



Pure Access Product Manual

1 — Last update: 21 June 2023

Isonas

Table of Contents

1. Using This Manual	8
2. Contact Support	10
3. Application Infrastructure and Architecture	11
3.1. Pure Access Cloud Infrastructure	12
3.1.1. Pure Access Cloud License Renewal FAQ	13
3.2. Pure Access Manager Infrastructure	15
3.2.1. Pure Access Manager System Requirements	16
3.3. Platform Update Process	17
3.3.1. Pure Access Cloud	18
3.3.2. Pure Access Manager	19
4. Setup and Configuration	20
4.1. Network Configuration and Troubleshooting	21
4.1.1. IP Addressing	22
4.1.2. Basic Firewall Information	23
4.1.3. Best Practices	25
4.1.4. Additional Troubleshooting	26
4.2. Configuring ISONAS Devices	28
4.2.1. Using the Configuration Tool	29
4.2.1.1. Advanced Configuration	32
4.2.1.2. Reviewing Network Config Settings	36
4.2.1.3. Connectivity Test	39
4.2.2. Discovering Units	41
4.2.2.1. Find device by IP	43
4.3. Updating Firmware	45
4.3.1. IP-Bridge Firmware Information	49
4.4. Wiring and Hardware Installation	51
4.4.1. RC-04 Installation Guide	52
4.4.2. IP-Bridge Installation Guide	53
4.4.2.1. IP-Bridge Status Light Indicators	54
4.4.3. RC-03 Installation Guide	56
4.4.3.1. RC-03 Jumper Configurations	57
4.4.4. ASM Status Light Indicators	61
4.4.5. Factory Resetting a Device	62
4.4.6. Wiegand Interface Module (WIM)	63
5. Getting Started in Pure Access	64
5.1. Pure Access Cloud	65
5.1.1. Logging into a Pure Access Cloud tenant	66
5.1.2. Tenant Name	68

5.1.3. Cannot Log into Pure Access Tenant	69
5.1.4. RMR License	71
5.1.4.1. Creating Subtenants	72
5.2. Pure Access Manager	75
5.2.1. Java Memory Allocation	76
5.2.2. SMTP Configuration (Pure Access Manager)	77
5.2.3. Configuring Pure Access Manager for SSL	80
5.3. Migrating from One Tenant to Another	81
5.4. Backup and Restore Process (Pure Access Manager).....	83
5.5. Integrations	84
5.5.1. PANRServ	85
5.5.2. Entrust Datacard TruCredential.....	86
5.5.3. Milestone XProtect.....	87
6. Online Interface	88
6.1. App Bar.....	90
6.1.1. Tenant Select.....	91
6.1.2. Quick Add	92
6.1.3. Send Commands	93
6.1.4. Help Button	95
6.1.5. User Profile	96
6.2. Dashboards.....	97
6.2.1. Create Dashboard.....	98
6.3. Widgets.....	99
6.3.1. History Widget	100
6.3.1.1. Standard History Events	101
6.3.2. Single Access Point Widget	103
6.3.3. Multiple Access Point Widget	104
6.3.4. Access Point Admit Widget	105
6.3.5. Lock Down Access Points Widget	106
6.3.6. User Profile Widget.....	107
7. Users	108
7.1. Create User.....	109
7.1.1. Importing Users	111
7.1.1.1. Importing Users into Pure Access Cloud (non-Engage tenant).....	112
7.1.1.2. Importing Users into Pure Access Cloud (Engage linked tenant).....	116
7.1.1.3. Importing Users into Pure Access Manager	118
7.2. Edit User.....	120
7.3. User Search and Filters.....	121
7.4. User Groups.....	123
7.4.1. Create User Group.....	124
7.4.2. Manage User Groups.....	125

7.5. Manage Credentials	130
7.5.1. Badge	133
7.5.2. Keypad Entry	136
7.5.3. ISONAS Mobile	137
7.5.3.1. Using the Mobile Credential to Unlock a Door	141
7.5.4. Schlage Mobile	142
7.5.5. Enrolling by Presentation	143
7.5.6. Special Credential Properties	145
7.5.6.1. Master Credential	146
7.5.6.2. Toggle Credential	148
7.5.6.3. Count Limit	151
7.5.6.4. Time Limit	152
7.5.6.5. Force Check-In	153
7.5.7. Migrate Credentials (Legacy to ENGAGE)	154
7.5.8. Deactivating Credentials	156
7.6. Manage Web Access	158
7.6.1. Setting up Web Access for a User	159
7.6.2. User Roles	161
7.6.3. Accepting the Web Access Invitation	163
7.6.4. Removing Web Access Privileges	166
7.7. Deactivate User	167
7.7.1. Viewing Deactivated Users	169
7.7.2. Activating a User Profile	170
8. Access Points	171
8.1. Access Point Main Page	172
8.1.1. Adding a Reader Controller (legacy device)	173
8.1.2. Adding a Schlage device using ENGAGE	175
8.1.3. Configuring an Access Point	176
8.1.3.1. Configuring the Advanced Security Module (ASM)	180
8.1.3.2. Configuration Settings	181
8.1.4. Edit Access Point	183
8.2. Deactivate Access Point	185
8.2.1. Viewing Deactivated Access Points	186
8.2.2. Replacing an Access Point with Another Device	187
8.2.3. Deleting an Access Point	188
8.3. Access Point Groups	189
8.3.1. Create Access Point Group	190
8.3.2. Add Access Point to Access Point Group	191
8.4. Update Firmware for Schlage Devices	192
9. Access Control	193
9.1. Weekly Rules	194

9.1.1. Create Weekly Rule	196
9.1.2. Edit Weekly Rule.....	201
9.1.3. Deactivate Weekly Rule	202
9.2. Events.....	204
9.2.1. Create Event.....	205
9.2.2. Edit Event	207
9.3. Custom Rules	208
9.3.1. Create Custom Rule.....	209
9.3.2. Custom Rule Conditions	210
9.4. Holidays	212
9.4.1. Create Holiday	213
9.4.2. Edit Holiday	214
9.5. Schedule Date Types	215
10. Reports.....	216
10.1. Access Point Groups Report	218
10.2. Access Point Permissions Report.....	219
10.3. Access Points Report	220
10.4. History Report	221
10.5. Holidays Report.....	222
10.6. User Attendance Report	223
10.7. User Export Report.....	224
10.8. User Group Attendance Report	225
10.9. User Group Permissions Report.....	226
10.10. User Groups Report	227
10.11. User Permissions Report.....	228
10.12. Users Report	229
11. Settings	230
11.1. Tenant Information	231
11.2. Integrator Information	232
11.3. Global Settings.....	233
11.3.1. Two-Factor Authentication	234
11.3.1.1. Card/PIN.....	235
11.3.1.2. Two User	236
11.3.1.3. Two-User – Card/PIN.....	237
11.3.1.4. Configuration Process.....	238
11.3.1.4.1. Enable Two-Factor Authentication	239
11.3.1.4.2. Adding Two-Factor PINs.....	240
11.3.1.4.3. Adding Two-Factor Rules	241
11.3.1.5. Two-Factor History Events	242
11.4. Areas	244
11.4.1. Why Use Areas?	245

11.4.2. How to Configure Areas	247
11.4.2.1. Assigning Dashboards to an Area	250
11.4.2.2. Assigning Groups to an Area	251
11.4.2.3. Assigning Access Points to an Area	252
11.4.2.4. Assigning Users to an Area	253
11.4.2.5. Assigning Holidays to an Area	254
11.4.2.6. Assigning Weekly Rules to an Area	255
11.4.2.7. Assigning Events to an Area	256
11.4.3. Managing Area Administrators	257
11.5. Credential	258
11.5.1. Bitmasking	259
11.5.1.1. Verifying the Currently Set Bitmask	260
11.5.1.2. Identifying Credential Data	261
11.5.1.3. Discover the Appropriate Bitmask	263
11.5.1.4. Setting a Bitmask	264
11.5.1.4.1. Pushing the Current Bitmask Setting to All Readers	265
11.5.1.4.2. Pushing Bitmask Setting to All Readers (PAM)	266
11.5.1.5. Setting an External Keypad Site Code	267
11.5.1.5.1. Configuring Keypad Site Code on an R-1 Reader	268
11.5.1.6. Custom Bitmasking	269
11.5.1.7. HID iClass Credentials	277
11.6. User Defined Fields	278
11.7. Active Directory	279
11.7.1. AD Connect Limitations and Requirements	280
11.7.2. Installation and Configuration	283
11.7.3. Configuring AD Sync Settings in Pure Access	284
11.8. API	285
11.8.1. Authentication	286
11.8.2. API Tokens	287
11.8.3. Additional API Information	288
11.9. ENGAGE	289
11.9.1. Linking to ENGAGE	290
11.9.2. Inviting Users to ENGAGE	292
11.9.3. Wireless Device Check-In	293
11.9.3.1. Force Wireless Device Check-In	295
12. Alerts	296
12.1. Alert Types and Setup Procedure	297
12.1.1. Unauthorized Open	298
12.1.2. Extended Open	299
12.1.3. Tamper	300
12.1.4. AUX/REX Alarm	301
12.1.5. Credential Rejected, Expired, or Over Limit	302

