



Pure Access Product Manual

1 — Last update: Apr 07, 2021

Isonas

Table of Contents

- 1. Using This Manual 5**
- 2. Contact Support 7**
- 3. Application Infrastructure and Architecture 8**
 - 3.1. Pure Access Cloud Infrastructure 9
 - 3.2. Pure Access Manager Infrastructure 10
 - 3.2.1. Pure Access Manager System Requirements 11
 - 3.3. Platform Update Process 12
 - 3.3.1. Pure Access Cloud 13
 - 3.3.2. Pure Access Manager 14
- 4. Setup and Configuration 15**
 - 4.1. Network Configuration and Troubleshooting 16
 - 4.1.1. IP Addressing 17
 - 4.1.2. Basic Firewall Information 18
 - 4.1.3. Best Practices 20
 - 4.1.4. Additional Troubleshooting 21
 - 4.2. Configuring ISONAS Devices 24
 - 4.2.1. Using the Configuration Tool 25
 - 4.2.1.1. Advanced Configuration 28
 - 4.2.1.2. Reviewing Network Config Settings 32
 - 4.2.1.3. Connectivity Test 35
 - 4.2.2. Discovering Units 37
 - 4.2.2.1. Find device by IP 39
 - 4.3. Updating Firmware 41
 - 4.4. Wiring and Hardware Installation 44
 - 4.4.1. RC-04 Installation Guide 45
 - 4.4.2. IP-Bridge Installation Guide 46
 - 4.4.2.1. IP-Bridge Status Light Indicators 47
 - 4.4.3. RC-03 Installation Guide 49
 - 4.4.3.1. RC-03 Jumper Configurations 50
 - 4.4.4. ASM Status Light Indicators 53
 - 4.4.5. Factory Resetting a Device 54
 - 4.4.6. Wiegand Interface Module (WIM) 55
- 5. Getting Started in Pure Access 56**
 - 5.1. Pure Access Cloud 57
 - 5.1.1. Logging into a Pure Access Cloud tenant 58
 - 5.1.2. Tenant Name 60
 - 5.1.3. Cannot Log into Pure Access Tenant 61
 - 5.1.4. RMR License 63

5.1.4.1. Creating Subtenants	64
5.2. Pure Access Manager	67
5.2.1. Java Memory Allocation	68
5.2.2. SMTP Configuration (Pure Access Manager)	69
5.2.3. Configuring Pure Access Manager for SSL	72
5.3. Migrating from One Tenant to Another	73
5.4. Backup and Restore Process (Pure Access Manager).....	75
5.5. Integrations	76
5.5.1. Entrust Datacard TruCredential.....	77
5.5.2. Milestone XProtect.....	78
6. Online Interface	79
6.1. Dashboards.....	81
6.1.1. Create Dashboard.....	82
6.2. Widgets.....	83
6.2.1. History Widget	85
6.2.1.1. Standard History Events	86
6.2.2. Single Access Point Widget	88
6.2.3. Multiple Access Point Widget.....	89
6.2.4. Access Point Admit Widget	90
6.2.5. Lock Down Access Points Widget	91
6.2.6. User Profile Widget.....	92
7. Send Command	93
8. Users	95
8.1. Create User.....	96
8.1.1. Importing Users	98
8.2. Edit User	103
8.3. Find a User	104
8.4. Filter Users	105
8.5. User Groups.....	107
8.5.1. Create User Group.....	108
8.5.2. Manage User Groups	109
8.6. Manage Credentials	114
8.6.1. Badge	116
8.6.2. Keypad Entry	117
8.6.3. ISONAS Mobile.....	118
8.6.3.1. Using the Mobile Credential to Unlock a Door.....	121
8.6.4. Enrolling by Presentation	122
8.6.5. Special Credential Properties.....	124
8.6.5.1. Master Credential	125
8.6.5.2. Toggle Credential	127
8.6.5.3. Count Limit	130

8.6.5.4. Time Limit.....	131
8.6.6. Deactivating Credentials	132
8.7. Manage Web Access.....	133
8.7.1. Setting up Web Access for a User.....	134
8.7.2. User Roles	135
8.7.3. Accepting the Web Access Invitation.....	137
8.7.4. Removing Web Access Privileges	140
8.8. Deactivate User	141
8.8.1. Viewing Deactivated Users	143
8.8.2. Activating a User Profile.....	144
9. Access Points	146
9.1. Access Point Main Page.....	147
9.1.1. Access Point Settings	148
9.2. Access Point Groups.....	151
10. Access Control	152
10.1. Weekly Rules	153
10.1.1. Create Weekly Rule	154
10.1.2. Edit Weekly Rule.....	156
10.1.3. Deactivate Weekly Rule	157
10.2. Events.....	158
10.2.1. Create Event.....	159
10.2.2. Edit Event	160
10.3. Custom Rules.....	161
10.3.1. Create Custom Rule.....	162
10.3.2. Custom Rule Conditions.....	163
10.4. Holidays	165
10.4.1. Create Holiday	166
10.4.2. Edit Holiday	167
10.5. Schedule Date Types	168
11. Reports.....	169
11.1. Access Point Groups Report	170
11.2. Access Point Permissions Report.....	171
11.3. Access Points Report	172
11.4. History Report	173
11.5. Holidays Report.....	174
11.6. User Attendance Report	175
11.7. User Export Report.....	176
11.8. User Group Attendance Report	177
11.9. User Group Permissions Report.....	178
11.10. User Groups Report	179
11.11. User Permissions Report.....	180

11.12. Users Report	181
12. Settings	182
12.1. Tenant Information	183
12.2. Integrator Information	184
12.3. Global Settings.....	185
12.3.1. Two-Factor Authentication	186
12.3.1.1. Card/PIN.....	187
12.3.1.2. Two User	188
12.3.1.3. Two-User – Card/PIN.....	189
12.3.1.4. Two-Factor History Events.....	190
12.4. Areas	192
12.4.1. Why Use Areas?	193
12.4.2. How to Configure Areas	195
12.4.2.1. Assigning Dashboards to an Area.....	198
12.4.2.2. Assigning Groups to an Area	199
12.4.2.3. Assigning Access Points to an Area.....	201
12.4.2.4. Assigning Users to an Area.....	202
12.4.2.5. Assigning Holidays to an Area	203
12.4.2.6. Assigning Weekly Rules to an Area	204
12.4.2.7. Assigning Events to an Area	205
12.4.3. Managing Area Administrators	206
12.5. Credential	207
12.5.1. Bitmasking	208
12.5.1.1. Verifying the Currently Set Bitmask.....	209
12.5.1.2. Identifying Credential Data.....	210
12.5.1.3. Discover the Appropriate Bitmask	212
12.5.1.4. Setting a Bitmask.....	213
12.5.1.4.1. Pushing the Current Bitmask Setting to All Readers	214
12.5.1.4.2. Pushing Bitmask Setting to All Readers (PAM).....	215
12.5.1.5. Setting an External Keypad Site Code	216
12.5.1.5.1. Configuring Keypad Site Code on an R-1 Reader	217
12.5.1.6. Custom Bitmasking	218
12.5.1.7. HID iClass Credentials.....	225
12.6. User Defined Fields.....	226
12.7. Active Directory.....	227
12.7.1. AD Connect Prerequisites	228
12.7.2. Installation and Configuration.....	230
12.7.3. Configuring AD Sync Settings in Pure Access	231
12.8. API.....	232
12.8.1. Authentication	233
12.8.2. API Tokens	234
12.8.3. Additional API Information.....	235

- 13. Alerts..... 236**
 - 13.1. Alert Types and Setup Procedure..... 237
 - 13.1.1. Unauthorized Open 238
 - 13.1.2. Extended Open 239
 - 13.1.3. Tamper 240
 - 13.1.4. AUX/REX Alarm 241
 - 13.1.5. Credential Rejected, Expired, or Over Limit..... 242
 - 13.2. Alert Settings..... 243

- 14. Glossary..... 244**
 - 14.1. Admit..... 245
 - 14.2. ASM..... 246
 - 14.3. AUX 247
 - 14.4. Compile..... 248
 - 14.5. Door..... 249
 - 14.6. Fail Safe..... 250
 - 14.7. Fail Secure..... 251
 - 14.8. First Person In..... 252
 - 14.9. Lock Down 253
 - 14.10. REX 254
 - 14.11. Secured..... 255


1. Using This Manual

Use the **table of contents** on the left or the **search bar** at the upper right corner of this page to quickly jump to topics:

The screenshot displays the ISONAS Pure Access Manual interface. At the top, a blue header contains the ISONAS logo, the text 'Pure Access Manual', a page number '1', and a search bar. A red arrow points from the search bar to the text 'You can use the search bar at the upper right corner of this page to quickly jump to topics:'. On the left side, a vertical table of contents lists various manual sections, with 'Using This Manual' highlighted. The main content area features the title 'Using This Manual' and a sub-section titled 'Application Infrastructure and Architecture'. At the bottom, a 'Feedback' section asks 'Was this helpful?' with 'Yes' and 'No' buttons.

Example:

ISONAS PUREACCESS Pure Access Manual 1



Using This Manual

- Application Infrastructure and Architecture
- Platform Update Process
- Setup and Configuration
- Getting Started in Pure Access**
- Managing Access Points
- Managing Users
- Weekly Rules, Schedules, and Events

Search

Setting up a Holiday

[Weekly Rules, Schedules, and Events](#) » [Scheduled Events and Holidays](#) » [Setting up a Holiday](#)

Navigate to Access Control, then select the "Calendar" tab: There are two ways to add a "Holiday": Select from the upper right corner of the page. Navigate to and click on the day, then select the button. Give your holiday a...

How to set up a Dashboard

[Dashboard Widgets](#) » [How to set up a Dashboard](#)

From the main page in Pure Access, click the button on the right hand side of the screen to bring up the "Create New Dashboard" window. Type the name of the new dashboard then select General (to use widgets) or Floor Plan. If Areas are configured, you...

Set up Email Notifications for Alerts

[Alerts and Notifications](#) » [Set up Email Notifications for Alerts](#)

When Alerts occur you have the ability to trigger an email to specific users, during specific times for specific alerts. Below is the view of how to set up the notifications. You can establish the time range to be alerted, the users (please note: to be notified users...

2. Contact Support

For further information about Pure Access, feel free to utilize our [YouTube channel](#) where there is a complete video library with tutorials on the platform.

Should you run into an issue, you can reach out to our support team at (800)-581-0083 option 2 or by emailing support@isonas.com.

Any feature requests can be submitted to feedback@isonas.com. This mailbox is monitored by our product management team who communicate directly with our developers about implementing new features.

3. Application Infrastructure and Architecture

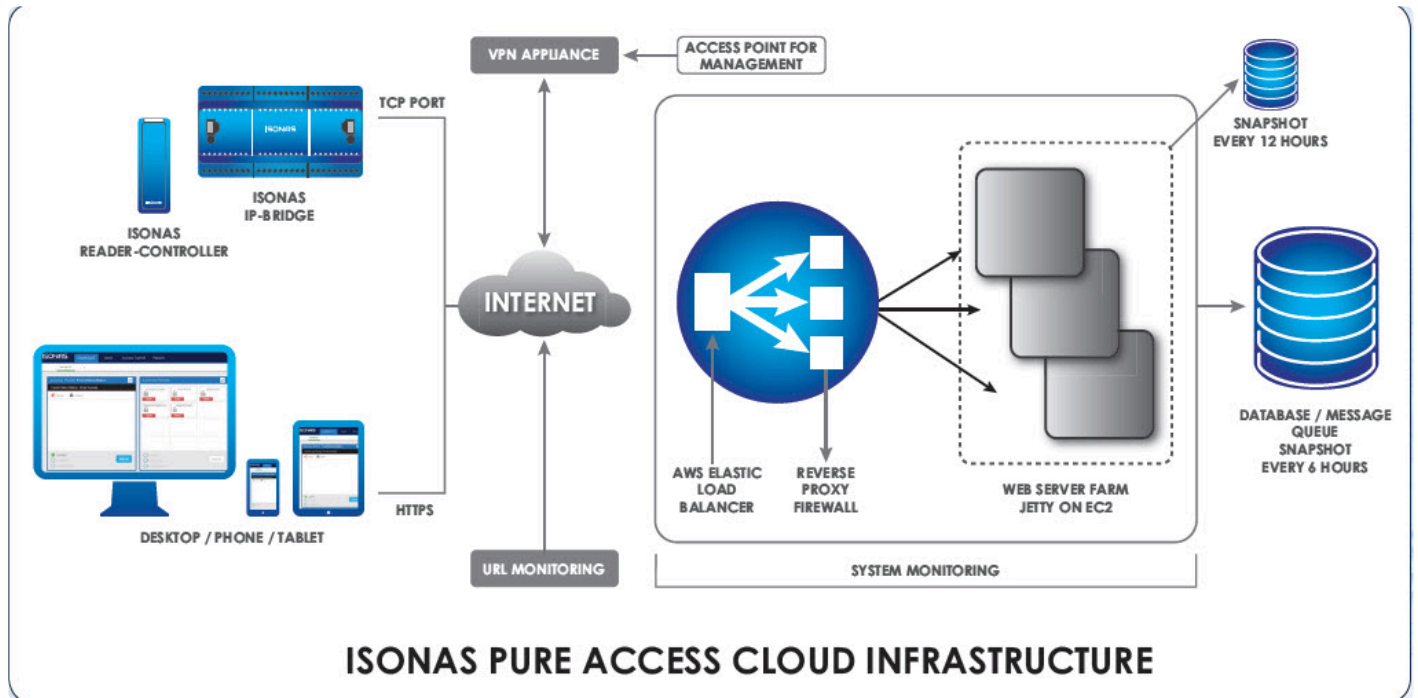
Pure Access Cloud is a web-based platform hosted by ISONAS through *Amazon Web Services (AWS)*. The infrastructure uses a *PostgreSQL* database on a Windows server (on premise version only). The web application is written in *Java* and served up by *Apache Tomcat*.

Pure Access Manager is housed in the same set up, but instead of being hosted by *AWS*, you are providing the server to host the platform within your internal network.

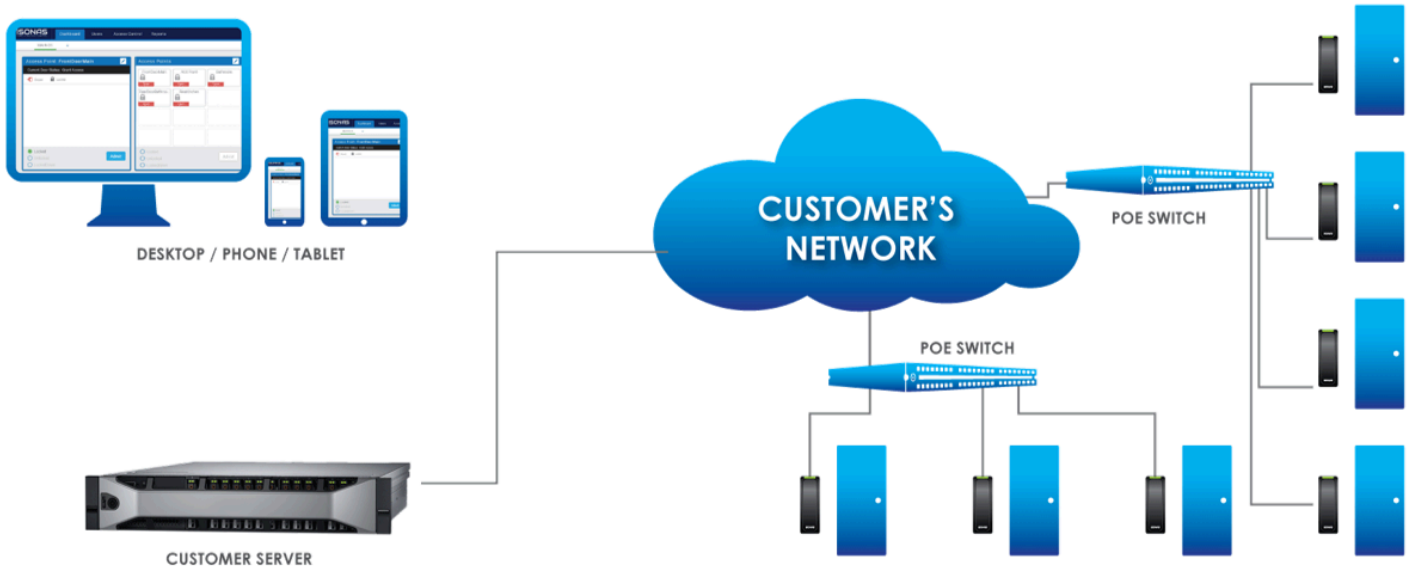
The following pages will display the infrastructure of each platform:

- [Pure Access Cloud](#)
- [Pure Access Manager](#) (on-premise)

3.1. Pure Access Cloud Infrastructure



3.2. Pure Access Manager Infrastructure



3.2.1. Pure Access Manager System Requirements

A dedicated machine running:

- *Windows® Server 2012 R2 or Server 2016*
- *Intel i5 or greater*
- *8GB RAM minimum (16GB recommended)*
- *500 GB HDD*

OR

- *Virtual Environment with a Hypervisor download*
- *At least 80GB of disk space available from the VM*

3.3. Platform Update Process

The following pages will explain the update process for Pure Access Cloud and Pure Access Manager.

3.3.1. Pure Access Cloud

All software corrections and feature releases are included in the annual license of Pure Access Cloud.

Upgrades are typically released once per quarter.

Our deployment team will provide a 24 hour notification prior to any planned release so you are aware of the update. All updates take place during off hours to reduce any potential interruption to your system.

(See next page for [Pure Access Manager](#))

3.3.2. Pure Access Manager

Pure Access Manager follows a yearly release schedule with a notification that an update is available.


If issues are found in the software, an update will be available for our Pure Access Manager customers free-of-charge. A link will be provided from which the update can be downloaded and installed directly.

4. Setup and Configuration

All ISONAS hardware is configured to contact the Pure Access Cloud servers by default.

Here's what is needed to ensure a smooth setup:

1. Correctly configured [network settings](#).
2. The [ISONAS Configuration Tool](#).
3. Pure Access tenant license information.

 **Tenant license information** can be found in your order confirmation email. Check with your installer, distributor, or our sales team for this information.

4.1. Network Configuration and Troubleshooting

The ISONAS reader-controller and IP-Bridge are IoT style devices that require minimal network configuration to function.

When using the reader-controller or IP-Bridge in conjunction with Pure Access Cloud, the devices must have a clear path to the internet on **port 55533**. No other ports are required.

Resources

- [IP Addressing](#)
- [Firewall Information](#)
- [Best Practices](#)
- [Troubleshooting connectivity issues](#)

4.1.1. IP Addressing

The recommended setting for ISONAS hardware devices connecting to Pure Access is **Dynamic Host Configuration Protocol (DHCP)**. When using DHCP, ensure that the DHCP has the correct default gateway and DNS address configured. These settings are critical for the device to connect outside the network (gateway) and to resolve the Pure Access address to an IP address (DNS).

If you prefer to reserve IP's for your devices, we would recommend using **DHCP with reservation** as opposed to statically addressing devices. With that said, static addresses *can* be used with Pure IP and PowerNet™ devices connecting to Pure Access.

When assigning static addresses, ensure all of the following items are [configured](#) with the correct address:

1. IP Address
2. Subnet Mask
3. Gateway
4. DNS Address

4.1.2. Basic Firewall Information

When connecting ISONAS hardware devices to Pure Access™, the device (client) initiates the connection to the software. This setting is “**Client Mode**” for reader-controller devices (see figure 3 below).

Since the device initiates the connection out to Pure Access, minimal firewall configuration is needed. If your firewall is blocking outbound ports or ephemeral ports, then **rules may need to be added to the firewall** to ensure a connection can be made.

✿ An ephemeral port is a random port used to complete a TCP connection for the session (typically between 49152 and 65535). The port number is used only for that connection period and will change if the connection is reset. In most cases, this is not an issue, but it can become one if severe security restrictions are placed on a network.

ISONAS RC-03 and RC-04 reader-controller devices will initiate a connection on port **55533** and Pure Access will use an ephemeral port to complete the connection.

```
TCP 192.168.1.210:55533 192.168.1.97:10001 ESTABLISHED
TCP 192.168.1.210:55533 192.168.1.97:10002 ESTABLISHED
TCP 192.168.1.210:55533 192.168.1.97:10003 ESTABLISHED
```

Figure 1 - RC-03 Example Connection

PowerNet™ IP-Bridge devices will initiate a connection on port **55533** and Pure Access will use ports **10001-10003** to complete the connection. IP-Bridges come in either two or three-door units.

- For a two-door unit, ports 10001 and 10002 will be used.
- For a three-door unit, the same ports are used in addition to 10003.

```
TCP 192.168.1.210:55533 192.168.1.32:54259 ESTABLISHED
TCP 192.168.1.210:55533 192.168.1.97:10001 ESTABLISHED
```

Server Connection Ephemeral Port

Figure 2 – IP-Bridge Example Connection

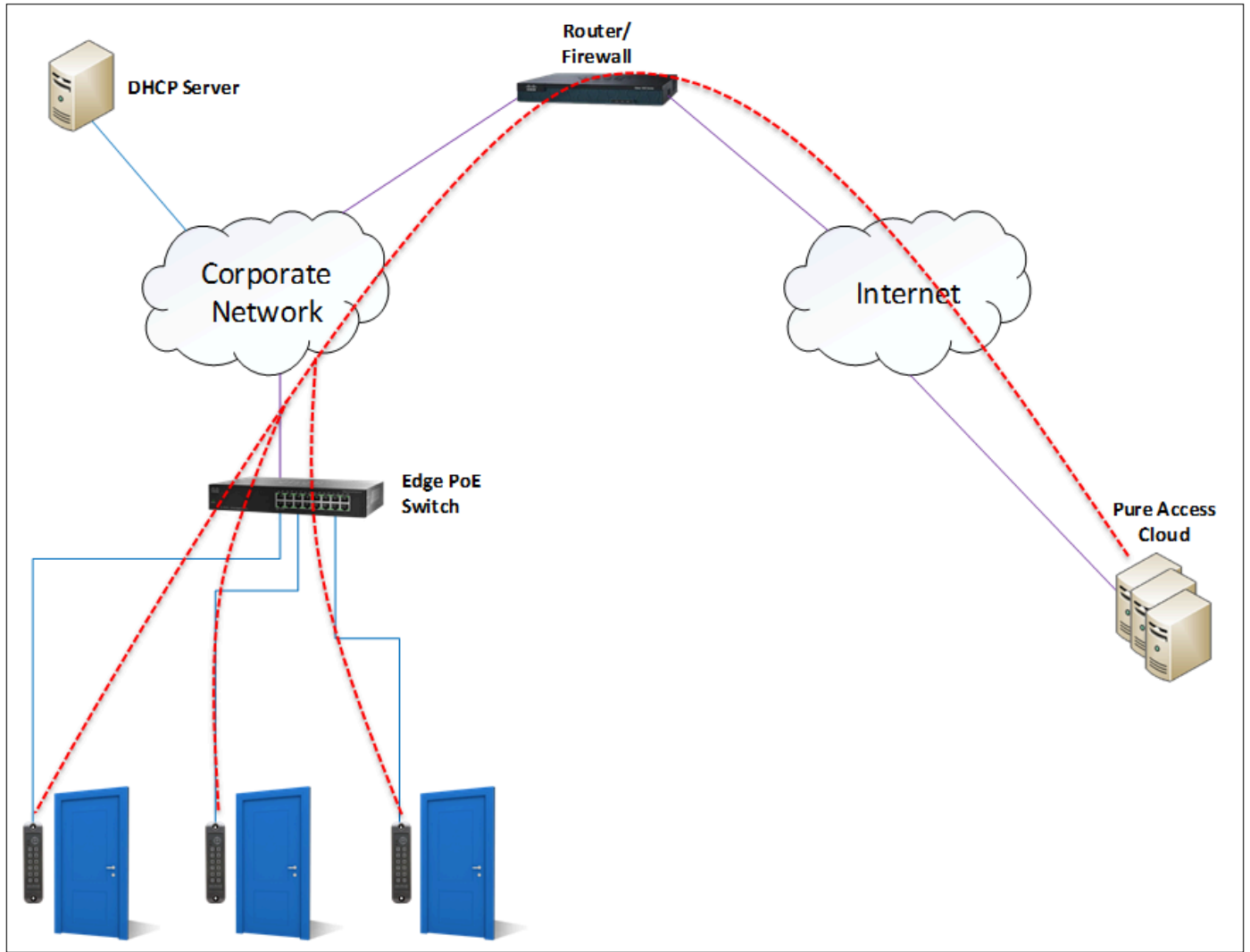


Figure 3 – Reader-controller Connections

4.1.3. Best Practices

Network

- If possible, the reader-controllers should be in a **dedicated subnet** or **VLAN**.
 - This is not a requirement, but can be considered a best practice for IoT style devices.
 - **High traffic devices** (such as IP cameras) that share the same subnet as reader-controllers *may negatively impact* the controller's ability to maintain a stable path of communication with Pure Access.
- The PoE switch should have enough power to run all ports and account for in-rush.
- We recommend the ethernet cable length **does not exceed 100 feet** unless a PoE injector is in use at the reader-controller. See pages 13-14 of the [installation manual](#) for more information.

Port Speeds

We recommend that the network switch/switches your ISONAS reader controllers are running on are set to **10Mb full duplex** and that **auto-negotiate** is **disabled**.



The one exception to this is with **RC-03 Classic** units which should be set to 10Mb **half duplex**.

Firewall

- If **Intrusion Detection and Prevention** is enabled, double check the firewall logs for dropped packets with a source IP that matches a device and create bypass rules as needed.
- A **firewall egress rule** allowing the IP addresses of the devices is required.
 - Note: The devices *do not proxy*.
- **Multiple NATs** and **multiple firewalls** are *strongly discouraged* as they can cause communication issues for the ISONAS devices.
 - If these must be used for security purposes, **ensure that all rules are configured properly** and that the IP address and ports are free to communicate through the multiple layers of firewall and/or NAT.



Recommendation: Create a group for the IP addresses and apply this group to a rule allowing port 55533 to communicate with *isonaspureaccesscloud.com* (52.38.127.152). Both UDP and TCP should be allowed to pass.

4.1.4. Additional Troubleshooting

General

- Do you have **port 55533** open to the internet or at least open to **isonaspureaccesscloud.com**?
 - If you are using the on-premise version of Pure Access, is port 55533 open across your enterprise?
- How is your latency? If the latency to the **isonaspureaccesscloud.com** site is greater than 100ms, you may see minor issues. If greater than 200ms there could be larger communication problems.
 - You can use a site like [SpeedTest.net](https://www.speedtest.net) to get a good idea of your speed and latency.
 - You can also use a simple [ping command](#) from your desktop. Note that the ability for your PC to successfully ping a device *does not* mean the controllers can also communicate with the Pure Access servers.
- Can you log into the switch? When connecting a network device, it's always a good idea to make sure either you or an IT staff member has access to the network switches to troubleshoot connectivity issues.

Connectivity Issues

- Ensure that the device is [configured properly](#). If you have a unit that is currently connected and fully operational, you may want to [compare the configuration settings](#) of this device with that of the device that is not communicating.
 - Note that the reader mode will need to be set to **Client** and the remote host name will need to match the correct Pure Access environment (if directing to an IP address this *will not* be displayed):

The screenshot shows a window titled "Reader Information" with a "Current Settings" section. The settings are as follows:

MAC address:	00:18:C8:40:18:A9	Reader Type:	RC04
DHCP:	Enabled	Reader mode:	Client
Current IP:	10.45.155.12	Server port:	10001
Static IP:	192.168.1.81	Client port:	55533
Subnet:	255.255.254.0	Remote host IP:	0.0.0.0
Gateway IP:	10.45.154.1	DNS IP:	8.8.4.4
Remote host name:	isonaspureaccesscloud.com		

At the bottom of the window, there is a checkbox labeled "Advanced Diagnostics" which is currently unchecked.

- If you are **unable to discover a unit**, plug the reader into an unmanaged PoE switch connected to your PC and try again.
 - Alternatively, you can use a PoE injector and a crossover cable to connect the reader directly to a PC.
- If using DHCP, try to statically set a reader's IP to an available address instead. Setting the reader to a static IP will let us know if DHCP is preventing the connection.
- If running Pure Access Cloud, try **bypassing the DNS**.
 - To do this, you will need to configure the reader(s) using the Cloud server's IP – **52.38.127.152** – as the host address (click "*Specify Host IP Address*" in [the configuration tool](#)).
 - Alternatively, you can find the public IP address of our Cloud environment via command prompt by typing ***nslookup isonaspureaccesscloud.com*** then hitting enter.
 - If the device is able to connect this way, we know there is a DNS issue.
- If running Pure Access Manager (on-premise), ensure that the **Windows Firewall** is not blocking the connection. You may want to disable the firewall entirely to test.
- Run a packet capture application such as Wireshark to determine where/when the data is dropping.

Physical Issues

- If possible, power-cycle the switch where the affected device(s) are connected.
- Verify that the CAT cable connected to the device is not faulty. It may be best to try another cable entirely.

- Verify that the PoE port on the switch is fully operational.
 - If you are able to test the port with a spare reader (or swap this port with the port of a functional reader), that can be useful in narrowing down the root of the issue.
 - For issues related to powering on the device, a PoE tester is useful determining whether or not the port is supplying the proper voltage.

4.2. Configuring ISONAS Devices

Overview

The ISONAS Hardware Configuration Tool is a program that allows an installer to configure ISONAS devices to connect to Pure Access. This application can be downloaded from the quick links on [our website](#) or by simply [clicking here](#).

The tool broadcasts out on the local network to discover ISONAS hardware. Once found, the reader controllers/bridges can then be configured to connect to Pure Access.

The [following articles](#) will detail how to do this.

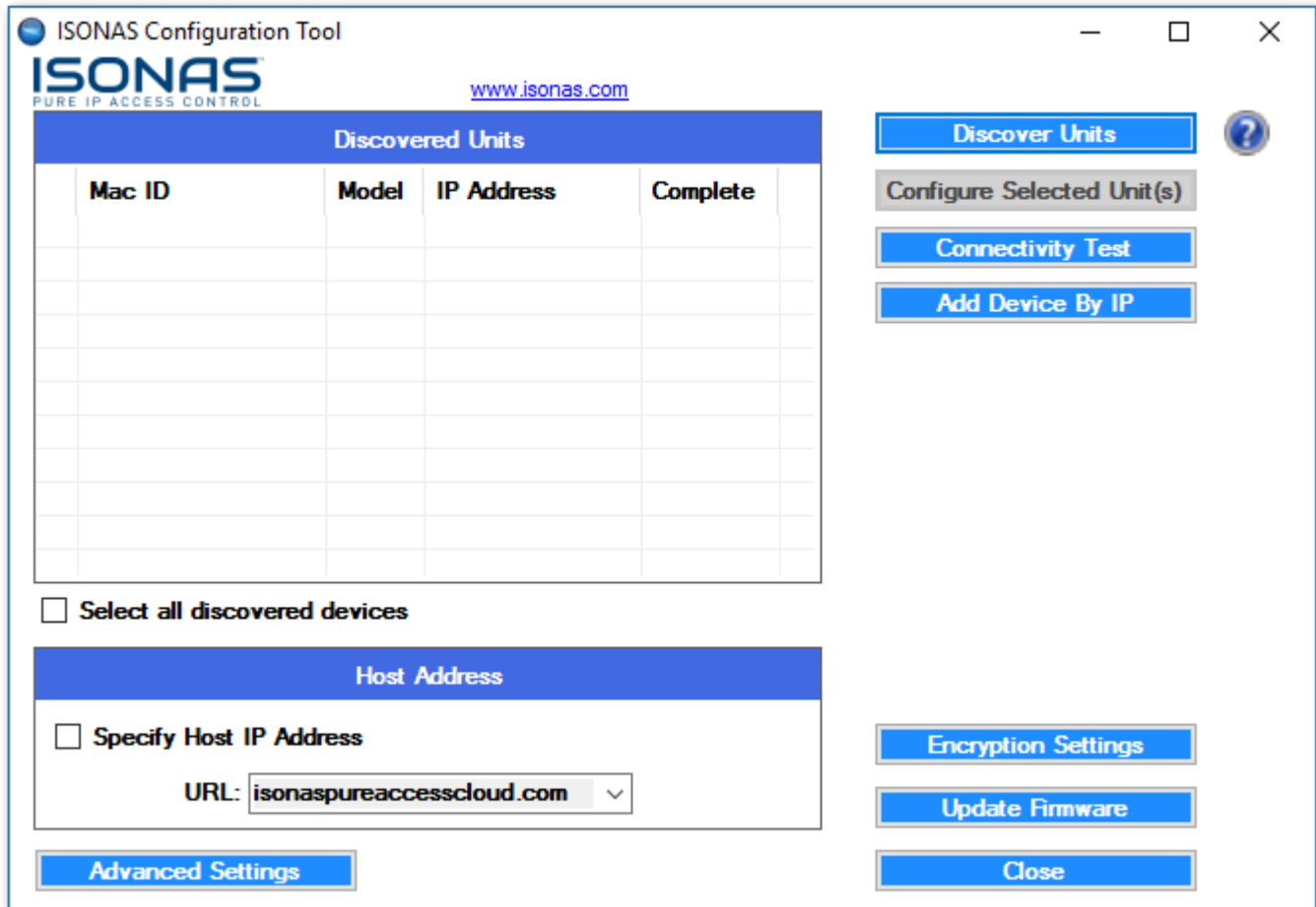
Additional Hardware Resources (optional)

For information on how to install RC-03's and IP-Bridges (including LED status information and jumper configuration), please review these PDF documents:

1. [RC-03 Installation](#)
2. [IP-Bridge Installation](#)

4.2.1. Using the Configuration Tool

[Download](#) the latest version of the Configuration Tool. Note that you will need a Windows PC to run this application.



