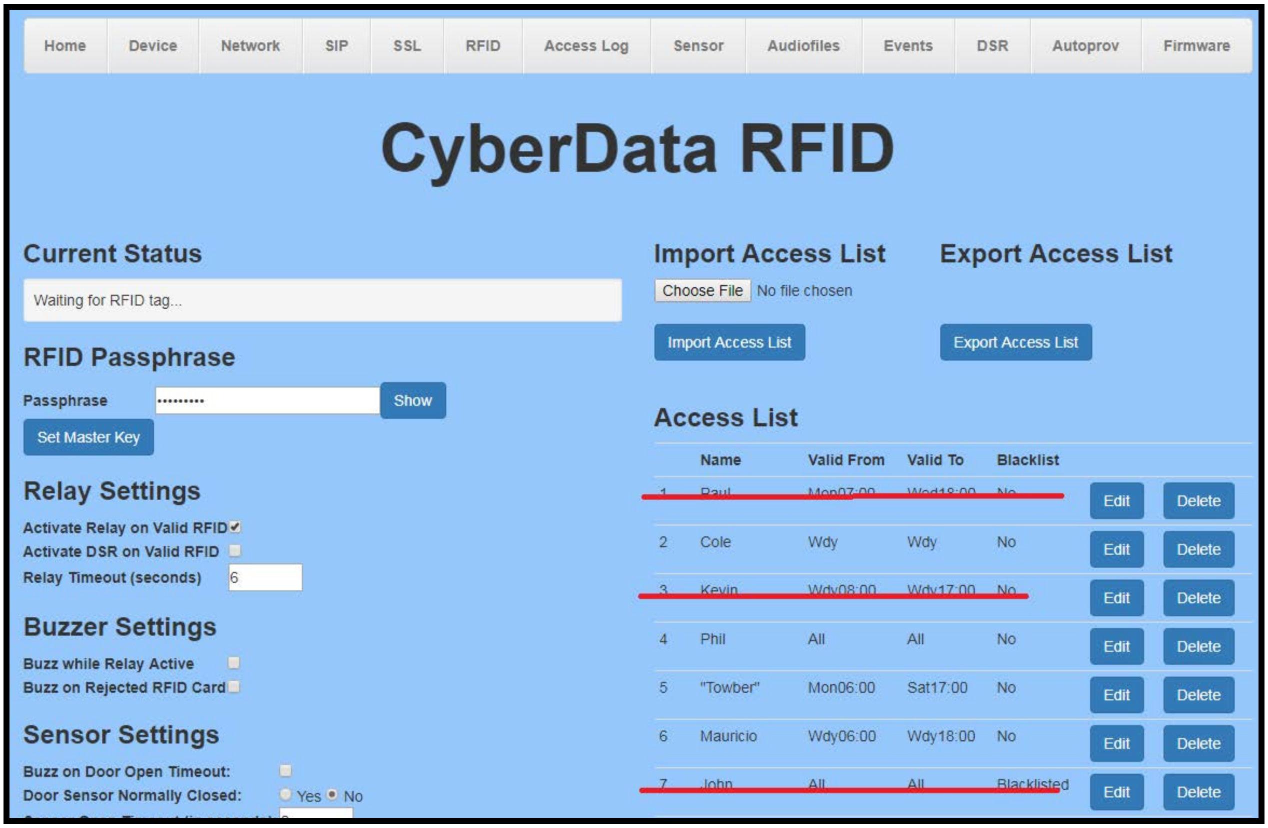
**Figure 6-1. Example of different security levels**



After adding all users to the main access level or 'Master List' export that list and store it in a safe location. Users can then be removed from the Master list to create a new access list or different security level. It will be easier to go from the least secure access list (list with most users) to a more secure list (less users).

1. Starting from the 'Master List' determine which users have access to the other door.

**Figure 6-2. Master List**



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

No file chosen

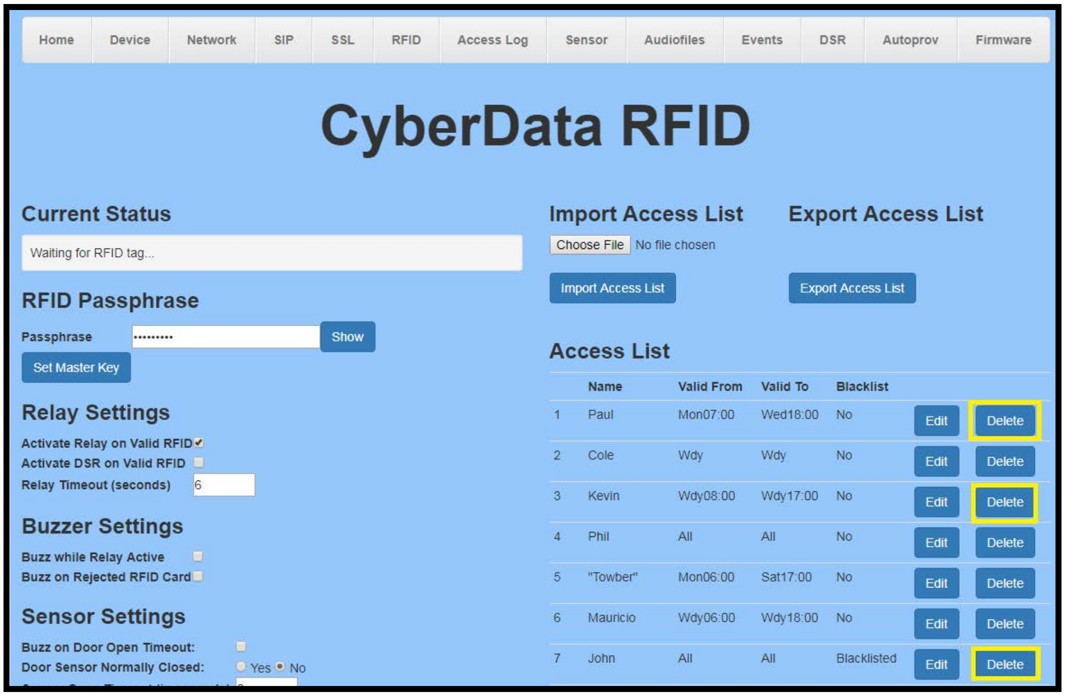
Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| ~~1~~ | ~~Paul~~ | ~~Mon07:00~~ | ~~Wed18:00~~ | ~~No~~ | Edit | Delete |
| 2 | Cole | Wdy | Wdy | No | Edit | Delete |
| ~~3~~ | ~~Kevin~~ | ~~Wdy08:00~~ | ~~Wdy17:00~~ | ~~No~~ | Edit | Delete |
| 4 | Phil | All | All | No | Edit | Delete |
| 5 | "Towber" | Mon06:00 | Sat17:00 | No | Edit | Delete |
| 6 | Mauricio | Wdy06:00 | Wdy18:00 | No | Edit | Delete |
| ~~7~~ | ~~John~~ | ~~All~~ | ~~All~~ | ~~Blacklisted~~ | Edit | Delete |