12.2. Alert Settings..... 303

13. Glossary 304

13.1. Admit..... 305

13.2. ASM 306

13.3. AUX 307

13.4. Compile..... 308

13.5. Door 309

13.6. Fail Safe..... 310

13.7. Fail Secure..... 311

13.8. First Person In..... 312

13.9. Lock Down 313

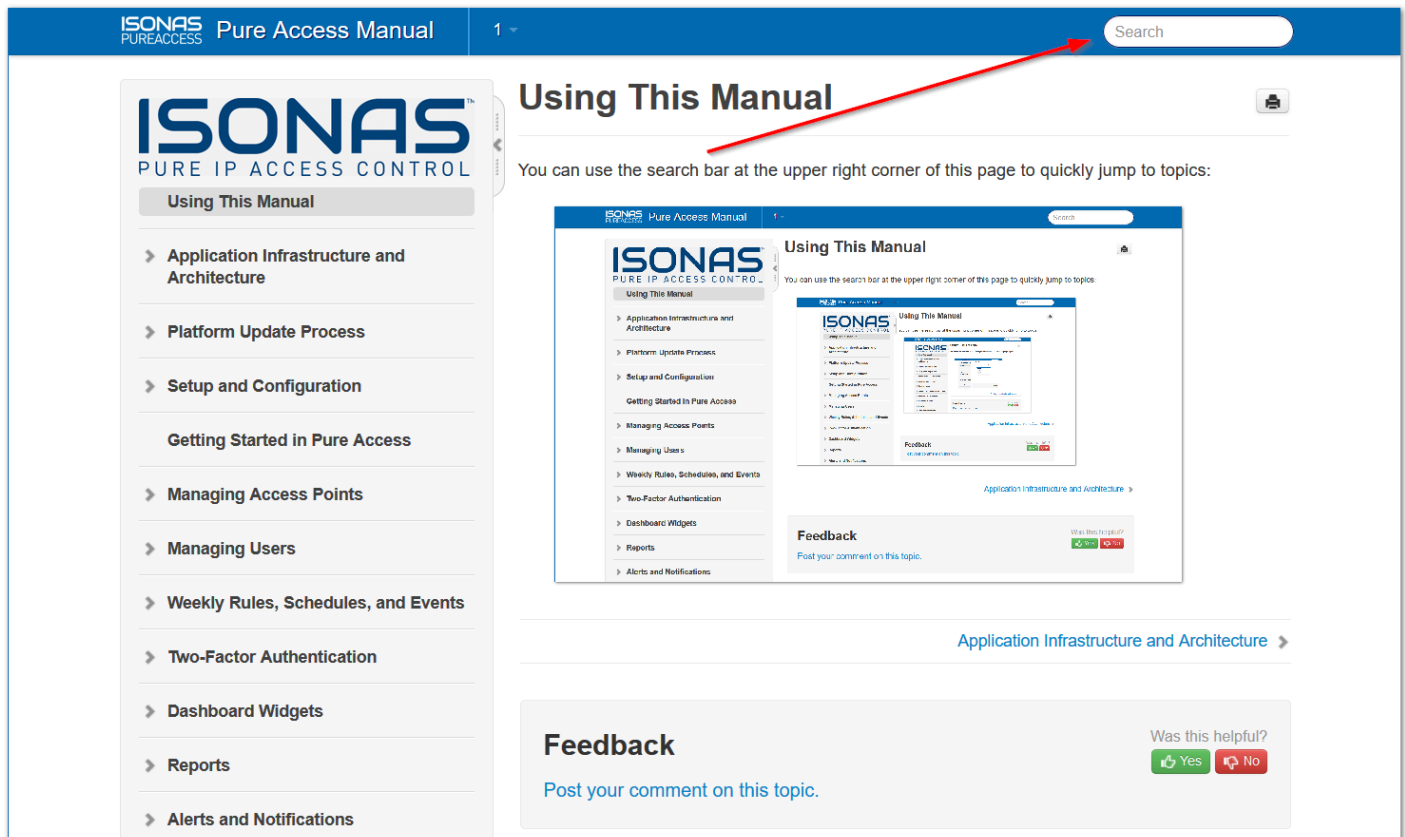
13.10. REX 314

13.11. Secured..... 315

14. Appendix A: Linking ENGAGE Site to Pure Access 316

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:



Example:

ISONAS
PUREACCESS

Pure Access Manual

1

set a holiday

ISONAS
PURE IP ACCESS CONTROL

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

set a holiday

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 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.

Sales/System related questions: Reach our collective sales team at: ISONAS.Sales@Allegion.com or Call us directly at (800) 581-0083 where any member of the team will be able to assist.

Order Status: <https://360portal.allegion.com/launchpad>

Customer Support – 877-671-7011 Option #1

Tech Support – 877-671-7011 Option #2

3. Application Infrastructure and Architecture

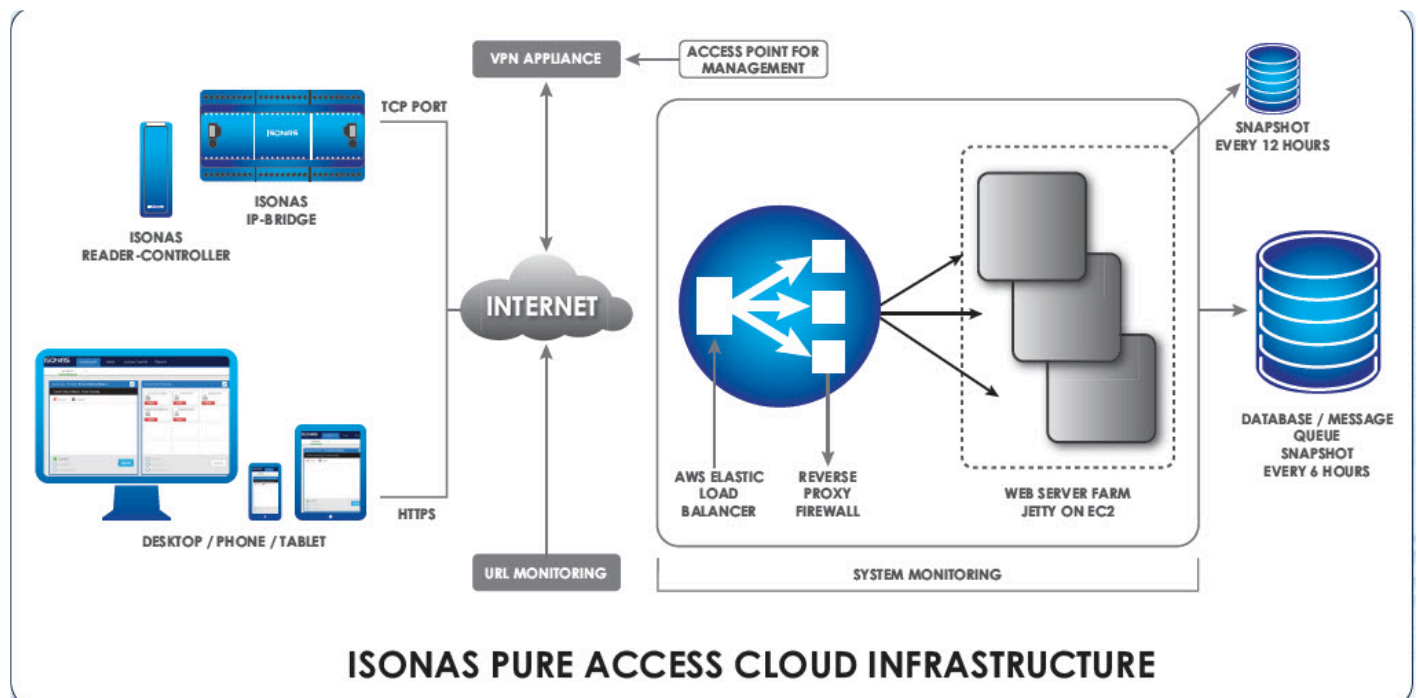
Pure Access Cloud is a web-based platform hosted by ISONAS through *Amazon Web Services (AWS)*. The infrastructure uses a *PostgreSQL* database on a Windows server (on premise version only). The web application is written in *Java* and served up by *Apache Tomcat*.

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



3.1.1. Pure Access Cloud License Renewal FAQ

How do I renew my license?

The best way to renew your Pure Access Cloud license is to contact the original installer you purchased the license from. Upon registration, their information was added under the settings tab in the Pure Access software.

If you select settings, you should see **Integrator Information** with the populated data.

ISONAS PUREACCESS Tenants ▾

TENANT INFORMATION **INTEGRATOR INFORMATION** GLOBAL SETTINGS AREAS

Contact Name
Your Integrator's Name

Contact Email
integrator.email@example.com

Company Name
Integrator's Company

Street Address

City

State/Province

Zip/Postal Code

Phone Number

How do I know when my license is due?

All administrators on the account will receive email reminders at 60, 30, 15 and 5 days that the license is due for renewal. These notifications will be sent to the web access email address that was set up on their user profile.

In addition, a notification banner will populate in the application showing how many days are left until the license is due for renewal.

To view the license expiration date, navigate to the **Tenant Information** section within the tenant's settings. Here the license type, license key, and the expiration date are all listed for you.

How do I know what license I have?

This information is housed in the **Tenant Information** section within the tenant's settings. The license type will reflect the application, so in this instance Pure Access Cloud and then the number of doors your license allows.