Clicking on [Discover Units](#) will find any ISONAS devices on the local area network. If no devices are discoverable, you will need to ensure that the configuration tool is being run on a system that is **on the same subnet** as the readers/bridges.

Here is how the list will look once populated with discovered devices:

ISONAS Configuration Tool

www.isonas.com

Discovered Units

	Mac ID	Model	IP Address	Complete
<input type="checkbox"/>	00-18-C8	RC03	10.45.154.71	
<input type="checkbox"/>	00-18-C8	IPBR	10.45.155.194	
<input type="checkbox"/>	00-18-C8	RC03	10.45.155.11	
<input type="checkbox"/>	00-18-C8	IPBR	10.45.155.154	
<input type="checkbox"/>	00-18-C8	RC03	10.45.155.200	
<input type="checkbox"/>	00-18-C8	IPBR	10.45.155.53	
<input type="checkbox"/>	00-18-C8	RC03	10.45.155.182	
<input type="checkbox"/>	00-18-C8	RC03	10.45.154.88	
<input type="checkbox"/>	00-18-C8	RC04	10.45.154.242	
<input type="checkbox"/>	00-18-C8	RC03	10.45.154.9	
<input type="checkbox"/>	00-18-C8	IPBR	10.45.155.100	

Select all discovered devices

Host Address

Specify Host IP Address

URL:

Advanced Settings

Buttons: Discover Units, Configure Selected Unit(s), Connectivity Test, Add Device By IP, Encryption Settings, Update Firmware, Close

✿ If you are not able to find the devices on the network, see the [Discovering Units section](#).

Clicking on “**Connectivity Test**” will determine if the network segment that the Configuration Tool is running on can make a connection to Pure Access.

The default test will determine if there is a path to communicate with Pure Access Cloud over the internet:

Connectivity Test

Start

Test Setup

Use Default Test Parameters

Host URL:

DNS:

Host Port:

Test Results

Status: *Untested*

Step: *Untested*

DNS Connectivity.....	<input type="text" value="N/A"/>
NS Lookup.....	<input type="text" value="N/A"/>
Host Connectivity.....	<input type="text" value="N/A"/>
Mock Connection Test....	<input type="text" value="N/A"/>

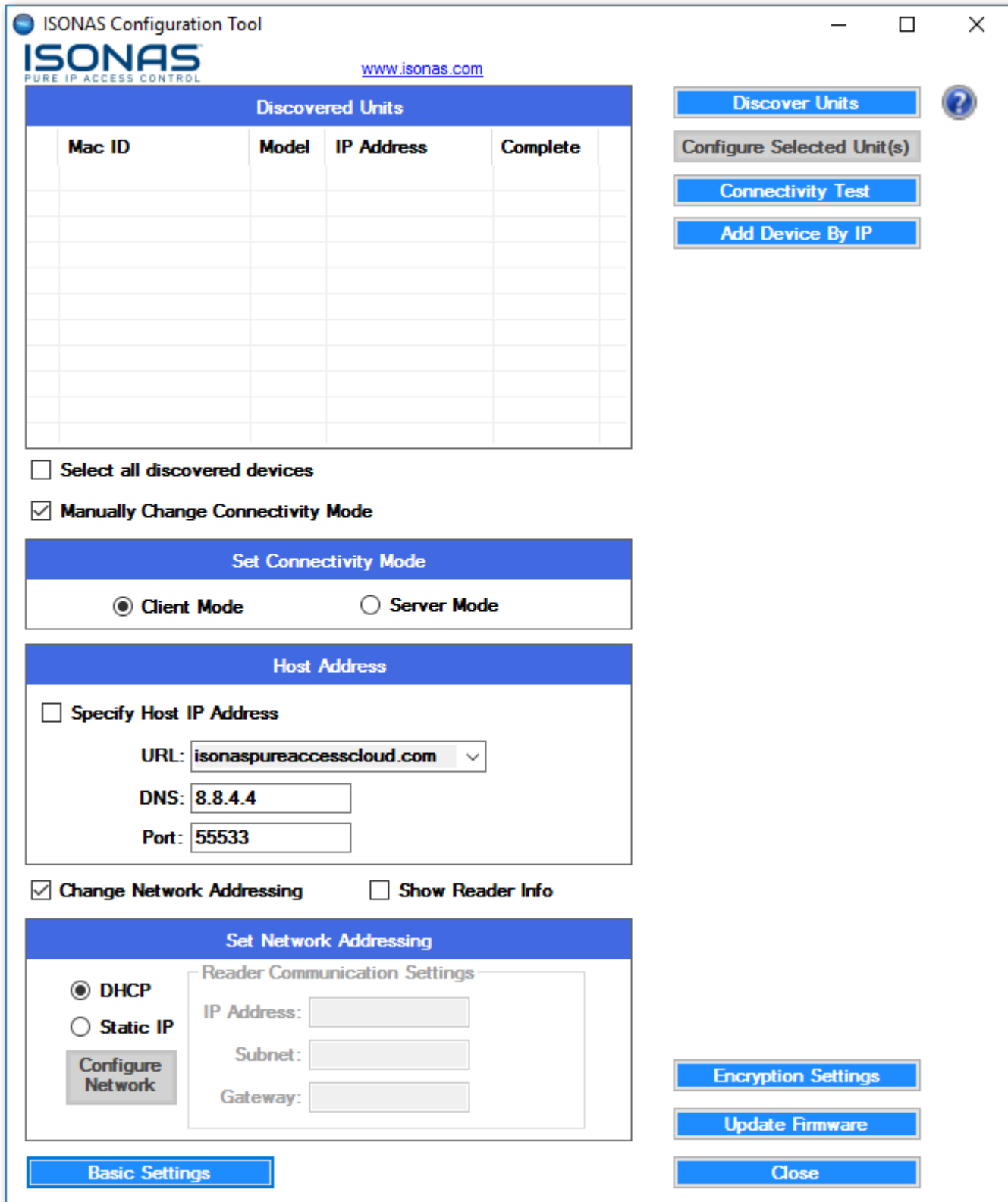
Export **Print**

If the devices were discovered, proceed to [Advanced Configuration](#) to continue setting up the controllers.

4.2.1.1. Advanced Configuration

Clicking on  will bring up the options needed to fully configure a device.

The options now available allow you to change where the device(s) will be attempting to connect as well as the ability to set the readers to either [DHCP \(preferred\) or static IP addresses](#).



Establishing a connection to Pure Access:

1. All devices must be set to **Client Mode** in order to initiate a connection with Pure Access. **Server Mode** is reserved for updating the firmware of the devices only.

2. The **Host Address URL** can be accessed via the drop-down menu.
 - a. The host address is set to *isonaspureaccesscloud.com* by default.
 - b. If you are attempting to connect to a Demo tenant, you will need to direct the device to *isonaspureaccessdemo.com*.

The screenshot shows a window titled "Host Address". At the top, there is a checkbox labeled "Specify Host IP Address" which is currently unchecked. Below this, the "URL:" field is set to "isonaspureaccesscloud.com". A dropdown menu is open, showing the following options: "isonaspureaccesscloud.com", "isonaspureaccess.com", "isonaspureaccessdemo.com", and "Custom Host URL...". A mouse cursor is pointing at the "isonaspureaccessdemo.com" option. To the left of the dropdown, there is a partially visible button labeled "Advanced Set".

- c. If your tenant is on our legacy environment, this will need to be *isonaspureaccess.com*.
3. For **Pure Access Manager**, you must click "**Specify Host IP Address**" and then input the server's IP in the "IP Addr" field.

The screenshot shows the "Host Address" window with the "Specify Host IP Address" checkbox checked. Below the checkbox, there is a text input field labeled "IP Addr:" which is currently empty.

4. DNS should be left as the default 8.8.4.4 (which is Google's free DNS service provider). If this value is changed, ensure it is being directed to a working DNS server.
5. All devices are set to **DHCP** by default. This is the recommended IP addressing method for Pure Access. If static addresses are being used, ensure that all of the network addressing values are correct.
6. Once all values have been set, select the checkbox of the device in the "**Discovered Units**" window and click the **Configure Selected Unit(s)** button. The "**Complete**" column should say "Yes," the configure button should have a green check mark next to it, and the unit should reboot (see image below).
7. The **Configure Selected Unit(s)** button can be used to push the configuration settings out to multiple readers at the same time. If static IP addresses are being assigned, however, units must be configured individually.

✿ To verify the above settings, you can highlight a device then click on **Show Reader Info**. More information on this can be found in the [Review Existing Settings on a Device](#) article.

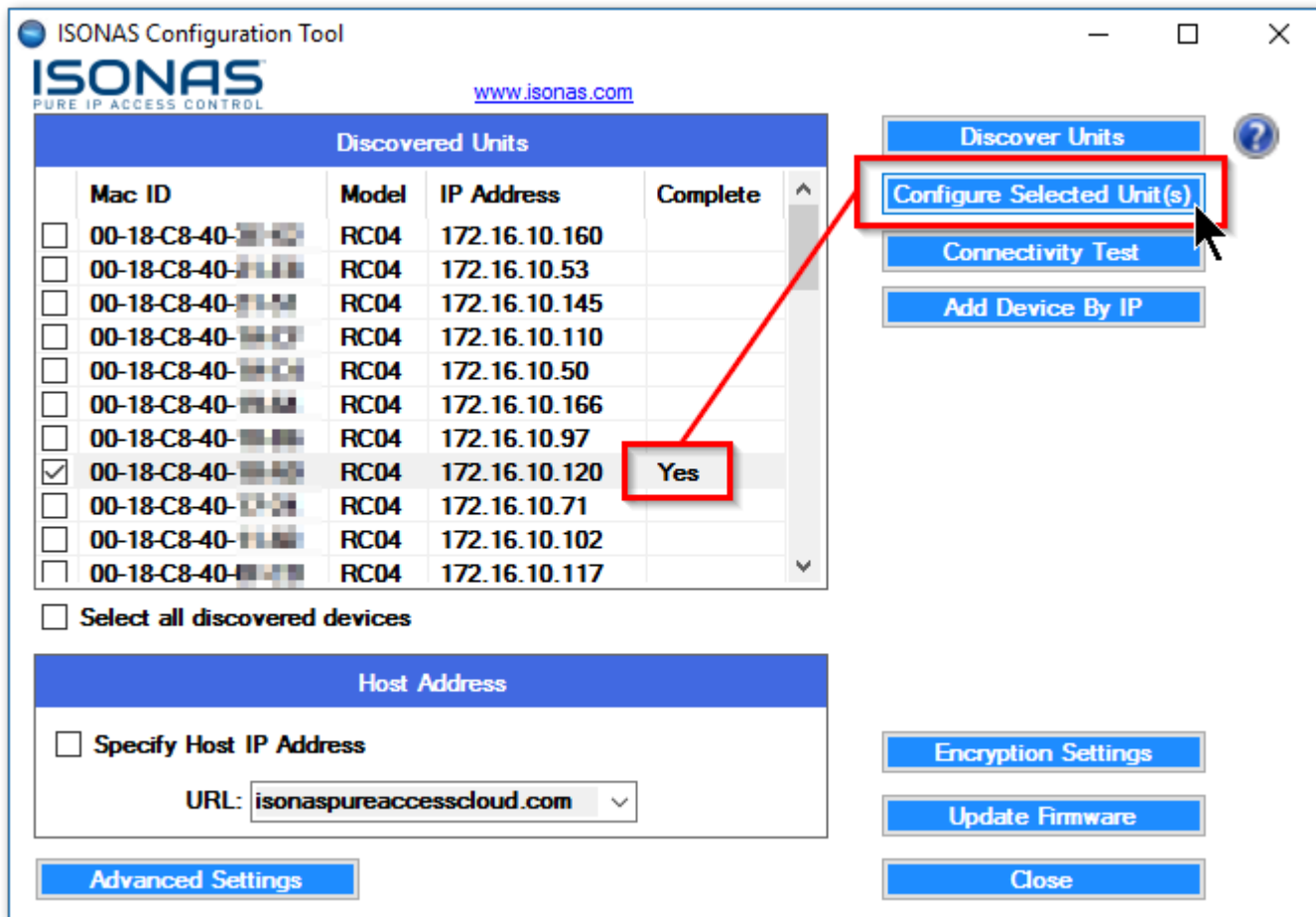


Figure 8 – Configure Selected Unit

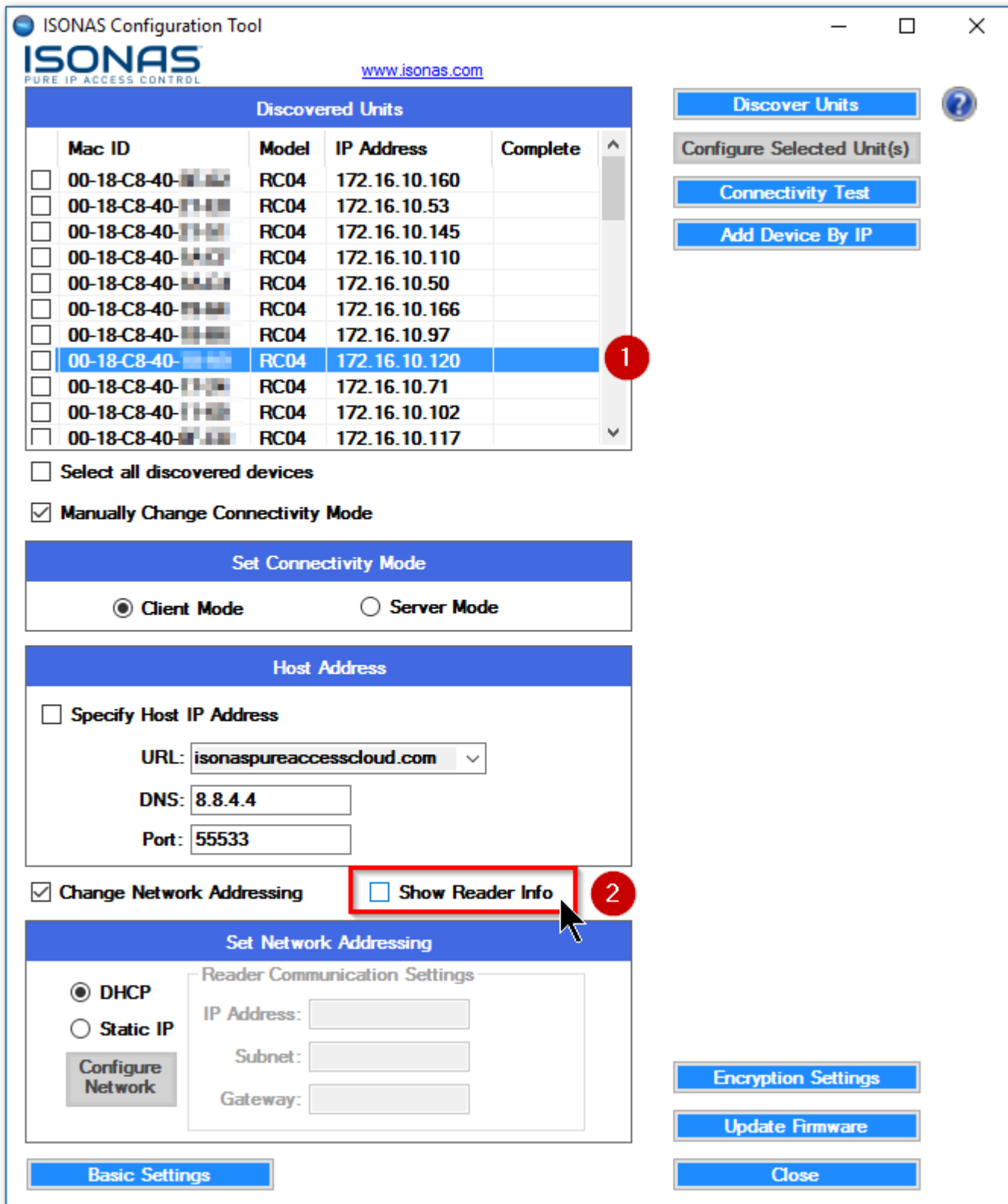
Your devices have now been configured to point to Pure Access. The next step is to log in to the Pure Access portal and begin [adding your access points using their MAC addresses](#).

! If you were unable to configure the units using the above information, please see [Review Existing Settings on a Device](#) to ensure everything is configured correctly. If the reader information appears correct, please have your IT team review the [network configuration settings and best practices](#).

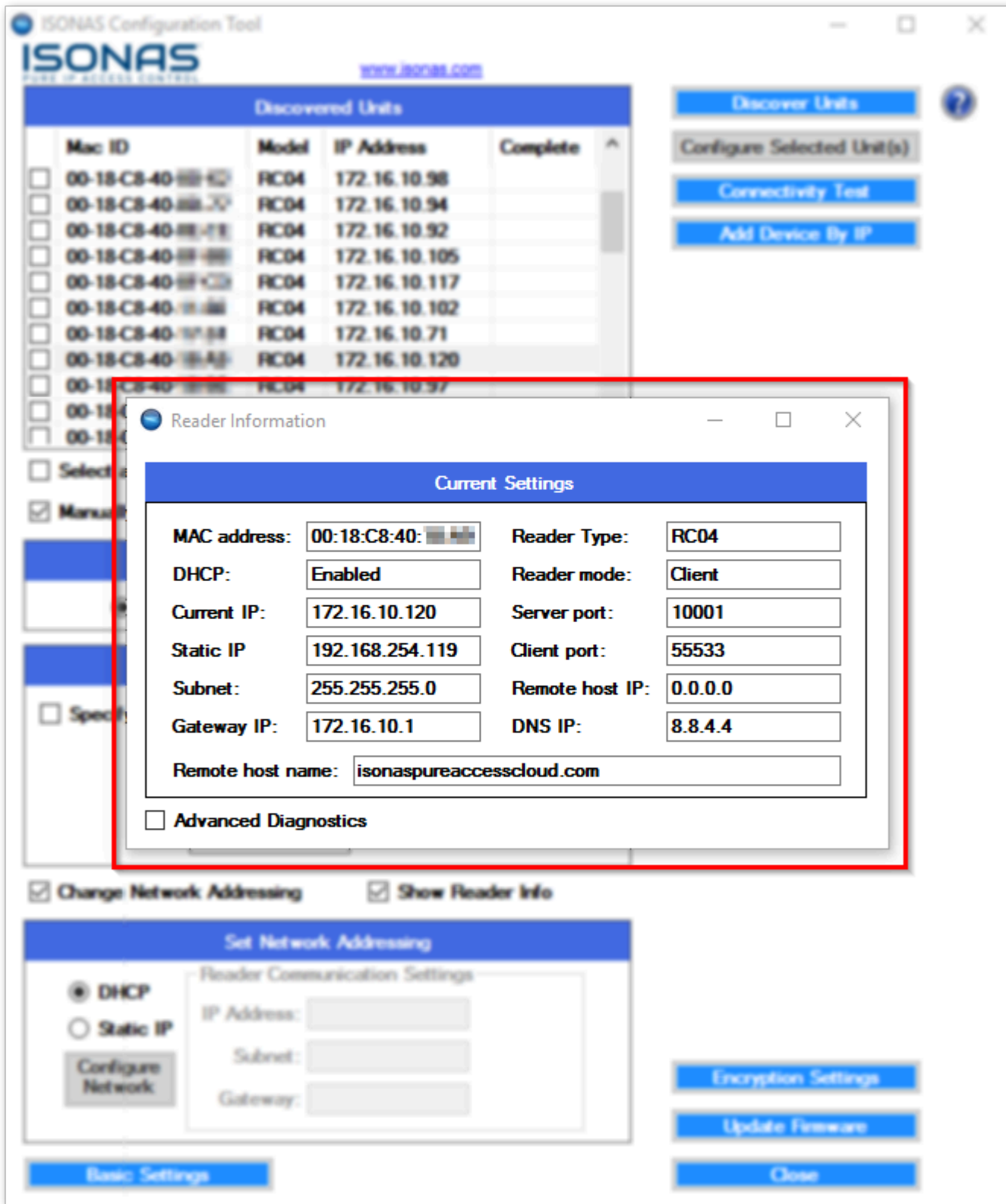
4.2.1.2. Reviewing Network Config Settings

To see the current configuration of a device:

1. Discover the unit on the subnet
2. **Highlight** it from the discovered units field
3. Click on “**Advanced Settings**”
4. Click “**Show Reader Info**”



Once the “**Show Reader Info**” box is clicked, a “**Current Information**” window will appear displaying the configuration settings of the device.

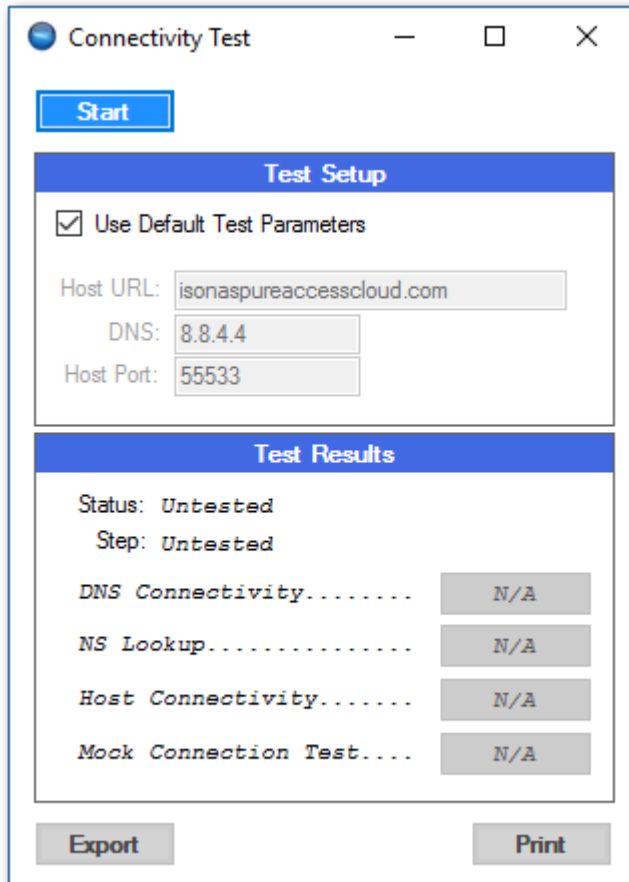


How the device is currently configured

✿ With the **Current Information** window open, you can simply highlight another device in the config tool to quickly display its settings. This is a handy way to compare the configuration settings of multiple units.

4.2.1.3. Connectivity Test

The **Connectivity Test** is meant to ensure that your network environment is properly configured and ready to add ISONAS devices. This will save time during set up by limiting network troubleshooting and narrowing potential networking configuration changes that may prevent connectivity to Pure Access.



The screenshot shows a window titled "Connectivity Test" with a "Start" button. Below the button are two sections: "Test Setup" and "Test Results".

Test Setup

- Use Default Test Parameters
- Host URL:
- DNS:
- Host Port:

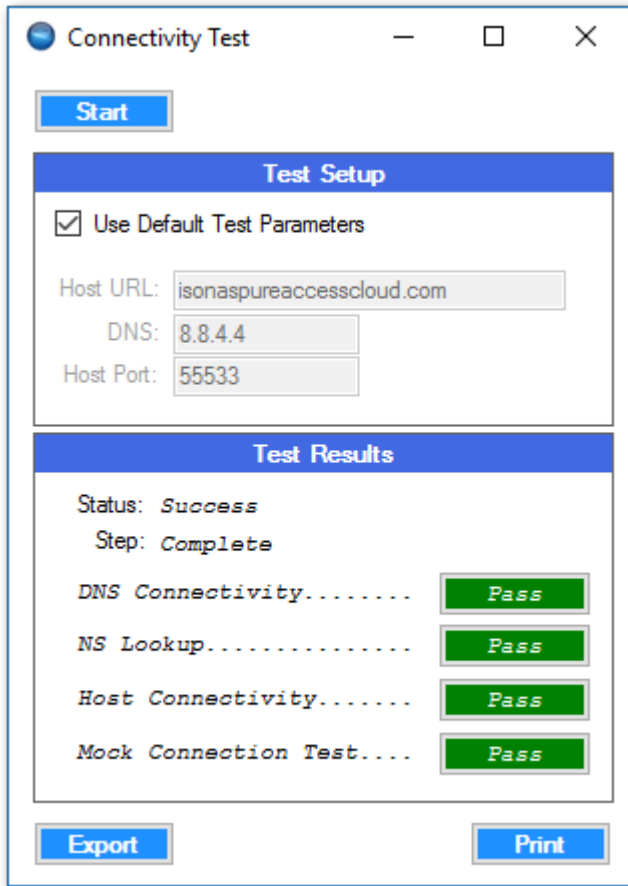
Test Results

Status:	Untested
Step:	Untested
DNS Connectivity.....	<input type="text" value="N/A"/>
NS Lookup.....	<input type="text" value="N/A"/>
Host Connectivity.....	<input type="text" value="N/A"/>
Mock Connection Test....	<input type="text" value="N/A"/>

At the bottom of the window are "Export" and "Print" buttons.

The connectivity test will run a series of four tests:


- **Test 1:** Pings the specified DNS server (Google DNS by default) 4 times and averages the response time to confirm DNS connectivity
- **Test 2:** Finds routing info for ISONAS Pure Access Cloud using the specified DNS server (Google DNS by default)
- **Test 3:** Tests connectivity to ISONAS Pure Access Cloud by pinging the environment 4 times and averaging the response times.
- **Test 4:** Simulates a device connection by ensuring a simulated ISONAS device can make a connection to Pure Access through port 55533.



The results of the test can be clicked on to display more information. Alternatively, one can export or print the results of the test for further review.

* An export of this test can be helpful for an IT or network team to investigate communication issues.

4.2.2. Discovering Units

If no devices appear after clicking the  button or you do not see all devices, check the following items:

1. Verify that all devices are powered up and fully booted. A fully booted RC-03 will have the top LED on with a color of red. A fully booted IP-Bridge will have the top left LED on with a color of green (see images below).
2. Verify that the Windows PC (with which the Configuration Tool is running) is connected to the correct network and has a valid IP address for that network.
 - a. Ensure that all devices are on the **same subnet**. The Configuration Tool uses broadcast packets on the network to find devices.
 - b. Broadcast traffic is dropped by routers so only devices on the network segment that the Configuration Tool is running on will be seen.
3. If using VLAN's, verify with an IT Administrator that all of the switch ports' devices are on the correct VLAN.
4. There is also an option to [discover a device by IP](#) or an IP address range.

If there are still issues with discovering units and/or connecting devices to Pure Access, review our [documentation on basic network configuration](#) and best practices.



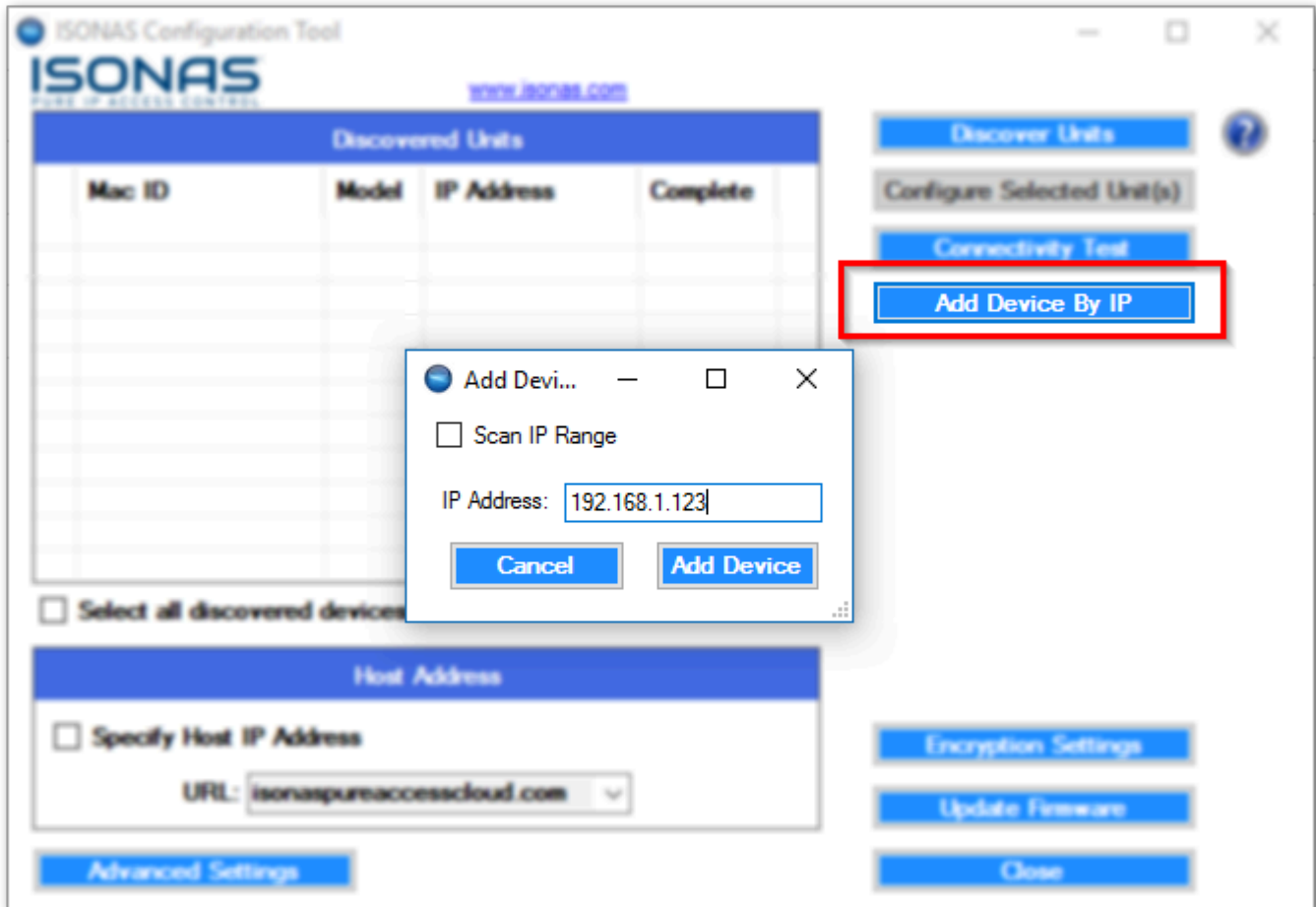
Fully booted RC-03



Fully booted IP-Bridge

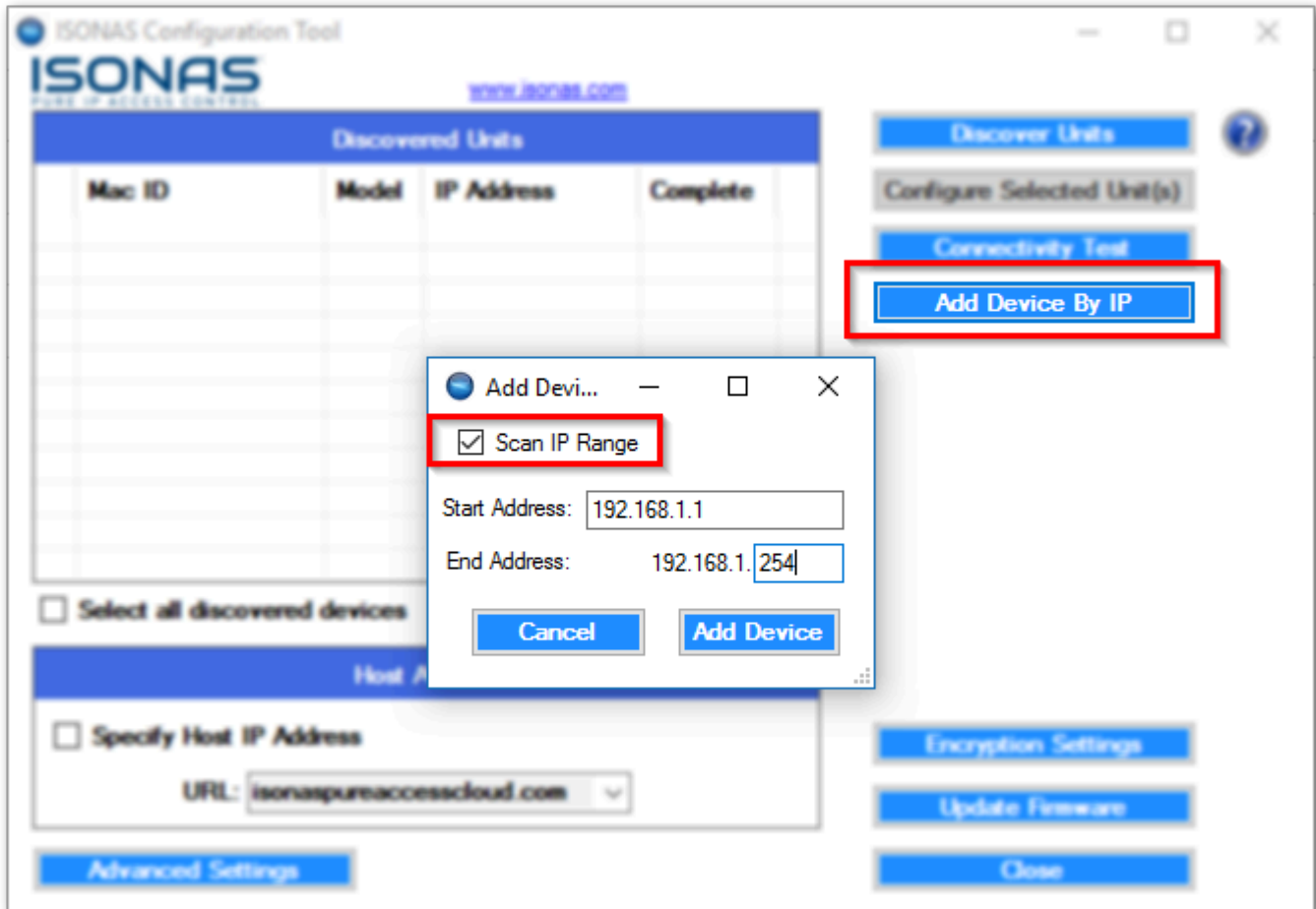
4.2.2.1. Find device by IP

Another way to configure devices is to use the configuration tool to scan an IP address or range of addresses.