2. From the master list we will be removing "Paul", "John" and "Kevin" from the master list.

3. Use the '**Delete Button'** next to a user to delete the user

## 6-3. Removing users



Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase ········· Show

Set Master Key

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

Import Access List

Choose File No file chosen

Import Access List

Export Access List

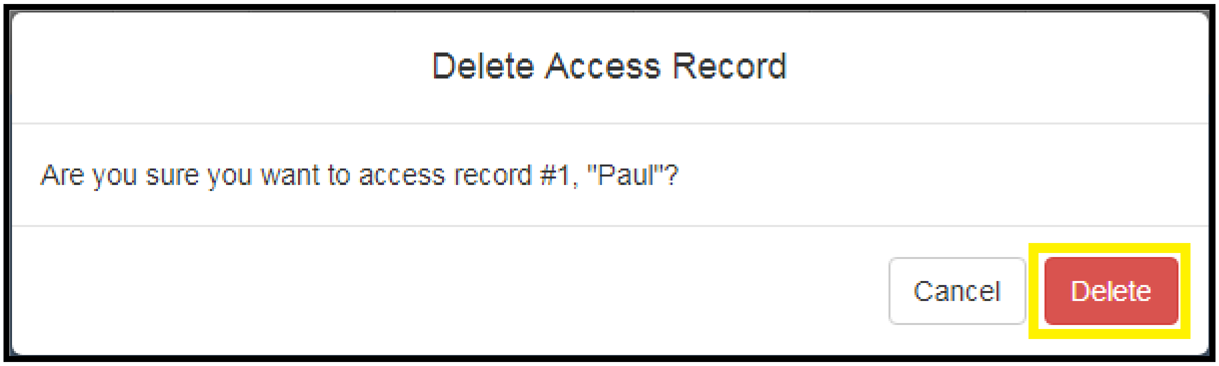
Export Access List

Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | Paul | Mon07:00 | Wed18:00 | No | Edit | Delete |
| 2 | Cole | Wdy | Wdy | No | Edit | Delete |
| 3 | Kevin | Wdy08:00 | Wdy17:00 | No | Edit | Delete |
| 4 | Phil | All | All | No | Edit | Delete |
| 5 | "Towber" | Mon06:00 | Sat17:00 | No | Edit | Delete |
| 6 | Mauricio | Wdy06:00 | Wdy18:00 | No | Edit | Delete |
| 7 | John | All | All | Blacklisted | Edit | Delete |

4. Confirm the pop-up to delete the user.

**Figure 6-4. Delete User**

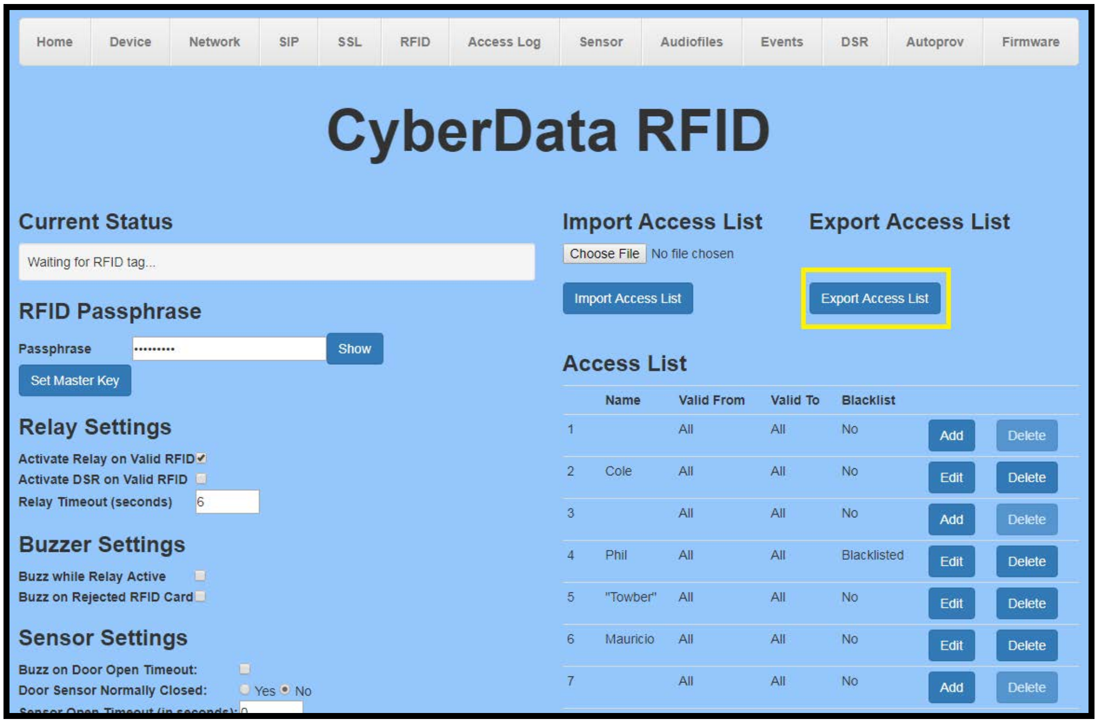


Delete Access Record

Are you sure you want to access record #1, "Paul"?

5. After deleting the users press the 'Export Access List' Button to save the access list.

**Figure 6-5. Export Access List**



CyberData RFID

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase ••••••••• Show

Set Master Key

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

Import Access List

Choose File No file chosen

Import Access List

Export Access List

Export Access List

Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | | All | All | No | Add | Delete |
| 2 | Cole | All | All | No | Edit | Delete |
| 3 | | All | All | No | Add | Delete |
| 4 | Phil | All | All | Blacklisted | Edit | Delete |
| 5 | "Towber" | All | All | No | Edit | Delete |
| 6 | Mauricio | All | All | No | Edit | Delete |
| 7 | | All | All | No | Add | Delete |