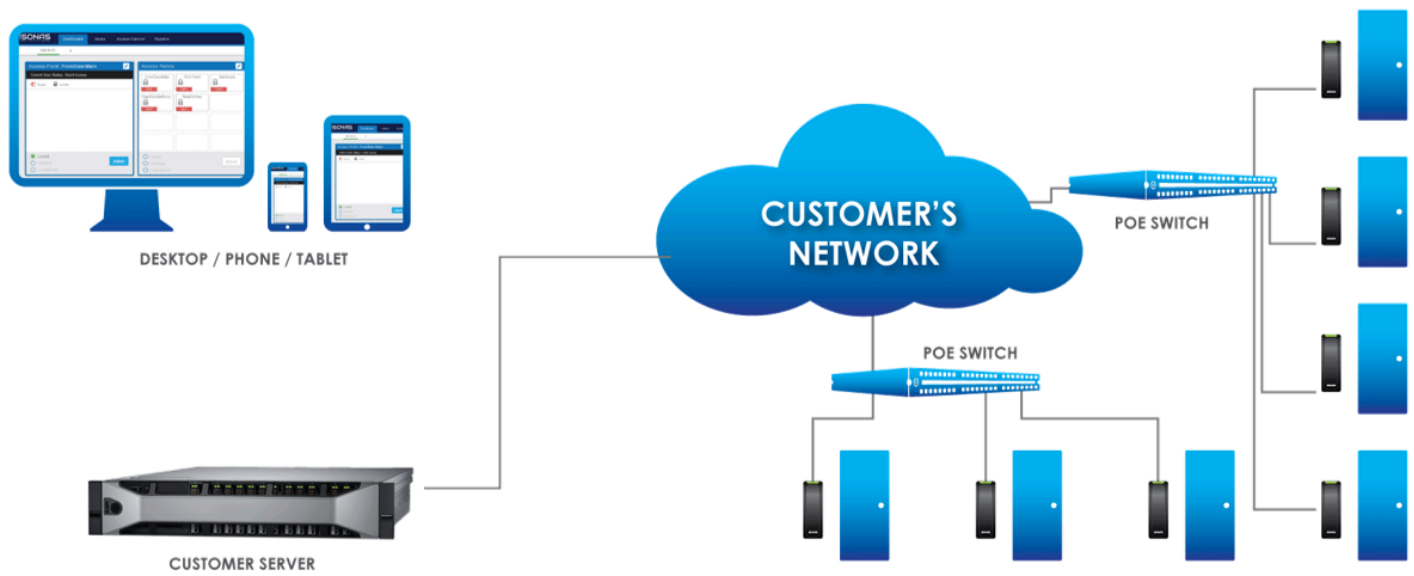
How do I update my contact information?

Simply select the settings button and you can update the tenant information or integrator information at any time. Please note you must have administrator access to update this information.

What if I don't know who my installer is?

No problem if the integration information is not completed in your application, feel free to give us a call at 800-581-0083 and we can assist with connecting you to your installer.

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

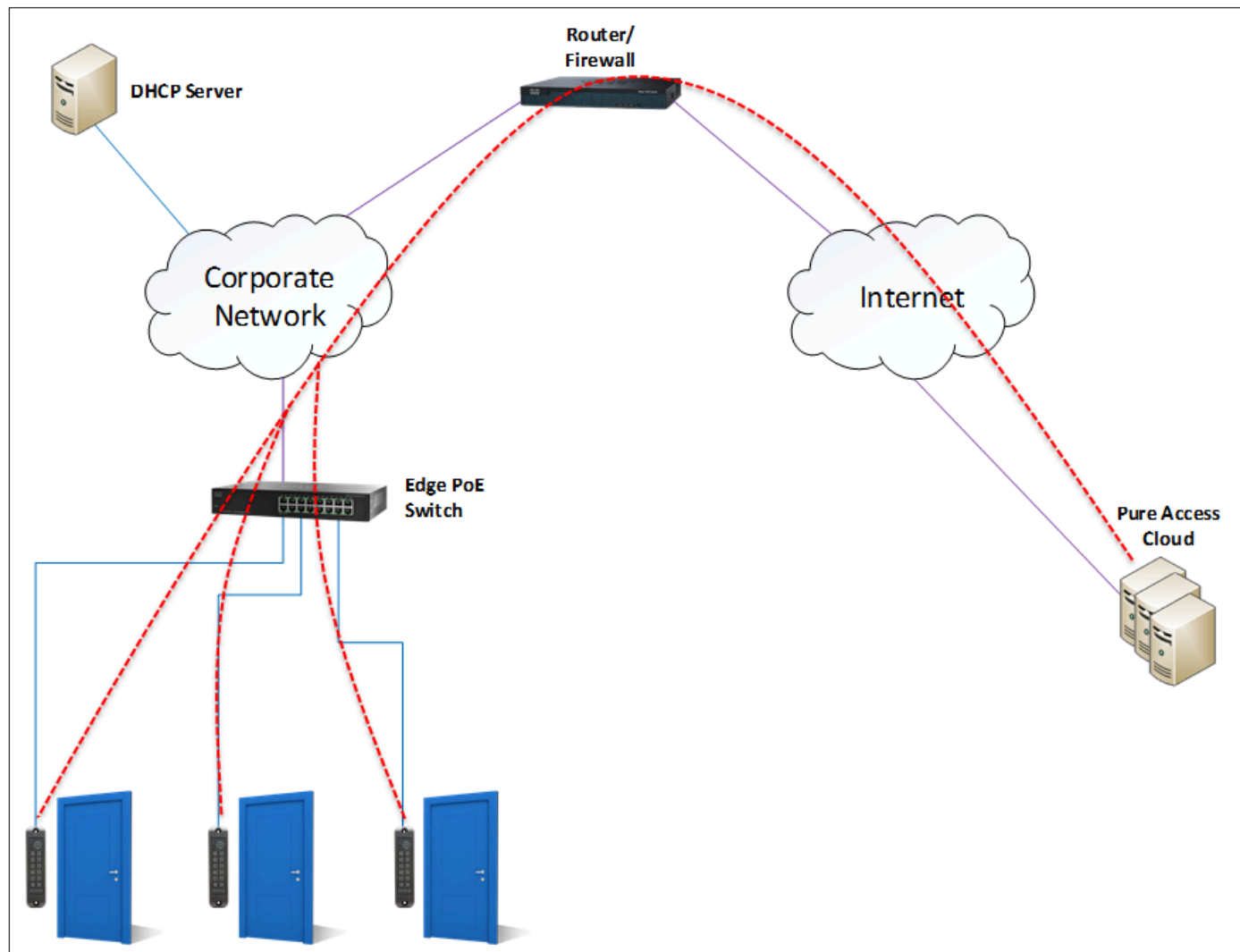


Figure 3 – Reader-controller Connections

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 *app.pureaccess.com*. Both UDP and TCP should be allowed to pass. *app.pureaccess.com* resolves to a [CloudFlare IP Address](#)

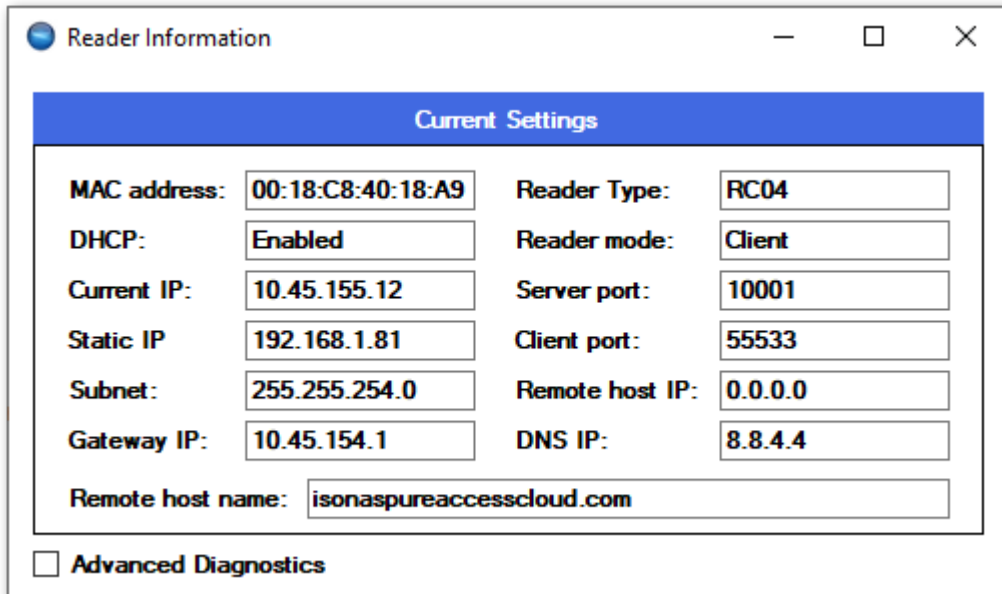
4.1.4. Additional Troubleshooting

General

- Do you have **port 55533** open to the internet or at least open to **app.pureaccess.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 **app.pureaccess.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 blue header bar. Below the header, there is a section titled "Current Settings" with a blue background. This section contains two columns of settings, each with a label and a text input field. The settings are: MAC address (00:18:C8:40:18:A9), DHCP (Enabled), Current IP (10.45.155.12), Static IP (192.168.1.81), Subnet (255.255.254.0), Gateway IP (10.45.154.1), Reader Type (RC04), Reader mode (Client), Server port (10001), Client port (55533), Remote host IP (0.0.0.0), DNS IP (8.8.4.4), and Remote host name (isonaspureaccesscloud.com). At the bottom of the window, there is a checkbox labeled "Advanced Diagnostics" which is currently unchecked.

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

☐ Advanced Diagnostics

- 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 as the host address (click "*Specify Host IP Address*" in [the configuration tool](#)).
 - You can find the public IP address of our Cloud environment via command prompt by typing ***nslookup app.pureaccess.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.
- Pure Access Cloud runs on Cloudflare. If firewall exceptions need to be made, you can find a list of [Cloudflare's IP address ranges here](#).
- 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.