Adding a device by IP

Simply select **Add Device by IP**, then select the **Scan IP Range** check box. Enter the start address and the last octet of the end address and select add device.



Add Devices by IP range

From here you simply select the units that are discovered by selecting the check box or select all discovered devices and configure them to the appropriate URL.

For more information on how to set up your access points, check out our [YouTube channel](#) for further details.



4.3. Updating Firmware

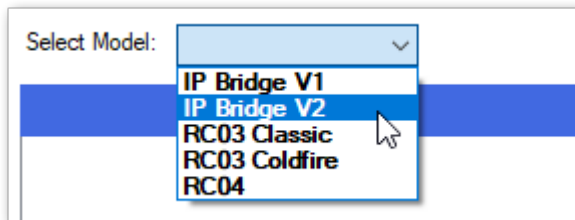
There are two necessary components for updating firmware on your ISONAS hardware:


1. The [ISONAS hardware configuration tool](#)
2. The latest [firmware files](#) for your device

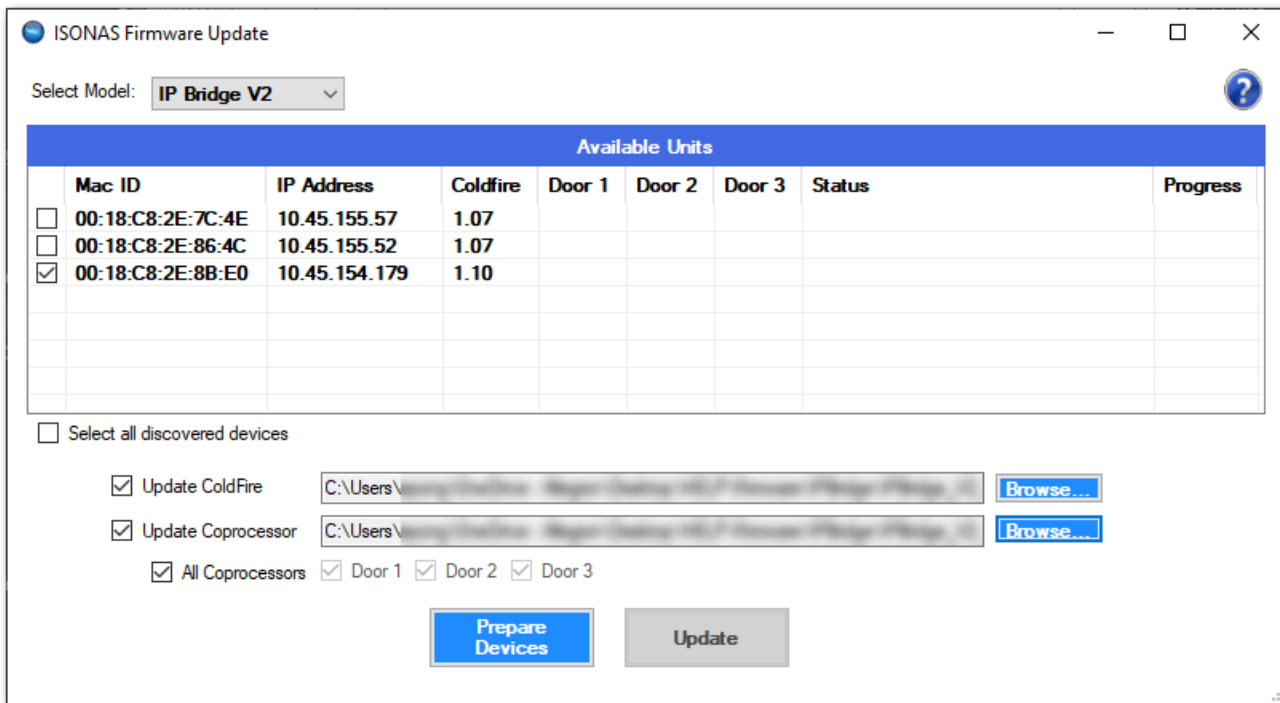
! **Before beginning the update process**, please note that we *do not* recommend updating **more than five** devices simultaneously since the increase in network traffic may cause complications/failure of the firmware to update properly.

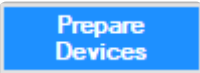
Instructions

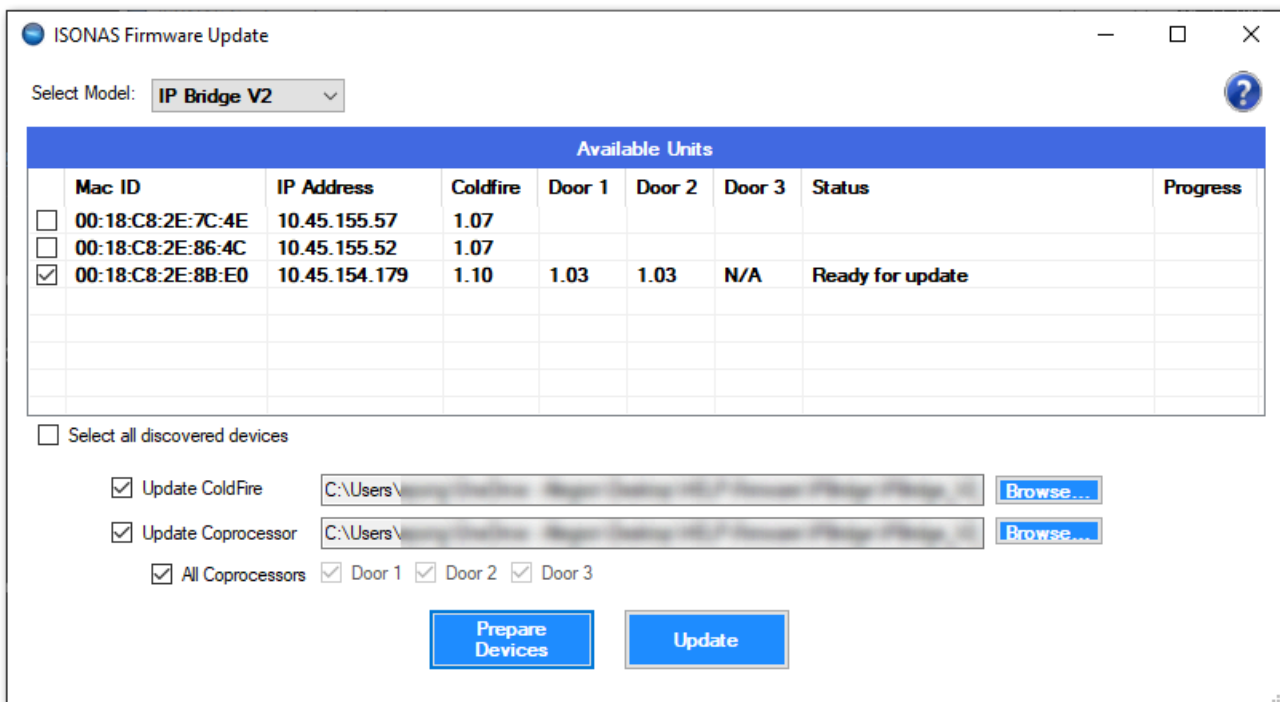
1. Download and unzip the latest firmware files onto your machine.
2. Launch the ISONAS hardware configuration tool and then click the  button.
3. Once devices have been discovered, click  to open the firmware update window.
4. Select your device's model from the "Select Model" drop-down menu.

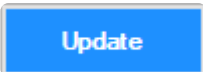


5. Use the check-boxes to select the device(s) that need to be updated.
 - a. For RC-03's and IP-Bridges: Select **Update ColdFire** as well as **Update Coprocessor**. Both of these will need to be updated.
 - b. For RC-04's: Select **Update ColdFire**. See note below for more information.
6. Click  then navigate to the folder where the firmware files have been unzipped.
7. Select the firmware file (only the correct file type will appear) then click "Open".



- Once the firmware files have been selected, click  which will reboot the device(s) into **Server Mode**. Once the reader is in this state it will display **“Ready for update”** under the **Status** column.



- Click 
- Once finished, the **Status** will read **“Complete”** and the device(s) will reboot and return to **Client**

Mode where they will re-connect with Pure Access.

ISONAS Firmware Update

Select Model: **IP Bridge V2**

Available Units								
	Mac ID	IP Address	Coldfire	Door 1	Door 2	Door 3	Status	Progress
<input type="checkbox"/>	00:18:C8:2E:7C:4E	10.45.155.57	1.07					
<input type="checkbox"/>	00:18:C8:2E:86:4C	10.45.155.52	1.07					
<input checked="" type="checkbox"/>	00:18:C8:2E:8B:E0	10.45.154.179	1.13	1.03	1.03	N/A	Complete	100%

Select all discovered devices

Update ColdFire

Update Coprocessor

All Coprocessors Door 1 Door 2 Door 3

* The RC-04's Coprocessor board and BLE (Bluetooth Low Energy) chip have not received updates in quite some time and are no longer included in this process.

4.4. Wiring and Hardware Installation

Please review our [Hardware Wire Designer Tool](#) or [this PDF](#) to find diagrams for basic configurations.

If you cannot find your particular setup using the above, please contact support@isonas.com.

4.4.1. RC-04 Installation Guide

Here is an [installation guide](#) for the RC-04 in PDF format.

For information on how to add an RC-04 to Pure Access, please review the [Managing Access Points](#) section.

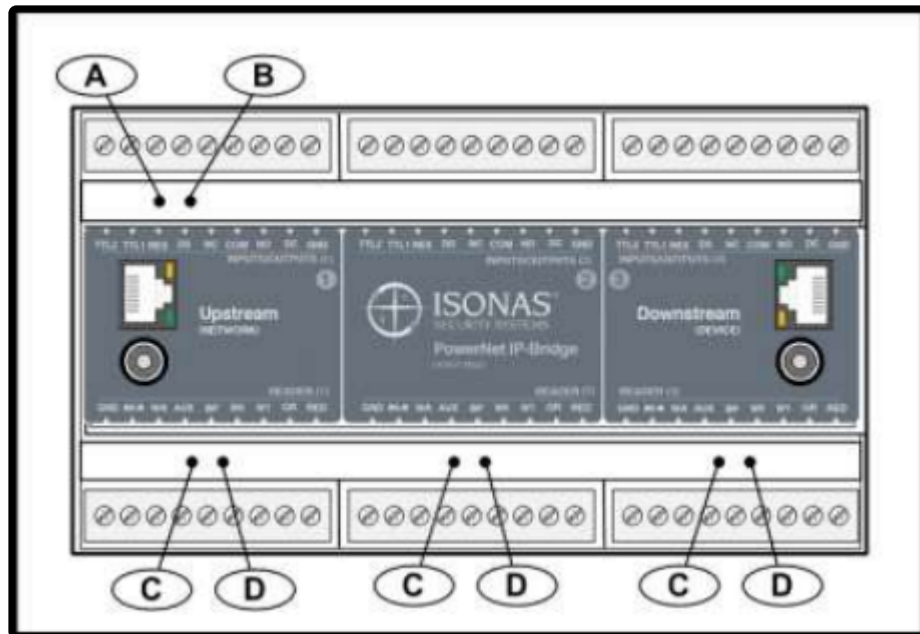
4.4.2. IP-Bridge Installation Guide

Here is an [installation guide](#) for the IP-Bridge in PDF format as well as the [insert that comes in the box](#).

For information on how to add a bridge to Pure Access, please review the [Managing Access Points](#) section.

4.4.2.1. IP-Bridge Status Light Indicators

The IP-Bridge has multiple LED status indicators to assist in monitoring and troubleshooting the status of the unit. LED's are labeled below.



LED's A and B are used to indicate the status of the IP-Bridge itself.

The C & D LED pairs indicate the status of individual doors.

IP-Bridge Status	LED "A" Color	LED "B" Color
IP-Bridge is not powered on	Off	Off
Power Turned On – Waiting in Boot Loader mode (~10 sec)	Red	Red
Performing All IP work, all mode, duration depends on settings	Amber	Red
IP Work completed (except long DNS lookups), ports/DNS	Red	Amber
Startup Complete – Errors reported	Green	Amber
Startup Complete – No issues reported	Green	Off
IP-Bridge is on and in a normal state	Green	Green

Door Status	LED "C" Color	LED "D" Color
No Door (2-door Bridge)/Deactivated Door	Off	Off
Normal Operation	Red	Off
Door is unlocked	Green	Green
Door is unlocked for the latch interval	Green	Off

Door is in the Lockdown state	Red	Red
Waiting in Startup or Performing Boot Load	Amber	Amber
Waiting to be activated or door process issue	Off	Amber

4.4.3. RC-03 Installation Guide

Here is an [installation guide](#) for the RC-03 in PDF format.

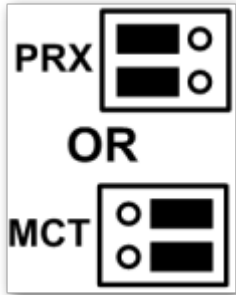
For information on how to add an RC-03 to Pure Access, please review the [Managing Access Points](#) section.

4.4.3.1. RC-03 Jumper Configurations

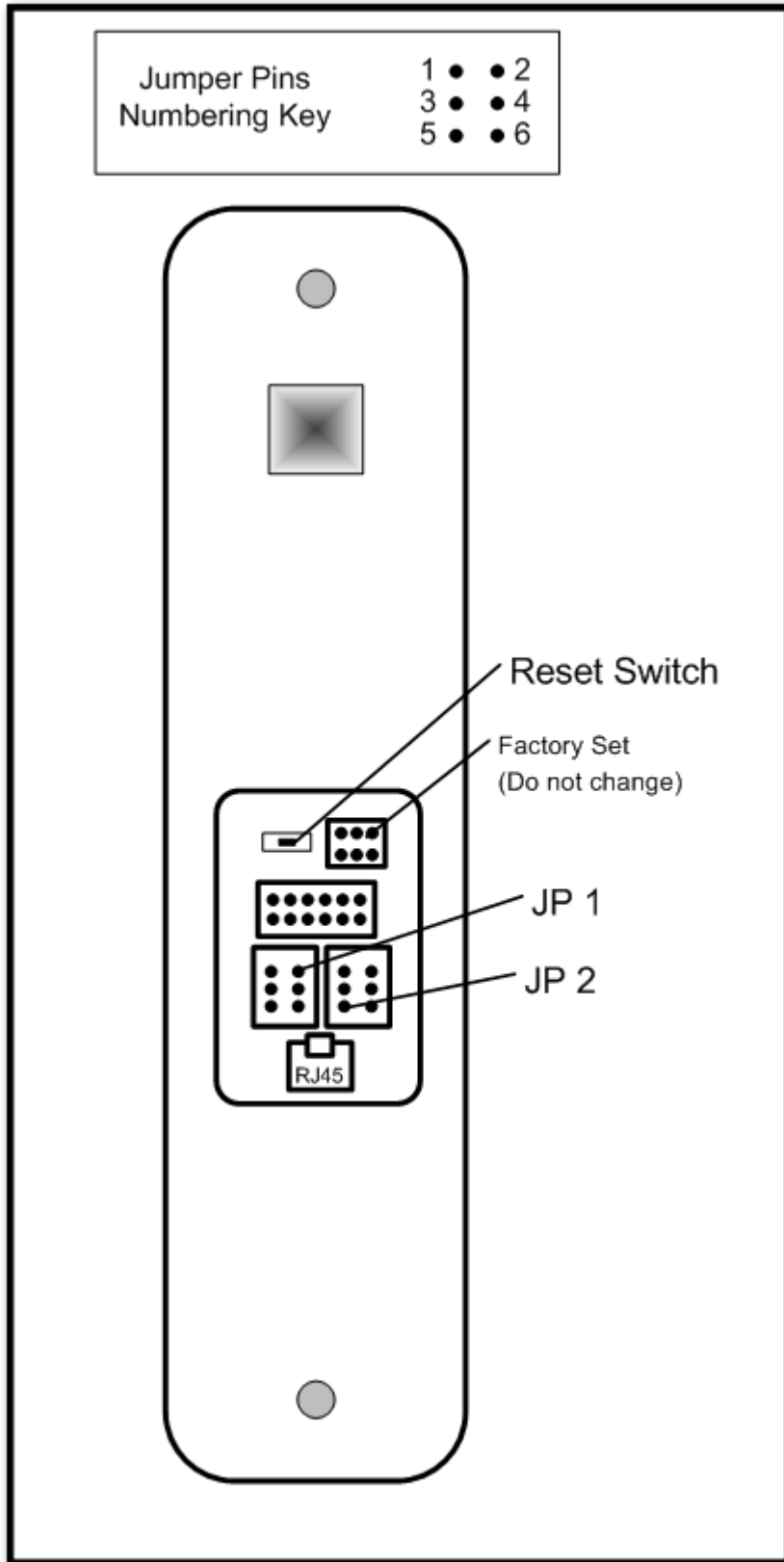
The RC-03 PowerNet reader-controller has a set of jumper pins that configure both its input power source and its lock control circuit. The device can be configured for power to be supplied to it through the 12 conductor pigtail (either 12VDC or 24VDC) or through the RJ45 connector (Power Over Ethernet).

If PoE is used, the reader-controller can supply 12VDC through its pigtail which may be used to power the lock or other devices at the door location.

- * The RC-03 has an additional set of jumpers. These jumpers **should not** be changed. The jumpers are set at the factory, based on the PowerNet's internal hardware. If these jumpers are changed, the PowerNet **will not operate correctly**. If accidentally moved, replace the jumpers to the positions shown.

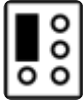

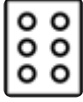


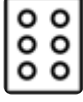





The below image shows the components on the back of the RC-03:



RC-03 Jumper Configurations:

Feature	JP 1 Jumpers	JP 2 Jumpers
---------	--------------	--------------

Input Power – 12VDC through Pigtail	1 to 3 	
Input Power – 24VDC through Pigtail	3 to 5 & 4 to 6 	
Input Power – PoE through RJ45 connector	None 	
Input Power – PoE through RJ45 connector (See Note 1)	1 to 3 	
Input Power – No effect, place-holder for extra jumper	2 to 4 	
Lock's power/signal is externally supplied on the pigtail's pink wire		None 
Supply internal 12VDC to relay common (See Note 2)		1 to 3 
ISONAS External Door Kit being used		3 to 4 
Connect GROUND to relay's common contact		3 to 5 

Note 1 – Special case: The unit is PoE powered AND you want 12v output power supplied on the pigtail's red conductor.

Note 2 – Used when powering an external lock device. This option only available if JP 1 is configured for PoE.

4.4.4. ASM Status Light Indicators

The Advanced Security Module/ASM (formerly referred to as an Exterior Door Kit or EDK) has two status LEDs.

Power LED:

Located on the side towards the Pure IP Reader-Controller's pigtail.

A **red** LED indicates 12VDC power is being supplied to the ASM.

Communication Status LED:

Located on the side towards the lock wiring.

LED status meanings are described in the table below.

Pure IP Reader Controller Locked	Pure IP Reader Controller Unlocked	Lock State when Pure IP Reader Controller is Unlocked	Description or Item to Check
OFF	GREEN	Normal Operation	
Flash Amber	Flash Amber	No Operation	Yellow wire may be disconnected.
OFF	Flash Amber	No Operation	White wire may be disconnected.
OFF	Flash Amber	No Operation	Invalid encryption key received from Pure IP Reader-Controller.
OFF	OFF	No Operation	If power cycle of Pure IP Reader-Controller allows for one or more lock operations, and then the lock stops operating, then the BackEMF diode may not be installed correctly.

4.4.5. Factory Resetting a Device

To factory reset an RC-03, RC-04, or IP-Bridge; you will need to hold the reset button down for approximately 15 seconds. The location of the reset button differs from device to device.

RC-03:

Small horizontal button above the RJ-45 input.

RC-04:

Small round button on the back of the device (center). You will need a paperclip to press this.

IP-Bridge:

Small round hole on the right side of the device. You will need a paperclip to press this.

4.4.6. Wiegand Interface Module (WIM)

The **Wiegand Interface Module** (WIM) is an add-on device available from ISONAS.

Function:

- It allows connecting an external, Wiegand-only reader to the serial port on an RC-03.
- A credential presented on the Wiegand-only reader is treated like a presentation on the RC-03.
 - Allows for in/out style doors.
- Allows for two-factor authentication on an RC-03 using 3rd party devices.
 - Factor 1 can be a read from a credential on RC-03.
 - Factor 2 could be a read from a Wiegand fingerprint sensor.
 - Factor 2 could be a read from a Wiegand license plate reader.

The main function it is used for is in/out style doors. The door remains locked at all times, a valid badge on either the interior reader (RC-03) or exterior reader (Wiegand device) unlocks the door.

To enable this functionality:

1. Put the RC-03 in server mode.
2. Open the Reader Commander tool and connect to the device.
3. Issue a “*Set Wiegand*” command .
 - a. Disable (no WIM support).
 - b. Wiegand Raw (WIM support, no bitmasking).
 - c. Wiegand w/ HID processing (WIM support, bitmasking applied) – most common setting when using a WIM.
4. Close Reader Commander and point your reader back to Pure Access (set it into Client Mode).

Once the above is complete your device will support the WIM in Pure Access.

5. Getting Started in Pure Access

1. [Logging into a Pure Access Cloud tenant](#)
2. [Bitmasking](#)
3. Configuring [Areas](#) (optional)
4. Managing [Users](#)
5. Managing [Access Points](#)
6. Configuring [Schedules, Weekly Rules, Events and Holidays](#)
7. Setting up [Dashboards](#)
8. Setting up [Widgets](#)

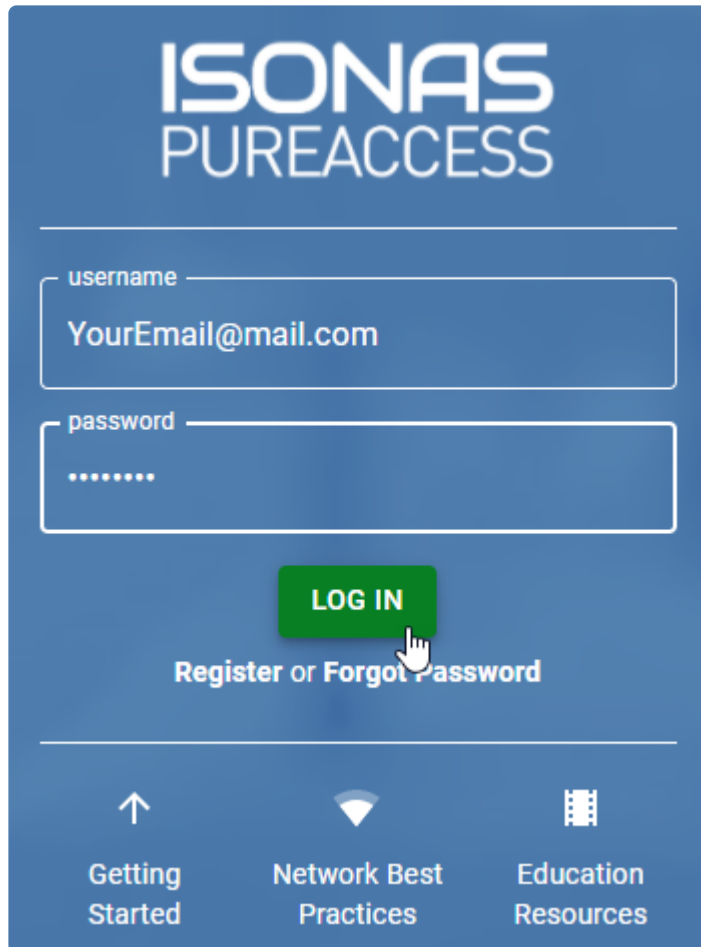
5.1. Pure Access Cloud

This section of the manual will cover these common topics:

- [How to log into a Pure Access Cloud tenant](#)
- [Finding the name of the current tenant](#)
- [Current version and release notes](#)
- [Trouble logging into a tenant](#)

5.1.1. Logging into a Pure Access Cloud tenant

From the login page located at <https://isonaspureaccesscloud.com/>, simply type in your username and password then click “**Log In**”:



ISONAS
PUREACCESS

username
YourEmail@mail.com

password
.....

LOG IN

Register or Forgot Password

↑
Getting Started

Network Best Practices

Education Resources

If you have access to multiple tenants, you will be met with a list to select from:

Select Tenant

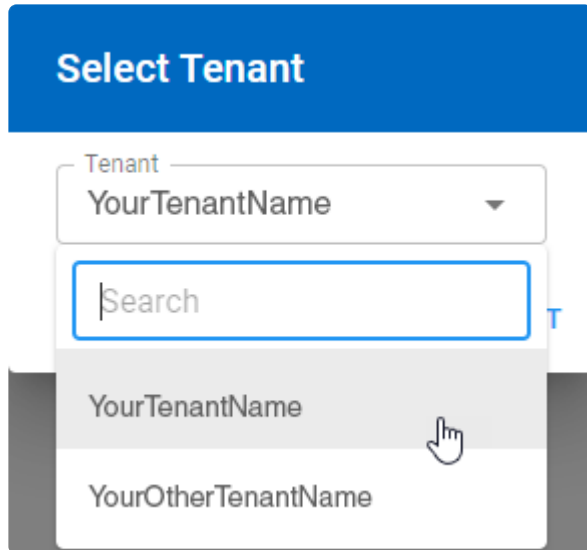
Tenant

YourTenantName

Search

YourTenantName

YourOtherTenantName



* There are multiple Pure Access environments with similar web addresses. When attempting to log in, please ensure you are going to the correct environment.

Forgot password? Locked out?

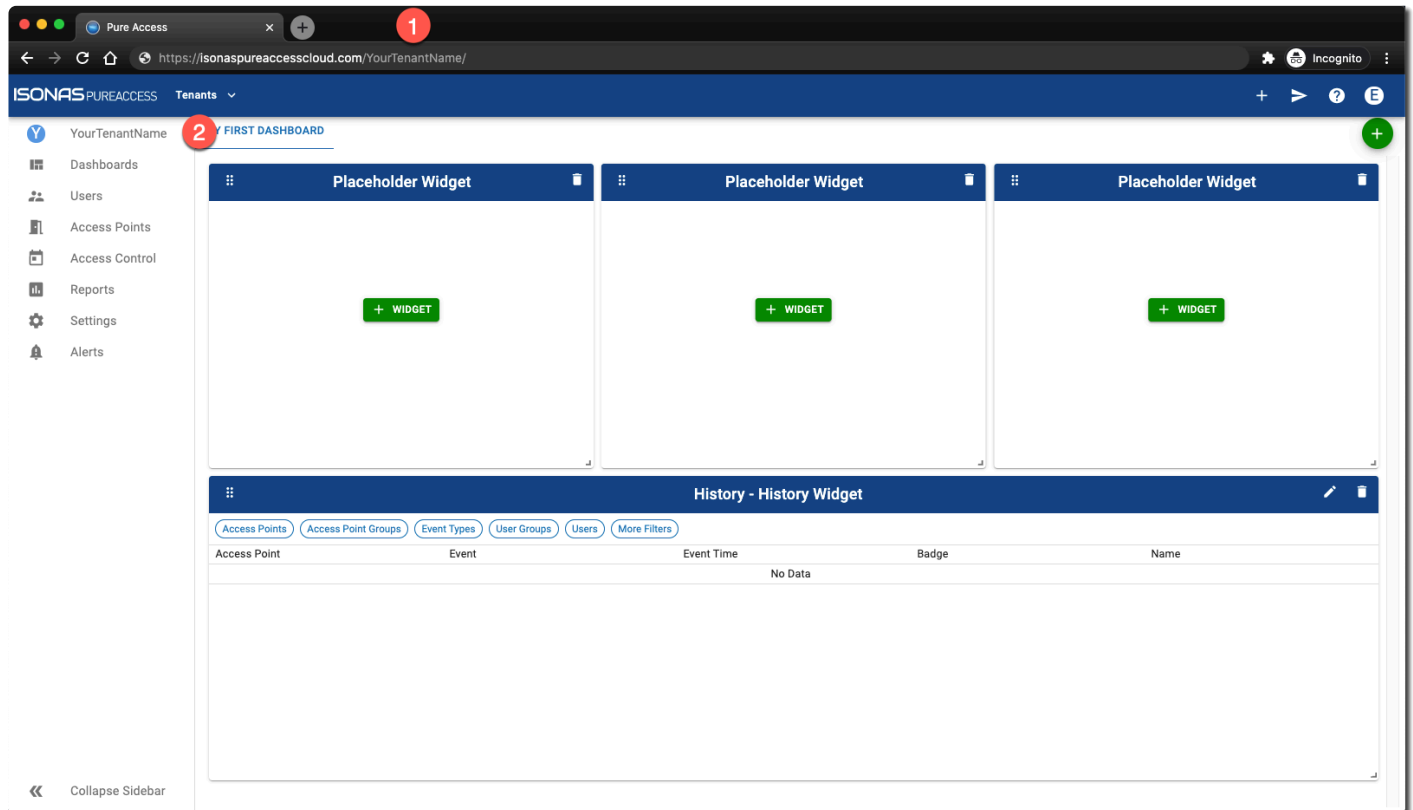
For security, we are not able to reset passwords upon request. You can reset your password by clicking on the **“Forgot Password”** link from the login page. See [next page](#) for instructions.

5.1.2. Tenant Name

What's my tenant name?

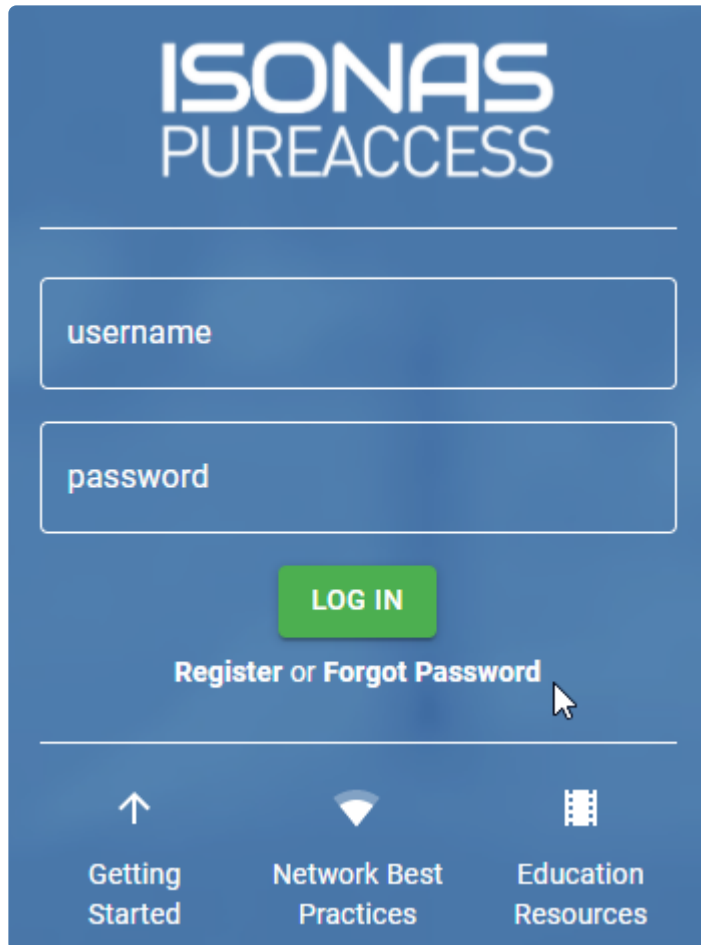
You can find the name of your tenant from two places:

1. In your address bar, immediately after “isonaspureaccesscloud.com/” (see image below)
2. At the top of the left navigation bar (must be expanded)



5.1.3. Cannot Log into Pure Access Tenant

If you're unable to log into your tenant because either your password is not working or it has been forgotten, you will need to click on the [Forgot Password](#) link from the [Pure Access Cloud login page](#).



ISONAS
PUREACCESS

username

password

LOG IN

Register or Forgot Password

↑
Getting Started

Network Best Practices

Education Resources

Once you've filled out the email address associated with your web access profile, click "**Continue**" and an automated email will be sent which must be followed within 20 minutes.

Reset Password

Email

CONTINUE

CANCEL

Success

The password reset link was sent. If this is a valid email, the link should be in your inbox.


CLOSE

! We are not able to reset passwords per request as it is against Isonas security policy. If you have followed the instructions above but have not received an email, please ensure that you have spelled your email address correctly and check your spam filter.