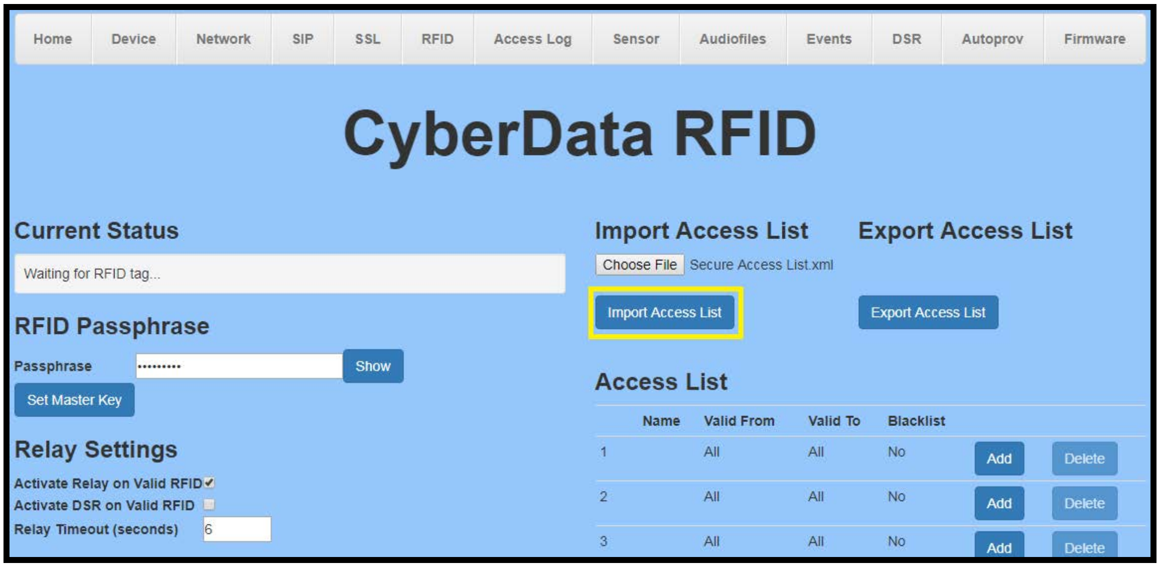
6. Save the new access list to a safe location as you will want to retain this file.

7. Log into the unit that will use the new secure access list.

8. On the RFID tab use the **‘Choose File’** button and select the new access list.

9. After selecting the file press the **‘Import Access List’** button.

**Figure 6-6. Import Access List**



CyberData RFID

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

Import Access List

Secure Access List.xml

Export Access List

Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | | All | All | No | Add | Delete |
| 2 | | All | All | No | Add | Delete |
| 3 | | All | All | No | Add | Delete |

**10.** Finally set the passphrase of the unit to match the passphrase used for any other devices.

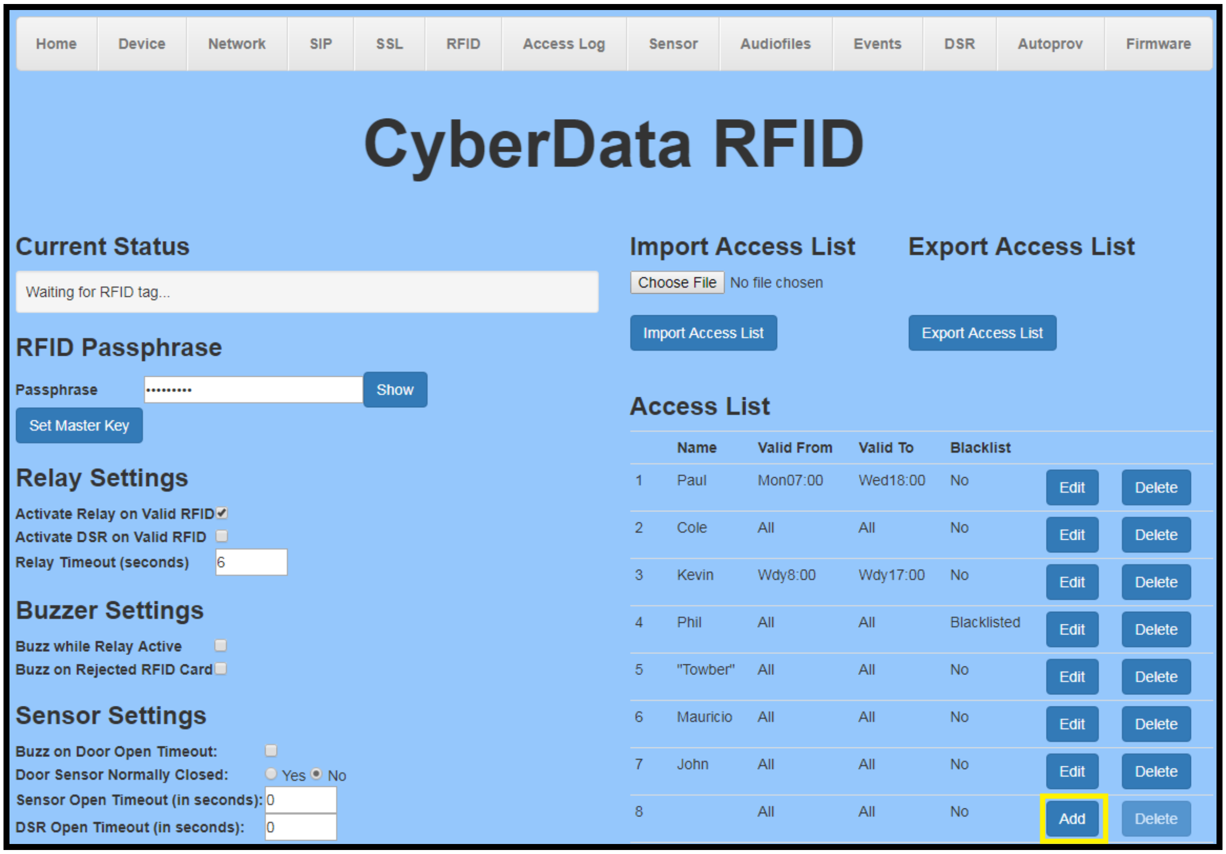
***Note:*** *Setting the passphrase to the same used by other endpoints will allow for the programming of cards on this unit that can be transferred to other units.*

# 7.0 Adding a new user to an existing access list

There will come a time when new users need to be added to the access lists. Determine the different access lists the user will need to be added to and add the new user to those lists.

1. Starting from the '**Master List**´ add the new user to the bottom of the access list.

**Figure 7-1. Add new user to existing list**



CyberData RFID

Current Status

Waiting for RFID tag...