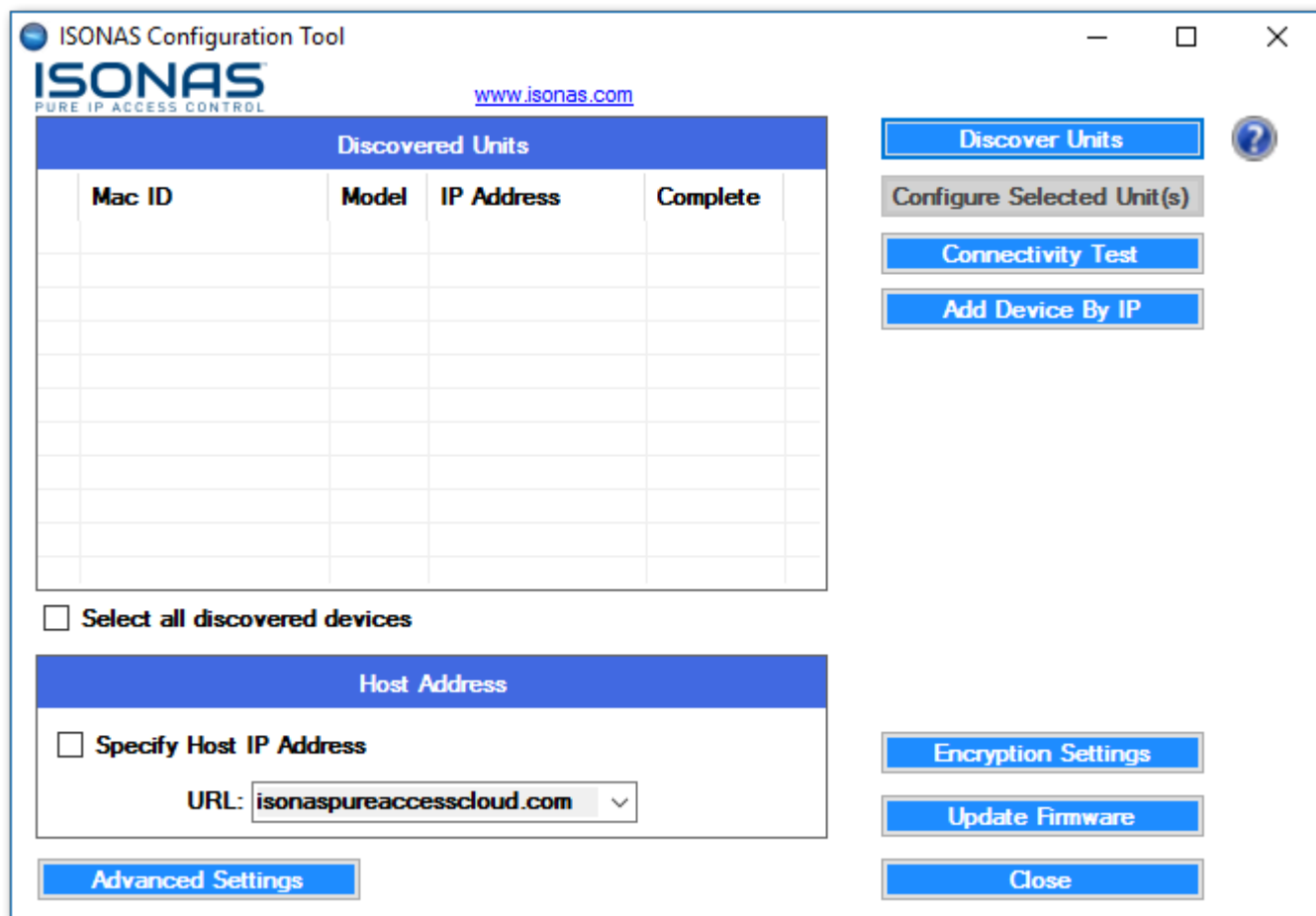
Additional Hardware Resources (optional)


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  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

ISONAS
PURE IP ACCESS CONTROL

www.isonas.com

	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

Discover Units

Configure Selected Unit(s)

Connectivity Test

Add Device By IP

Encryption Settings

Update Firmware

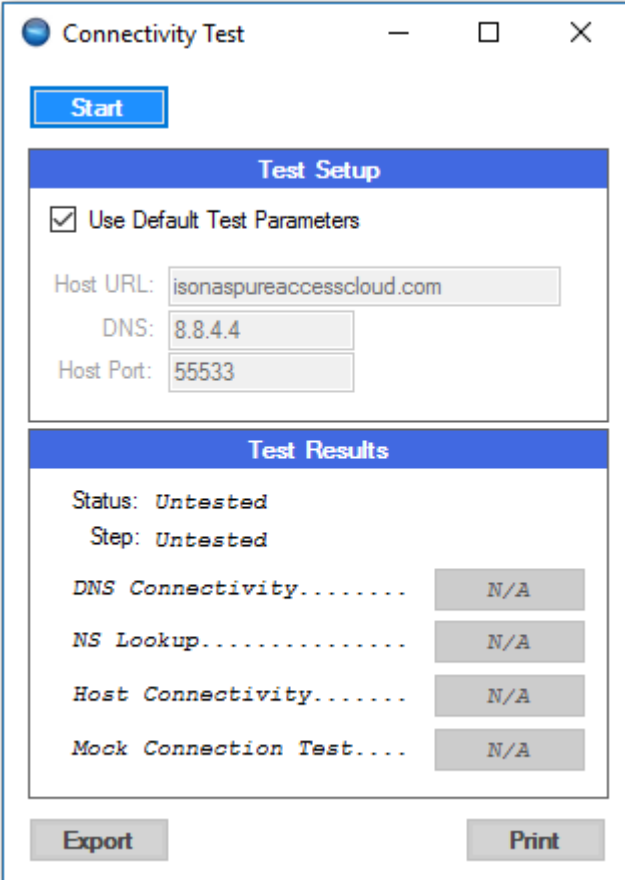
Close



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:



The image shows a 'Connectivity Test' window with a blue title bar and standard window controls. It contains a 'Start' button, a 'Test Setup' section with a checked 'Use Default Test Parameters' option and input fields for Host URL, DNS, and Host Port, and a 'Test Results' section showing a table of test results. At the bottom are 'Export' and 'Print' buttons.

Test Setup	
<input checked="" type="checkbox"/> Use Default Test Parameters	
Host URL:	isonaspureaccesscloud.com
DNS:	8.8.4.4
Host Port:	55533

Test Results	
Status:	Untested
Step:	Untested
DNS Connectivity.....	N/A
NS Lookup.....	N/A
Host Connectivity.....	N/A
Mock Connection Test....	N/A

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](#).

ISONAS Configuration Tool

PURE IP ACCESS CONTROL

[www.isonas.com](#)

Discovered Units				
Mac ID	Model	IP Address	Complete	

☐ Select all discovered devices
☒ Manually Change Connectivity Mode

Set Connectivity Mode

☒ Client Mode ☐ Server Mode

Host Address

☐ Specify Host IP Address

URL: ▾
 DNS:
 Port:

☒ Change Network Addressing ☐ Show Reader Info

Set Network Addressing

☒ DHCP
☐ Static IP

Configure Network

Reader Communication Settings

IP Address:

Subnet:

Gateway:

Discover Units

Configure Selected Unit(s)

Connectivity Test

Add Device By IP

Basic Settings
Encryption Settings
Update Firmware
Close

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*. [**Note: This environment has been deprecated.**]

The screenshot shows the 'Host Address' configuration window. 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 'Custom Host URL...' option. On the left side of the window, there is a button labeled 'Advanced Set'.

- c. If your tenant is on our legacy environment, this will need to be *isonaspureaccess.com*. [**Note: This environment has been deprecated.**]
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' configuration window. The checkbox labeled 'Specify Host IP Address' is now checked. Below this, the 'IP Addr:' field is empty and ready for input. The 'Advanced Set' button is still visible on the left.

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.