5.1.4. RMR License

An RMR license will allow an integrator to create and manage **subtenants** under their **parent tenant**.

Each subtenant will have its own distinct administrators, users, access points, etc.

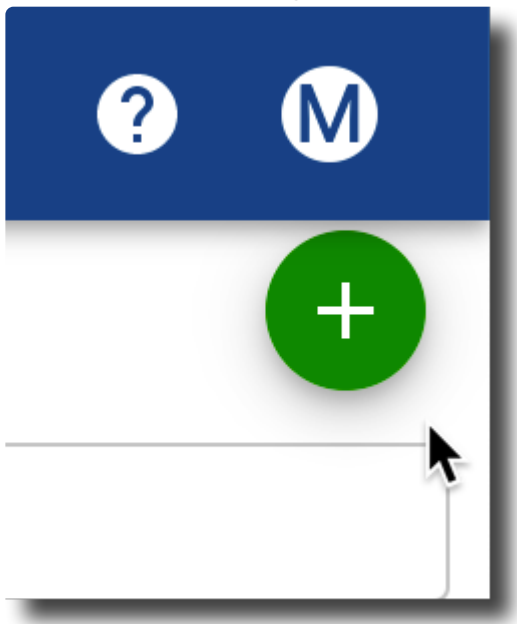
 We advise against using a parent tenant for access control. Please create a new subtenant to be used for this purpose.

5.1.4.1. Creating Subtenants

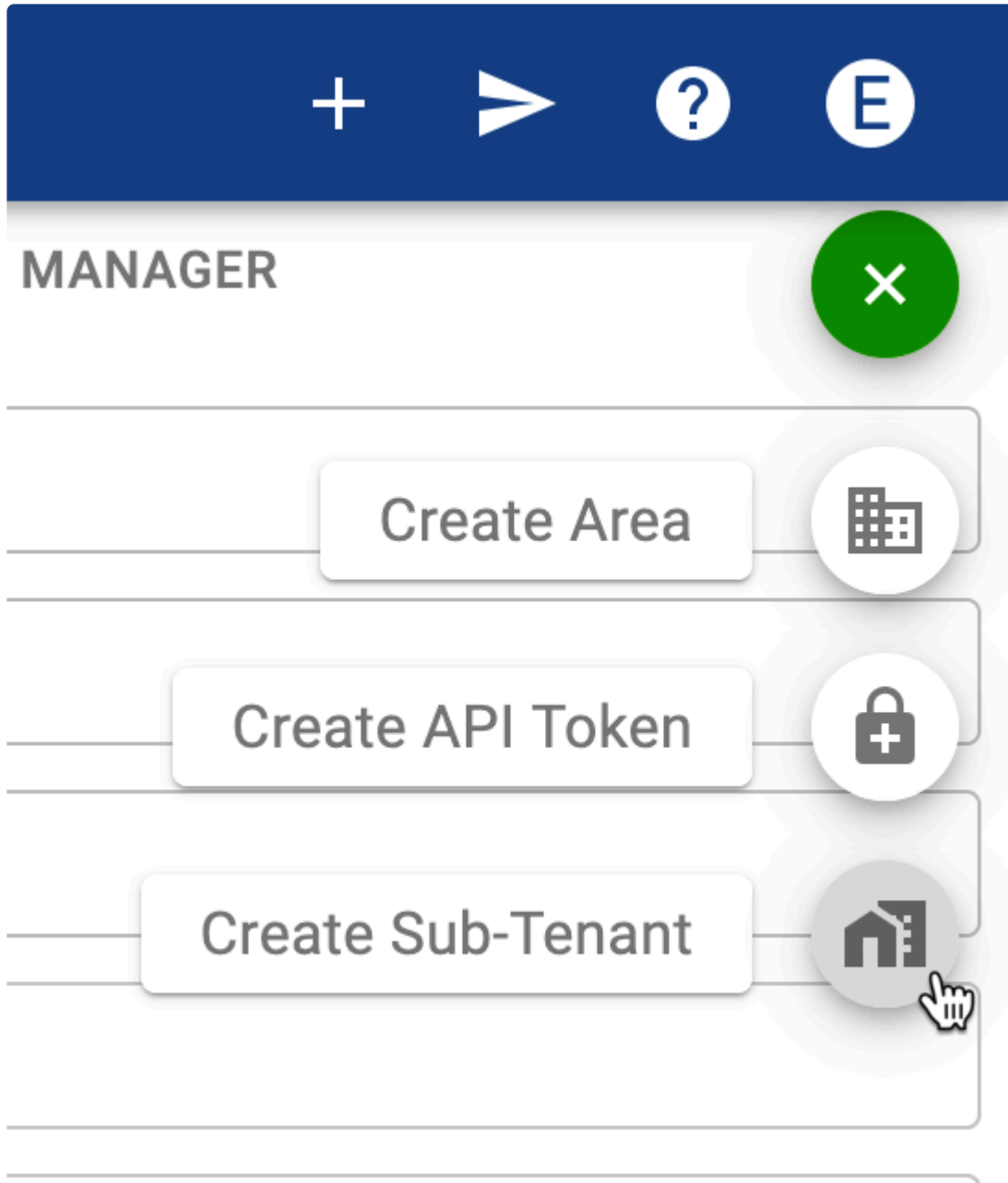
1. Navigate to **Settings**.



2. Hover over the plus sign to reveal the menu. You may need to scroll to the right to see this menu.



3. Click on the **Create Sub-Tenant** button in the upper right corner of the page.



4. Fill in the **Add Tenant** window. Then click **CREATE**. Note that the only required field is “Tenant Name”.

The screenshot shows a 'Create Tenant' form with a dark blue header. The form contains the following fields:

Tenant Name	Company Name
Timezone (UTC-07:00) Mountain Time (US & Canada)	Contact Name
Administrator Email	State/Province
Street	Zip/Postal Code
City	Phone number

At the bottom right of the form, there are two buttons: 'CANCEL' and 'CREATE'.

The new subtenant will now be listed on the **Tenant Manager** page.



While possible, we advise against using the parent, top-level tenant for access control purposes.

5.2. Pure Access Manager

Information and Best Practices

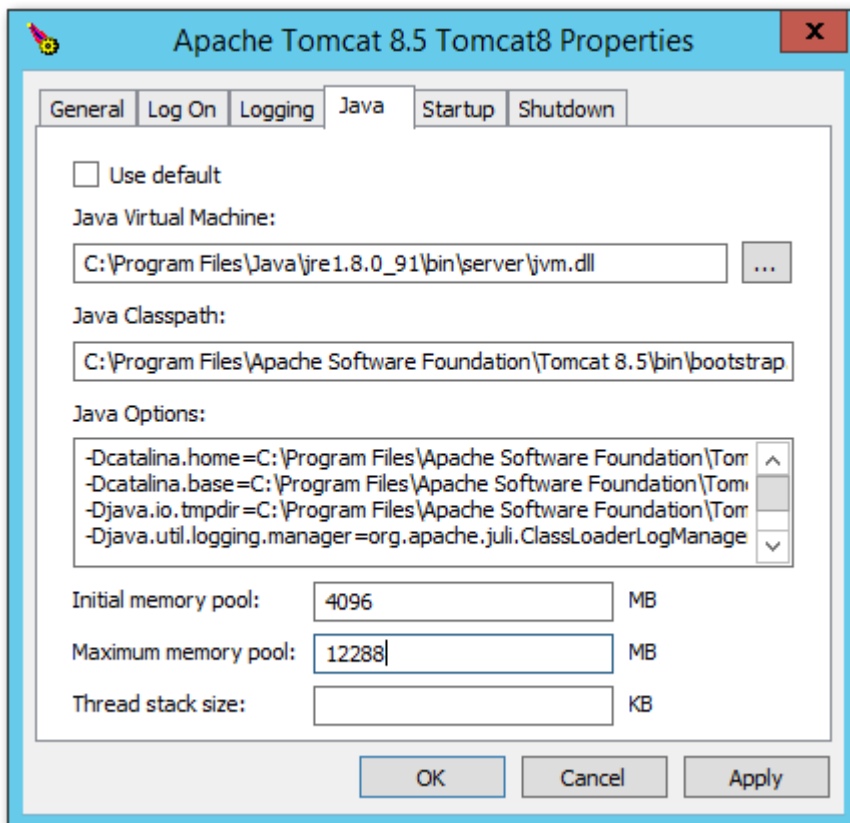
- Make sure this is a fresh installation of Windows.
 - There are many prerequisite software packages that Pure Access needs in order to function. If one of these pieces of software is already installed on the system but it is an incompatible version or if there is something using the same network ports that Pure Access uses (Port 80, 443, 55533), the installation will fail.
 - Make sure that you are not installing any additional Windows features or services such as IIS as these can conflict with the software used by Pure Access Manager.
- If you are using a virtual machine, make sure you have the networking in your Hypervisor set up correctly. If the high availability, internal VM switch or subnet mask is off in any way it can cause disconnects to the reader controllers.
- Pure Access Manager out-of-the-box has a nightly scheduled backup that gets set in the *C:\Program Files\ISONAS* directory. To make sure you don't run out of disk space, only 3 days' worth of backups are kept. If you want to keep more than this, you should use your existing backup system to backup the *C:\Program Files\ISONAS\DB_Backups* folder or copy the files to another computer.

If you have not already reviewed the system specifications, please see [this article](#).

5.2.1. Java Memory Allocation

After installing Pure Access Manager, you will need to adjust the amount of memory that is allocated to Java in order for the system to perform optimally.

1. Open the Windows File Explorer and navigate to *C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin*
2. Run **Tomcat8w.exe**
3. Click on the **Java** tab
 - Initial memory pool: Set to 4096 (4GB of RAM)
 - Maximum memory pool: Enter approximately 80% of the system memory.
 - If you have a server with 8 GB of RAM, enter 6144 (6 × 1024)
 - If you have a server with 16 GB of RAM, enter 12288 (12 × 1024)
4. Click **Apply** then reboot the server

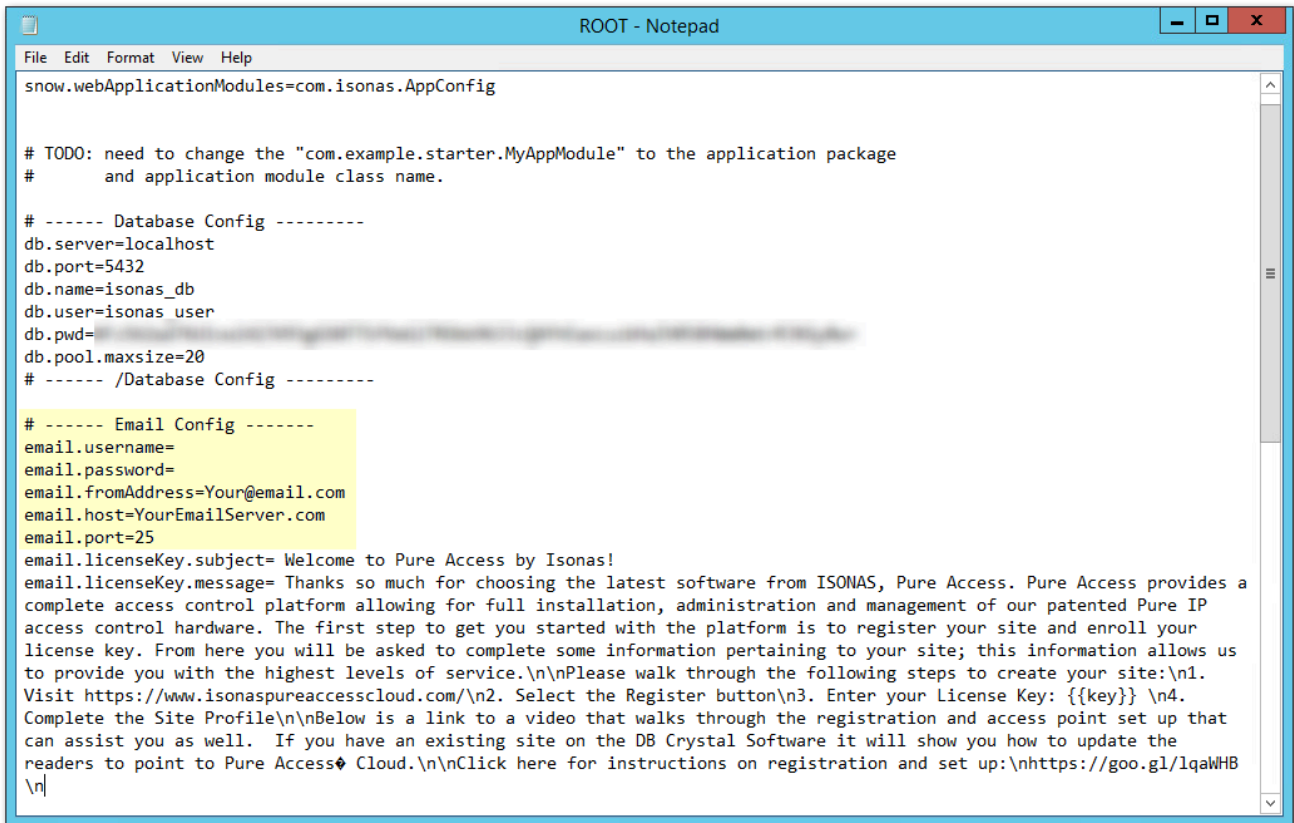


5.2.2. SMTP Configuration (Pure Access Manager)

In order to configure email/SMTP for receiving alerts, password resets, and web access invitations in Pure Access Manager, please follow the below steps.

Note that if you are running **PAM 2.12.2**, you **will need to configure allowed hosts** in order for password reset emails to send. See the bottom of this page for more information.

1. Navigate to the **ROOT.properties** file located in the folder *C:\Program Files\Apache Software Foundation\Tomcat 8.5\webapps*
2. Open file using Notepad or your preferred text editor.
3. Change the “*Email Config*” section to your preferred settings:



```
ROOT - Notepad
File Edit Format View Help
snow.webApplicationModules=com.isonas.AppConfig

# TODO: need to change the "com.example.starter.MyAppModule" to the application package
#       and application module class name.

# ----- Database Config -----
db.server=localhost
db.port=5432
db.name=isonas_db
db.user=isonas user
db.pwd=
db.pool.maxsize=20
# ----- /Database Config -----

# ----- Email Config -----
email.username=
email.password=
email.fromAddress=Your@email.com
email.host=YourEmailServer.com
email.port=25
email.licenseKey.subject= Welcome to Pure Access by Isonas!
email.licenseKey.message= Thanks so much for choosing the latest software from ISONAS, Pure Access. Pure Access provides a
complete access control platform allowing for full installation, administration and management of our patented Pure IP
access control hardware. The first step to get you started with the platform is to register your site and enroll your
license key. From here you will be asked to complete some information pertaining to your site; this information allows us
to provide you with the highest levels of service.
Please walk through the following steps to create your site:
1. Visit https://www.isonaspureaccesscloud.com/
2. Select the Register button
3. Enter your License Key: {{key}}
4. Complete the Site Profile
Below is a link to a video that walks through the registration and access point set up that
can assist you as well. If you have an existing site on the DB Crystal Software it will show you how to update the
readers to point to Pure Access Cloud.
Click here for instructions on registration and set up: https://goo.gl/lqaWHB
\n
```

4. Additionally, you need to set the **email.file.base.path** value so that the hyperlinks within emails can direct users to the correct system. By default, this is set to *https://isonaspureaccesscloud.com*, but must be changed to the **PAM server's IP address or hostname**:

```

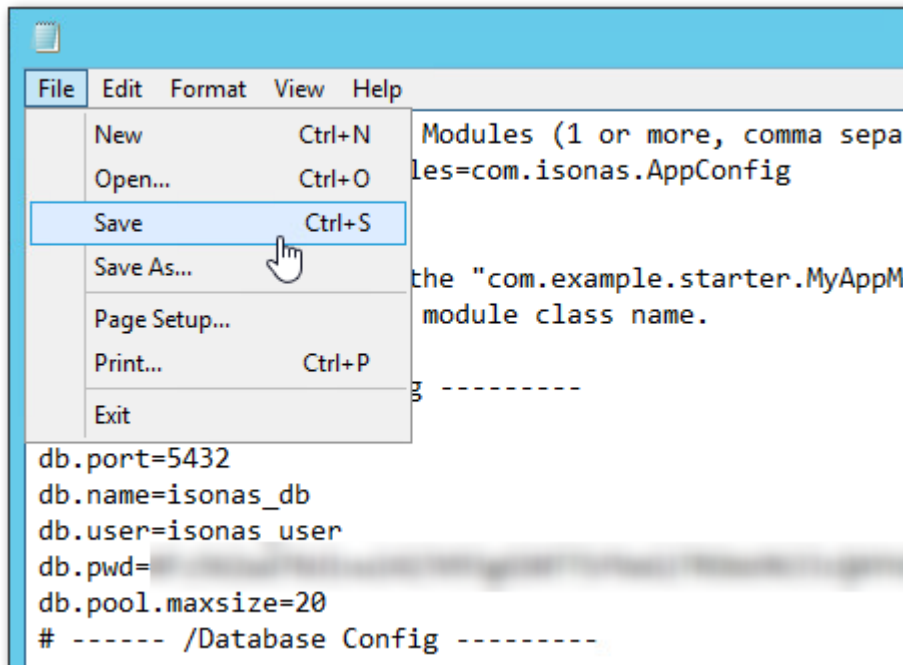
email.passwordReset.message.subject= ISONAS - Password Reset Instructions
email.file.passwordReset.path=/_emails/password_reset.html
email.file.register.path=/_emails/registration.html
email.file.alert.path=/_emails/alert.html
email.file.customrule.path=/_emails/customrule.html
email.file.scheduledReport.path=/_emails/scheduled_report.html
email.file.base.path=https://isonaspureaccesscloud.com/
# ----- /Email Config -----

cache.file.path=../_cacheFiles
attachments.path=../_attachmentFiles

importdata.tenant.mapping.path=/WEB-INF/data_tenant_map.json

```

5. If running **Pure Access Manager v2.12.2**, see the bottom of this page before continuing.
6. For Pure Access Manager v2.9.2 or earlier, you can now save the document and then reboot the server (or restart the Apache Tomcat service):



If you have an email server which requires SSL or TLS for a connection, you will need to speak with your system administrator about setting up an [email relay server](#) for Pure Access to use.

 Using **Pure Access Manager version v2.12.2?** See below.

Additional information (**allowed.hosts**) will need to be added to the bottom of the **ROOT.properties** file to get SMTP to function. This section will need to contain comma-separated values for the addresses with which the server can be accessed.

Example:

```
# -- PDF config
pdf.logo.path=css/image/logo1.jpg
pdf.font.light=_common/fonts/Roboto-Light.ttf

# -- Auth
auth.attemptsAllowed=4
  # JWT Timeout in Minutes
auth.jwt.timeout=2

eula.path=/_docs/eula.html

server.urllist=http://localhost

allowed.hosts=localhost,192.168.0.200,pureaccess.yourdomain.com,www.pureaccess.yourdomain.com
```

! For any of the above changes to take effect, the Apache Tomcat service will need to be restarted. Rebooting the PAM server is also sufficient.

5.2.3. Configuring Pure Access Manager for SSL

There are two methods for enabling SSL for Pure Access Manager:

1. Use a reverse proxy and route all traffic via the reverse proxy.
 - You can read about IIS reverse proxy setup on iis.net here: <https://www.iis.net/learn/extensions/url-rewrite-module/reverse-proxy-with-url-rewrite-v2-and-application-request-routing>
2. Install and configure a certificate in Tomcat.
 - You can read about installing a certificate directly in Tomcat here: <https://tomcat.apache.org/tomcat-8.5-doc/ssl-howto.html>

! Note that ISONAS on-premise products are supported as installed. Modifications to the third party applications that support the applications functionality are **not supported by ISONAS**. Support for the third party applications for the express purpose of modifications and troubleshooting those modifications should come from the third party support.

5.3. Migrating from One Tenant to Another

There is currently no tool/feature in Pure Access able to migrate tenant information from one account to another. This article will provide a best practice, step-by-step guide on how to move tenant data.

This is applicable for moving from one Pure Access Cloud tenant to another as well as from Pure Access Manager to Pure Access Cloud (and vice versa).

1. Moving users from one tenant to another

1. In the new tenant, re-create your user groups. You can use this as an opportunity to clean up any redundancies and/or create new groups that make sense for your access control needs.
2. In the original tenant, generate a [Users report](#) then save this report as a CSV file. Open this file using Excel.
3. Download the [user import CSV file](#) then open it in Excel.
4. Copy and paste the relevant data from the users report into the template. Please note that **the formatting of the user import file is vital**.
 - a. You will want to carefully review each step of the [user import article](#) to ensure it is done correctly.
 - b. Note that once users have been imported, you *will not* be able to append information to the user profiles using the import feature.
 - c. If a subsequent import is attempted that contains the same users, **it will create duplicate profiles**.
5. Once the template has been filled out, perform the user import into the new tenant.

2. Re-create schedules, access point groups, weekly rules, etc.

1. The rest of the tenant will need to be re-created from scratch.
2. Re-create your schedules.
3. Re-create your access point groups.
 - a. Note that you will want to move the physical access points into the new tenant *after* all of the weekly rules have been re-established.
4. Re-create your weekly rules.
 - a. Remember that you can use this as an opportunity to clean up any redundancies and/or create new rules that make sense for your access control needs.
5. Re-create and re-add any calendar events, holidays, and custom rules.

3. Moving access points

1. Before proceeding, please be aware that once an access point is deleted from a tenant you will **no longer be able to view reports** for that device.
 - a. If you need to view historical events for auditing purposes, you will want to [generate and download the reports](#) now.
2. [Deactivate and then delete](#) an access point from the old tenant.
3. Add this access point to the new tenant.
 - a. It is best practice to delete the access points and then add them to the new tenant one at a time.
 - b. Once added to the new tenant, [update access points](#) and then test a credential.
4. Repeat steps 2 and 3 until all of the access points have been moved over.

5.4. Backup and Restore Process (Pure Access Manager)

Ensure that both Pure Access Manager instances are on [the latest version](#) before proceeding.

Backup Pure Access Manager:

On the Pure Access Manager server, go into the *C:\Program Files\ISONAS\Utils* directory and run the **ISONAS-PAM_Backup** executable as admin. You will see a command prompt window pop up and then disappear shortly after.

Now go into the *C:\Program Files\ISONAS\DB_Backups* directory. You will see a **.dmp** file that has today's date and time. The latest time stamp on the modify date is the back up that was just created.

Restoring Pure Access Manager:

Once you have Pure Access installed on another machine, copy the **.dmp** file you will use to that machine.

Rename the file to **isonas_db.dmp** and place the file in the *C:\Program Files\ISONAS\DB_Restore* directory.

Go into the *C:\Program Files\ISONAS\Utils* directory and run the **ISONAS-PAM_Restore** executable as admin and follow the prompts. After the command prompt window closes, the database should be restored on this Pure Access Manager instance.

5.5. Integrations

1. [Active Directory](#)
2. [Pure Access API](#)
3. [Entrust Datacard TruCredential](#)

5.5.1. Entrust Datacard TruCredential

Please review the following links for more information on the [Entrust Datacard TruCredential](#) integration:

1. [ISONAS + Entrust Datacard Brochure](#)
2. [ISONAS + Entrust Datacard Webinar Presentation](#)
3. [Entrust Datacard Trucredential Software Specifications](#)
4. [How to Integrate ISONAS Pure Access and Entrust Datacard TruCredential](#)
5. [Configuring TruCredential](#)

5.5.2. Milestone XProtect

Please review the following links for more information on the [Milestone XProtect](#) integration:

















1. [ISONAS Pure Access + Milestone XProtect installation instructions](#)
2. Installation files:
 - a. [Pure Access Cloud](#)
 - b. [Pure Access Manager](#)

6. Online Interface

Navigation

Side Menu

The menu on the left side of the screen can be expanded by clicking **»** from the lower left corner of the page.

Collapsed	Expanded
	 Tenant_Name
	 Dashboards
	 Users
	 Access Points
	 Access Control
	 Reports
	 Settings
	 Alerts

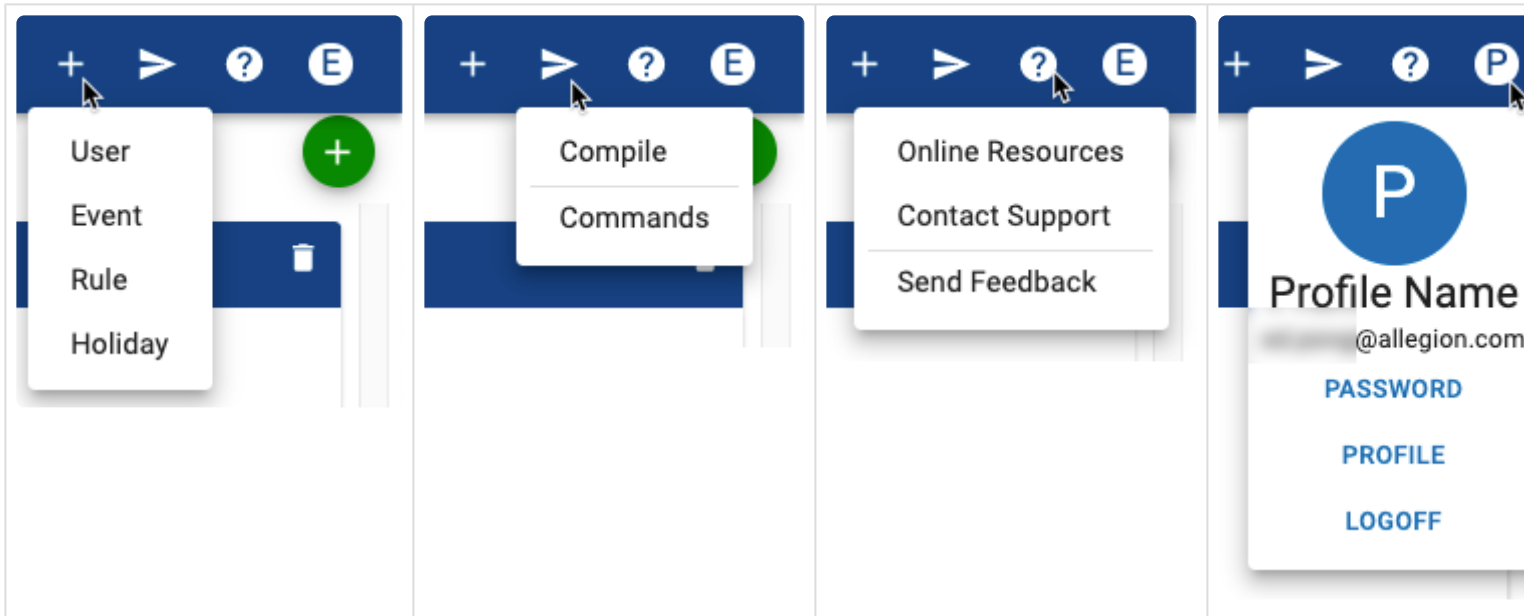
Context Menu

Hover over the green + circle on any page to see a context-sensitive menu.



Quick Links

Quick Add	Commands	Help	Profile
------------------	-----------------	-------------	----------------





6.1. Dashboards

The **dashboard** in Pure Access allows you to monitor your system in real-time, take actions on specific doors or groups of doors, and provides the ability to search and find events quickly.

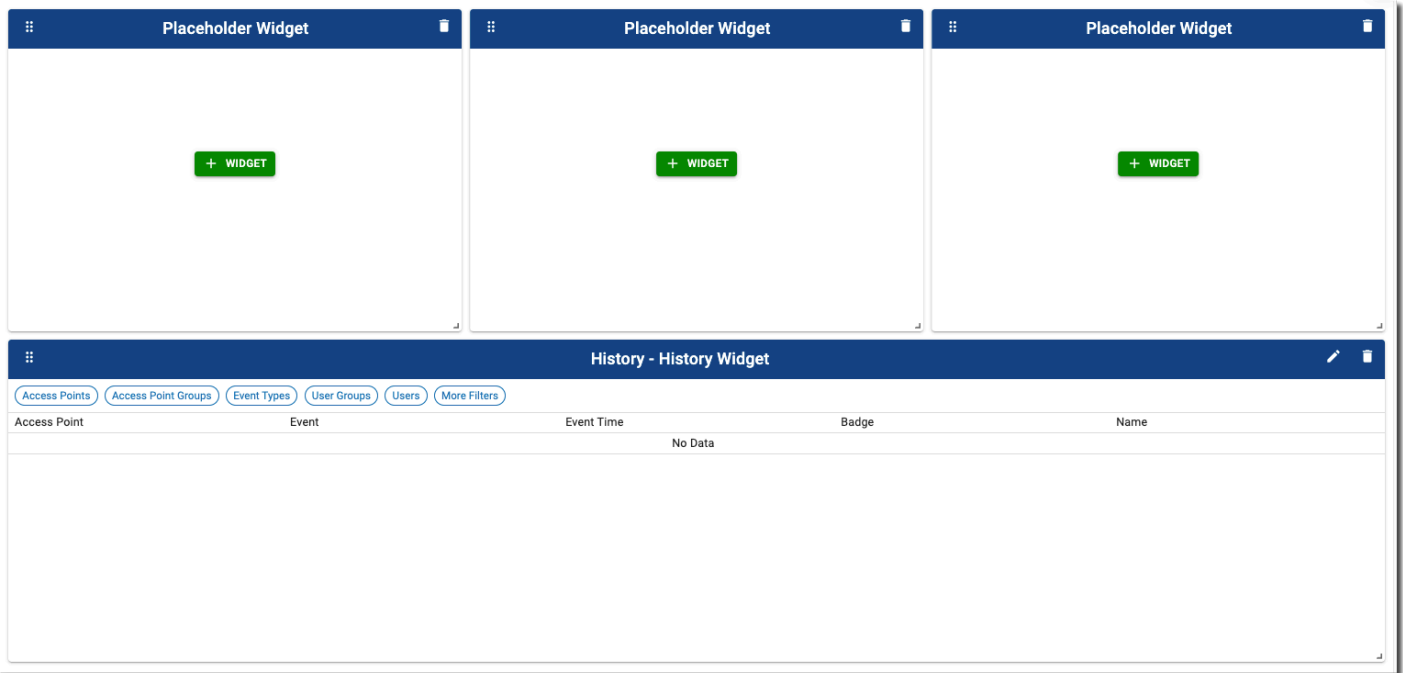
You can create an unlimited number of dashboards for various applications.

6.1.1. Create Dashboard

1. From the main page, hover over  and then choose “**Create Dashboard**”.
2. Enter a name and choose the **Area** (if applicable) and/or **User Group** for whom the dashboard should be visible, then click .
3. When the new dashboard is created, there will be four placeholder [Widgets](#).



6.2. Widgets

Widgets are panels on a dashboard that can be configured to show custom information at a glance. Each dashboard can have a different set of Widgets (up to 12). Three Placeholder Widgets and one History Widget are displayed by default.




You can replace any placeholder widget by clicking . There are six different widget types to choose from:

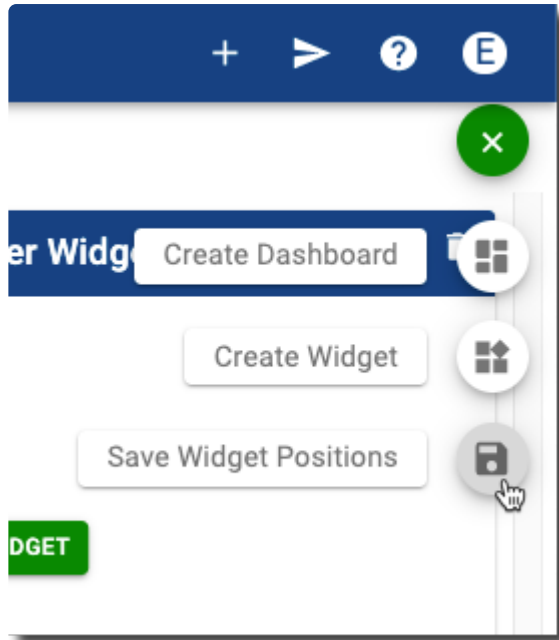
- [Single Access Points](#) allow you to track and monitor real time activity, status as well as take actions on a single door.
- [Multiple Access Points](#) allows you to track and monitor real time status and take actions on multiple doors (up to 12).
- [History](#) provides the ability to see real-time monitoring of access points but provides further abilities to filter to specific people, events or actions.
- [Access Point Admit](#) and [Lockdown Access Points](#) allow you to configure buttons to take immediate actions. The lock down function also allows you to reset a lockdown to its normal state.
- [User Profiles](#) allow you to view a user's image along with the event or activity that happened at a specific door or group of doors.

Widgets can be reconfigured at any time by clicking  and changing the options. The filters can also be changed to show a different subset of information. Click  in any Widget to delete it.

Moving widgets

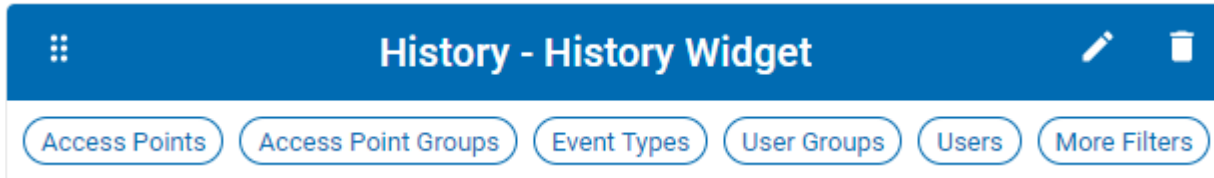
You can move widgets around by clicking and holding the  icon from the upper left corner.