RFID Passphrase

Passphrase ••••••••• Show

Set Master Key

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

Import Access List

Choose File No file chosen

Import Access List

Export Access List

Export Access List

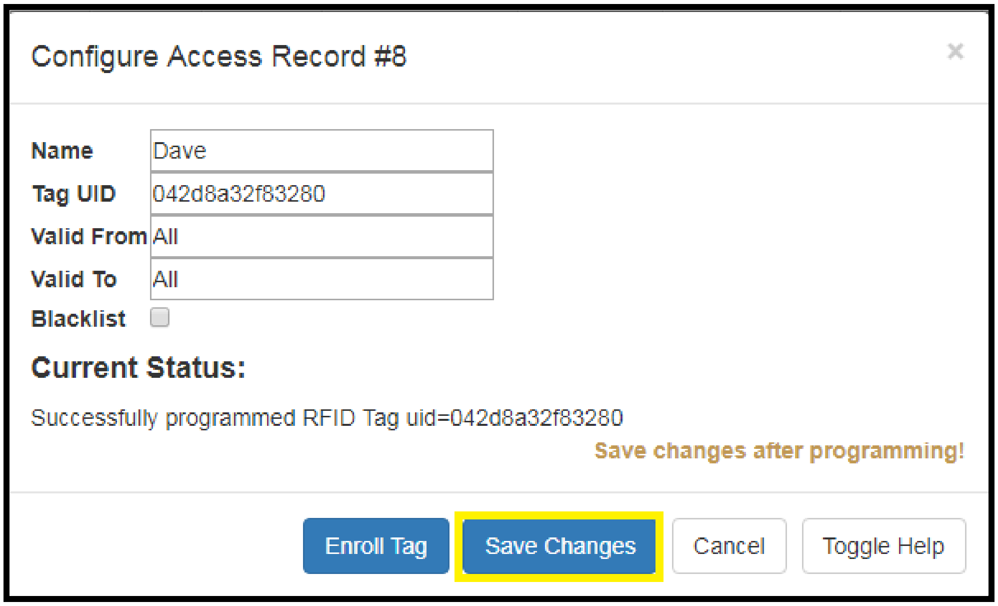
Access List

| | Name | Valid From | Valid To | Blacklist | | |
|---|---|---|---|---|---|---|
| 1 | Paul | Mon07:00 | Wed18:00 | No | Edit | Delete |
| 2 | Cole | All | All | No | Edit | Delete |
| 3 | Kevin | Wdy8:00 | Wdy17:00 | No | Edit | Delete |
| 4 | Phil | All | All | Blacklisted | Edit | Delete |
| 5 | "Towber" | All | All | No | Edit | Delete |
| 6 | Mauricio | All | All | No | Edit | Delete |
| 7 | John | All | All | No | Edit | Delete |
| 8 | | All | All | No | Add | Delete |

2. Press the add user button to add the new user.

3. Add the user in the pop-up.

**Figure 7-2. Add New User**



Configure Access Record #8

| | |
|---|---|
| **Name** | Dave |
| **Tag UID** | 042d8a32f83280 |
| **Valid From** | All |
| **Valid To** | All |
| **Blacklist** | □ |

**Current Status:**

Successfully programmed RFID Tag uid=042d8a32f83280

**Save changes after programming!**

***Note:*** *Take note of the number of the user in the 'Master List'. CyberData recommends that this same number is used in other lists to prevent list merger issues in the future.*

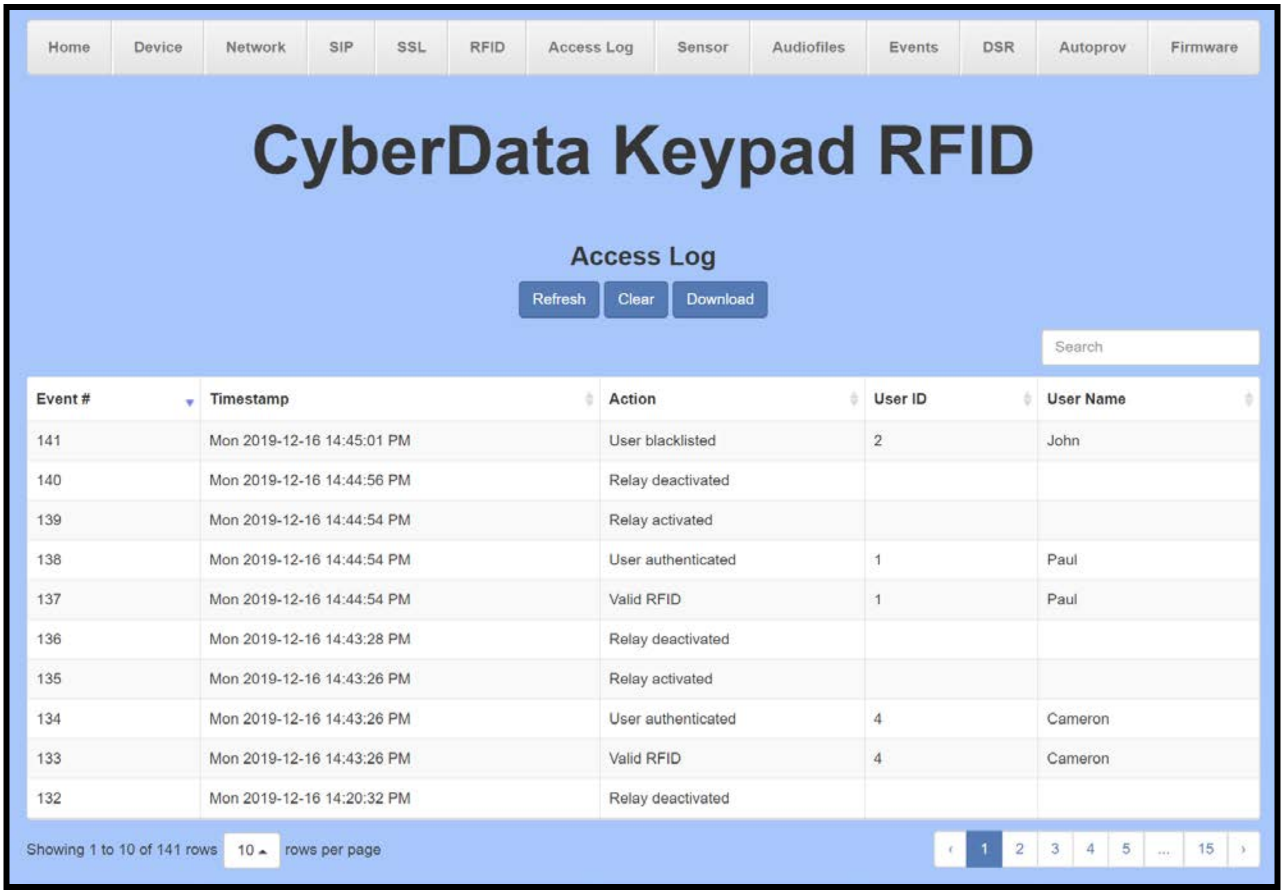
**4.** After adding the new user export the new 'Master List' and upload that to any RFID readers that will use this master list.

# 8.0 Download the Access Log

The CyberData RFID Access control devices contain a log of actions taken by the reader during its operation. The log file can get up to 100,000 lines which is about 25,000 entries with four lines per entry. Once the log files get to a certain size, they will begin to overwrite some of the older events, so it is important to download and backup the log for access records. The file is exported in a .CSV (comma separated value) format so it can be read in Microsoft Excel and other spreadsheet viewing programs.