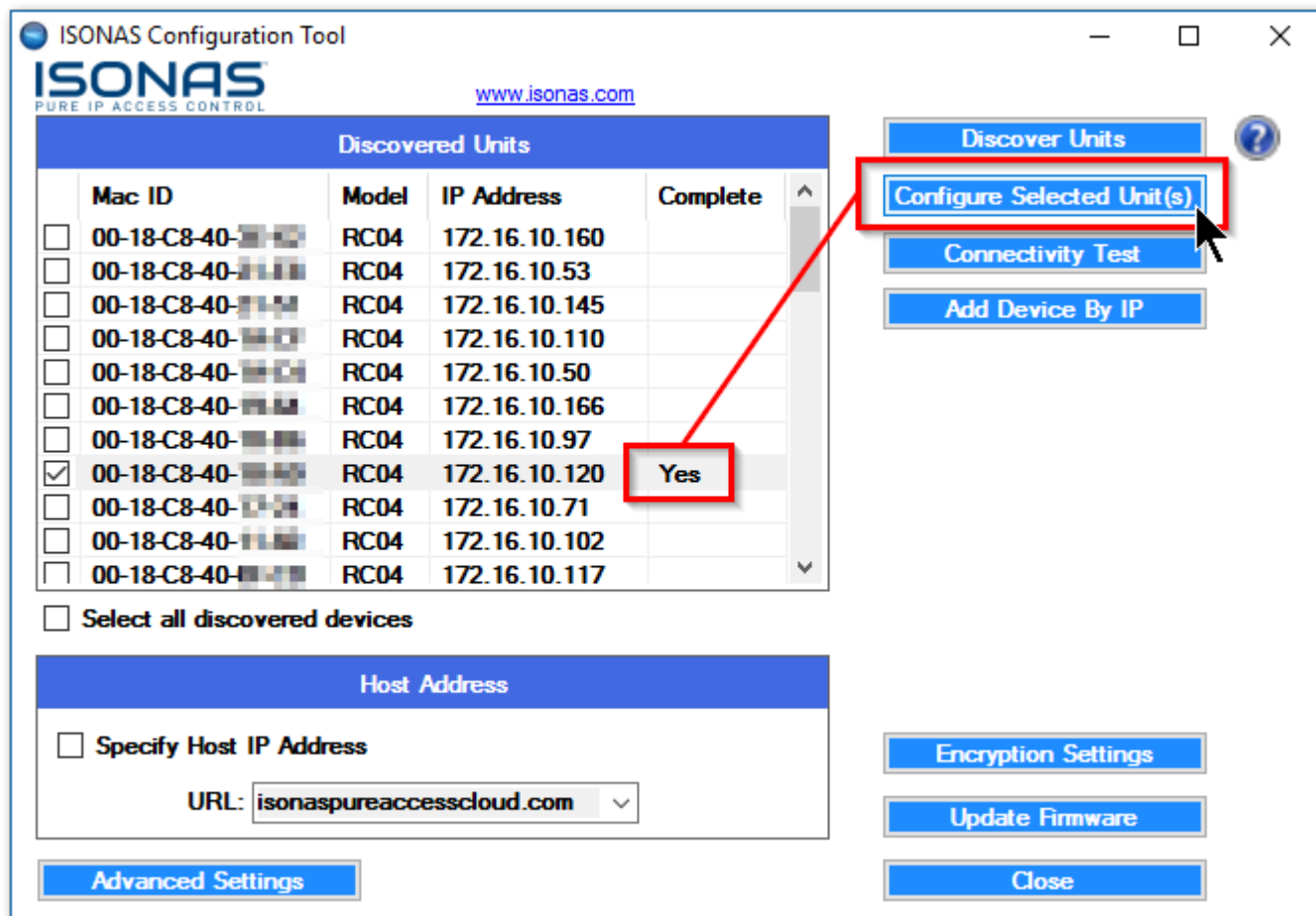


Figure 8 – Configure Selected Unit

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**”

ISONAS Configuration Tool

www.isonas.com

Discovered Units

	Mac ID	Model	IP Address	Complete
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.160	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.53	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.145	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.110	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.50	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.166	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.97	
<input checked="" type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.120	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.71	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.102	
<input type="checkbox"/>	00-18-C8-40-...	RC04	172.16.10.117	

☐ Select all discovered devices

☒ Manually Change Connectivity Mode

Set Connectivity Mode

☒ Client Mode ☐ Server Mode

Host Address

☐ Specify Host IP Address

URL:

DNS:

Port:

☒ Change Network Addressing ☐ Show Reader Info

Set Network Addressing

☒ DHCP ☐ Static IP

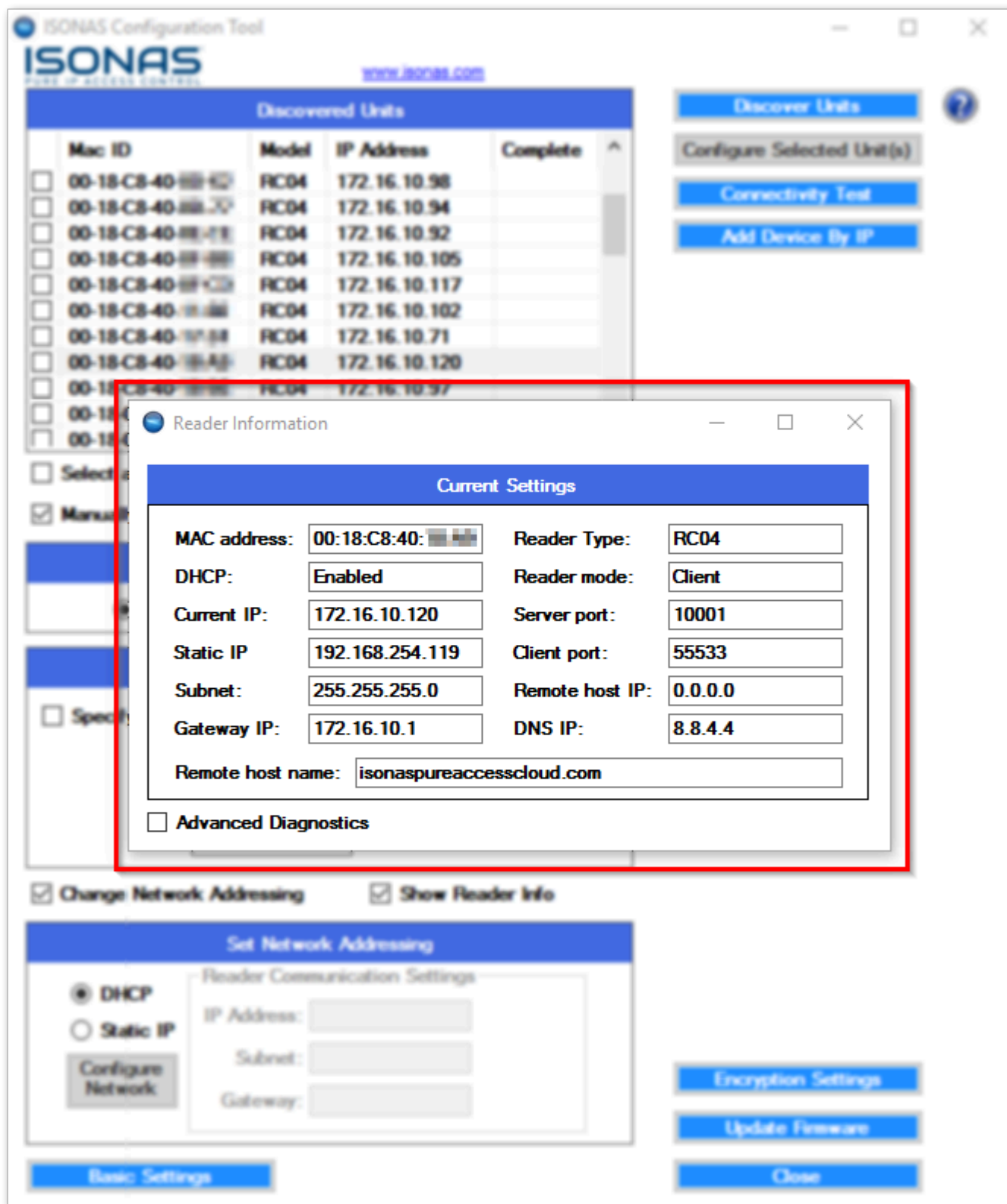
Reader Communication Settings

IP Address:

Subnet:

Gateway:

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



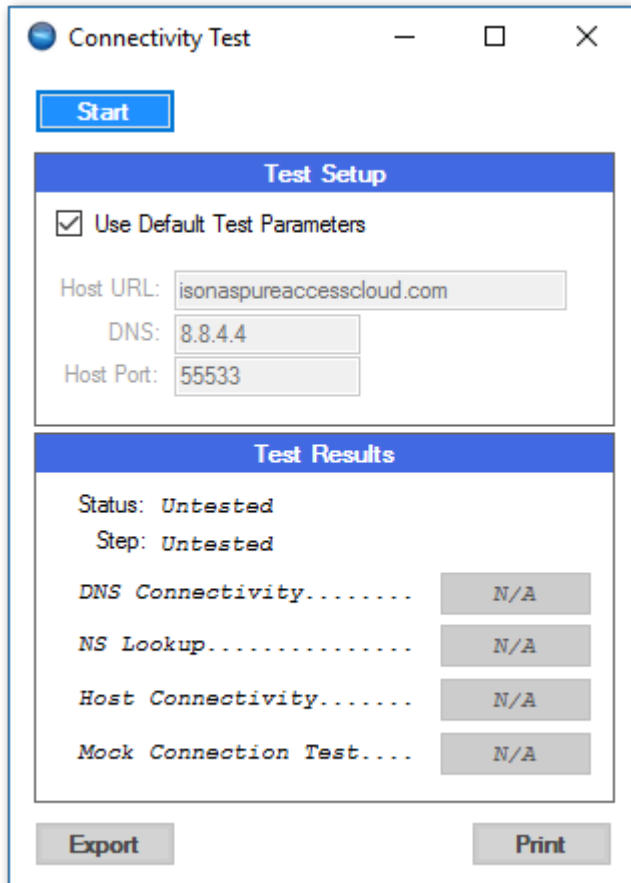
How the device is currently configured



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.