Once moved, you will need to save the positions of the widgets by selecting the **Save Widget Positions** button from the speed dial menu:



6.2.1. History Widget

By default, the bottom widget on every dashboard is reserved for viewing **history** events. You also have the ability to add an additional history widget in one of the top panels if you prefer to monitor specific users, access points, or events.









All history events will be displayed. To filter events, choose options from any of the filter buttons, and then choose **SAVE** for that individual filter. The filters will remain active until changed or cleared.

Adding an additional history widget:

1. Click **+ WIDGET** on one of the three **Placeholder Widget** panels.
 - Alternately, hover over **+** and then choose **Create Widget**.
2. Enter a name for the widget, and then choose **History** from the drop-down menu.
3. Click **CREATE**
4. The new widget will be displayed in the space you chose. Use any of the filter buttons to change exactly what data is displayed. Remember to click **SAVE** in each filter box.

* See [Standard History Events](#) for icon and message definitions.

6.2.1.1. Standard History Events

Icon	Event	Event Description
	Schedule	Device has been set to return to the scheduled weekly rules.
	Approve	User presented a credential that has been accepted.
	Admit	An admit has been sent from a dashboard widget.
	Unlocked	An access point was set to an unlocked state from the dashboard.
	Auto-Unlock	An auto-unlock schedule has started.
	Badge Unlock	An Auto-Unlock w/ Badge rule has started.
	Decline Credential Not Found	Presented credential has not been accepted (ensure the weekly rules have been configured properly)
	Decline Outside Schedule	Presented credential has access to this reader but not at the time the credential was read (too early or too late, see the current rule's schedule).
	Decline Tamper	A credential is declined because there is a tamper alert.
	Device Connect	The device has connected to the software.
	Device Disconnect	The device has lost connection to the software.
	Compile Send	New/Updated information has been sent to all access points.
	Compile Complete	New/Updated information has been sent to all connected access points.
	Compile Failed	Some or all information was not able to reach the reader.
	Credential Sent to Reader	The user is configured for access in the software, but an update had not been pushed/received so the credential has been sent to the reader as a partial compile.
	Locked Down	A lockdown of access points has been activated.
	Lockdown Ended	Reader has been set back to the current schedule and is no longer locked down.
	Decline Lockdown	Credential has been declined because access point is currently locked down.
	REX Admit	There was a REX event on the device, unlocking the door unless set to "REX w/o Unlatch."
	AUX Admit	AUX admit occurred from an input button tied into the device.
	Status Only	Command sent to reader unrelated to active process.
	Reader Error	Hardware error (the Coldfire and Coprocessor firmware may be mismatched). Please contact support if this persists.



	Internal Error	Hardware error. Please contact support if this persists.
	Offline	The virtual device has been deactivated.




The name **System Admin** is a generic system profile that will not appear in the users' list but will appear for certain events. This indicates that an action has occurred which does not have an administrator or cardholder associated with it. Such events include *Device Connect*, *Device Disconnect*, *Auto-Unlock*, *REX Admit*, *Credential Sent to Reader*, etc.

6.2.2. Single Access Point Widget

If one door needs to be monitored or controlled more than others, you can use a **Single Access Point** widget. This will show the history of the door of your choice which can be customized to only display specific events if necessary.

1. Click  on one of the three **Placeholder Widget** panels.
 - Alternately, hover over  and then choose **Create Widget**.
2. Enter a name for the widget, and then choose **Single Access Point** from the drop-down menu.
3. Click **CREATE**
4. The new widget will be displayed in the space you chose. Use any of the filter buttons to change exactly what data is displayed. Remember to click **SAVE** in each filter box.




 See [Standard History Events](#) for icon and message definitions.

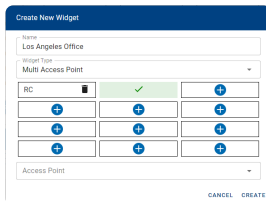
You can also control the Access Point in the widget by using the drop-down box and  button in the lower right corner of the widget. Actions include:


- [Admit](#)
- [Lock Down](#)
- Unlocked
- Lock (Engage devices only)


6.2.3. Multiple Access Point Widget

To manage up to 12 readers at once, you can use a “**Multiple Access Point**” widget. Unlike the **Single Access Point** widget, this will not show history events.

- Click  on one of the three **Placeholder Widget** panels.
 - Alternately, hover over  and then choose **Create Widget**.
- Enter a name for the widget, and then choose **Multiple Access Point** from the drop-down menu.
- The screen will change to show a grid of Access Points. To add an Access Point to one of the boxes, click , and then choose the Access Point from the drop-down box.





- Continue adding other desired Access Points to the grid.
 - If you want to delete an Access Point from the grid, click  next to that Access Point.
 - If you want to edit which Access Point is in a box, click on it and then select the Access Point from the drop-down box.
- When you are done setting up the grid, click **CREATE**.

You can also control any of the Access Points in the widget by clicking on the individual Access Point and then using the drop-down box and  button in the lower right corner of the widget. Actions include:

- [Admit](#)
- [Lock Down](#)
- Lock
- Unlocked
- Clear Tamper

6.2.4. Access Point Admit Widget



This widget is useful when there is one access point that needs to be opened manually from the system. For example, a receptionist can use this to grant access with the single push of a button.

1. Click  on one of the three **Placeholder Widget** panels.
 - Alternately, hover over  and then choose **Create Widget**.
2. Enter a name for the widget, and then choose **Access Point Admit** from the drop-down menu.
3. Choose the Access Point you want to control with this widget.
4. Click **CREATE**
5. The new widget will be displayed in the space you chose. You can send an **Admit** command to the access point at any time by clicking the **Admit** button.
 - The status of the Access Point is displayed at the bottom of this widget.

6.2.5. Lock Down Access Points Widget



This widget is used to set your access points into [Lock Down](#). You can set it up to lock down a *single access point* or an *access point group*. A locked down reader will have a red LED which blinks every few seconds.

! Only a credential set with the [master property](#) can open a door in lockdown.

1. Click  on one of the three **Placeholder Widget** panels.
 - Alternately, hover over  and then choose **Create Widget**.
2. Enter a name for the widget, and then choose **Lock Down Access Point** from the drop-down menu.
3. Choose the Access Point or Access Point Group you want to control with this widget.
4. Click **CREATE**
5. The new widget will be displayed in the space you chose.
 - You can send a **Lock Down** command to the access point(s) at any time by clicking the **Lock Down** button.
 - You can send a **Return to Schedule** command to the access point(s) at any time by clicking the **Return to Schedule** button.

6.2.6. User Profile Widget

This dashboard widget allows you to see a user's image along with real-time activity so you can monitor and match a user with their events.


1. Click  on one of the three **Placeholder Widget** panels.
 - Alternately, hover over  and then choose **Create Widget**.
2. Enter a name for the widget, and then choose **User Profiles** from the drop-down menu.
3. Choose one or more Access Points or Access Point Groups from the drop-down menus.
 - You must choose at least one to create the widget, but you can change these at any time by using the filter buttons along the top of the widget.
4. Click **CREATE**
5. The new widget will be displayed in the space you chose. Use any of the filter buttons to change exactly what data is displayed. Remember to click **SAVE** in each filter box.

7. Send Command

Update Access Points

After changes are made to users, rules, or access points; the updates will need to be sent to the device(s) before any of the changes will be active at the door.




1. Click  from the upper right corner of the page.
2. Select **Compile**.

Sending a compile requires the user to have one (or more) of the following permissions:

- User Details Modify
- User Groups Modify
- Access Points Modify
- Access Point Groups Modify
- Weekly Rules Modify
- Holidays & Events Modify

Other Commands



1. Click  from the upper right corner of the page.
2. Select **Commands**.
3. Select the access point(s) you would like to send a command to, then choose the action:
 - **Admit**: unlocks the access point or access point group for the latch interval set per device
 - **Lock Down**: locks down the access point or access point group
 - **Schedule**: places access point into a normal state (following the configured weekly rules)
 - **Unlocked**: unlocks the access point or access point group)
 - **Clear Tamper**: clears a tamper alarm on an access point

Permissions

Sending command via the app bar requires the user to have one (or more) of the following permissions:

- Access Points Modify
- Access Point Groups Modify
- Weekly Rules Modify
- Holidays & Events Modify

8. Users

1. Click the **Users** tab on the left side navigation.

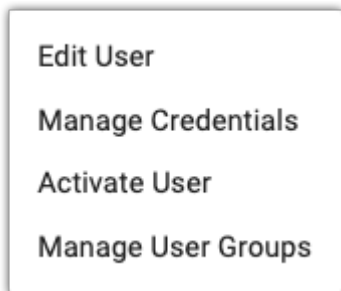


2. All active users in your system will be displayed.

 A screenshot of the 'Users' management page. At the top, there's a search bar and a 'Filter' button. Below that, a table displays 11 results. The table has columns for 'Name', 'Web Access', 'Web Access', 'Group', and 'Last Update'. The first row is highlighted in blue. Below the table, there are several checkboxes and a 'SAVE' button.

Name	Web Access	Web Access	Group	Last Update	Action
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y
Admin User	Y	Y	Admin	01-01-2024 17:00:00	Y

- After selecting one or more check boxes next to user(s), the following buttons will show:
 - **ADD TO GROUP** : Select a group from the drop-down and then click **SAVE**
 - **ACTIVATE** : The user(s) will be activated.
 - **DEACTIVATE** : The user(s) will be deactivated.
- Select **>** to show the **User Group**, **Rules**, **Credentials**, and **Web Access** for a user.
- Select **:** to show the menu for **Edit User**, **Manage Credentials**, **Manage User Groups**, **Manage Web Access**, and **Deactivate User**.

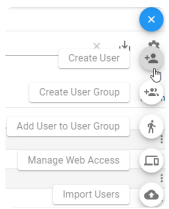


8.1. Create User

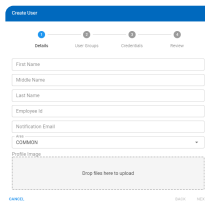
1. Click the **Users** tab on the left side navigation:



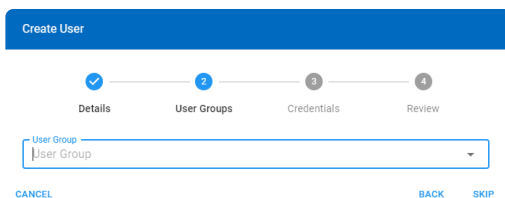
2. Hover over **+** to show the Users menu. Select **Create User**.



3. Fill in the information and select an [area](#) from the drop-down list.
4. To add a profile photo, drag a file to the **Profile Image** area. Then, click **NEXT**.



5. Choose the user group from the drop-down list, and then click **NEXT**. Click **SKIP** to skip this step for now.



6. Fill in the credential information. See [Manage Credentials](#) for details. Click **SKIP** to skip this step for now.

7. Review the information. Use the **BACK** button if you need to go back and change anything. If everything is correct, click **CREATE**.

8.1.1. Importing Users

With the **Import Users** feature, you can use a CSV file to upload users and their credentials into a tenant.


Before continuing, please note that the **formatting** of this file, including proper **capitalization**, is very important.

Any incorrect or extraneous information may have unintended results and/or **cause the import to fail**. If you have any questions or would like your import to be tested, feel free to [contact the help desk](#) for assistance.

Note: *Modifying and/or removing any of the column headers from the template below will cause the import to fail.*

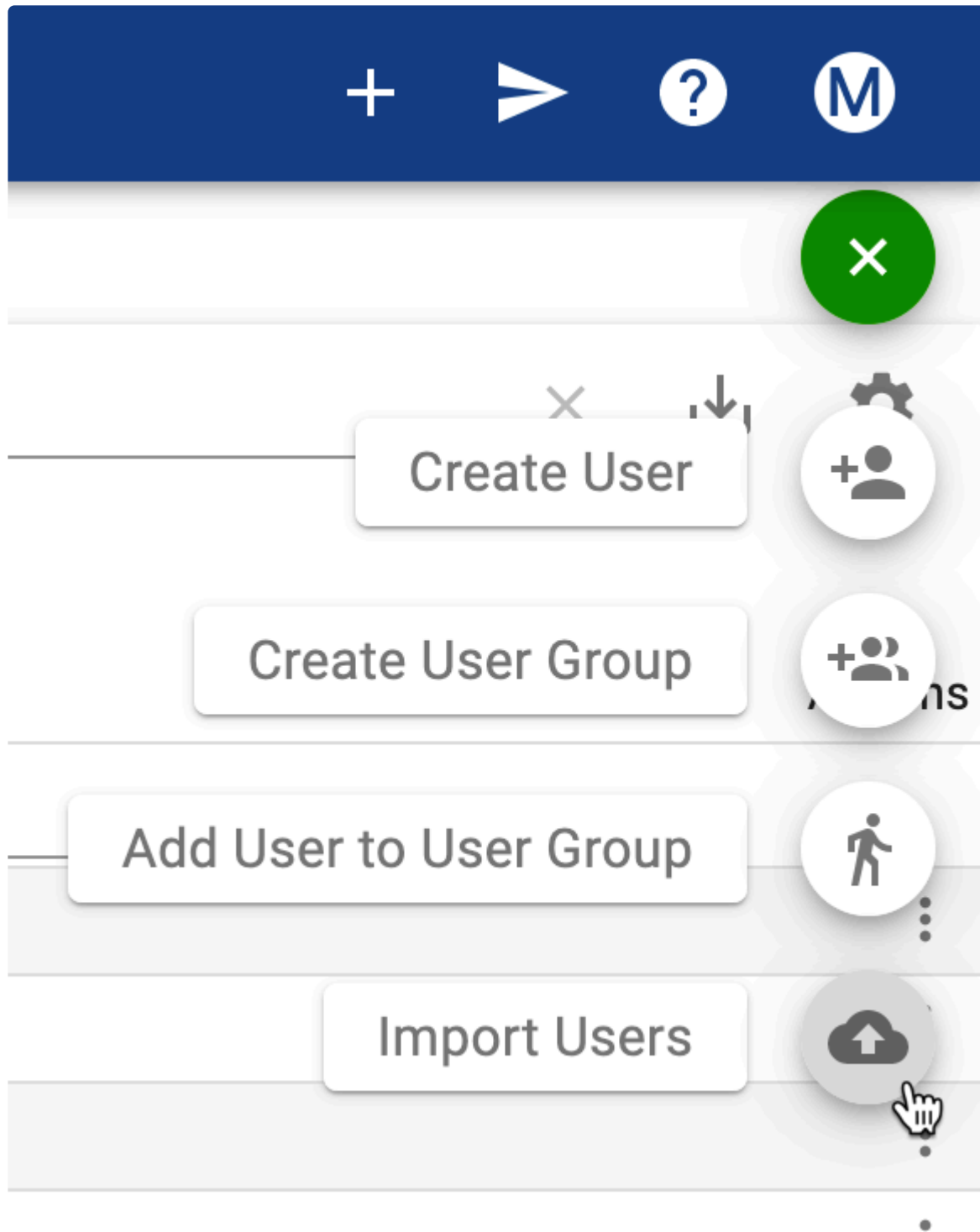
Instructions

Summary: A user import CSV file will need to be downloaded, populated, zipped, then uploaded using Pure Access.

1. There are two different user import template files depending on the Pure Access environment being used:
 - a. For **Pure Access Cloud**, either download this [template CSV file](#) or download it from Pure Access by navigating to **Import Users** from the quick dial  on the Users page.
 - b. For **Pure Access Manager** (on premise), please use [this template](#) and see the note at the bottom of this page.
2. Input the users' information. The required fields are: **LastName**, **FirstName**, **BadgeID**, and **CredentialType**.
 - a. The **BadgeID** column should contain either the hot-stamped number printed on the user's [badge](#), a [keypad code](#), or a [mobile/bluetooth DeviceID number](#).
 - If you intend on adding a user profile *without* a credential, you *must* have a "0" in this column or the *import will fail*.
 - To import multiple credentials for a single user, they will need more than one row in the CSV (one row for each credential they have, see Alyx Vance in the example at the bottom of this page for reference). The same required fields apply to each subsequent row that is added.
 - Note that if the user's first or last name does not match the original row's data, it will create a new user profile and *will not* simply append the additional credential(s).
 - b. **CredentialType** will need to be either a "1" (if the credential is a *badge*), "2" (if it's a

keypad), or “3” (for *mobile/bluetooth* credentials).

- c. To add users to user groups, populate the **UserGroups** column using the following formatting and notes:
 - i. Ensure that the user group(s) **already exist** in Pure Access. The user import **will not** create new groups.
 - ii. Ensure that the capitalization and punctuation of the group(s) are correct in the import. The *All Users* group in Pure Access must be *All Users* in the import.
 - iii. To add a user to multiple groups, you will need to separate the names of the groups with a semi-colon (;) *without* spaces. For example, to add a user to *All Users* and to *Managers*, the field would look like this: **All Users;Managers**
 - Note: If the **UserGroups** field is not populated, the user(s) will not be assigned to a group.
 - Note 2: **This is for Pure Access 3.1+ only.**
3. If areas are being used in this tenant, please review the following formatting and notes:
 - a. Ensure that the area(s) **already exist** in Pure Access. The user import **will not** create new areas.
 - b. Populate the **AreaName** column.
 - c. Ensure that the capitalization and punctuation match the area in Pure Access.
 - d. Note: To reiterate, the import **will not** create new areas. If an **AreaName** field is populated with an area that does not exist in Pure Access, the user will be placed into *COMMON*.
4. You can ignore the columns titled **CountLimitFlag**, **RemainingUses**, and **ExpirationDate** as they are not necessary for the import to be successful. These fields must remain in the import, however.
 - a. If you wish to set an **ExpirationDate** on one or more credentials, you can do so using the format: *yyyyMMdd*
 - b. **Example**: April 1st, 2020 would be *20200401*
5. Once completed, the CSV file will need to be [zipped](#).
6. Click the **Import Users** button from the **Users** page.



7. Drag the zipped .csv file (.zip file) into the upload area. Then click **save**.

Import Users

☁
DOWNLOAD USER IMPORT
TEMPLATE

?

Import Users Zip

userimport.zi...

CANCEL

SAVE

✿ If the import fails, please ensure that no changes have been made to row 1 of the CSV. Pure Access is looking for specific data so these fields must remain **exactly** as they are found in the template.

Example:

	A	B	C	D	E	F	G	H	I	J
1	LastName	FirstName	MiddleName	AreaName	BadgeId	CredentialType	CountLimitFlag	RemainingUses	ExpirationDate	UserGroups
2	Sanchez	Quico		COMMON	0					
3	Brooks	Senalda		COMMON	0					
4	Cox	Tucker		COMMON	0					
5	Martin	Keeley		COMMON	0					
6	Butler	Kallen		COMMON	0					
7	Hughes	Holden		COMMON	0					
8	Edwards	Callan		COMMON	0					
9	Richardson	Keahi		COMMON	0					
10	Reed	Dianne		COMMON	0					
11	Adams	Eryn		COMMON	0					

How the above import would look once in Pure Access:

<input type="checkbox"/> Name	Web Access	User Active	Engage User	Last Update	Actions
Filter...	Filter...	Filter...	Filter...	Filter...	
> <input type="checkbox"/> Adams, Eryn	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Brooks, Senaida	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Butler, Kallen	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Cox, Tucker	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Edwards, Callan	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Hughes, Holden	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Martin, Keeley	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Reed, Dianne	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Richardson, Keah	N	Y	N	01-19 12:38:52	
> <input type="checkbox"/> Sanchez, Quico	N	Y	N	01-19 12:38:52	



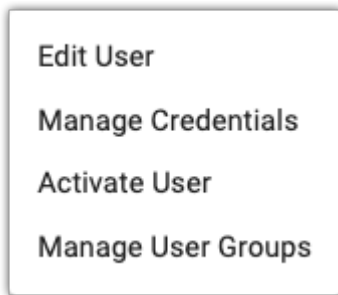
For Pure Access Manager 2.12.2 and lower, **CountLimitFlag** will be **CountLimit** (as provided in the template). The ability to add users to groups via user import was added into Pure Access in version 3.1 and is not available in any version of PAM.

8.2. Edit User

1. Click the **Users** tab on the left side navigation.



2. Select  next to the User you want to edit and then choose **Edit User**.



3. Edit the profile as necessary.
4. Drag an image file to the **Profile Image** area to add a photo.
5. Click **SAVE**.

8.3. Find a User

1. Click the **Users** tab on the left side navigation:



2. Type all or part of the user's name, credential number, email address (if applicable), etc. in the search field from the upper right corner of the screen.

A search input field with a magnifying glass icon, the text "Search", a close button (X), a download icon, and a settings gear icon.

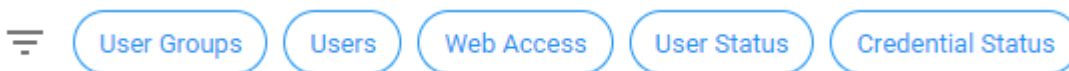
3. The results will be displayed in the Users list.

8.4. Filter Users

1. Click the **Users** tab on the left side navigation:

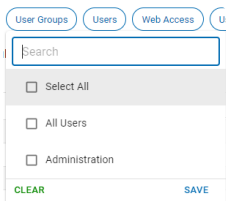


2. Select the filter icon and then select any buttons to filter which users are shown.

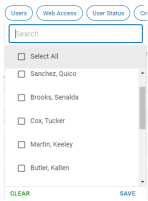


3. Select any of the check boxes and then click **SAVE** to change which users are shown. Click **CLEAR** to remove the filters for that category.

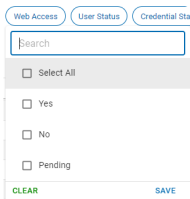
- User Groups



- Users



- Web Access



- User Status

User Status Credential Status

Search

Select All

Active

Deactivated

CLEAR **SAVE**

- [Credential Status](#)

Credential Status

Search

Select All

Enabled

Disabled

CLEAR **SAVE**

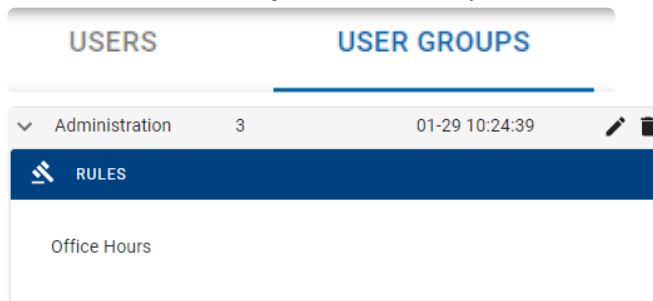
8.5. User Groups




User groups are used to organize users into groups of people who all have the same access rights. Organizing users into groups allows you to manage many users with a single group rather than managing many individual users separately.

1. Click the **Users** tab on the left side navigation:



2. Click the **User Groups** tab at the top of the users list.




- a. Click  next to a user group to display the rules applied to that group.
- b. Click  to change which users are included in the group.
 - When a user is added to a group, they are granted all access associated with that group.
- c. Click  to delete the group.
 - When a group is deleted, all users associated with that group will lose all the access that was associated with that group.

8.5.1. Create User Group

1. Click the **Users** tab on the left side navigation:



2. Hover over the speed dial  icon then select **Create User Group**.
3. Enter the information for the group:
 - Name: meaningful name for the group
 - [Area](#): appropriate area for the group (if applicable)
 - Description: further details about the group
 - [User](#): Choose which users should be included in the group.
 - You can leave this blank for now and then add Users later.
4. Click **CREATE**.

8.5.2. Manage User Groups


User groups should only consist of people who should all have the same access rights. Organizing users into groups allows you to manage many users with a single group vs. managing many individual users separately.

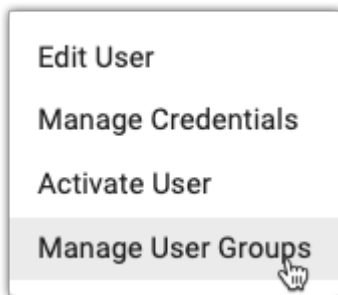
There are several ways to change which user groups a user is included in:

Add a user(s) to a group from the Users page

1. Click the **Users** tab on the left side navigation:



2. Navigate to the **Users** tab.
3. Select  next to the user you want to edit and choose **Manage User Groups**.



4. The user groups the user is enrolled in will be displayed.

User Group	Weekly Rules
Standard Users	
All Users	
All Contractors	
Administrators	All Doors - 24/7 Weekend Access

5. To change which user groups the user is enrolled in, select the **User Group** drop down and select/deselect user groups.


User Group	Weekly Rules
Standard Users	
All Users	
All Contractors	
Administrators	All Doors - 24/7 Weekend Access

6. Click **SAVE**

Add a user(s) to a group from the User Groups page

1. Click the **Users** tab on the left side navigation:



2. Navigate to the **User Groups** tab.
3. Select the pencil icon () under **Actions** to open the **Edit** dialog.

Edit User Group

Name

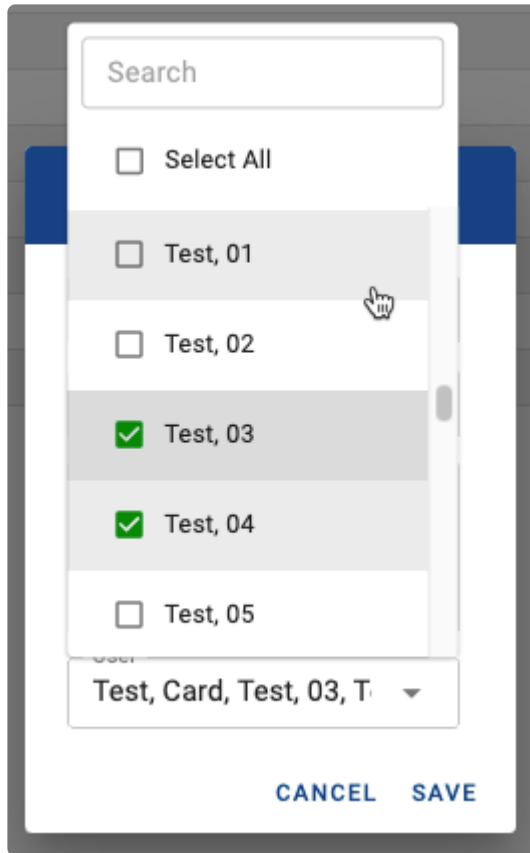
Area

Description

User

CANCEL **SAVE**

4. Select/Deselect user(s) from the drop-down list.



5. Click **SAVE**

Viewing user group details

To review the weekly rules to which a user group is assigned, select the arrow to the left of the group's name to expand additional details:

ISONAS PUREACCESS Tenants ▾

USERS **USER GROUPS**

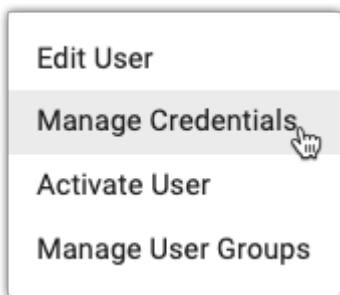
Name	Member Count	Last Update
Filter...	Filter...	Filter...
> Active Contractors	15	09-13 10:24:32
> Administrators	17	02-26 13:26:20
RULES		
All Doors - 24/7 Weekend Access		
> All Contractors	43	09-13 10:33:32
> All Users	47	09-01 08:45:18
> IT	19	02-26 15:39:14
> Pharmacists	0	09-01 08:45:47
> Standard Users	41	05-31 15:01:28
> Terminated	12	02-19 09:45:22
> Two Factor Users	24	03-01 16:02:45

8.6. Manage Credentials

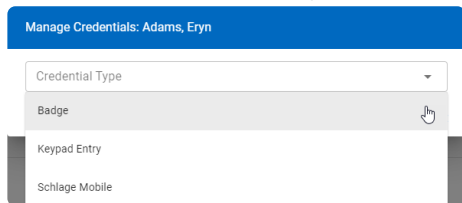
1. Click the **Users** tab on the left side navigation:



2. Click  next to the user to which you want to add a credential. Then choose **Manage Credentials**.



3. Choose the credential type from the drop down box.



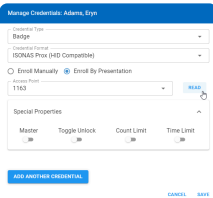
4. Click on one of the credential types in the table for more information.

Credential Types						
Type	Format	Facility Code	Issue Level	Hot Stamp	Badge ID	Special Properties
Badge	26A, 37X, 33D, 48X, 28G, 40X, 37P, 34N, 36L, 37B, 36M, 36B	X			X	Master, Toggle, Unlock, Count Limit, Time Limit

	37H				X
	ISONAS Prox (HID Compatible)	X		X	
	28H, Isonas EV2, 32X				X
	32K	X	X		X
Keypad Entry	PIN	n/a			
Mobile	Mobile Phone Number				

8.6.1. Badge

1. If the [bitmask is set correctly](#), you can manually enter the badge ID from the card into the **Badge ID** field.
2. Alternatively, you can enroll by presenting the card/fob to a reader. After swiping the badge at a connected reader, simply select the access point you want to read the data from. See the [Enrolling by Presentation](#) section for further instructions.



Manage Credentials Admin, Enroll

Enroll Type

Badge

Credential

ISONAS Prox (400 Compatible)

Enroll Method

Enroll Manually Enroll By Presentation

Badge ID

1163

Special Properties

Master	Toggle Lock	Count Limit	Time Limit
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[ADD ANOTHER CREDENTIAL](#) [CANCEL](#) [NEXT](#)



Please note that if you are using an ISONAS credential, you will **not** need to set the bitmask for your cards. If you are not using an ISONAS credential, you **will** need to set the bitmask.

8.6.2. Keypad Entry

If you have a keypad device and would like to assign an entry code to a user, you will need to select **Keypad Entry** from the **Credential Type** drop-down:

See [Manage Credentials](#).

From here you can add a keypad entry of your choice or have the system assign a random code for you by selecting the “**Generate Random Pin**” button.

* To unlock a door, you will need to input star (*) followed by the assigned keypad code then pound (#).

8.6.3. ISONAS Mobile

If you have a keypad device and would like to assign an entry code to a user, you will need to change the credential type from **Badge** to **Schlage Mobile** or **Mobile**. See [Manage Credentials](#).

Enrolling by Presentation

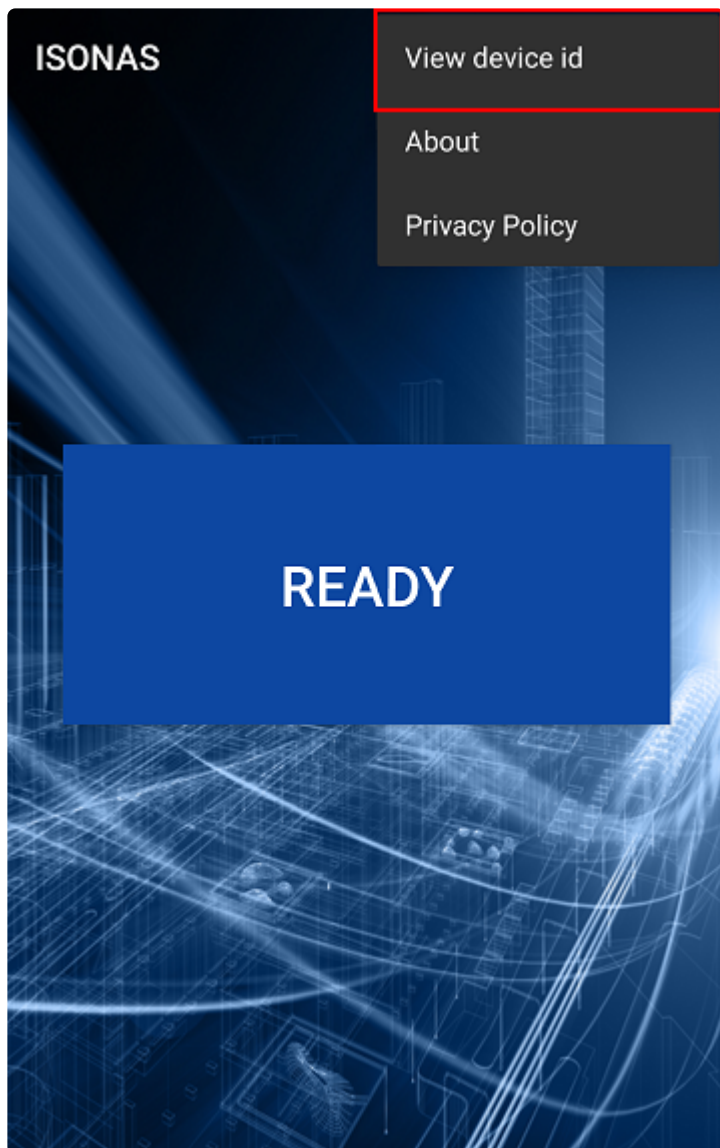
1. Touch “**TAP TO SEND**” in the **ISONAS Pure Mobile** application.
2. On the credential screen in Pure Access, click **READ**.
3. Click **SAVE**.

Enrolling Manually (ISONAS Pure Mobile App)

1. Click on the three dots in the upper right corner of the **ISONAS Pure Mobile** application (available for [iOS](#) and [Android](#)).



2. Click "**View device id.**"



3. Input this ID into the “**Device ID**” field on the add credential page in Pure Access.
4. Click **SAVE**.

! Please note that if the **ISONAS Pure Mobile** application is uninstalled then reinstalled on iOS, the Device ID will be renewed thus the credential will need to be re-enrolled. On Android the ID is linked to your Google account thus will stay the same.