1. Log into the RFID Tag Reader
2. Browse to the Access Log tab

**Figure 8-1. Access Log**



CyberData Keypad RFID

Access Log

| Event # | Timestamp | Action | User ID | User Name |
|---|---|---|---|---|
| 141 | Mon 2019-12-16 14:45:01 PM | User blacklisted | 2 | John |
| 140 | Mon 2019-12-16 14:44:56 PM | Relay deactivated | | |
| 139 | Mon 2019-12-16 14:44:54 PM | Relay activated | | |
| 138 | Mon 2019-12-16 14:44:54 PM | User authenticated | 1 | Paul |
| 137 | Mon 2019-12-16 14:44:54 PM | Valid RFID | 1 | Paul |
| 136 | Mon 2019-12-16 14:43:28 PM | Relay deactivated | | |
| 135 | Mon 2019-12-16 14:43:26 PM | Relay activated | | |
| 134 | Mon 2019-12-16 14:43:26 PM | User authenticated | 4 | Cameron |
| 133 | Mon 2019-12-16 14:43:26 PM | Valid RFID | 4 | Cameron |
| 132 | Mon 2019-12-16 14:20:32 PM | Relay deactivated | | |

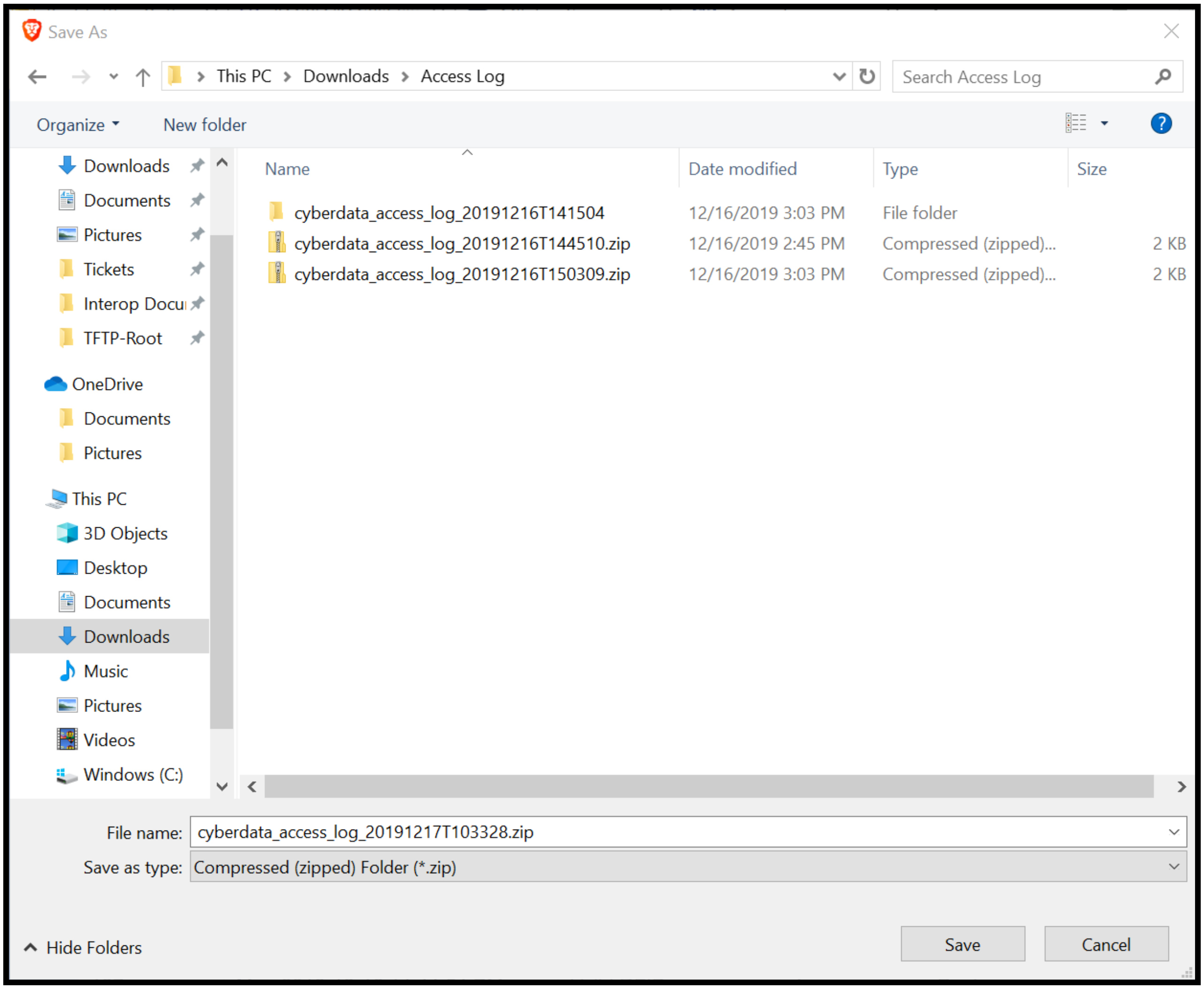
Showing 1 to 10 of 141 rows 10 rows per page

‹ 1 2 3 4 5 ... 15 ›

***Note:** The access control log can be viewed on this tab. The default presentation of the list displays the most recent entry first. Entries can be sorted by field, by clicking on the associated column, or filtered with the search box.*

3. Press the download button to save the logs to PC.

**Figure 8-2. Access log download popup**



| Name | Date modified | Type | Size |
|---|---|---|---|
| cyberdata_access_log_20191216T141504 | 12/16/2019 3:03 PM | File folder | |
| cyberdata_access_log_20191216T144510.zip | 12/16/2019 2:45 PM | Compressed (zipped)... | 2 KB |
| cyberdata_access_log_20191216T150309.zip | 12/16/2019 3:03 PM | Compressed (zipped)... | 2 KB |

File name: cyberdata_access_log_20191217T103328.zip

Save as type: Compressed (zipped) Folder (*.zip)

***Note:*** *The log is named "cyberdata_access_log_DateTime" with the date and time of export tacked on.*

Since the logs are named with the prefix "cyberdata" we recommend creating individual folders for each device to keep track of the readers.

## 8.1 Access Log Line descriptions

There are many different actions that can be taken by the RFID reader, here are definitions of the actions.

**Valid RFID** - Valid card was read.

**Invalid RFID** - Non valid card was read.

**Valid Code** - Valid access code was entered.

**Invalid code** - Invalid code was entered.

**User Authenticated** - User was validated.

**Relay Activated** – The relay was activated for the time configured on the RFID tab.

**Relay Deactivated** – They relay was deactivated based on the time configured on the RFID tab.

**DSR activated –** Door Strike Relay accessory activated for the time configured.

**DSR deactivated –** Door Strike Relay accessory deactivated after the configured time has expired.

**User Blacklisted** - Blacklisted user was read, the unit has acted based on the settings on the RFID tab.

**User Invalid Time -** Users card was read outside of allotted time.

**Two-factor timeout -** Time limit configured for two-factor authentication has expired.

## 8.2 Helpful tips

- Creating a desktop shortcut for the access control device can make it very easy to manage. If you are not sure how to make a shortcut check out our support knowledge base entry on the subject.
  How to create a desktop shortcut to a webpage.