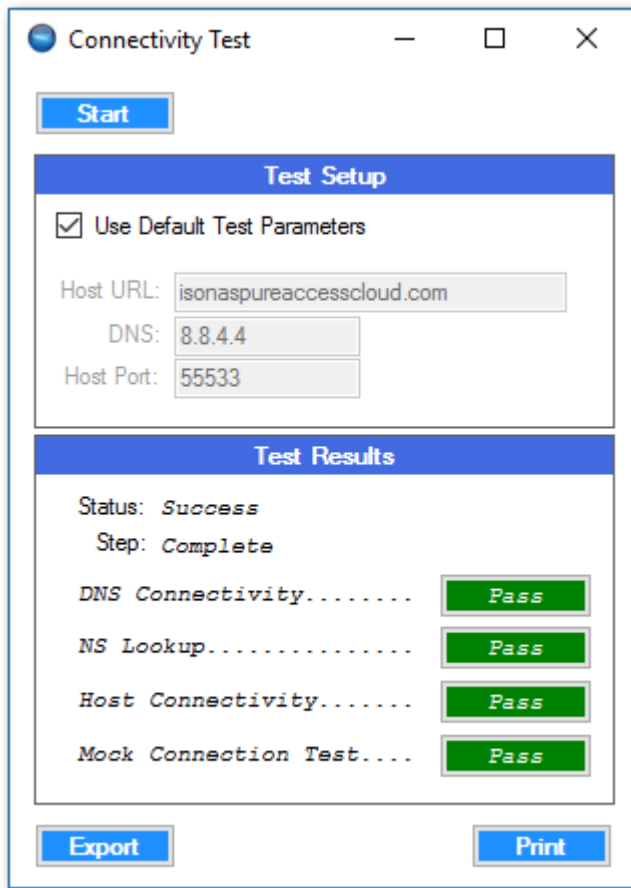


The screenshot shows a window titled "Connectivity Test" with a "Start" button at the top left. Below the button is a "Test Setup" section with a checked checkbox "Use Default Test Parameters". Under this, there are three input fields: "Host URL" with the value "isonaspureaccesscloud.com", "DNS" with the value "8.8.4.4", and "Host Port" with the value "55533". Below the "Test Setup" section is a "Test Results" section. It displays "Status: Untested" and "Step: Untested". Below these are four rows of test results, each with a label and a value in a grey box: "DNS Connectivity....." with "N/A", "NS Lookup....." with "N/A", "Host Connectivity....." with "N/A", and "Mock Connection Test...." with "N/A". At the bottom of the window are two buttons: "Export" and "Print".

Test Results	
Status:	Untested
Step:	Untested
DNS Connectivity.....	N/A
NS Lookup.....	N/A
Host Connectivity.....	N/A
Mock Connection Test....	N/A

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 screenshot shows a window titled "Connectivity Test" with a blue header bar. Below the header is a "Start" button. The main content area is divided into two sections: "Test Setup" and "Test Results".

Test Setup

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

Test Results

Status: *Success*
Step: *Complete*


DNS Connectivity.....	<input type="button" value="Pass"/>
NS Lookup.....	<input type="button" value="Pass"/>
Host Connectivity.....	<input type="button" value="Pass"/>
Mock Connection Test....	<input type="button" value="Pass"/>

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

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.