8.6.3.1. Using the Mobile Credential to Unlock a Door

ISONAS Pure Mobile App

1. When a user approaches an ISONAS hardware device, they *must have* **Bluetooth® Low Energy (BLE)** as well as **location services** turned on in order for the phone to communicate with the ISONAS hardware.
2. Open the **ISONAS Pure Mobile** app on your mobile device.
3. When in range, touch the **TAP TO SEND** button.
Note: The mobile app will show that the reader is in range when they are in close proximity, then it will show “Connecting” as the reader and phone try to connect. At this time the LED on the reader should turn amber (yellow).
4. The mobile app will show that the credential has been sent. If the user has been granted access, the LED will turn green and the door will unlock. If they do not have access, the LED will turn red.


Schlage Mobile App

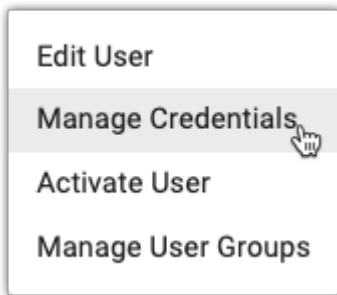
1. When a user approaches a Schlage hardware device, they *must have* **Bluetooth® Low Energy (BLE)** as well as **location services** turned on in order for the phone to communicate with the hardware.
2. Open the **Schlage Mobile** app on the mobile device.
3. When in range, touch **Tap to Unlock**.

8.6.4. Enrolling by Presentation

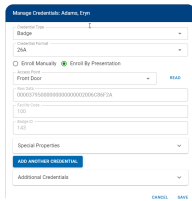
1. Click the **Users** tab on the left side navigation:




2. Click  next to the user to which you want to add a credential. Then choose **Manage Credentials**.



3. In the **Manage Credentials** window, choose **Badge** from the drop-down box.



4. Choose the **Credential Format** from the drop-down box.
5. Choose the **Enroll by Presentation** radio button.
6. Choose the access point to which you presented the credential from the drop-down box.
7. Click **READ**.
 - a. The raw data and badge ID of *the most recently declined card** will populate:
8. Click the **SAVE** button at the bottom right corner of the pop-up window.
9. You will now see this credential listed under the "**Credentials**" portion of the user profile page.

 The declined credential will clear after 15 minutes.*

8.6.5. Special Credential Properties

There are four types of special properties that can set for a credential:

1. **Master**: The ability to unlock a an access point that is in Lockdown.
2. **Toggle**: The ability to unlock/lock access points with which the user has Grant Access permissions to.
3. **Count Limit**: used to limit how many times a credential may be used.
4. **Time Limit**: used to limit the time during which a credential will be active.

8.6.5.1. Master Credential

The **master property** can be assigned to a badge, keypad code, or mobile credential and allows this credential to do the following:


- Bypass a locked down access point
- Bypass a two-factor rule
- Bypasses all schedules and holidays within a rule (essentially follows a 24/7 “Always” schedule).

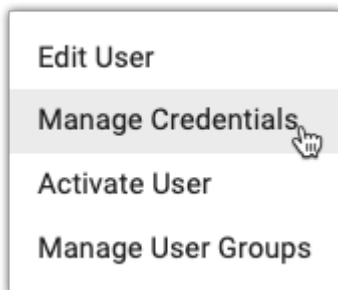
! Note that a master credential *does not* provide grant access permissions to all access points in a tenant. The user profile with a master credential must have **Grant Access** permission for the access point(s) they’re attempting to access otherwise they will be declined.


Adding Master Credential Special Property




1. Click the **Users** tab on the left side navigation:





2. Click  next to the user to which you want to add a master credential. Then choose **Manage Credentials**.



3. Click  next to the credential you want to make the master.

1 results		
Credential	Active	Actions
 1235		

4. Click  next to Special Properties. Then select the slider for **Master Credential** to enable the master property.

Special Properties 

Master Toggle Unlock Count Limit Time Limit

5. Click **SAVE**.

8.6.5.2. Toggle Credential

The **toggle property** allows a credential to “toggle” a door between an unlocked and locked state resembling a physical lock and key.


It *cannot*, however, be used to override an **Auto-Unlock** nor **Auto-Unlock w/ Badge** rule. Toggle lock can *only* reset a toggle unlock.

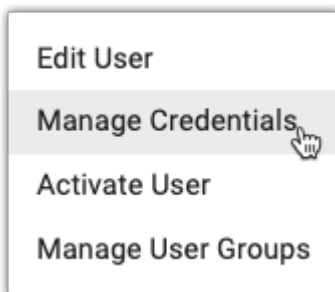
! ***Please note this is a function that requires the ISONAS hardware to be online and **will not** toggle the state of the device if it is not actively communicating with Pure Access.*


Adding Toggle Credential Special Property




1. Click the **Users** tab on the left side navigation:




2. Click  next to the user to which you want to add a master credential. Then choose **Manage Credentials**.



3. Click  next to the credential you want to make the master.

1 results		
Credential	Active	Actions
 1235		

- Click  next to Special Properties. Then select the slider for **Toggle Credential** to enable the master property.

Special Properties ^



Master
 Toggle Unlock
 Count Limit
 Time Limit

Toggle Access Point(s)

All Access Points
 Access Point Group
 Access Point

Access Point:

- Choose which access point(s) or access point group(s) the toggle credential should work with.
- Click **SAVE**.

 Credentials that are set with the toggle feature will show a padlock icon () next to them. *Note: If you select an access point group in Step 5, each door in the group will need to be toggled individually. You cannot use a toggle credential to unlock an entire group of access points with one swipe.*

Re-Lock Time

- In order to ensure your doors are not left in a toggle unlock state accidentally, set a **Re-lock** time.
- Click the **Settings** tab on the left side navigation.



- Click on the **Global Settings** tab.


GLOBAL SETTINGS

4. Enter the desired re-lock time into the **Re-lock Time** box. If the door is in an unlocked state at this time, the door will re-lock automatically.

Global Settings

Default PIN Length	4
Re-lock Time	23:59 
Timezone	(UTC-07:00) Mountain Time (US & Canada) ▼

- By default this is set to **23:59**

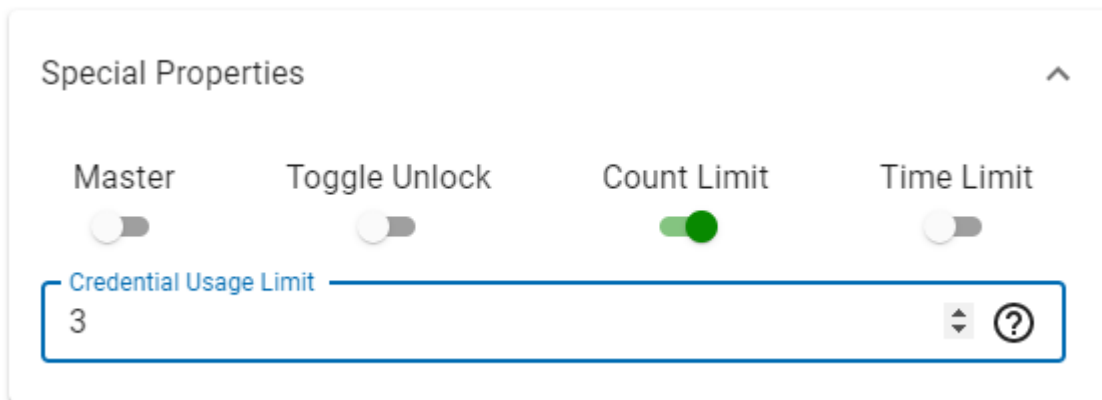
5. Click  and then enter your password.

- Any time you change global settings, your password is required.

8.6.5.3. Count Limit

Count Limit is used to limit how many times a credential may be used. After the credential is preset for the set number of times, it will become inactive.

1. Select the **Count Limit** slider.
2. Enter the appropriate number in the **Credential Usage Limit** box.
3. Click **SAVE**.







The screenshot shows a configuration panel titled "Special Properties" with an upward-pointing arrow in the top right corner. Below the title are four toggle switches: "Master" (off), "Toggle Unlock" (off), "Count Limit" (on, highlighted in green), and "Time Limit" (off). Below the "Count Limit" toggle is a text input field labeled "Credential Usage Limit" containing the number "3". The input field has a blue border and includes a dropdown arrow and a help icon (question mark) on the right side.

8.6.5.4. Time Limit

Time Limit is used to limit the time during which a credential will be active.

1. Select the **Time Limit** slider.
2. Choose the **Start Date**, **Start Time**, **End Date**, and **End Time**.
3. Click **SAVE**.

Special Properties ^

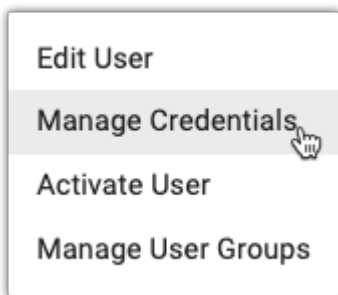
Master	Toggle Unlock	Count Limit	Time Limit
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Start Date 2021-01-29 		Start Time 08:00 	
End Date 2021-01-29 		End Time 05:00 	

8.6.6. Deactivating Credentials

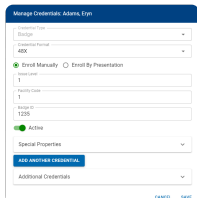
1. Click the **Users** tab on the left side navigation:




2. Click  next to the user to which you want to add a credential. Then choose **Manage Credentials**.



3. Click  next to the credential you want to deactivate. Then select the **Active** slider to turn it off.



4. Click **SAVE**

 Once deactivated, a credential can then be re-used on another user's profile.

8.7. Manage Web Access

In order to log into a [Pure Access Cloud](#) tenant, your user profile will need to be configured for **web access** and must have a user role *greater than* the default “**Cardholder**.”


If either of these criteria are not met but your user profile *should* be able to log in, an **Integrator** or **Administrator** of the tenant will need to ensure your user role is properly set and will need to send an invitation for web access to a valid email address (if this has not been done or the invitation has expired).

8.7.1. Setting up Web Access for a User

Web access rights allow a user to log into and manage a tenant.

1. Click the **Users** tab on the left side navigation.



2. Select  next to the User you want to configure and then choose **Manage Web Access**.
3. Select the **Web Access** slider.
4. Enter the email address the user will use for web access management.
5. Choose one of the four preset roles from the [User Role](#) drop-down menu, or choose **Custom**.
6. To view the specific permissions granted, click on the **User Permissions** drop-down. You can turn on or off specific permissions here. You may notice that the [User Role](#) in the above box changes based on what you choose.
7. Click **NEXT**.
8. From the drop-down boxes next to each area, select the type of Access the User should have.
9. Click **SEND INVITE**.
10. The User will receive an email inviting them to Web Access. You will notice a **P** in the **Web Access** column next to the User's name.
11. Once the User accepts the invitation, a **Y** will be displayed in the **Web Access** column.

8.7.2. User Roles

What do the pre-defined roles provide access to?

- **Administrator:** Provides access to view and modify all aspects of the system.
- **Operator:** Provides access to view only alerts, users, schedules, holidays/events, and dashboards.
- **Human Resources:** Provides access to view system settings and to modify users, schedules, holidays/events, and access points.
- **Custom:** Allows specific permissions to be added or removed.

You can view which permissions, specifically, by choosing a role from the drop-down menu, then by clicking the **User Permissions** drop-down box and scrolling through the list:

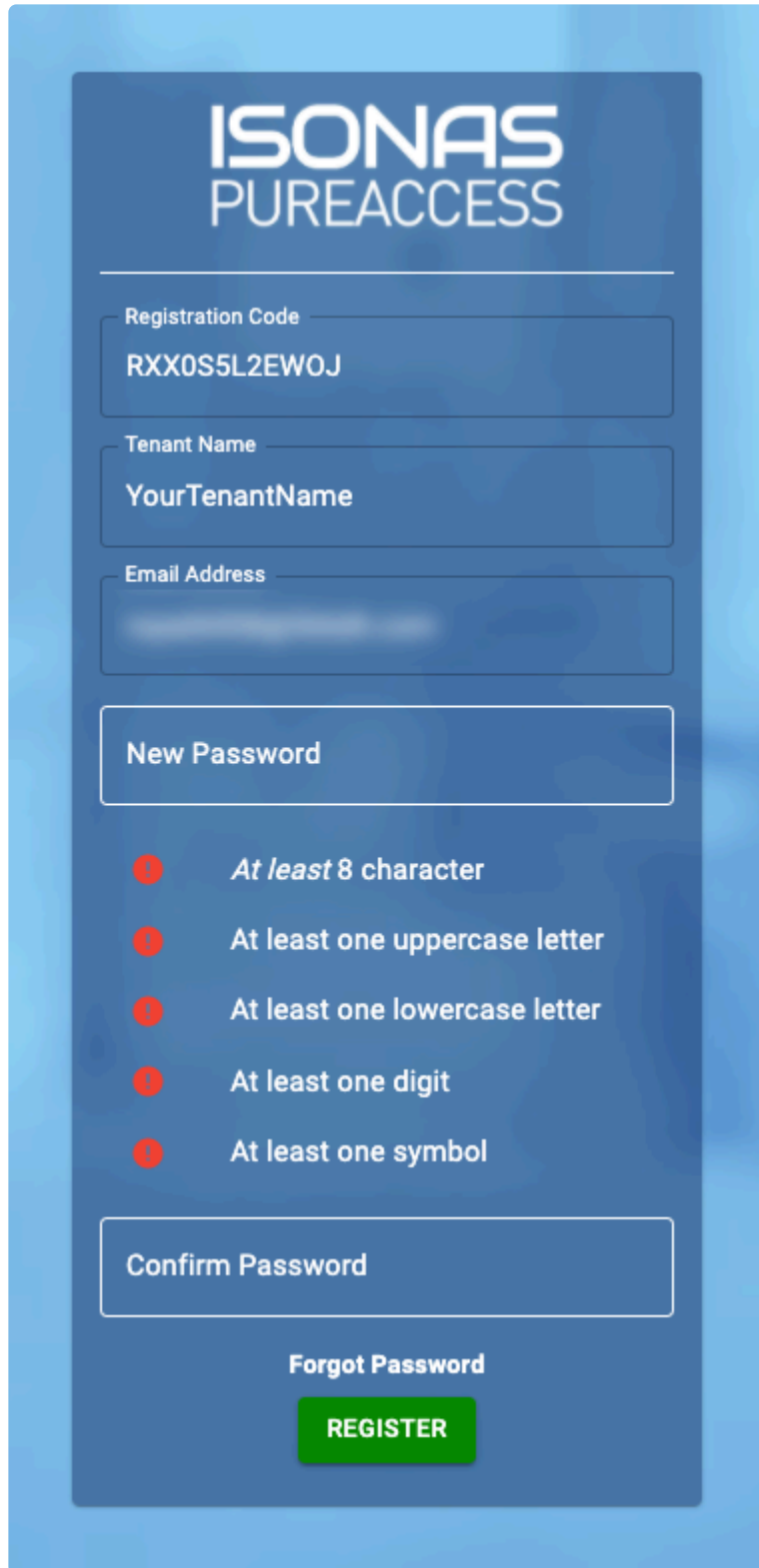
- Tenant Integrator
- Tenant Settings
- Areas
- Active Directory
- Credentials Settings
- Alerts
- Alert Settings
- Users
- User Details
- User Groups
- Access Points
- Access Point Groups
- Weekly Rules
- Holidays & Events
- Dashboard
- Custom Rules
- API Tokens
- Reports
- Scheduled Reports

* For RMR licenses only, there is an additional role called **Integrator**. Users with this role are able to view/modify *all areas* and all sub-tenants created under the primary tenant.

8.7.3. Accepting the Web Access Invitation

Once an invitation email has been sent, you will need to accept it to confirm your identity and create your password.

If you do not already have web access configured for a tenant in Pure Access, it will ask that you create a new password:



The image shows a registration form for ISONAS PUREACCESS. The form is set against a dark blue background with a lighter blue border. At the top, the logo 'ISONAS PUREACCESS' is displayed in white. Below the logo, there are several input fields: 'Registration Code' with the value 'RXX0S5L2EWOJ', 'Tenant Name' with the value 'YourTenantName', and 'Email Address' which is blurred. Below these is a 'New Password' field, followed by a list of five password requirements, each preceded by a red circle with a white exclamation mark. The requirements are: 'At least 8 character', 'At least one uppercase letter', 'At least one lowercase letter', 'At least one digit', and 'At least one symbol'. Below the requirements is a 'Confirm Password' field. At the bottom of the form, there is a link for 'Forgot Password' and a green 'REGISTER' button.

ISONAS
PUREACCESS

Registration Code
RXX0S5L2EWOJ

Tenant Name
YourTenantName

Email Address

New Password

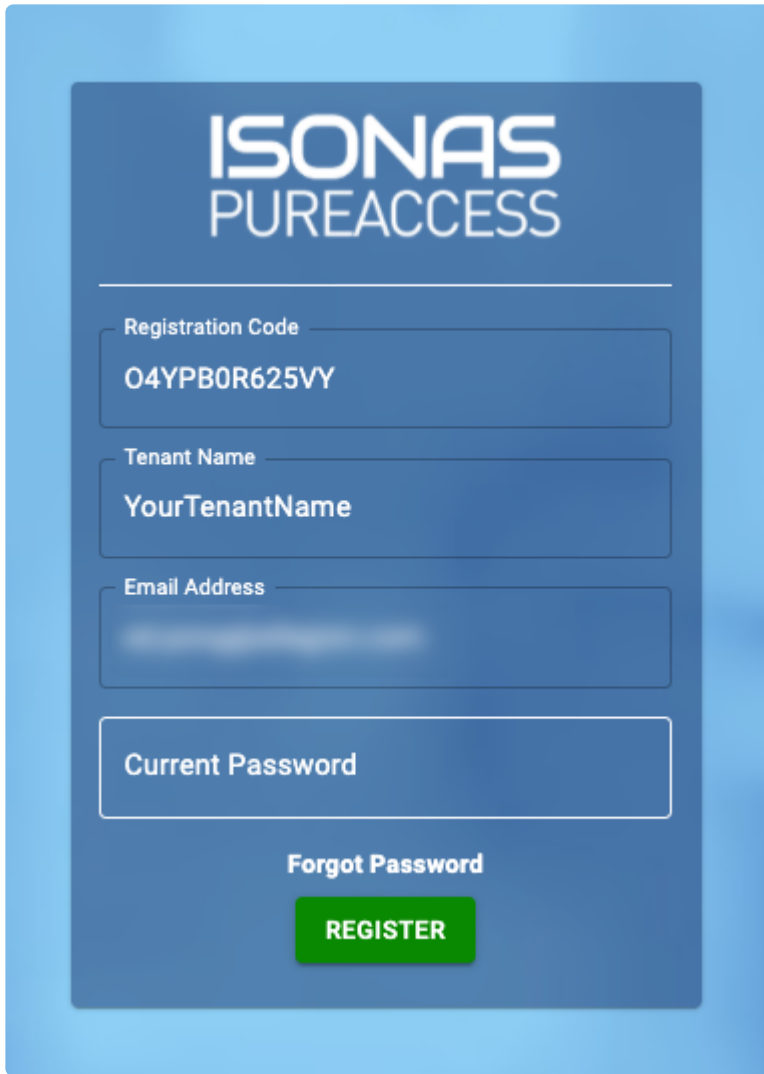
- At least 8 character
- At least one uppercase letter
- At least one lowercase letter
- At least one digit
- At least one symbol

Confirm Password

[Forgot Password](#)

REGISTER

If you already have web access to another tenant, it will ask that you simply confirm your existing password:



The image shows a registration form for Isonas PureAccess. The form is set against a dark blue background with a lighter blue border. At the top, the text 'ISONAS PUREACCESS' is displayed in white. Below this, there are four input fields: 'Registration Code' with the value 'O4YPB0R625VY', 'Tenant Name' with the value 'YourTenantName', 'Email Address' (blurred), and 'Current Password'. A link for 'Forgot Password' is located below the password field. At the bottom, there is a green 'REGISTER' button.

Don't know your password? You can reset it from the [Pure Access Cloud login page](#) or by [clicking here](#).


Invitation not working?

If you accept the web access invitation and it there is no space for you to enter your information, you are likely using Internet Explorer or another unsupported browser. Please retry using **Chrome** or **Firefox** instead.

8.7.4. Removing Web Access Privileges

1. Click the **Users** tab on the left side navigation.



2. Select  next to the User from which you want to remove web access and click **Manage Web Access**.
3. Select the slider next to **Web Access** so that it is no longer green.
4. Click **NEXT**, and then **SAVE**

Alternative

If you simply [deactivate a user's profile](#), they will no longer be able to log into the tenant.

! **For integrators with an RMR license:** Please note that removing web access from a user's profile in the parent tenant *will not* affect their web access in subtenants. For this reason, the user's web access will need to be removed from each subtenant individually.

8.8. Deactivate User

If you have a person from whom you need to remove all access rights, you can simply deactivate their user profile. This will automatically disable all credentials assigned to this user.

 *Due to the way in which reporting is structured in Pure Access, you cannot delete a user profile. This allows us to maintain data integrity within the Pure Access database.*

Deactivating multiple users:

1. Click the **Users** tab on the left side navigation:



2. All active users in your system will be displayed. Select one or more users who you wish to deactivate.

Name	Role	Status	Last Login	Actions
John Doe	Admin	Active	2023-10-27 10:15	[Deactivate] [Edit] [Delete]
Jane Smith	User	Active	2023-10-27 09:30	[Deactivate] [Edit] [Delete]
Mike Johnson	Admin	Active	2023-10-27 11:00	[Deactivate] [Edit] [Delete]
Sarah Lee	User	Active	2023-10-27 08:45	[Deactivate] [Edit] [Delete]
David Kim	Admin	Active	2023-10-27 10:30	[Deactivate] [Edit] [Delete]
Emily White	User	Active	2023-10-27 09:15	[Deactivate] [Edit] [Delete]
Chris Brown	Admin	Active	2023-10-27 11:15	[Deactivate] [Edit] [Delete]
Alex Green	User	Active	2023-10-27 08:00	[Deactivate] [Edit] [Delete]
Mia Black	Admin	Active	2023-10-27 10:45	[Deactivate] [Edit] [Delete]
Noah Grey	User	Active	2023-10-27 09:00	[Deactivate] [Edit] [Delete]


3. Click on **Deactivate**:

DEACTIVATE

Deactivating one user:

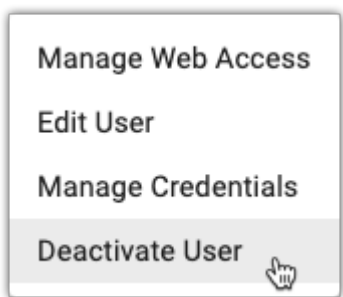
1. Click the **Users** tab on the left side navigation:



2. All active users in your system will be displayed. Click  next to the user you want to deactivate.

Name	Web Access	Web Admin	Manage User	Action
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮
Admin User	Y	Y	Y	⋮

3. Click on **Deactivate User**:



! Deactivating a user profile with web access privileges will prevent the user from logging into the tenant, but their email address will still be associated with this profile.

8.8.1. Viewing Deactivated Users

See [Filter Users](#).

8.8.2. Activating a User Profile

If a User was previously deactivated, you can easily reactivate the profile.

Due to the way in which reporting is structured in Pure Access, you cannot delete a user profile. This allows us to maintain data integrity within the Pure Access database.

Activating multiple users:

1. Click the **Users** tab on the left side navigation:



2. All active users in your system will be displayed. Select one or more users who you wish to activate.


Name	Role	Status	Last Update	Action
Admin User	Admin	Active	01-01-2024	
John Doe	User	Inactive	01-01-2024	
Jane Smith	User	Active	01-01-2024	
Bob Johnson	User	Inactive	01-01-2024	
Alice Brown	User	Active	01-01-2024	
Michael Davis	User	Inactive	01-01-2024	
Emily White	User	Active	01-01-2024	
David Green	User	Inactive	01-01-2024	
Sarah Black	User	Active	01-01-2024	
Christopher Lee	User	Inactive	01-01-2024	

3. Click on **ACTIVATE**.

Activating one user:

1. Click the **Users** tab on the left side navigation:



2. All active users in your system will be displayed. Click  next to the user you want to activate.
3. Click on **Activate User**.

9. Access Points

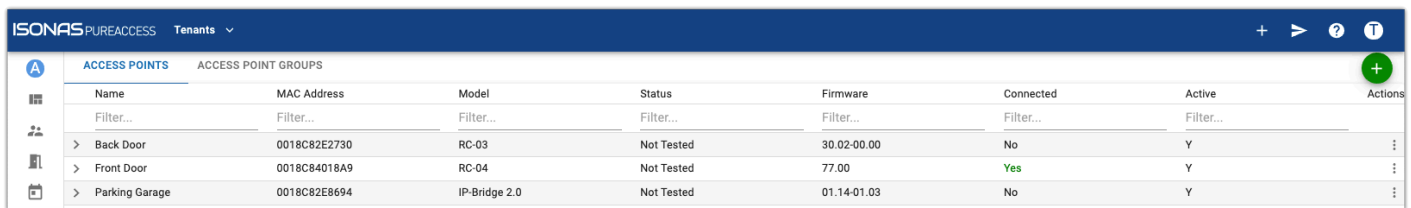
Once you have configured your hardware devices with the configuration tool to communicate with the correct domain you will need to add these access points to your Pure Access tenant.

For a full tutorial, visit the complete [video on Adding Access Points](#) to Pure Access.

9.1. Access Point Main Page

The Access Points main page shows of your access points by name, the groups they are associated with, their MAC address, status (which represents whether they had been tested), the last update (which is determined by when the settings were last changed from the AP screen), and whether or not they are currently connected to Pure Access.

Name	MAC Address	Model	Status	Firmware	Connected	Active	Actions
Name of the Access Point	MAC Address of the Access Point	Model of the Access Point	Test Status of the Access Point	Current Firmware Revision	Connection Status of the Access Point	Activated/ Deactivated	Modify Device



Name	MAC Address	Model	Status	Firmware	Connected	Active	Actions
Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	
> Back Door	0018C82E2730	RC-03	Not Tested	30.02-00.00	No	Y	⋮
> Front Door	0018C84018A9	RC-04	Not Tested	77.00	Yes	Y	⋮
> Parking Garage	0018C82E8694	IP-Bridge 2.0	Not Tested	01.14-01.03	No	Y	⋮


9.1.1. Access Point Settings

There are two different kinds of settings for each access point:

Access Point Settings

1. Click the **Access Points** tab on the left side navigation.



2. Select  next to the Access Point you want to edit and then choose **Edit Access Point**.

Edit Access Point - Front Door

MAC Address
0018C858028C

Access Point Name
Front Door

Description
RC-05

Serial Number
000000000000000006000000000001436

Access Point Groups
All Doors

Area
Los Angeles Office

Active

CANCEL SAVE

3. Here, you can see:

- **Name**
- **Description:** a helpful description of the Access Point
- **Serial Number:** this is the serial number of the physical device. It cannot be changed.

- **Access Point Groups:** you can change which Access Point Group(s) this device is associated with
- **Area:** you can change which Area this device is associated with.


4. Click **SAVE** to save your changes.

Device Settings

If you need to make any changes to the settings or retest an access point after you have finished the initial configuration:

1. Click the **Access Points** tab on the left side navigation.



2. Select  next to the Access Point you want to edit and then choose **Edit Device Settings**.

Configure Access Point - Front Door

Front Door 🔒 📄

First Person In 🔁

Door Sense

Latch Interval: seconds

Tamper Sensitivity:

Fail Modes:

ASM

REX

REX:

AUX

AUX:

Beeper

Beeper Sounds:

Keypad

Keypad Backlight

Keypad Back Light Timeout:

Lock On Close

CANCEL SAVE

3. Here, you can see:

- **First Person In:** The First Person In feature is used in combination with AutoUnlocks. If the First Person In feature is enabled, the lock will remain locked until a user presents a credential to open the door. The lock will then stay unlocked until the end of the AutoUnlock period. This feature guarantees that at least one person is present when the door is open. Not all devices are capable of this feature.
- **Door Sense:** enable this slider if the physical Access Point is equipped with a Door Sense Monitor.
- **Latch Interval:** controls the amount of time the electric latch will stay unlocked before relocking
- **Tamper Sensitivity:** controls the sensitivity of the tamper alarm
- **Fail Modes:** [Fail Safe](#) or [Fail Secure](#)
- **ASM:** enable this slider if the physical lock is equipped with an [Advanced Security Module](#)
- **REX:** enable this slider if the physical Access Point is equipped with a REX (Request for Exit) switch.
- **REX** drop-down box: choose the action that occurs when someone presses the REX switch.
- **AUX:** enable this slider if the physical Access Point is equipped with and AUX (Auxilliary) switch.
- **AUX** drop-down box: choose the action that occurs when someone presses the AUX switch.
- **Beeper:** turn the beeper (where equipped) on or off.
- **Beeper Sounds:** select which events trigger the beeper to sound.
- **Keypad:** enable this slider if the physical device is equipped with a keypad.
- **Keypad Backlight:** enable this slider to enable the keypad backlight, where equipped.
- **Keypad Back Light Timeout:** the number of seconds the keypad backlight will stay illuminated after a button press
- **Lock on Close:** enable this slider to lock the physical door any time the door is closed.

4. Click **SAVE** to save your changes.

9.2. Access Point Groups

Access Point Groups are used to control a set of Access Points that should all behave the same way. You can create a new Access Point Group before adding any Access Points and new Access Points can be added to or removed from the group at any time.

10. Access Control



The **Access Control** section allows you to control who has access to access points, and when they have access to them. Navigate to the **Access Control** section to see the default **Weekly Rule**.



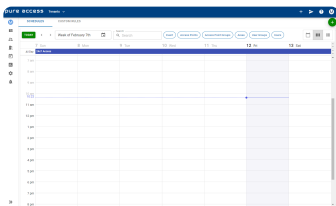
At the top, you will see two tabs: **Schedules** and **Custom Rules**.

- Schedules are [Weekly Rules](#), [Events](#) or [Holidays](#).
- [Custom Rules](#) are if-then rules that can trigger events based on conditions.

Navigating Schedules

The default view is the **weekly view**. You can change this to a **monthly view** by clicking , or to a **list view** by clicking .

A search box and filter buttons are available across the top in every view. They can be used when you are having a difficult time locating a rule or event.



Be aware that, in the list view, the **Date Range** filter is set to the current month. So, if you are looking for an event in a different month, you will need to change the **Date Range** filter.

10.1. Weekly Rules

Weekly Rules are schedules that control **WHO** will have access to which doors (**WHERE**) during a period of time (**WHEN**). Weekly Rules have three different types:


- **Grant Access:** provides access with credential to Access Points or Access Point Groups during a Schedule (the most common rule type).
- **Auto-Unlock:** unlocks the Access Points or Access Point Groups for the duration of the Schedule.
- **Auto-Unlock w/ Badge:** after a user with permissions has presented their credential, keeps the Access Points or Access Point Groups unlocked for the duration of a Schedule.

In order to visualize this better, you may want to map it out using columns:

1. A column for the name of the rule (best practice is to be as descriptive as possible).
2. A column for the users and/or user group(s) who need access.
3. A column for which access points or access point groups they will need to access.
4. A column for the days of the week and times (schedule).

Rule Name	Who?	Where?	When?
24/7 Admin Access	Upper Management	All Doors	24/7
IT Closet & Server Access	IT Managers	Server Room + IT Closet	M-F 5AM to 9PM
<i>[weekly rule name]</i>	<i>[user group]</i>	<i>[access point group]</i>	<i>[schedule]</i>


You should review every scenario and ensure there is no overlap or redundancies. In general, it's best to keep rules as simple as possible.

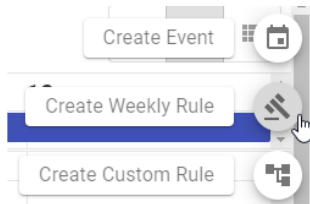
 We *highly recommend* utilizing groups (for both users and access points) when configuring any rule. Assigning individual people or doors to rules adds unnecessary complexities that can put a strain on the system when compiling this data to the devices.

10.1.1. Create Weekly Rule

1. Navigate to the **Access Control** page.



2. Hover over  and then choose **Create Weekly Rule**.



3. Enter the **Name** and **Description**, and choose the **Rule Type** and **Area** (if necessary). Then click **NEXT**.

4. Choose the **User Group** or **Users** who should be included. Then click **NEXT**.

- You can use either User Groups, Users or both. We recommend using User Groups for ease of management.

5. Choose the **Access Point Group** or **Access Point** that should be included. Then click **NEXT**.

The screenshot shows the 'Create Weekly Rule' interface at the 'Where' step. A progress bar at the top indicates that 'Details' and 'Who' are completed, 'Where' is the current step, and 'When' is pending. Below the progress bar, there are two dropdown menus: 'Access Point Group' with 'All Doors' selected, and 'Access Point' which is currently empty. At the bottom of the form, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

- You can use either Access Point Groups, Access Points, or both. We recommend using Access Point Groups for ease of management.

6. Choose the **Date Type** for the rule.

This option is not available in Engage linked sites.