- While the access log can store up to 100,000 lines of activity it is a good idea to back up the log to a local PC. Please review Section 8.0 to learn how to download the log files.

- Save the logs in a folder for each specific device to make it easier to find logs if necessary.

# 9.0 Provisioning the access list

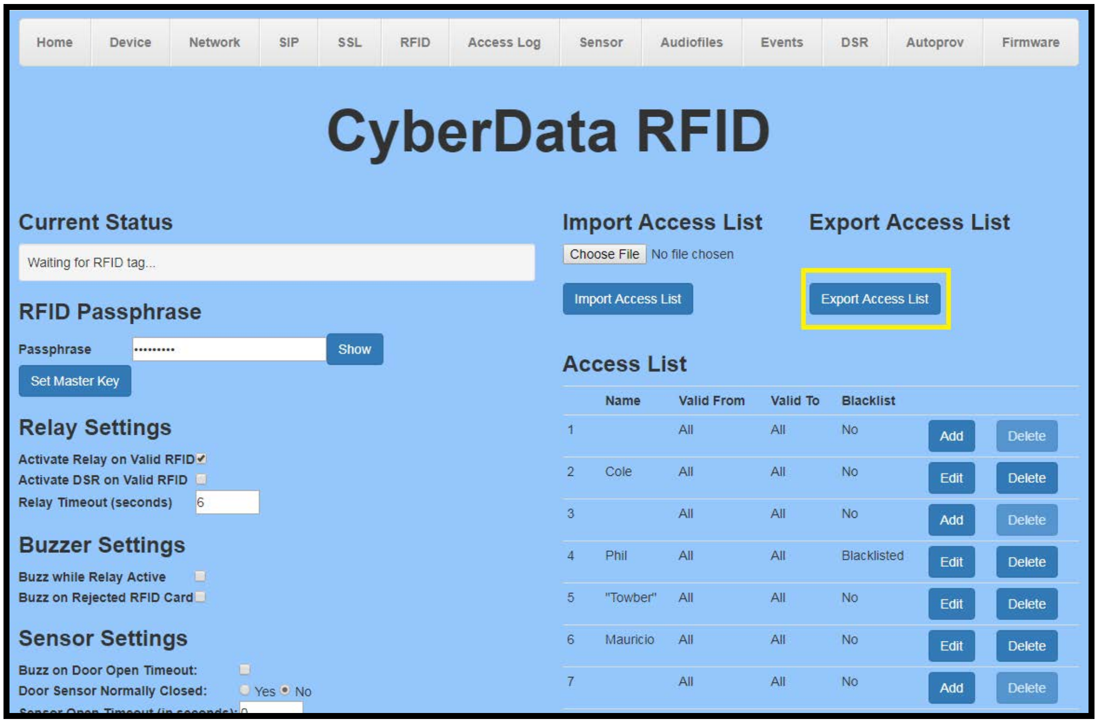
The best way to make changes to multiple access control devices simultaneously is provisioning. Instead of importing the access list individually to each device via the web page, provisioning allows changes to be made to multiple devices simultaneously. This will allow changes to be made on one unit, then exported to the provisioning server. The other devices can then reference the exported configuration and update their settings accordingly. The devices can be provisioned via TFTP, HTTP, and/or HTTPS. However, based on the data being provisioned, it is not recommended to use TFTP or HTTP since the data will be transmitted in plaintext. The plaintext transmission may allow for an attacker to intercept the transmission and potentially gain access to the facility.

This will be covered in several subsections to explain how to prepare the file, the different options of how to point the devices to the provisioning server, and how to load the file in a server.

# 9.1 Prepping the files

Once the access log is complete and ready to be used on other readers download the log to your local PC. The log can be downloaded with the “Export Access List” button.

**Figure 9-1. Export Access List**



CyberData RFID

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

Import Access List

No file chosen

Export Access List

Access List

|  | Name | Valid From | Valid To | Blacklist |  |  |
|---|---|---|---|---|---|---|
| 1 |  | All | All | No | Add | Delete |
| 2 | Cole | All | All | No | Edit | Delete |
| 3 |  | All | All | No | Add | Delete |
| 4 | Phil | All | All | Blacklisted | Edit | Delete |
| 5 | "Towber" | All | All | No | Edit | Delete |
| 6 | Mauricio | All | All | No | Edit | Delete |
| 7 |  | All | All | No | Add | Delete |

1. Once the file is downloaded rename the file for easier administration purposes.

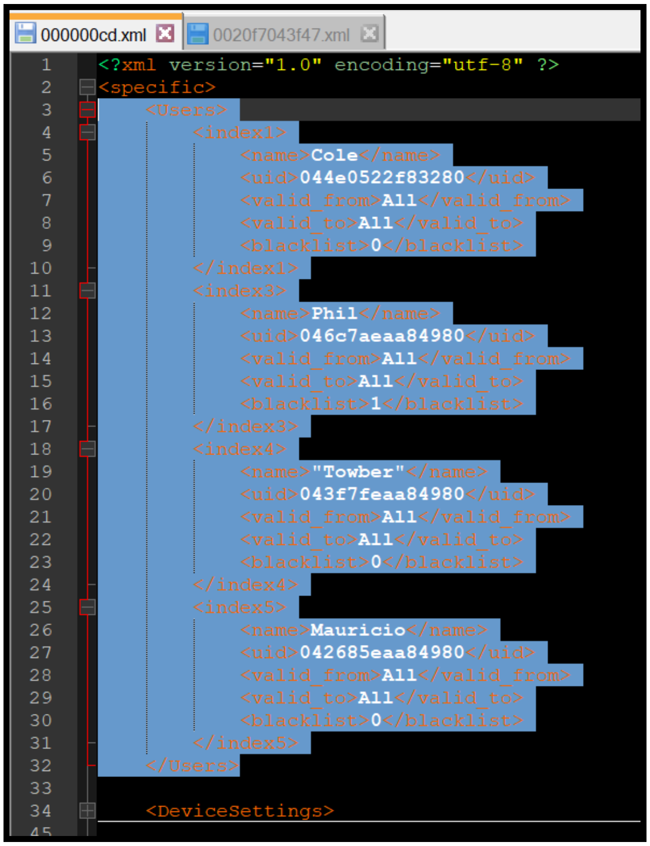
***Note:*** *At this point the access log can be directly provisioned or the file can be listed in a master provisioning file to provision all the device settings at once. For the purposes of the guide, all the settings will be provisioned using multiple files.*

***Note:*** *When provisioning multiple devices, it is best to use multiple files since some settings will be specific to a device and can not be shared on multiple units. Examples settings that cannot be shared are IP-Addresses or SIP extension numbers and passwords.*

2. Create a 'common' provisioning file named **<u>"000000cd.xml"</u>** that will contain settings that can be shared across multiple devices. The provisioning template is available for download with every firmware file on our website OR directly from the device on the "Provisioning tab".