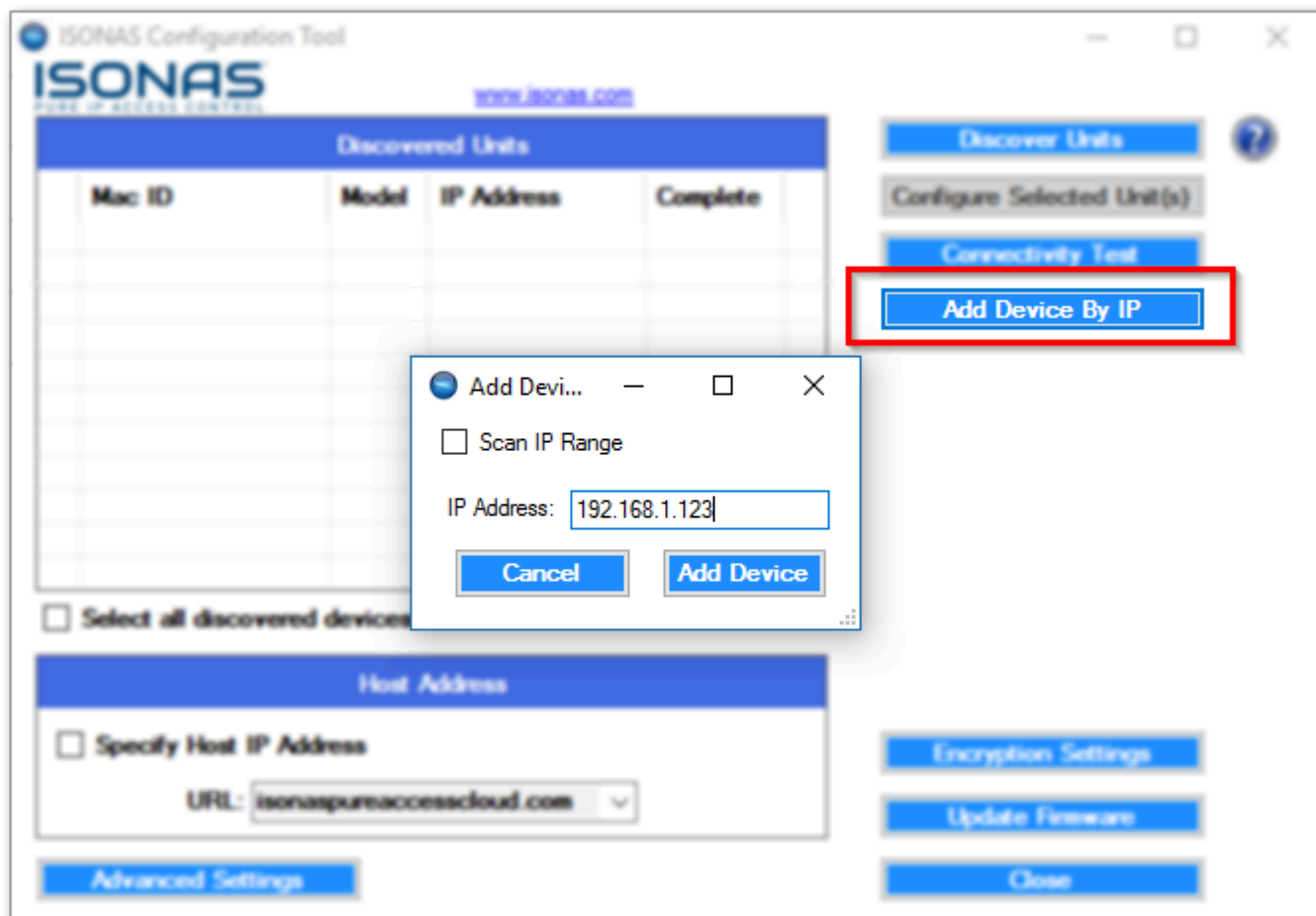
Fully booted RC-03



Fully booted IP-Bridge

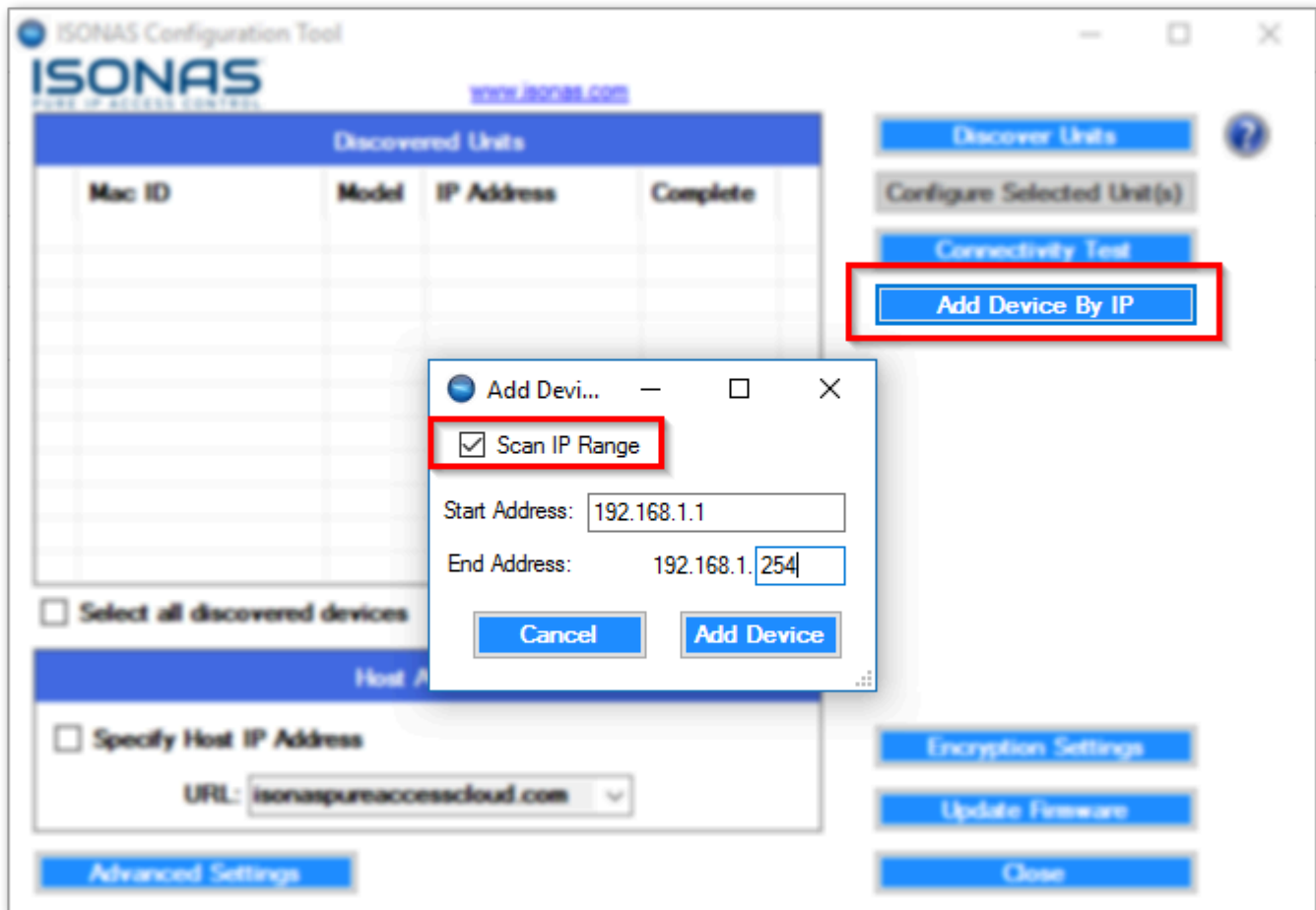
4.2.2.1. Find device by IP

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

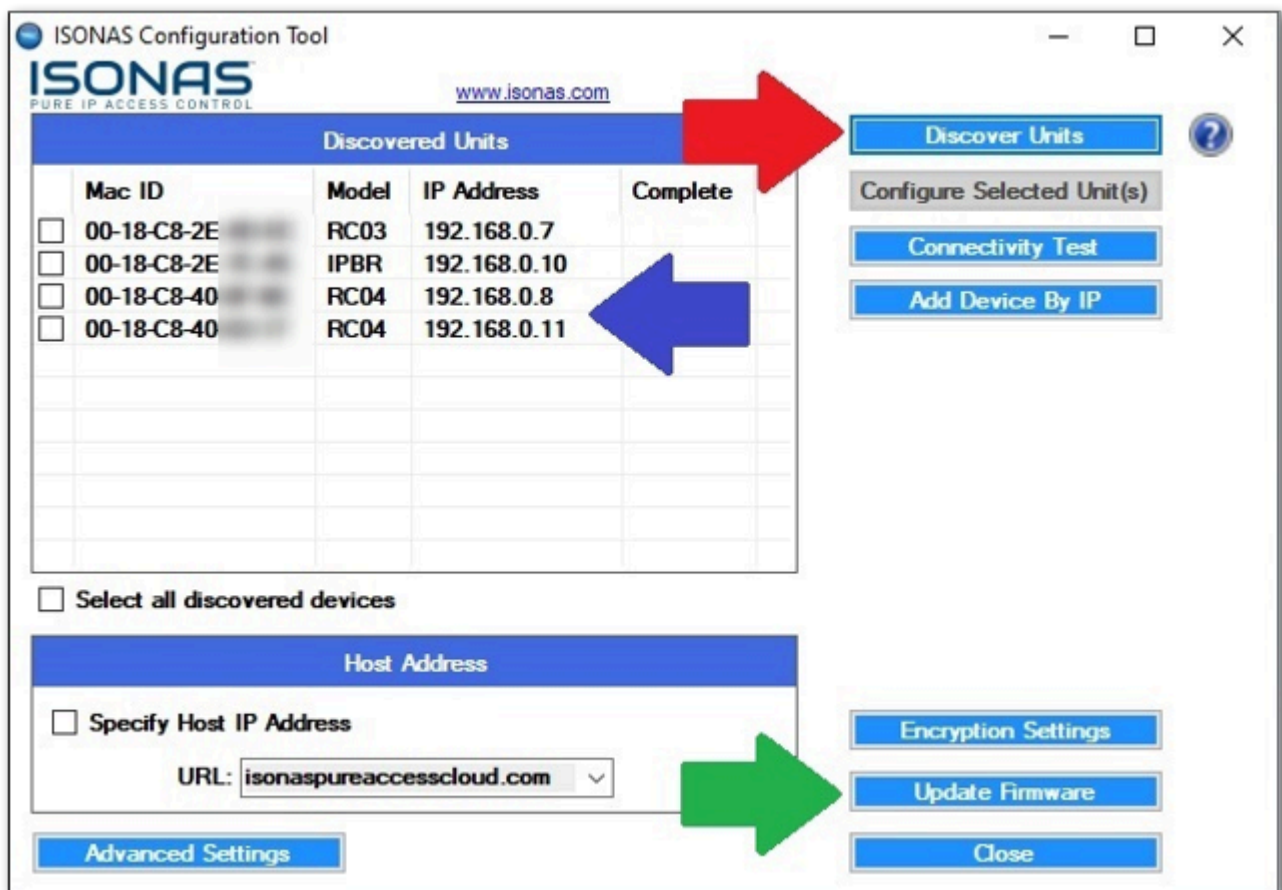
There are two necessary components for updating firmware on your ISONAS hardware:

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

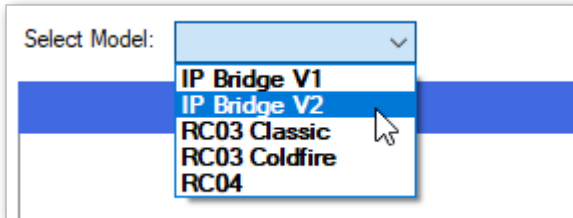
1. Download and unzip the latest firmware files onto your machine.
2. Launch the ISONAS hardware configuration tool and then click the **Discover Units** button to populate a list of devices on your network (**red arrow below**).



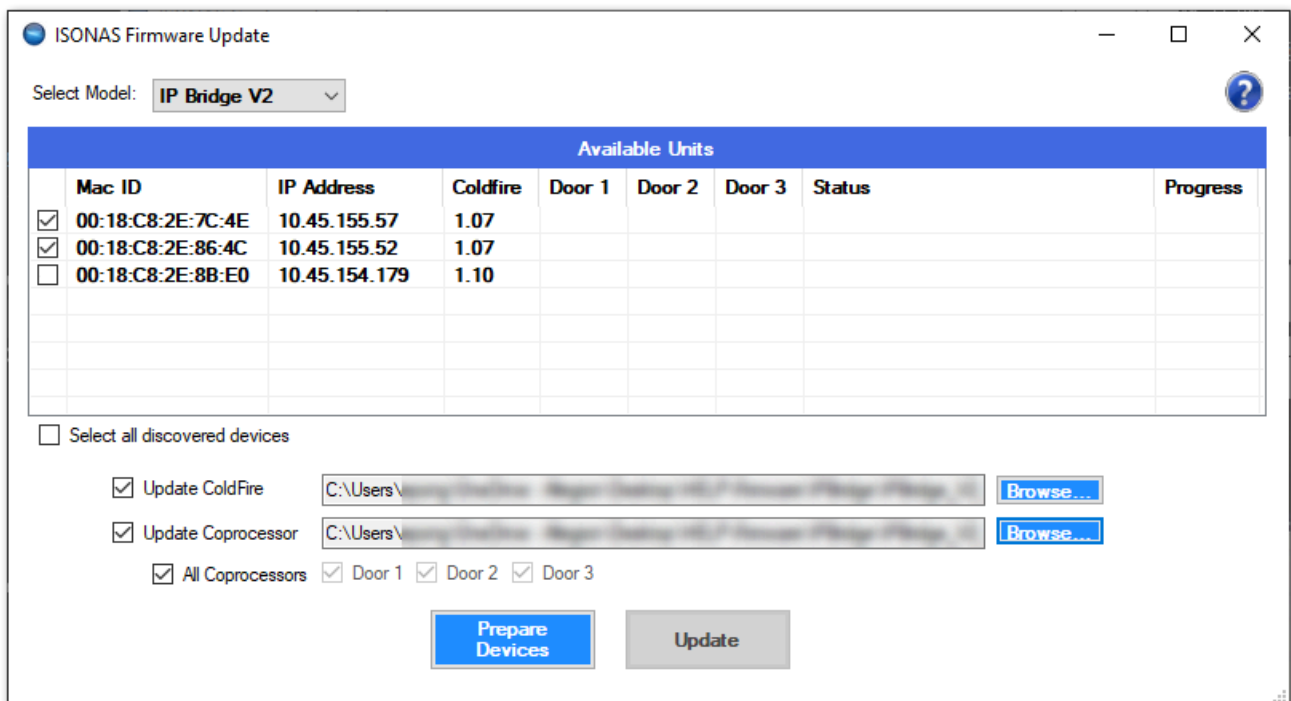
- a. If devices do not appear in this list, the computer in use is either not on the same VLAN as the readers or is on a different subnet. Try connecting the computer to a different VLAN

connection until the devices can be discovered.

3. Once devices have been discovered (**blue arrow above**), select **Update Firmware** to open the firmware update window (**green arrow above**).
4. Select your device's model from the "Select Model" drop-down menu.



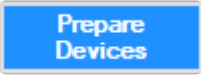
- a. The device(s) should populate the "Available Units" field.
- b. Note that the ColdFire version displayed will confirm whether the Coprocessor needs to be loaded.
 - i. With an IP-Bridge v2 on ColdFire version **1.07 or lower**, the Coprocessor will need to be updated to v1.03 (current as of ColdFire v1.19).
 - ii. With an IP-Bridge v2 on a ColdFire version **higher than 1.07**, the Coprocessor updates are not necessary.
5. Use the check-boxes to select the device(s) that need to be updated.
6. Click **Browse...** 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".