- Non-Holiday: the rule will be active only on non-holiday days
- Holiday: the rule will be active only on days designated as [Holidays](#)
- Always: the rule will be active on all days

7. Choose the **Days** and **Times** during which the rule should be active. Then click **CREATE**.


The screenshot shows the 'Create Weekly Rule' interface at the 'When' step. The progress bar now shows 'Details', 'Who', and 'Where' as completed. Under 'Date Type', the 'Always' radio button is selected. Under 'Days', the '7 Days a Week' radio button is selected. Under 'Times', the '24 Hours a Day' radio button is selected. At the bottom, the buttons are 'CANCEL', 'BACK', and 'CREATE'.

- Click the **Custom Days** and/or **Custom Times** button(s) to choose specific days and times.

10.1.2. Edit Weekly Rule



1. Navigate to the **Access Control** page.



2. Find the rule you want to edit and click on it to bring up the information pop-out. Click .



- Badge Access during Office Hours
Weekly Recurring

- Alternately, if you are in list view, click  next to the rule you want to edit and then choose **Edit**.
- You can also delete the rule here by clicking .
- See [Access Control](#) for more information on navigating this screen.

3. Edit the rule as necessary.



- Click **NEXT** to move to the next screen.
- You can skip ahead to any of the items by clicking **Details**, **Who**, **Where** or **When**.

4. Click **SAVE** when you are finished.

10.1.3. Deactivate Weekly Rule


1. Navigate to the **Access Control** page.



2. Click  to enter list view.
3. Click  next to the rule you want to deactivate. Then choose **Deactivate**.


10.2. Events

In addition to your normal weekly schedules, you may wish to set up events. **Events** are used to override weekly rules. An Event can be set for an entire day, or for several hours during a day.

 An Event cannot span multiple days. [Holidays](#) can span multiple days.

Event Types


- **Lock:** locks an access point or access point group (overrides an unlock schedule)
- **Auto-Unlock:** unlocks an access point or access point group for the duration of the event
- **Auto-Unlock w/ Badge:** unlocks an access point (for the duration of the event) after a valid badge is presented
- **Lock Down:** puts an access point or access point group into lockdown

 For the most consistent performance, please ensure your hardware is on the latest [firmware](#).

10.2.1. Create Event

1. Navigate to the **Access Control** page.






2. Hover over  and then choose **Create Event**.
3. Enter the details into the **Create Event** screen.

- Name: name of the Event
 - Description: a longer description of the Event
 - Area: choose an Area, if necessary
 - Date: the day the Event should be active
 - All Day OR Start Time/End Time: the start and end times for the Event, or choose the All Day slider
 - Access Point Group or Access Point radio buttons: choose one of the radio buttons, as appropriate
 - Access Point Group or Access Point: this box will change depending on which radio button you chose. Choose the appropriate group or access point.
 - Event Type: choose the appropriate [Event Type](#)
4. Click **CREATE**.

10.2.2. Edit Event

1. Navigate to the **Access Control** page.



2. Find the Event you want to edit and click on it to bring up the information pop-out. Click .
 - Alternately, if you are in list view, click  next to the Event you want to edit and then choose **Edit**.
 - You can also delete the Event here by clicking .
3. Edit the details into the **Edit Event** screen.
 - Name: name of the Event
 - Description: a longer description of the Event
 - Area: choose an Area, if necessary
 - Date: the day the Event should be active
 - All Day OR Start Time/End Time: the start and end times for the Event, or choose the All Day slider
 - Access Point Group or Access Point radio buttons: choose one of the radio buttons, as appropriate
 - Access Point Group or Access Point: this box will change depending on which radio button you chose. Choose the appropriate group or access point.
 - Event Type: choose the appropriate [Event Type](#)
4. Click **SAVE**.

10.3. Custom Rules

Custom Rules provide the ability to set *IF*, *THEN* actions in the system. This feature allows you to script a process to trigger the desired response to a specific event/action.

You will be allowed to choose *if* an action/event occurs to a specific door, person, or during a shift, *then* a follow up event will be triggered.

Example:

If you want doors on your system to go into lockdown by pressing an auxiliary button, you can set up the following custom rule:

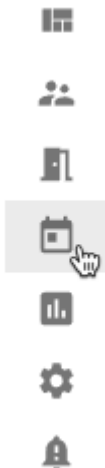
The **IF** action would be “*An AUX input is triggered*” + “*At a particular door/group of doors*”, then the **DO** action would be “*Lock down a specified door/group of doors.*”




Custom Rule functionality requires an active connection to the Pure Access software. If an ISONAS device is offline or disconnected, custom rules associated with this device will not be triggered.

10.3.1. Create Custom Rule

1. Navigate to the **Access Control** page.



2. Hover over  and then choose **Create Custom Rule**.

Create Custom Rule

Name

IF

AND

THEN

- Name: a descriptive name of the the rule
 - IF: choose the first condition to meet
 - AND: if you want to add more conditions, first click the **ADD CONDITION** button and then select further conditions
 - THEN: choose what should happen if the condition(s) are met.
3. Click **SAVE**

 The options on this screen will change depending on which condition(s) you choose from the drop-down boxes. See [Custom Rule Conditions](#) for more information.

10.3.2. Custom Rule Conditions

This is a list of all the possible conditions and actions for **Custom Rules**.

IF

- An alert is present at an access point
- There is an unauthorized open alert
- There is an extended open alert
- A user's card is rejected multiple times
 - Rejections/Interval
- A user's card is accepted
- An AUX input is triggered
- A REX input is triggered
- An access point is disconnected

AND

- At a particular door/group of doors
 - Access Point Group
 - Access Point
- To a particular person/group of people
 - User Group
 - User
- During These times
 - Days of the week
 - Start Time
 - End Time
- Not during these times
 - Days of the week
 - Start Time

- End Time
- When a door is in lock down
- When a door is in X status
 - Door Status

THEN

- Send an email to a specified person
 - Email Users
 - Email User Groups
- Lock down a specified door/group of doors
 - Access Point Group
 - Access Point
- Present an alert notification
- Unlock a specified door/group of doors
 - Access Point Group
 - Access Point
 - Duration (HH:MM)
- Reset a specified door/group of doors to a normal schedule
 - Access Point Group
 - Access Point
- Deactivate a credential for a particular person
 - User
 - Credential

10.4. Holidays

When a day is set as a Holiday, standard [Weekly Rules](#) configured with a “Non-Holiday” schedule will be overridden.



If an access point is following a weekly rule that is configured with an “Always” schedule, the door will continue to follow this rule on days set as a Holiday on the calendar.




Holidays will not be available for **Engage** enabled tenants.

10.4.1. Create Holiday

1. Navigate to the **Access Control** page.



2. Hover over  and then choose **Create Holiday**.
3. Enter the details into the **Create Holiday** screen.

Create Holiday

Name

Description

Does this holiday span multiple days?

Start Date
05/28/2021

End Date
05/31/2021




CANCEL CREATE

- Enter the Name and Description.
 - Select the slider for **Does this holiday span multiple days?** if the Holiday lasts more than one day.
 - Choose the day(s) for the Holiday from the calendar(s).
4. Click **CREATE**

10.4.2. Edit Holiday

1. Navigate to the **Access Control** page.



2. Find the Holiday you want to edit and click on it to bring up the information pop-out. Click  .
 - Alternately, if you are in list view, click  next to the Holiday you want to edit and then choose **Edit**.
 - You can also delete the Holiday here by clicking .
3. Edit the details in the **Edit Holiday** screen.
 - Edit the Name and Description.
 - Select the slider for **Does this holiday span multiple days?** if the Holiday lasts more than one day.
 - Choose the day(s) for the Holiday from the calendar(s).
4. Click **SAVE**

10.5. Schedule Date Types

1. **Non-Holiday:** This schedule will not run on days set as a “Holiday” on the calendar.
2. **Holiday:** This schedule will *only* run on days set as a “Holiday” on the calendar.
3. **Always:** This schedule will run on both “Non-Holiday” days as well as on days set as a “Holiday” on the calendar.

11. Reports

There are a variety of reports that can be utilized within Pure Access. These reports can be run by start date and end date, filtered by users, access points, event types, badge information, and areas.

All reports can be exported as a .PDF or .CSV for further analysis. In addition, all headers on the reports can be selected and the report can then be sorted ascending/descending by that field.

1. Navigate to the **Reports** page.



2. Choose the kind of report you want to view from the drop-down box.
3. Set any desired filters using the filter buttons.

4. Click



5. If you want to download a file, click



and then choose either **Download as CSV** or **Download as PDF**.

Types of reports:

- [Access Point Groups Report](#)
- [Access Point Permissions Report](#)
- [Access Points Report](#)
- [History Report](#)
- [Holidays Report](#)
- [User Attendance Report](#)
- [User Export Report](#)
- [User Group Attendance Report](#)
- [User Group Permissions Report](#)
- [User Groups Report](#)
- [User Permissions Report](#)
- [Users Report](#)

11.1. Access Point Groups Report

Access Point Group	Access Point	MAC Address	Test Status
Name of each Access Point Group in the system. Only Access Point Groups that have Access Points in them will be displayed.	Name of each Access Point in the system.	MAC Address of the Access Point	Status of the Access Point Test

The downloaded report will also include the description of each Access Point, from the Description field of the Access Point properties.

11.2. Access Point Permissions Report

Access Point	Users	Rules
Name of each Access Point in the system	List of all Users who have access to the Access Point	List of the Rules assigned to the Access Point

11.3. Access Points Report

- Name: Name of each Access Point in the System
- MAC Address: MAC Address of each Access Point
- Test Completed: Status of the test of the Access Point
- Description: Text from the Description field of the Access Point properties

11.4. History Report

- Access Point: Name of the Access Point involved in the event
- Name: Name of the User
- Event Time: Time the event occurred
- Event Type: Type of event
See [Standard History Events](#) for event descriptions.
- Credential: Credential used during the event

* Note that the name “**System Admin**” is not a user profile. This is displayed when there is no user associated with the event (i.e. to display a declined credential that is not currently attached to a user, REX/AUX admits, or with device connectivity notifications).

11.5. Holidays Report

The **holiday's report** provides an overview of all currently scheduled holidays in the system. You can use the date range filter to show you all past, current or future holidays to ensure you have all appropriate holidays in place.

11.6. User Attendance Report

The **attendance report** shows the “Time In” and “Time Out” activity for users. This reflects the time in which they first badged in for the day and then the final time they presented their badge (it *does not* capture times presented in-between these).

For example, if a user enters at 8am, exits at noon, comes back in at 1pm, and then out again at 5pm – the report will reflect an 8am “Time In” and a 5pm “Time Out” and show the total time of 9 hrs.

11.7. User Export Report

The **user export report** allows you to export user data in CSV format. This information can then be imported into a 3rd party badge printing application or into other systems.

The initial report only displays data from six fields. Once exported, all of this information as well as [User Defined Fields](#) will be displayed in the CSV file:

	A	B	C	D	E	F	G	H	I	J
1	First Name	Last Name	Created	Email	Employee ID	Department	Home Address	License Plate#	Any Relevant Information	
2	John	Marston	2/25/2019 18:38			N/A	N/A	N/A	N/A	
3	Bonnie	MacFarlane	2/25/2019 18:37			N/A	N/A	N/A	N/A	
4	Jill	Valentine	2/25/2019 18:35			N/A	N/A	N/A	N/A	
5	Gordon	Freeman	2/25/2019 18:31			N/A	N/A	N/A	N/A	
6	Sam	Fisher	2/25/2019 18:33			N/A	N/A	N/A	N/A	
7	Integrator	Isonas	2/25/2019 16:14			N/A	N/A	N/A	N/A	
8	Nathan	Drake	2/25/2019 18:31			N/A	N/A	N/A	N/A	
9	Lara	Croft	2/25/2019 18:33			N/A	N/A	N/A	N/A	
10										
11										

This report can be filtered by a date range (according to when people were created in the system) as well as filtered by user and/or area.

11.8. User Group Attendance Report

The **User Group Attendance Report** shows attendance by [User Group](#). You can filter by **Date** or **User Groups**.

11.9. User Group Permissions Report

The **User Group Permissions Report** shows the [Weekly Rules](#) or “**Custom Rules**”:#custom-rules that are applied to [*User Groups](#). You can filter this report by User Groups.

11.10. User Groups Report

The **User Groups Report** shows which [Users](#) are members of which [User Groups](#). It can be filtered by User Status, Credential Status, and User Groups.


11.11. User Permissions Report

The **User Permissions Report** shows specific users who are assigned specific rules. This report can be filtered by Users.

 If you have set up all rules by user group, then this report will not show any data.

Field Descriptions:

1. **Name:** this represents the name of the user group or user if you have individual rules assigned
2. **Access Point:** this is the list of doors that are included in the rule
3. **Rule Type:** is the type of action that takes place during this rule
4. **Day:** the day that the rule is active
5. **Start:** the start time of the rule
6. **End:** the end time of the rule.

 The rule type lists that name of the rule and provides a hyperlink to the rule within the application so you can review the rule and make changes if necessary.

11.12. Users Report

A **users report** allows you to review the users on your system, their assigned badge ID (or keypad entry), and the GUID of the credential.

1. Navigate to the **Reports** page.



2. Choose “Users” from the drop-down box.
3. Set any desired filters using the filter buttons.

4. Click



RUN REPORT

5. If you want to download a file, click



DOWNLOAD

and then choose either **Download as CSV** or **Download as PDF**.



If there are multiple badges assigned to a user (activated or deactivated), they will all show in this report.



If a user has web access to log into the tenant, their **Email Login ID** will be displayed. If they are not assigned a login and are merely a “Cardholder,” this field will show **N/A**.

If you filter the report by user group, you can see the user groups and then all users and badge ID’s that are in those specific user groups. This will allow you to audit your user groups and ensure the appropriate people are on the appropriate group.

12. Settings

The **Settings** section gives you control over the back-end settings of the system.

- [Tenant Information](#)
- [Integrator Information](#)
- [Global Settings](#)
- [Areas](#)
- [Credential](#)
- [Active Directory](#)
- [User Defined Fields](#)
- [API](#)

12.1. Tenant Information

Tenant Information is information that is entered when you first create the Tenant site. Some of the information can be edited and some cannot.

The following cannot be changed:

- License Type
- License Key
- License Expiration Date

The rest of the information can be edited, and should be kept up-to-date.

- Contact Name
- Contact Email
- Company Name
- Street Address
- City
- State/Province
- Postal Code
- Phone Number
- Notes

12.2. Integrator Information

This information should be kept up-to-date.

12.3. Global Settings

Global Settings are settings that will populate throughout the system, to all Access Points. Best practice is to set these settings before adding any Access Points and before enrolling any readers or other equipment.

 Changing any setting on this page requires the password to be entered.

Default PIN Length

This setting controls how many digits long a PIN is, by default. If you create a new Keypad Entry credential for a User, the **Pin Length** box will default to this setting. You can change the length at the time you create the credential. If credentials were already created when you changed this setting, the credentials will all still be valid.

Re-lock Time

This setting controls the default time of day that Access Points will relock if still unlocked.

Timezone

This setting controls the time zone that the system will follow.

Access Point Encryption

Adding encryption will enable it for all Access Points. You must also use the ISONAS Config Tool to enable encryption on all reader controllers. If you proceed with this change, once currently connected devices disconnect they will not be able to reconnect to Pure Access until this is completed.

[Two-Factor Authentication](#)

12.3.1. Two-Factor Authentication

ISONAS **Two-Factor Authentication** adds an additional layer of security for important points in your access control system. Two Factor is compatible with the following ISONAS hardware devices: RC-04, RC-03, and IP-Bridge v2.0.

Note: Two-factor authentication is *not compatible* with the IP-Bridge version 1.0.

We offer three different configurations of “two-factor” security in Pure Access:

1. [Card/PIN](#)
2. [Two User](#)
3. [Two-User – Card/PIN](#)



Due to the way our system encrypts two-factor credentials, you may notice an increase in the amount of time it takes to compile data. The rough estimate is ~2 additional seconds per two-factor credential.

12.3.1.1. Card/PIN

Card/PIN offers a standard two-factor entry in which a user must first present a valid badge or mobile credential, then enter a 4-9 digit two-factor PIN tied to that credential.

After a badge or mobile credential is presented, the status light on the reader will blink yellow indicating that the reader is waiting for the associated two-factor PIN entry. PIN entries should be started with the star key (*****) and ended with the pound key (**#**) (same as standard keypad entries).

 **NOTE:** This PIN is separate from the keypad credential used for single authentication.

12.3.1.2. Two User

Two User authentication requires two different valid credentials to be presented for access. No additional credential configuration is required from normal badge or mobile credential setup.

After a badge or mobile credential is presented, the status light on the reader will alternate between red and green indicating that the reader is waiting for the second authorized badge or mobile credential.



Note: If a user has 2 valid credentials assigned to them, they will be able to authorize to a two-user access point. In order to prevent this, consider using the [Two-User – Card/PIN](#) mode.

12.3.1.3. Two-User – Card/PIN

Two-User Card and PIN requires two valid credentials configured with a two-factor PIN to be entered in succession for access.

Upon first badge scan, the reader will begin blinking yellow to indicate that it is waiting for that user's two-factor PIN. Upon valid PIN entry for the first user, the reader status light will alternate red and green to indicate it is waiting for the second user to begin the card and PIN process. The second user will need to perform the same credential presentation and associated PIN entry.

12.3.1.4. Two-Factor History Events

All new two-factor events will be available in your existing dashboard widgets and history reports. When globally enabled, you'll be able to add or remove two-factor events using filters on applicable widgets and reports.

Two-factor history events:

Event Name	Short Name	Description
Two-Factor – Credential 1 of 2 Accepted	<i>Approve (1)</i>	The first credential in a two-user or two-user card and PIN process has been accepted
Two-Factor – Credential 1 Rejected – Timeout	<i>Denied – Timeout (1)</i>	The first credential in a two-user or two-user card and PIN process has been denied due to reaching the configurable timeout interval.
Two-Factor – Credential 1 Rejected – Process Error	<i>Denied – Process Error (1)</i>	The first credential in a two-user or two-user card and PIN process has been denied due to a process error (ie presenting a badge when the reader is expecting a PIN or presenting the same badge twice.)
Two-Factor – Credential 1 Bad PIN	<i>Denied – Bad PIN (1)</i>	The first credential in a two-user or two-user card and PIN process has been denied due to an invalid two-factor PIN.
Two-Factor – Credential 2 of 2 Accepted	<i>Approve (2)</i>	The second credential in a two-user or two-user card and PIN process has been accepted. Access granted.
Two-Factor – Credential 2 Rejected – No Credential Found	<i>Denied – No Credential (2)</i>	The second credential in a two-user or two-user card and PIN process has been denied due to the credential not being found in Pure Access.
Two-Factor – Credential 2 Rejected – No Authorized Schedule	<i>Denied – No Schedule (2)</i>	The second credential in a two-user or two-user card and PIN process has been denied due to the credential not having access at the current day and time.
Two-Factor – Credential 2 Rejected – Device in Lockdown	<i>Denied – Lockdown (2)</i>	The second credential in a two-user or two-user card and PIN process has been denied due to access point being in lockdown.
Two-Factor – Credential 2 Rejected – Two-Factor Timeout	<i>Denied – Timeout (2)</i>	The second credential in a two-user or two-user card and PIN process has been denied due to reaching the configurable timeout interval.
Two-Factor – Credential 2 Rejected – Two-Factor Process Error	<i>Denied – Process Error (2)</i>	The second credential in a two-user or two-user card and PIN process has been denied due to a process error (ie presenting a badge when the reader is expecting a PIN or presenting the same badge twice.)

Two-Factor – Credential 2 Rejected – Bad PIN	<i>Denied – Bad PIN (2)</i>	The second credential in a two-user or two-user card and PIN process has been denied due to an invalid two-factor PIN.
Two Factor – Accepted (Card/PIN)	<i>Approve (Card/PIN)</i>	Valid credential and PIN presentation. Access granted.
Two-Factor – Timeout in PIN Entry (Card/PIN)	<i>Denied – Timeout (Card/PIN)</i>	Denied due to reaching the configurable timeout interval during the card and PIN procedure.
Two-Factor – Process Error (Card/PIN)	<i>Denied – Process Error (Card/PIN)</i>	Denied due to a process error during the card and PIN procedure.
Two-Factor – Bad PIN (Card/PIN)	<i>Denied – Bad PIN (Card/PIN)</i>	Denied due to an incorrect PIN during the card and PIN procedure.

12.4. Areas

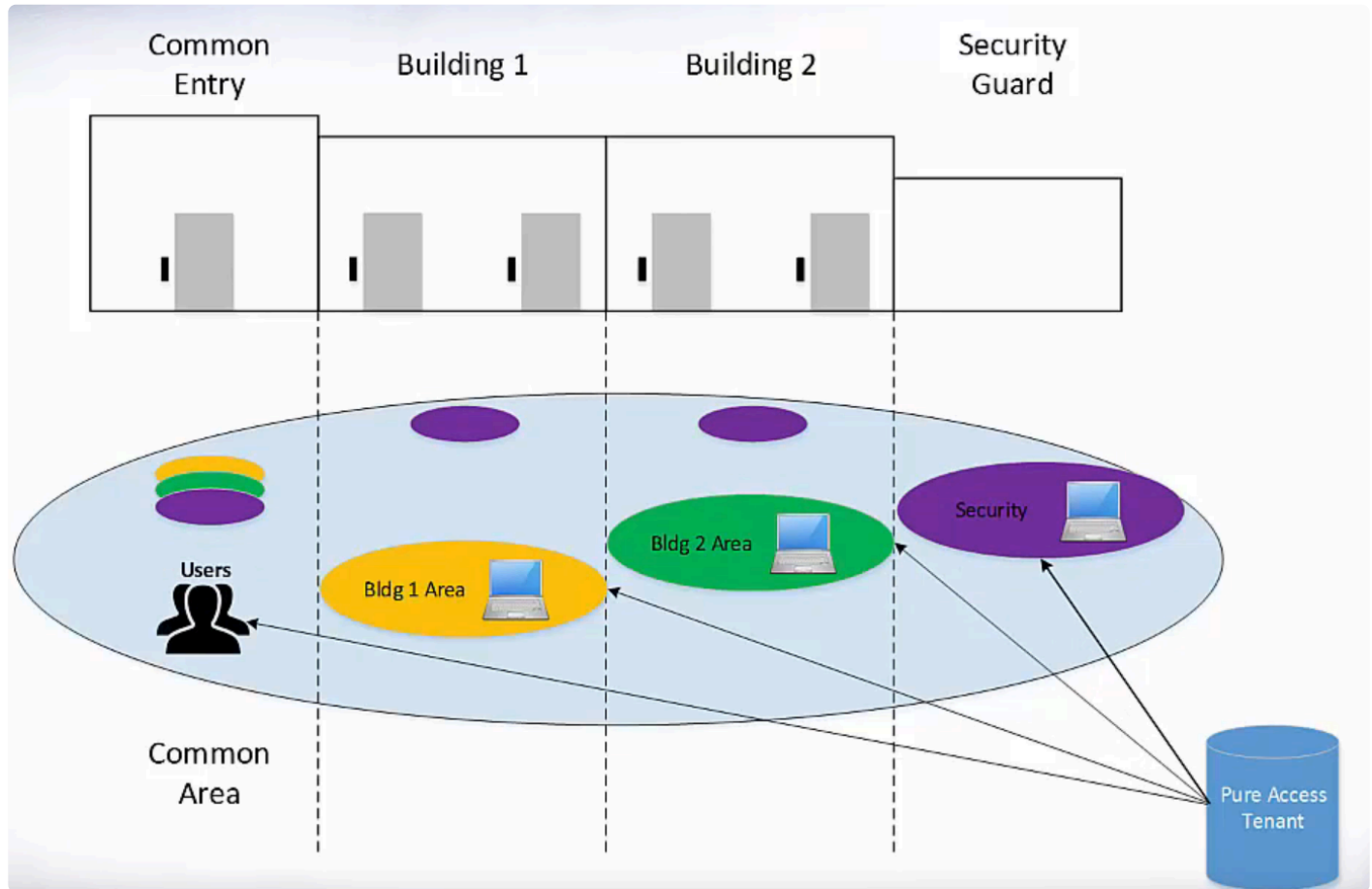
Areas are “containers” which are used to segment a Pure Access tenant for **administration purposes**.

- Areas *are not* used for access control and configuring them is optional.
- Areas should only be used if administrative segmentation is needed to protect the security of the system.
- Areas should be planned before the system is fully configured because every object in a Pure Access tenant must have an assigned area in order to be set up properly.

12.4.1. Why Use Areas?

Overview

A tenant may have certain administrators who need to see/administer *some* doors for their building or local area, but not others. These administrators would be assigned to the area(s) with which they require “View” or “Manage” privileges within the tenant and *will not* be able to view or manage any object (group, access point, user, schedule, etc.) that is associated with the area(s) of which they are **not** assigned.




In the graphic above, you can see a situation where the use of areas might be helpful in segmenting the administrative privileges of the tenant.

* Note that areas are most useful in larger, more complex configurations where different web access users need to manage **distinct groups of access points** within the same tenant.

In the above scenario:

- There is a common entry that all badge holders in the tenant would have access to.

- Separate areas are created for **Building 1** and **Building 2** so that the web access user(s) with administrative privileges for **Building 1** cannot see or make unauthorized changes for **Building 2** and vice-versa.
- The security guards have rights to all areas within this Pure Access tenant so they would be able to administer ALL access points, users, groups, dashboards, rules, etc.

 A common reason to use areas would be to split up a tenant that contains buildings, especially in different time zones.

12.4.2. How to Configure Areas

By default, your tenant will be configured with a single area named “**COMMON**”. In this default state, the areas feature is considered “off” and every object in the tenant (groups, access points, users, schedules, etc.) will automatically be added to the COMMON area.

Once another area is added to the system, the areas feature will be turned on and everything created in the system will need to be designated to an area.

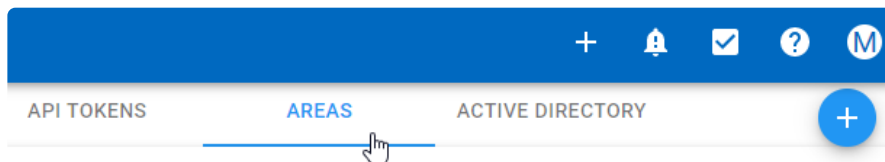
! Please note that newly created user profiles **will be associated with all of the areas** that the administrator (who created the user) is assigned to. There is currently **no way to remove a non-web access user from an area** once they have been assigned, so extra precaution is necessary when creating new profiles.

Creating an Area

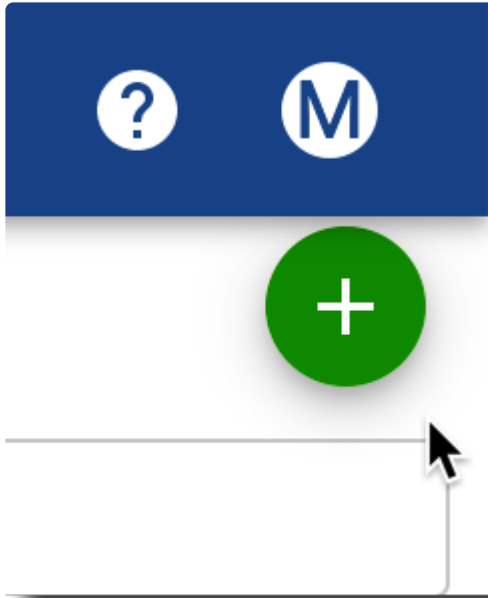
1. Navigate to the **Settings** page from the left navigation bar.



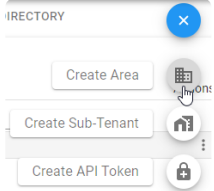
2. Select the **Areas** tab.



3. Hover over the plus sign to reveal the menu. You may need to scroll to the right to see this menu.



4. Click **Create Area**.




5. Enter the name of the area and select the correct time zone. Then click the **Next** button.

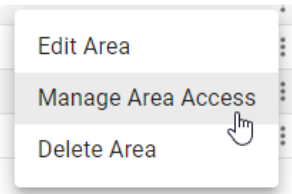
For the below example, we've created three new areas in addition to COMMON – *Los Angeles Office*, *New York Office*, and *Security Center*.

ENGAGE	TENANT INFORMATION	INTEGRATOR INFORMATION	USER DEFINED FIELDS	GLOBAL SETTINGS	CREDENTIAL	TENANT MANAGER	API TOKENS	AREAS	ACTIVE DIRECTORY
4 results									
Name		Timezone		Members		Last Update			
Filter...		Filter...		Filter...		Filter...			
>	COMMON	Mountain Time (US & Canada)-America/Yellowknife		1		12-11 11:14:33			
>	Los Angeles Office	Pacific Time (US & Canada)-America/Vancouver		0		01-19 10:44:02			
>	New York Office	Eastern Time (US & Canada)-America/New_York		0		01-19 10:55:31			
>	Security Center	Central Time (US & Canada)-US/Central		0		01-19 10:56:00			

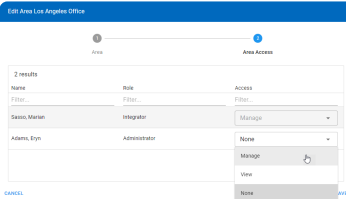
Assign Administrators to an Area


Administrators must be assigned to the area or areas of which they need to **View** or **Manage** the users, groups, schedules, rules, dashboards, etc.


1. Click the  next to the area you want to manage. Then click **Manage Area Access**.



2. Choose the appropriate level of access next to the user you want to assign.




 Users must have web access granted before they can be assigned as an administrator. See [Setting Up Web Access for a User](#).

 Remember, if areas have *not* been configured, everything will be set to **COMMON** by default. It is important to note that once areas are added to your tenant – every user, access point, group, schedule, rule, dashboard, and event must be assigned to one of the areas you've created.

12.4.2.1. Assigning Dashboards to an Area

1. Navigate to the **Dashboards** page from the left navigation bar.




2. Hover over the name of the dashboard you want to edit and choose  (or [create a new dashboard](#)).
3. From the **Area** drop-down menu, select the area with which this dashboard needs to be associated.

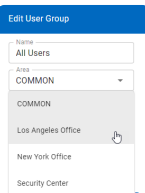
12.4.2.2. Assigning Groups to an Area

User Group

1. Navigate to the **Users** page from the left navigation bar.



2. Select the **User Groups** tab, then click on  next to a user group to view its configuration.
3. From the **Area** drop-down menu, select the area with which this group needs to be associated.




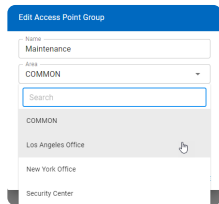
4. Then click **SAVE**.

Access Point Group

1. Navigate to the **Access Points** page from the left navigation bar.



2. Select the **Access Point Groups** tab, then click on  next to an access point group to view its configuration.
3. From the **Area** drop-down menu, select the area with which this group needs to be associated.




4. Then click **SAVE**.

12.4.2.3. Assigning Access Points to an Area

1. Navigate to the **Access Points** page from the left navigation bar.



2. Click  next to the Access Point you want to edit. Then choose **Edit Access Point**.
3. From the **Area** drop-down menu, select the area with which this access point needs to be associated.
4. Click **SAVE**

12.4.2.4. Assigning Users to an Area

1. [Edit a User](#).
2. Choose the appropriate Area from the **Area** drop-down menu.
3. Click **SAVE**

12.4.2.5. Assigning Holidays to an Area

1. [Edit a Holiday](#).
2. Choose the appropriate Area from the **Area** drop-down menu.
3. Click **SAVE**

12.4.2.6. Assigning Weekly Rules to an Area

1. [Edit a Weekly Rule.](#)
2. Choose the appropriate Area from the **Area** drop-down menu.
3. Click **SAVE**

12.4.2.7. Assigning Events to an Area



1. [Edit an Event](#).
2. Choose the appropriate Area from the **Area** drop-down menu.
3. Click **SAVE**


12.4.3. Managing Area Administrators

There are two steps to adding an Administrator to an Area:

1. [Enable Web Access](#)
2. Grant Area access to the User:



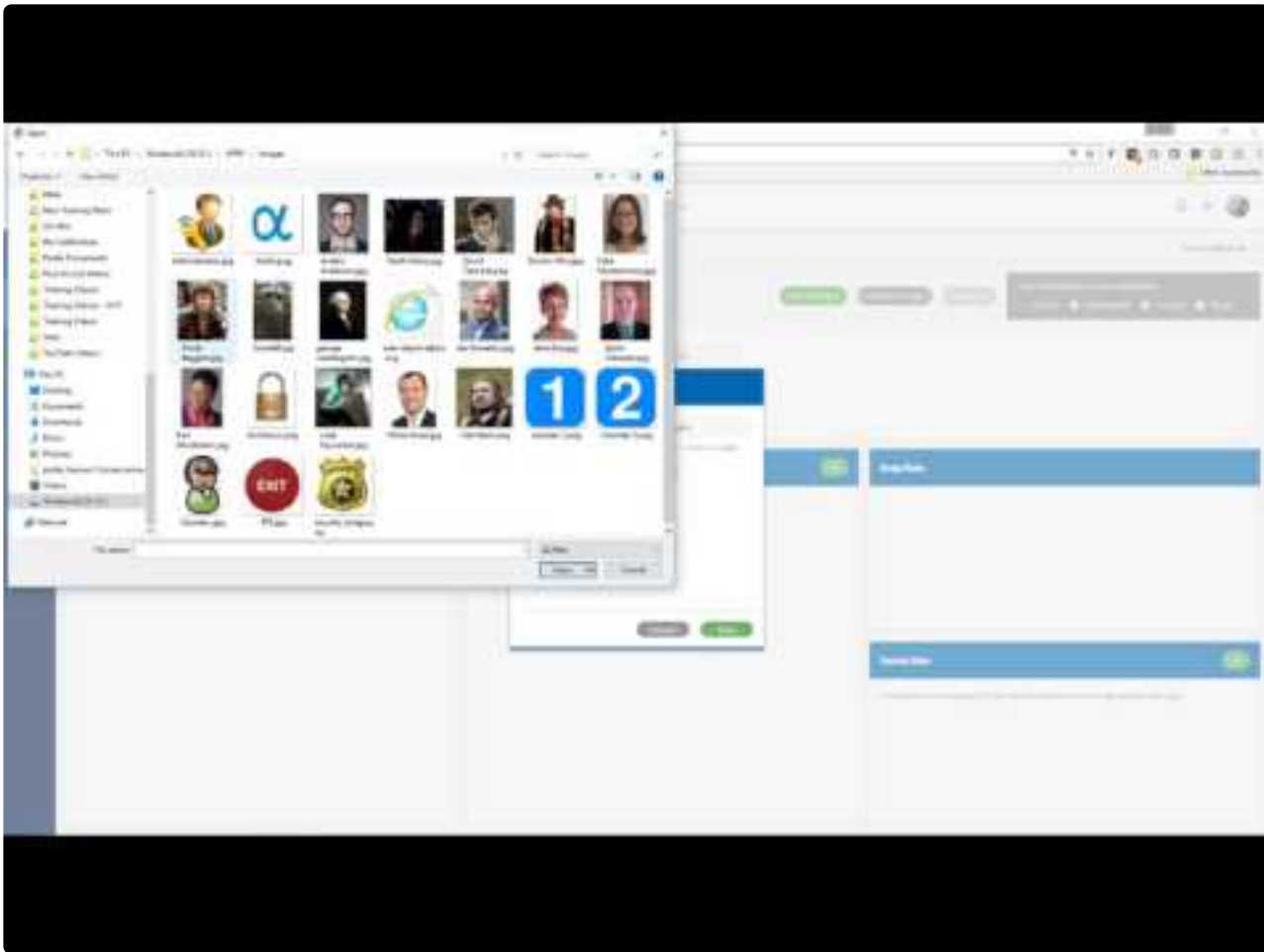
- a. Click  from the left-side menu.
- b. Click **Areas** from the top navigation.
- c. Click  next to the Area to which you want to add the Administrator.
- d. Select the level of **Access** you want to grant from the drop-down box next to the User name.
 - **Manage**: make changes in the system
 - **View**: view settings in the system
 - **None**: no access
- e. Click **SAVE**.