3. Copy and paste the <User> section from the exported access log into the 000000cd.xml; making sure to retain the <User> and </User> tags.

**<u>Figure 9-2. User section in common file.</u>**



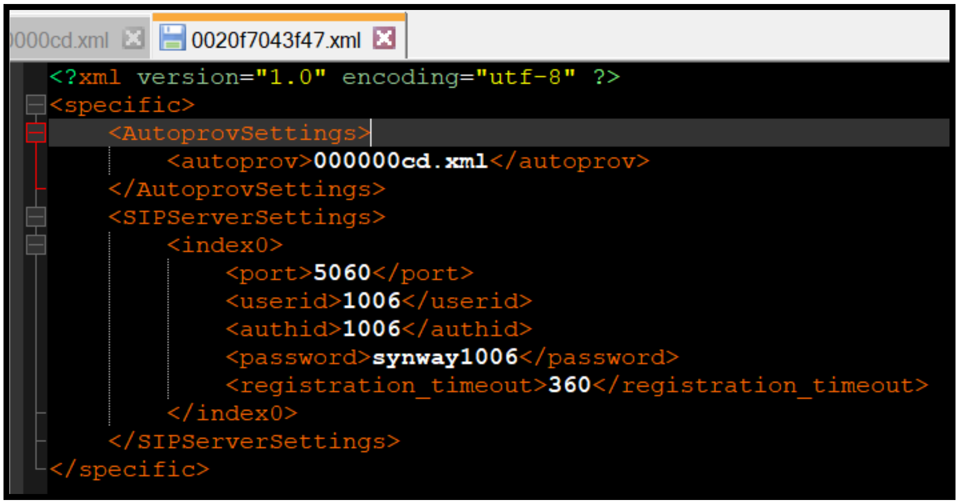
```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <Users>
        <index1>
            <name>Cole</name>
            <uid>044e0522f83280</uid>
            <valid_from>All</valid_from>
            <valid_to>All</valid_to>
            <blacklist>0</blacklist>
        </index1>
        <index3>
            <name>Phil</name>
            <uid>046c7aeaa84980</uid>
            <valid_from>All</valid_from>
            <valid_to>All</valid_to>
            <blacklist>1</blacklist>
        </index3>
        <index4>
            <name>"Towber"</name>
            <uid>043f7feaa84980</uid>
            <valid_from>All</valid_from>
            <valid_to>All</valid_to>
            <blacklist>0</blacklist>
        </index4>
        <index5>
            <name>Mauricio</name>
            <uid>042685eaa84980</uid>
            <valid_from>All</valid_from>
            <valid_to>All</valid_to>
            <blacklist>0</blacklist>
        </index5>
    </Users>

    <DeviceSettings>
```

4. Create a 'device specific' provisioning file that will have all the unique settings for the device. Name the provisioning file the MAC address of the device.

5. In the device specific file include the “AutoprovSettings” section and in this section list all files to be downloaded with the tag, “<autoprov></autoprov>.

**Figure 9-3. Auto-prov Device specific file**

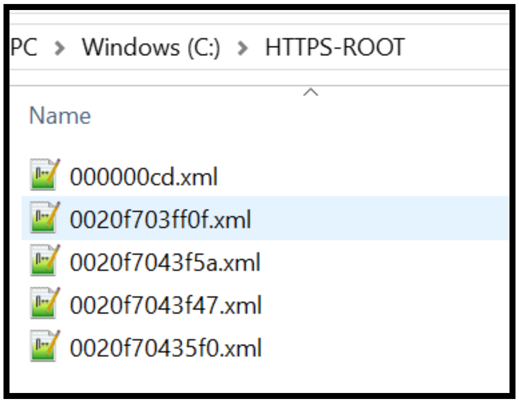


```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <AutoprovSettings>
        <autoprov>000000cd.xml</autoprov>
    </AutoprovSettings>
    <SIPServerSettings>
        <index0>
            <port>5060</port>
            <userid>1006</userid>
            <authid>1006</authid>
            <password>synway1006</password>
            <registration_timeout>360</registration_timeout>
        </index0>
    </SIPServerSettings>
</specific>
```

6. Create device specific files for each device that will be provisioned.

7. Once all the files are created load them into the directory for your provisioning server.

**Figure 9-4. Files loaded in server**



000000cd.xml
0020f703ff0f.xml
0020f7043f5a.xml
0020f7043f47.xml
0020f70435f0.xml

8. Once the files are loaded in the server the devices are ready to be provisioned.

## 9.2 Setting up provisioning

There are a few different ways to point the devices to the provisioning server. The devices can be manually pointed to the server through the Autoprov tab or through DHCP options.

**A.** To provision the units manually, log into the unit and browse to the Autoprov tab. On the autoprov page input the FQDN (Fully Qualified Domain Name) of the server or its IP-Address. Then set the Username and Password that will be used to authenticate the unit to the server. A security certificate can also be loaded in the unit desired.

**B.** The unit can also be provisioned in a "Zero-Touch" method by using DHCP options. Once the unit gets a DCHP address from the server it will then check the various DHCP options that are also listed. If a provisioning server is listed the unit will attempt to contact the server and request a file names with its unique MAC Address.

***Note:*** *For the purposes of this document the units will be manually pointed to the server for provisioning.*

1. Log into the unit and navigate to the Autoprov tab. On the Autoprov tab, specify the address of the server (IP Address or FQDN).

2. Next set the username and password so the unit can be authenticated by the server. If necessary, load a certificate in the RFID unit so it can verify the server.

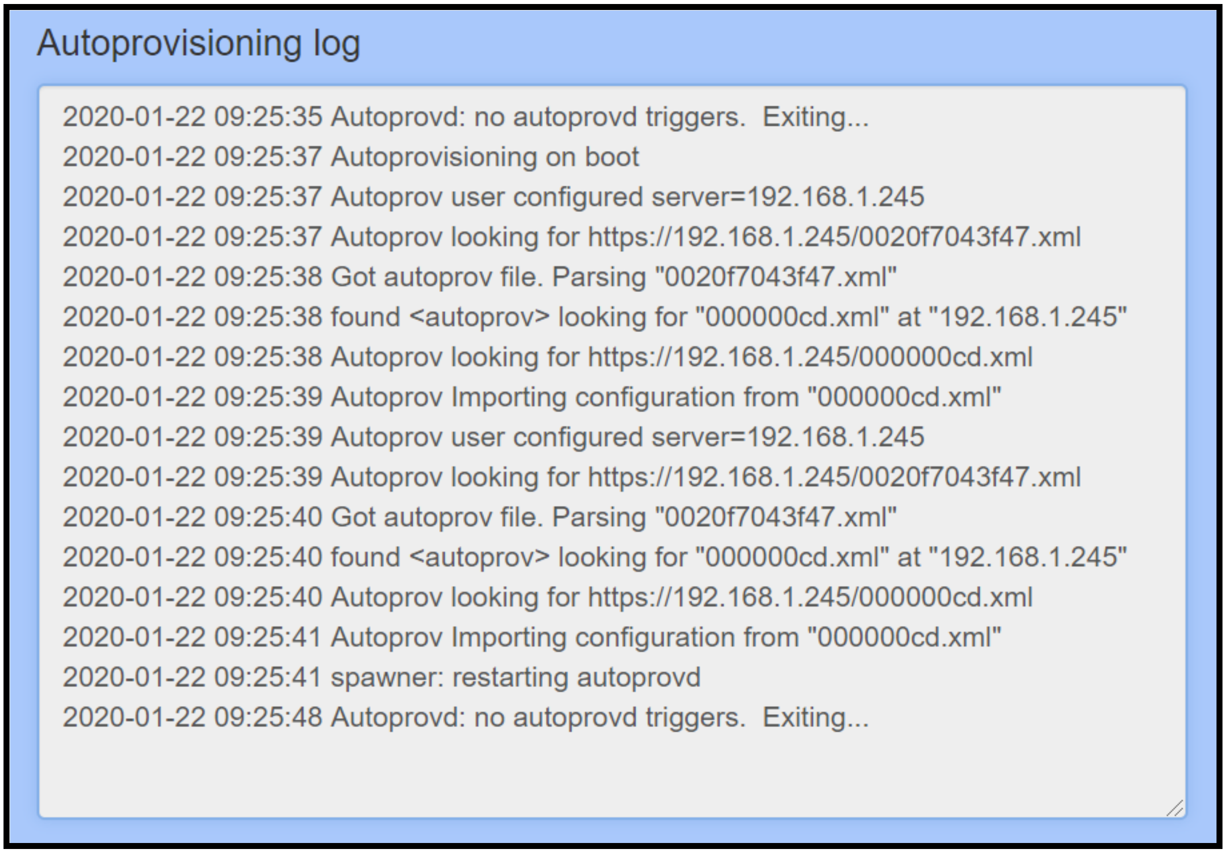
***Note:*** *The server certificate can be loaded to the unit on the SSL tab.*

3. Once the provisioning settings are configured Save and Reboot the unit.

4. After the device has finished rebooting it will contact the server and download all the relevant files.

5. The files downloaded can be verified in the Autoprovisioning log.

**Figure 9-4. Autoprovisioning Log**



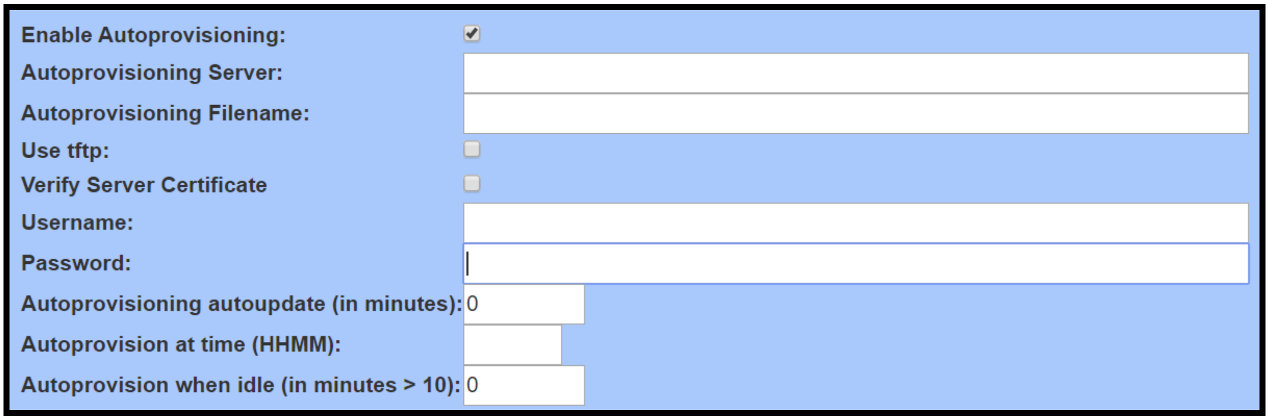
Autoprovisioning log

```
2020-01-22 09:25:35 Autoprovd: no autoprovd triggers.  Exiting...
2020-01-22 09:25:37 Autoprovisioning on boot
2020-01-22 09:25:37 Autoprov user configured server=192.168.1.245
2020-01-22 09:25:37 Autoprov looking for https://192.168.1.245/0020f7043f47.xml
2020-01-22 09:25:38 Got autoprov file. Parsing "0020f7043f47.xml"
2020-01-22 09:25:38 found <autoprov> looking for "000000cd.xml" at "192.168.1.245"
2020-01-22 09:25:38 Autoprov looking for https://192.168.1.245/000000cd.xml
2020-01-22 09:25:39 Autoprov Importing configuration from "000000cd.xml"
2020-01-22 09:25:39 Autoprov user configured server=192.168.1.245
2020-01-22 09:25:39 Autoprov looking for https://192.168.1.245/0020f7043f47.xml
2020-01-22 09:25:40 Got autoprov file. Parsing "0020f7043f47.xml"
2020-01-22 09:25:40 found <autoprov> looking for "000000cd.xml" at "192.168.1.245"
2020-01-22 09:25:40 Autoprov looking for https://192.168.1.245/000000cd.xml
2020-01-22 09:25:41 Autoprov Importing configuration from "000000cd.xml"
2020-01-22 09:25:41 spawner: restarting autoprovd
2020-01-22 09:25:48 Autoprovd: no autoprovd triggers.  Exiting...
```

## 9.3 Maintaining provisioned devices

Once the devices have been provisioned the process to update or alter the configuration is a breeze. By default, the unit will search for provisioning files when it boots. There are a variety of settings that can automate the provisioning process.

**Figure 9-5. Provisioning Settings**



| | |
|---|---|
| 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 |

Autoprovisioning autoupdate (in minutes): *The device will search for new provisioning files at an interval depending on this setting.*

Autoprovision at time (HHMM): *The device will search for new provisioning files at the specified time.*

Autoprovision when idle (in minutes > 10): *The device will search for new provisioning files after being idle for the specified amount of time.*

# 10.0 Contact CyberData Corporation

**Sales**

For sales-related questions, please visit our Contact CyberData Sales web page for more information.

**Technical Support**

For CyberData Technical Support, please submit a Contact CyberData VoIP Technical Support form on our website.

The CyberData VoIP Technical Support Contact form initiates a troubleshooting ticket which CyberData uses for quality assurance purposes.

Additionally, the Contact VoIP Tech Support form tells us which phone system you are using, the make and model of the network switch, and other essential troubleshooting information we need to efficiently assist with a resolution. Please also include as much detail as possible in the Describe Problem section of the form. Your installation is extremely important to us.

**Documentation Feedback**

We realize changes to the software or hardware of the solution may render this document obsolete.  We welcome and encourage documentation feedback to ensure continued applicability.