 Please note that a newly created user profile will inherit ALL areas that the integrator/administrator account is associated with.

12.5. Credential

This section is used to control [Bitmasking](#) of the credentials in your system.

12.5.1. Bitmasking



<https://www.youtube.com/embed/L7LqRbUqp9I?rel=0>

Resources

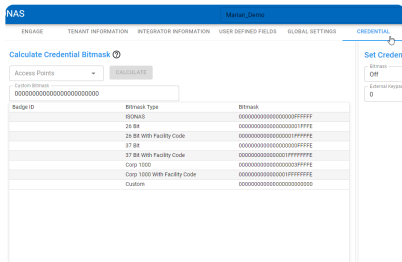
- Verifying the [currently set bitmask](#).
- [Discover and set](#) a bitmask.
- [Pushing bitmask settings](#) to all readers.
- [Pushing bitmask settings](#) to all readers in PAM 2.12.2 or below.
- Setting an [external keypad site code](#).
 - Configuring [site code on an R-1 reader](#).
- Creating a [custom bitmask](#).

12.5.1.1. Verifying the Currently Set Bitmask

1. Navigate to the **Settings** tab:



2. Click the **Credential** tab. You may need to scroll to the right to see this tab.
3. The set bitmask will be displayed.



- Calculate and use a [custom bitmask](#)



Note that, once a credential has been presented, the data will store in Pure Access and can be calculated for 15 minutes before clearing.

12.5.1.4. Setting a Bitmask

1. Under “**Set Credential Bitmask**”, select the mask you wish to set your devices to (or the mask that was [determined above](#)), then click **SAVE**.

The screenshot shows a web interface for setting a credential bitmask. At the top, the title is "Set Credential Bitmask" with a question mark icon. Below the title is a dropdown menu labeled "Bitmask" with "26 Bit" selected. Underneath the dropdown is a search bar with the placeholder text "Search". Below the search bar is a list of options: "ISONAS", "26 Bit", "26 Bit With Facility Code", "37 Bit", and "37 Bit With Facility Code". A mouse cursor is hovering over the "26 Bit" option. To the right of the list is a button labeled "SEND BITMASK TO ALL READERS". Below that are two buttons: "CANCEL" and "SAVE".

1. You will be prompted to enter your password for security.

Once saved, your connected readers will be updated immediately. You can now [enroll credentials](#) by typing in the badge ID manually.

! Changing your bitmask after badges/fobs have been enrolled can cause all of the previously enrolled credentials to be rejected. Clicking the “**Save**” button will affect *every* connected reader.

12.5.1.4.1. Pushing the Current Bitmask Setting to All Readers

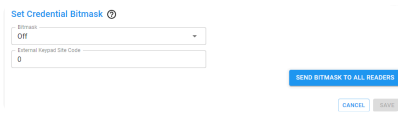
1. Navigate to the **Settings** tab:



2. Click the **Credential** tab.






3. Click the **SEND BITMASK TO ALL READERS** button.



* The selected bitmask will be pushed out to all **connected** devices on the tenant. Note that this feature was added in Pure Access 3.1.0 and is not currently available in Pure Access Manager. Instructions for pushing bitmask settings in PAM can be [found here](#).

12.5.1.4.2. Pushing Bitmask Setting to All Readers (PAM)

1. Navigate to the **Settings** tab.
2. Click the **Credential** tab under **General Settings**.
3. Select any other mask (so that the  button appears), then return to the desired/original bitmask.
4. Click .
5. Input your password when prompted then click **Confirm Change**.

 The selected bitmask will be pushed out to all **connected** devices on the tenant.

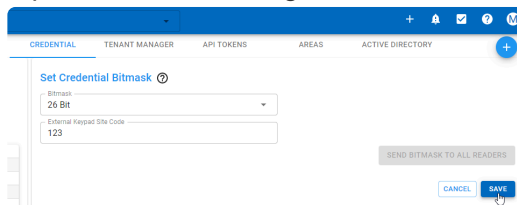
12.5.1.5. Setting an External Keypad Site Code

1. Navigate to the **Settings** tab:



2. Click the **Credential** tab.

3. Input the desired 3-digit code next to **External Keypad Site Code** then click  .




* You will also need to configure this same code onto the reader(s) tied to any IP-Bridges. Failure to do this will result in keypad entries not working correctly.

12.5.1.5.1. Configuring Keypad Site Code on an R-1 Reader

1. Power cycle the R-1 reader.
2. Within one minute from powering on the unit, enter: ***8889999**
The LED will turn green and the keypad will beep three times.
3. Within five seconds, enter **#** followed by any three-digit facility code: **# _ _ _**
The LED will turn green and the keypad will beep three times.

In this mode, the reader sends the PIN (packaged as a 26-bit Wiegand output with the fixed facility code). We recommend PIN numbers to be at least four-digits long between 1 and 32767.

The PIN should always be entered starting with ***** and ending with **#**.

 Most sites will not have a site code already established. If no site code had ever been set, we recommend 001.

12.5.1.6. Custom Bitmasking

Overview:

This article is applicable for situations where the badge ID printed on the credential does not match any of the badge ID's that are generated from the calculate button on the **Settings > Credential** page in Pure Access.

This article contains instructions on how to calculate a custom bitmask by comparing the desired badge ID with the raw data read from the card. This new bitmask will allow credentials to be enrolled by typing in the heat-stamped number manually.

! This will only work for **standard proximity fobs** and *will not work* with high frequency credentials.




Prerequisites:

- A web access profile with the **Credentials Settings** permission.
- A calculator that can convert hexadecimal and decimal values to binary. Note that the default Windows calculator has this ability when set to programmer mode.
- A sample badge/fob for which the custom bitmask is intended.
- A reader that is connected to Pure Access and is currently online.


Gathering Data:

In order to calculate our custom bitmask, we must first get the bits of our card data.

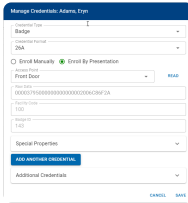
1. Present the unenrolled credential to a reader to produce a **“Decline Badge Not Found”** event in the dashboard history. Take note of the value under the “BADGE” column:

Access Point	Event	Event Time	Badge	Name
Front Door	 Decline Credential Not Found	02-25 13:44:35	 0000379500	 System Admin.

In this example, we have 0000379500. When calculating a new bitmask, this portion of the data will need to be discarded. More on this later.

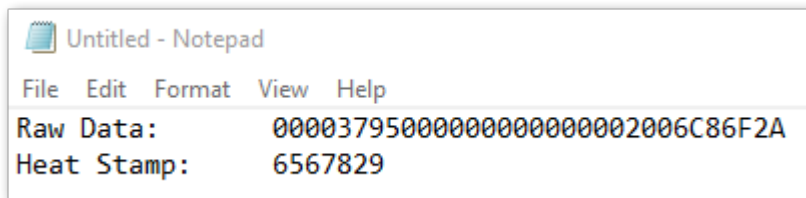
2. Gather the **“Raw Data”** value of the credential:
 - a. Navigate to **Users** and then click  > **Manage Credentials** next to a User.
 - b. Choose **Badge** from the **Credential Type** drop-down box.
 - c. Choose the **Credential Format** (bit format) from the drop-down box.

- d. Click the **Enroll by Presentation** radio button.
- e. Choose the **Access Point** to which you just presented the credential from the drop-down box.
- f. Click **“Read”**:

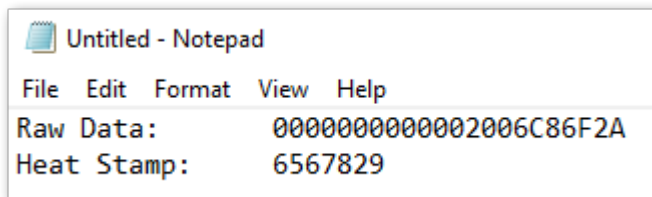


- g. Copy the entire **“Raw Data”** value into a Notepad document.

3. Copy the heat-stamped number printed on the badge into Notepad:



4. If we compare this raw data value with the badge number from the decline event in the history (see step one above), we can see that *0000379500* matches between the two. Delete this portion of the raw data from the document:



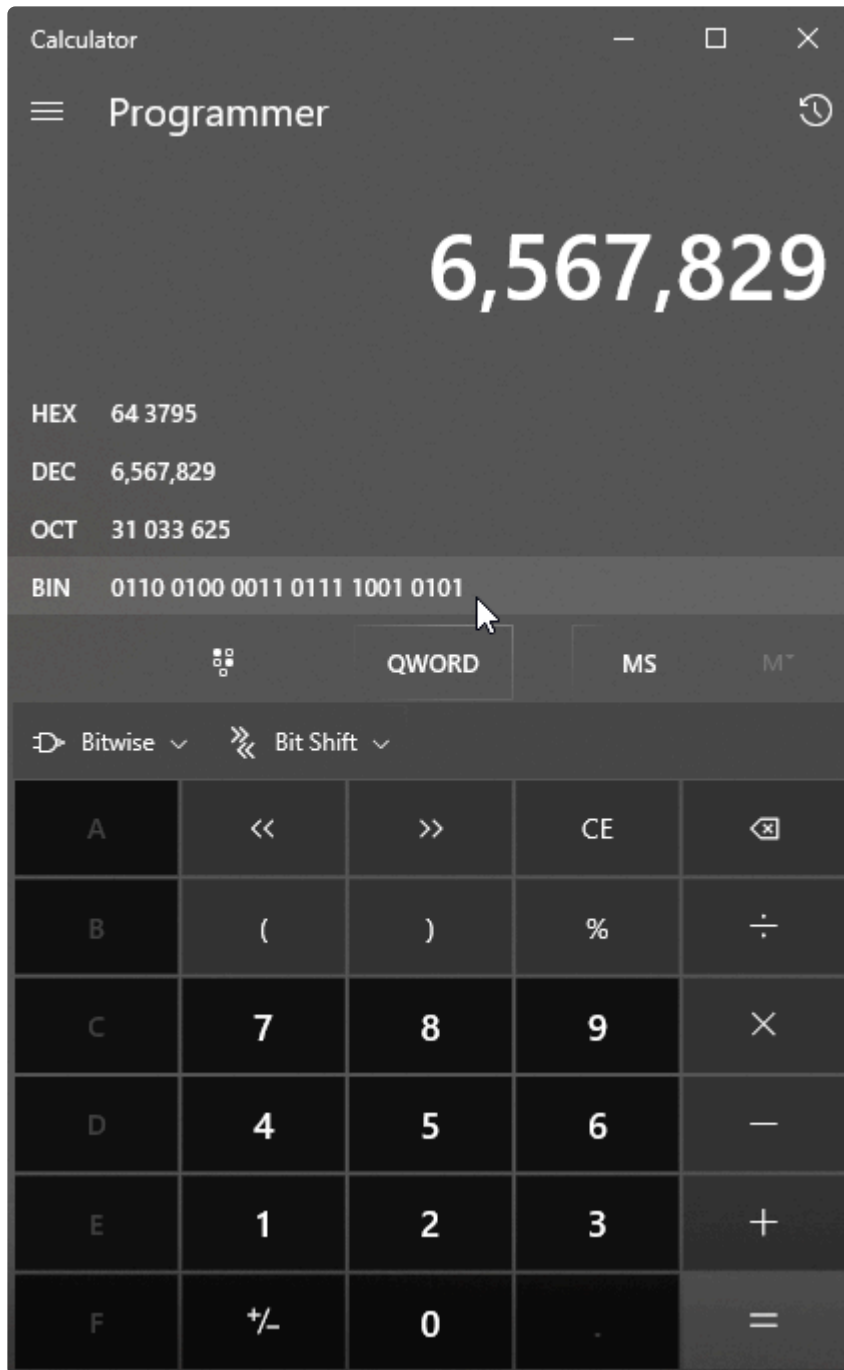
Converting data to binary:

We will now take the values in our Notepad document and convert them to binary. To do this, open the [Windows calculator in programmer mode](#) and set it to **“HEX”** (hexadecimal).

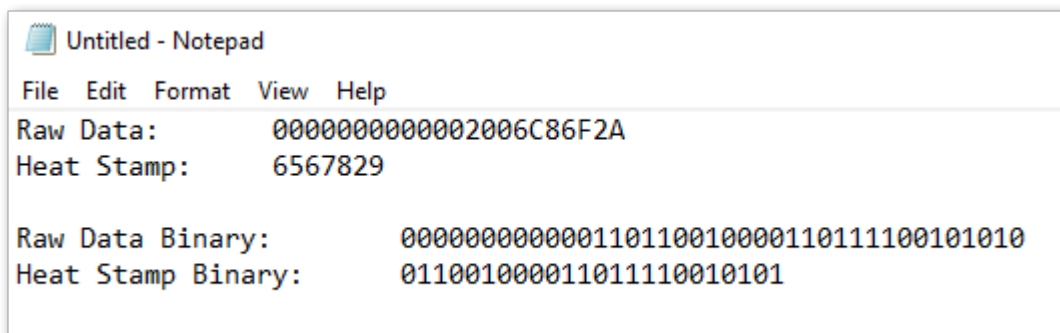
1. Copy the raw data value from Notepad and paste it into the calculator, then click **“BIN”** (binary).



2. Copy this binary data into the Notepad document.
3. Clear your calculator and set it to **DEC** (decimal). Paste or type the heat-stamped value and then click **BIN** to see the binary equivalent:



4. Copy this to Notepad under your binary raw data:



Comparing the raw data with the badge ID:

Now that we have our binary value of both the raw data and the badge ID, we must align the 1's and 0's to start our custom bitmask calculation.

1. Shift the heat-stamped binary value to the right until each 1 and 0 aligns to match the 1's and 0's from the raw data binary value above it.

```
Raw Data Binary:      0000000000000110110010000110111100101010
Heat Stamp Binary:           011001000011011110010101
```

2. From here we can determine which bits we want vs. which we don't want. On a third line, compare the binary values and type 0 for any mismatch and 1 for any match.
3. The rightmost bit on the raw data binary is a parity bit which can be ignored for now. In our example, this is a 0.
4. Going from right to left, we want to keep every bit that matches (up to the first 1 that we encounter) in our Raw Data Binary.
5. Any data preceding our heat-stamp binary will be 0's.

```
Raw Data Binary:      0000000000000110110010000110111100101010
Heat Stamp Binary:           011001000011011110010101
Wanted Bits:           00000000000000011111111111111111111110
```

6. Take the wanted bits binary value and put this in your calculator while it is in **BIN** mode, then select **HEX** to get the hexadecimal equivalent:



- This value is our custom bitmask.

```
Wanted Bits: 1111111111111111111111111110 = 1FFFFFFE
0000 0000 0000 0000 01FF FFFE
```

We can now put this into our custom bitmask field in Pure Access with all preceding zeros (24 digits total):

- Click the **Settings** tab on the left side navigation.

12.5.1.7. HID iClass Credentials

It is not possible to create a bitmask that can read the heat-stamped badge number for HID iClass credentials. The reason for this is that the HID iClass credential stores this badge value in the credential's encrypted secure sector. This encrypted information can only be accessed by HID's own hardware.

The ISONAS hardware can read the card serial number (CSN) from these credentials and generate a unique and secure value, but it will bear no relation to the credential's heat-stamped number. Users who wish to use the HID iClass credential will need to [enroll by presentation](#) to add this style of credential.

* The above also applies to non-HID branded high frequency credentials and will need to be treated in this same fashion.

12.6. User Defined Fields


You can add additional fields to user profiles in order to maintain other important information within the access control platform.

For example: Department, Home Address, License Plate, or any other necessary information that needs to be tracked can be added. If you print badges, all of these fields can be exported with the [User Export report](#) and then imported into your badge printing software.

To add these fields to user profiles:

1. Click the **Settings** tab on the left side navigation:



2. Select **User Defined Fields** from the secondary navigation. There are 10 available fields you can add to user profiles.
3. Simply enter the field name you would like to use.
4. Click .
5. These fields will now all appear on the [user profile page](#).

12.7. Active Directory

Larger* Pure Access Cloud licenses and Pure Access Manager allow for Active Directory integration to manage users and credentials via the AD Connect software.

Functionality includes:

- Creating, updating, or deactivating users in Pure Access based on changes made in Active Directory.
- Adding/Removing users from a Pure Access user group by adding/removing users from a group in Active Directory.
- Badge or keypad credential management in Pure Access by adding Badge ID's or Keypad numbers to a user in Active Directory.

For system requirements and additional info, see the Active Directory Installation Guide which can be downloaded from our [support portal](#) or by clicking [here](#).

** 51-100 license and above*

12.7.1. AD Connect Prerequisites

Requirements

- Active Directory running on Windows Server 2008 R2 or later.
- PC/Server/VM with Windows OS to run the *Isonas AD Connect* service.
 - .NET 4.5 framework is required on this system.
- Pure Access user with the [Administrator user role](#).
 - Only users with *Modify* privileges for the “Active Directory” role will be able to manage the Active Directory configuration in Pure Access.
- Active Directory user with Administrator level privileges.
- A Pure Access tenant with one of the below license types:
 - PA-C-51-100, PA-C-101-250, PA-C-251, PA-MANAGER
- An active API token with “Read Only” unchecked.

Service Account:

The service account must be able to read the entire directory.

- You may attempt a less privileged account to see if this can read your directory. If authentication fails, elevate the account to Domain Admin. You may reduce privileges and retest to find the appropriate level for your directory.
- The service account name should only contain alphabetic characters.
 - Good username: isonasadconnect
 - Bad username: isonas-ad-connect, ison@sadconnect
- The username as entered will entirely depend on the AD configuration.
 - AD username Possibilities
 - isonasadconnect
 - isonasadconnect@domain.com
 - domain\isonasadconnect
 - You may need to modify based on your directory.
- There is not official support for authentication with a .local domain.

Directory Structure and Groups:

- There should be a dedicated OU that collects all of the user groups that you wish to use. This is a clean way to ensure a successful sync.
- Groups should not be within groups. It's cleaner and easier to manage if the groups are not nested.
 - It is recommended to name the groups for their purpose according to MS best practices.
 - i.e. DoorAccess-MainEntrance or DAMainEntrance
- Users should be collected in a single root OU according to MS best practices.
 - i.e. Community/Office1/User Community/Office2/User
- Usernames should only contain alphanumeric characters.

AD Connect Software:

- It is recommended to run the AD Connect software on a Domain Controller.
- The AD Connect Tool will require internet access in order to communicate with Cloud.
 - If Pure Access Manager is in use, an internet connection is not required, however, the tool will need clear access to the PAM server.

Structures that will NOT work:

- The AD Connect Tool will not traverse trusts between domains.
 - Users added to a group from a trusted domain will not sync.
- If existing groups are used and users are in more than one nested group, you may encounter errors.
- Groups and/or users that have non-alphanumeric characters may cause errors.

Resources:

- [General Best Practices for AD](#)
- [Key Principles on OU design](#)

12.7.2. Installation and Configuration

1. In Pure Access, create a new API token and uncheck “Read Only.”
 - This is done from the **Settings** > [API Tokens](#) page.
2. Download and install the latest version of the ADConnect tool located on our [support portal](#) or by clicking [here](#). By default, this will install to the *C:\Program Files (x86)\Isonas\Isonas AD Connect* directory.
3. Run **ADConnectConfiguration.exe** as an administrator.
4. Configure Pure Access:
 - a. If connecting to Pure Access Cloud, the URL will be *https://isonaspureaccesscloud.com*
 - b. If connecting to Pure Access Manager, this will either be: *http://localhost* or the IP address of the PAM server (preceded by *http://*).
 - c. Paste the “API Token ID” and “API Token Value” from step 1 into the appropriate fields.
5. Configure Active Directory:
 - a. Input the domain.
 - b. Depending on the AD environment, the username field will use one of the following formats:
 - **username**
 - **username@domain.com** – (this may also end in .org, .edu, etc.)
 - **domain\username**
6. Run through the tests to ensure there was a successful connection.
 - The most important tests are **Get Tenant** for Pure Access and **Get Groups** for Active Directory.
7. If any of the Active Directory tests are failing, you may want to use another one of the username formats from step 4 above.



Still need help? Please send the **adpod.log** file (located in the same directory that ADConnect is installed) and a description of your issue to our [support team](#) for review.

12.7.3. Configuring AD Sync Settings in Pure Access

1. Log into your Pure Access tenant.
2. Create [User Groups](#) which will be populated with user profiles from AD.
3. Navigate to **Settings > Active Directory**
4. Set sync times under **General Configuration**.
5. Map AD fields to Pure Access fields under [User Field Mapping](#) (you may need to refresh the fields for them to appear).
6. Map AD groups to Pure Access user groups under [User Group Field Mapping](#) (you may need to refresh the groups for them to appear).
7. Once everything is set up properly, click **FULL SYNC**.
 - Please note that this may take some time to complete if this is the first time syncing. If there doesn't appear to be activity after 10 minutes, refresh the page and try to sync again.
 - If the above did not work, restart the **Isonas AD Connect** Windows service and try again.



Still need help? Please send the **adpod.log** file (located in the same directory that ADConnect is installed) and a description of your issue to our [support team](#) for review.

12.8. API

The Pure Access API is a restful API using HTTP basic authentication. It has simple, resource-oriented URLs and uses standard HTTP response codes to indicate errors. All API responses are returned in JSON.

The API is available for Pure Access Cloud or Pure Access Manager. Use of the API requires familiarity with software development, web services, and the Pure Access platform.


12.8.1. Authentication

Authenticate when using the API by including your secret API token in the request. You can manage your API token from the Pure Access Dashboard. Your API tokens carry many privileges so be sure to keep them secret! Do not share your API tokens in publicly accessible areas such as GitHub, client-side code, and so forth.

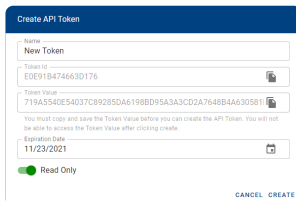
Authentication to the API is performed via [HTTP Basic Auth](#). Provide your API ID and token pair (TokenID:TokenValue) as the basic auth username value. You do not need to provide a password.


12.8.2. API Tokens

You can manage your API tokens by logging in to your tenant in Pure Access and navigating to the **Settings** page, then to the **API Tokens** page from the top navigation bar.

To assign a token, hover over  and then select **Create API Token**. You can assign both a name and an optional expiration date for your new token. By default, **all new tokens will only provide read only access**.

You can create a token with both read a write access by unchecking the “Read Only” checkbox.



You *must* copy/paste the **Token ID** and **Token Value** before saving the token as they are **NOT** stored in Pure Access for security reasons. Click  to copy the value to the clipboard, and then paste into your own document. Make sure to get *both* the **Token ID** and the **Token Value**.

12.8.3. Additional API Information

Errors

Isonas uses standard HTTP responses to indicate the success or failure of an API request. In general, codes in the **2xx** range indicate success, codes in the **4xx** range indicate an error that failed because of the information provided (e.g., a required parameter was omitted), and codes in the **5xx** range indicate a server error.

Throttling

To improve API speed and responsiveness for all users, Isonas enforces some API rate limiting measures. Each API token is limited to 30 requests per minute, enforced on a 1 minute, 5 minute, 1 hour, and 24 hour rolling average. Certain resource intensive endpoints can have stricter rate limits enforced. If you think you might exceed this limit, please contact Isonas support.

Resources

For information about the resources available in the Isonas API, please visit:

<https://app.swaggerhub.com/apis/isonaspureaccess/api-v2/1.0.2>

13. Alerts

Alerts are used to notify administrators that there is an event in their system that is not following the current rules and may require further investigation.

To view/modify your alerts, select the **Alerts** tab from the left:



ALERTS		ALERT SETTINGS		
Date Range	Alert Types	Alert State - 2	Access Points	
<input type="button" value="DOWNLOAD"/>				
10 results				
Access Point	Alert Time	Alert Type	Alert State	Actions
Filter...	Filter...	Filter...	Filter...	
<input type="checkbox"/> Front Door	03-08 19:28:09	Custom Rule	New	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-23 11:13:57	Credential Rejected	Acknowledged	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-21 17:43:09	Custom Rule	Acknowledged	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-19 07:57:11	Custom Rule	New	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-17 16:41:52	Extended Open	New	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-17 16:41:50	Unauthorized Open	New	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-17 16:41:48	Tamper	New	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-17 16:41:47	REX Alarm	New	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-03 17:58:19	Credential Rejected	Acknowledged	✓ <input type="checkbox"/>
<input type="checkbox"/> Front Door	02-03 17:58:12	REX Alarm	Acknowledged	✓ <input type="checkbox"/>

From here, you can see all alerts that have been generated:

- You can filter these alerts by choosing options from any of the filter buttons.
- To **Acknowledge** an alert, click ✓ next to the alert you want to acknowledge.
- To **Acknowledge Multiple** alerts, click the check box next to the alert(s) you want to acknowledge, and then click **ACKNOWLEDGE**.
- To **Clear** an alert, click next to the alert you want to clear.
- To **Clear Multiple** alerts, click the check box next to the alert(s) you want to clear, and then click **CLEAR**.
- To **Download** alerts, click .

13.1. Alert Types and Setup Procedure

Alerts are displayed by clicking the **Alerts** tab on the left side menu.



Access Point	Alert Time	Alert Type	Alert State	Actions
Name of the Access Point where the alert occurred	Date and time of the alert	Type of Alert	State of the Alert: Acknowledged or New	Actions: Acknowledge or Clear

You can filter Alerts by choosing any of the filter bubbles above the table. Click **SAVE** to change the table. Click **CLEAR** to remove the filter.

You can select more than one alert by selecting the box next to each alert, or all of them by selecting the box next to the Access Point heading. Then you can choose **Acknowledge** or **Clear** from the blue bar to affect all selected alerts.

Alert Types

- [Unauthorized Open](#)
- [Extended Open](#)
- [Tamper](#)
- [AUX/REX Alarm](#)
- [Credential Rejected, Expired, or Over Limit](#)

13.1.1. Unauthorized Open

Unauthorized Open is an alert that is intended to notify the user that a door has been opened without a valid admit.

Causes

The main cause of this alert would be a forced entry where someone opens the door in a way that breaks the contact on the door position sensor. Other causes of this alert could be improperly installed door position sensors or faulty wiring.

Physical Requirements

To utilize this alert, a door sensor will need to be installed and enabled in the access point's settings. If door sense is not enabled, the alert will not work.

Setting Up

1. Install and enable the door position sensor.
2. Enable **Door Sense** on the Access Point for which you want to receive alerts.
 - See **Device Settings** under [Access Point Settings](#).

13.1.2. Extended Open

Extended Open is an alert that is intended to notify the user that a door was left open after a valid admit.

Causes

This alert will trigger when a door is open past its latch interval plus the extended open threshold.

Physical Requirements

To utilize this alert, a door sensor will need to be installed and enabled in the access point's settings. If door sense is not enabled, the alert will not work.

Setting Up

1. Install and enable the door position sensor.
2. Enable **Door Sense** on the Access Point for which you want to receive alerts.
 - See **Device Settings** under [Access Point Settings](#).

13.1.3. Tamper

Tamper is an alert that is intended to notify the user when the reader needs to be visually inspected as it may have been tampered with. In order to reset the tamper alert you will need to re-calibrate the reader's tamper sensor.

Setting the Tamper Sensitivity

1. Set the **Tamper Sensitivity** to the desired level on the Access Point for which you want to receive alerts.
 - See **Device Settings** under [Access Point Settings](#).

Setting Up the Hardware (RC-03 only)

1. In order to set up the tamper alert, the reflective sticker that comes with the RC-03 reader will need to be installed. We recommend wiring up the door position sensor before attempting to install the sticker (which goes behind the reader).
2. Place the sticker on the wall behind where the readers "eye" is and securely mount the reader. After the reader has been securely mounted, plug the reader into its power source. It will automatically begin to calibrate.

! To avoid triggering the tamper alarm, *do not* remove the reader from the wall once this setting has been enabled.

13.1.4. AUX/REX Alarm

AUX Alarm or **REX Alarm** are alerts that are intended to notify the user that an AUX or REX device has been triggered.

Physical Requirements

To utilize this alert, an AUX/REX device will need to be installed and configured in the access point's settings.

Setting Up

1. Install and enable the AUX or REX switch on the device.
2. Enable **REX** and or ***AUX**", and set the action on the Access Point for which you want to receive alerts.
 - See **Device Settings** under [Access Point Settings](#).

13.1.5. Credential Rejected, Expired, or Over Limit

Credential Rejected, **Credential Expired**, and **Credential Over Limit** are alerts that are intended to notify the user that a credential has been presented and declined at a reader.

- *Credential Rejected*: A credential with insufficient access has been presented to a reader.
- *Credential Expired*: A credential which has exceeded its [time limit](#) has been presented to a reader.
- *Credential Over Limit*: A credential which has exceeded its [count limit](#) has been presented to a reader.

13.2. Alert Settings

1. Click the **Alerts** tab on the left side navigation.



2. Click the **Alert Settings** tab.

3. Adjust any of the **Alert Settings**:

- **Extended Open Threshold:** how long a door must remain open before an alert is sent. Default is three (3) seconds.
- **Auto Clear Alerts:** choose which alerts should be cleared automatically
- **Disable Alerts:** choose which events should not generate an alert
- **Email Alert Start Time:** choose the start time for when alerts should be emailed
- **Email Alert End Time:** choose the end time for when alerts should be emailed
- **Email Users:** choose which users should be sent email when there is an alert
 - Only users who have been granted [Web Access](#) will be shown in this list.
- **Email Alerts:** choose which alerts should generate an email.

4. Click .

14. Glossary

- [Admit](#)
- [ASM](#)
- [AUX](#)
- [Compile](#)
- [Door](#)
- [Lock Down](#)
- [REX](#)

14.1. Admit

Command to temporarily unlock a locked Access Point to allow temporary access.

14.2. ASM

ASM: Advanced Security Module

14.3. AUX

AUX: Auxilliary Input

14.4. Compile

Compile is the action of updating access points.

14.5. Door

“Door “ is synonymous with “Access Point”.

Similarly, “Door Group” is synonymous with “Access Point Group”.

14.6. Fail Safe

Fail safe access points are unlocked when power is removed. Fail Safe will revert to an unlocked state if there is a power outage. Power is applied to lock the access point. Most access points provide free egress whether they are fail safe or fail secure.

14.7. Fail Secure

Fail secure access points are locked when power is removed. Fail Secure will revert to a locked state if there is a power outage. Power is applied to unlock the access point. Most access points provide free egress whether they are fail safe or fail secure.

14.8. First Person In

The First Person In feature is used in combination with AutoUnlocks. If the First Person In feature is enabled, the lock will remain locked until a user presents a credential to open the door. The lock will then stay unlocked until the end of the AutoUnlock period. This feature guarantees that at least one person is present when the door is open. Not all devices are capable of this feature.

14.9. Lock Down

When an Access Point is in Lock Down mode, access will be denied to all but Master credentials.

14.10. REX

REX: Request for Exit

14.11. Secured

Secured is another word for locked.