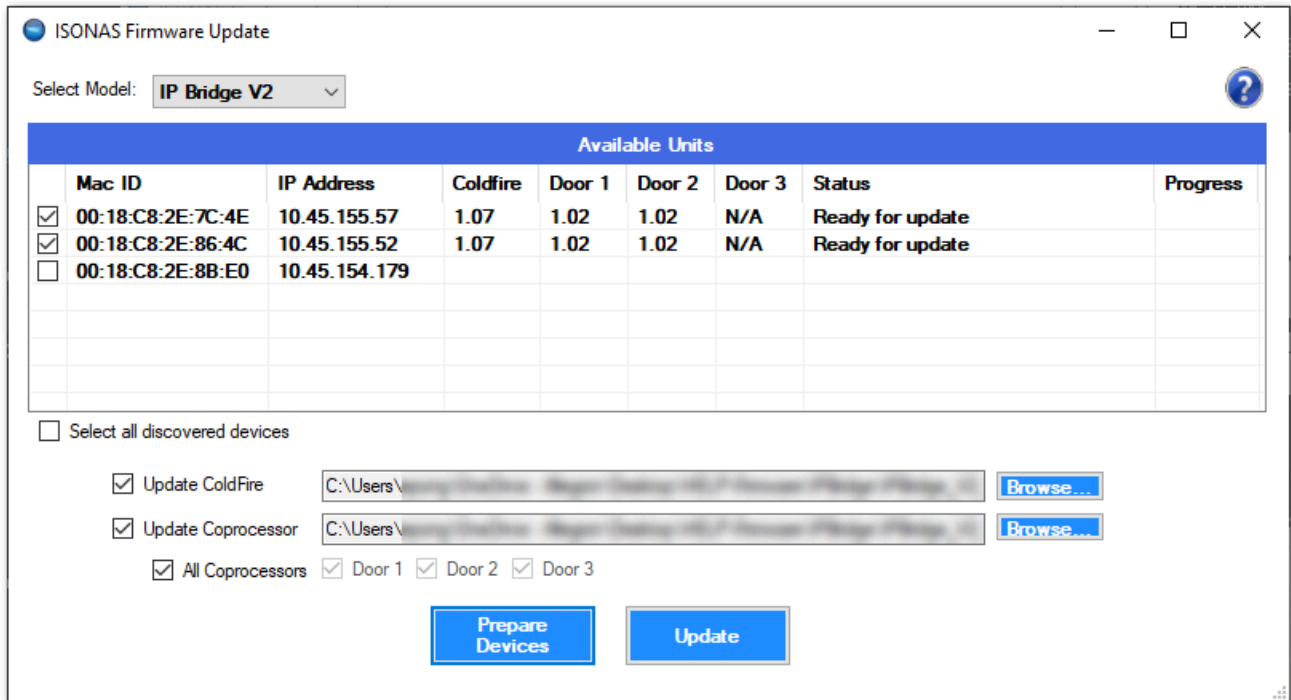


- a. For RC-03's: Select **Update ColdFire** as well as **Update Coprocessor**. Both of these will

need to be updated.

- b. For RC-04's: Select **Update ColdFire**. See note below for more information.
- c. For IP-Bridges: **Only update the Coprocessor if it is out-of-date**. Please review [this article](#) as it contains important information regarding when to update the Coprocessor.

8. 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.



ISONAS Firmware Update

Select Model: **IP Bridge V2**

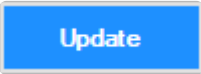
Available Units								
	Mac ID	IP Address	Coldfire	Door 1	Door 2	Door 3	Status	Progress
<input checked="" type="checkbox"/>	00:18:C8:2E:7C:4E	10.45.155.57	1.07	1.02	1.02	N/A	Ready for update	
<input checked="" type="checkbox"/>	00:18:C8:2E:86:4C	10.45.155.52	1.07	1.02	1.02	N/A	Ready for update	
<input type="checkbox"/>	00:18:C8:2E:8B:E0	10.45.154.179						

☐ Select all discovered devices

☒ Update ColdFire

☒ Update Coprocessor

☒ All Coprocessors ☒ Door 1 ☒ Door 2 ☒ Door 3

9. Click 
10. 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 checked="" type="checkbox"/>	00:18:C8:2E:7C:4E	10.45.155.57	1.19	1.03	1.03	N/A	Complete	100%
<input checked="" type="checkbox"/>	00:18:C8:2E:86:4C	10.45.155.52	1.19	1.03	1.03	N/A	Complete	100%
<input type="checkbox"/>	00:18:C8:2E:8B:E0	10.45.154.179						

☐ Select all discovered devices

☒ Update ColdFire

C:\Users\... \Program Files (x86) ISONAS Firmware Update V2

Browse...

☒ Update Coprocessor

C:\Users\... \Program Files (x86) ISONAS Firmware Update V2

Browse...

☒ All Coprocessors
 ☒ Door 1
 ☒ Door 2
 ☒ Door 3

Prepare Devices

Update

- ✿ 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.

4.3.1. IP-Bridge Firmware Information

2-Door IP-Bridges

Unlike the 3-Door variant, a 2-Door bridge will display “N/A” in the *Door 3* column. This is normal.

ISONAS Firmware Update

Select Model: **IP Bridge V2**

Available Units								
	Mac ID	IP Address	Coldfire	Door 1	Door 2	Door 3	Status	Progress
<input checked="" type="checkbox"/>	00:18:C8:2E:7C:4E	10.45.155.57	1.07	1.02	1.02	N/A	Ready for update	
<input checked="" type="checkbox"/>	00:18:C8:2E:86:4C	10.45.155.52	1.07	1.02	1.02	N/A	Ready for update	
<input type="checkbox"/>	00:18:C8:2E:8B:E0	10.45.154.179						

☐ Select all discovered devices

☒ Update ColdFire

☒ Update Coprocessor

☒ All Coprocessors ☒ Door 1 ☒ Door 2 ☒ Door 3

When to update the Coprocessor

- With an IP-Bridge v2 on ColdFire version **1.07 or lower**, the Coprocessor will need to be updated to v1.03 (current as of ColdFire v1.19).
- With an IP-Bridge v2 on a ColdFire version **higher than 1.07**, the Coprocessor updates are not necessary.



If a Coprocessor version is loaded onto a door already running that same Coprocessor, it can **break the firmware installation**. If this occurs, multiple attempts will be necessary to correctly reload the Coprocessor firmware to that door! **See the *Troubleshooting* section below for this process.**

Door displaying a question mark

If any ColdFire or Coprocessor errors on update, the device will display a “?”. See troubleshooting steps below for how to correct this.

Troubleshooting Firmware Update:

If a device displays the “**Error Updating**” message or a “?”, the firmware **MUST** be reloaded for the device to function properly:

1. If all other devices also being updated are either complete or have errored out as well, first **CLOSE** the Firmware Update tool
2. Re-open **Firmware Update**
3. Select proper **Model**
4. Select the checkmark to choose only **ONE** of the IP Bridges that failed to update completely
5. Click “**Prepare Devices**” then wait for the device to report all the firmware levels
 - a. If ColdFire failed, either the previous firmware revision will be displayed or there will be a “?”
 - b. If Coprocessor failed, the door(s) in question will display the previous firmware or a “?”
6. If ColdFire is **NOT** reporting the new revision, **ONLY** select “**Update ColdFire**”. Browse to the firmware file again, select “Open,” then click the “**Update**” button
 - a. The process should complete after a few minutes. If it errors again on ColdFire update, power cycle the IP-Bridge and try again
 - b. If still failing, try Factory Defaulting the IP-Bridge then try again
 - c. If still having issues, please call product support at 877-671-7011, opt 2, opt 3
7. Once ColdFire is correct on the device, validate which Doors are showing the previous firmware version or are reporting a “?” for firmware. **ONLY** select “**Update Coprocessor**,” uncheck “**All Coprocessors**,” and then select the Doors that still need to be updated. Click “**Update**”
 - a. The process should complete after a few minutes. If it errors again on Coprocessor update, power cycle the IP-Bridge and try again
 - b. If still failing, try Factory Defaulting the IP Bridge then try again
 - c. If still having issues, please call product support at 877-671-7011, opt 2, opt 3



The firmware update process for IP Bridges are a bit sensitive and require persistence. It can take several attempts to complete updating firmware. It will eventually complete.

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.

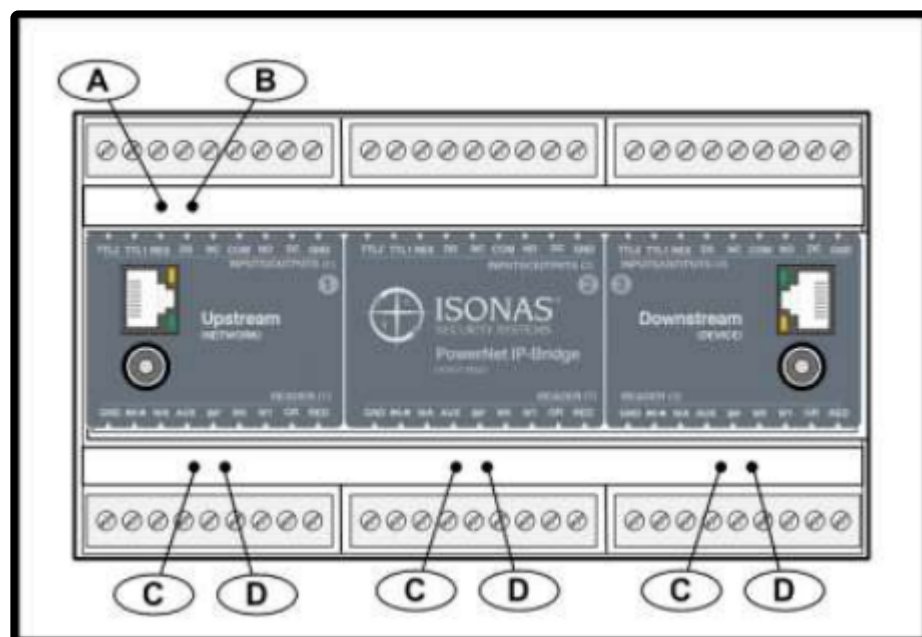
4.4.2. IP-Bridge Installation Guide

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.

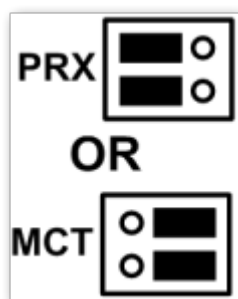
For information on how to add an RC-03 to Pure Access, please review the [Managing Access Points](#) section.

4.4.3.1. RC-03 Jumper Configurations

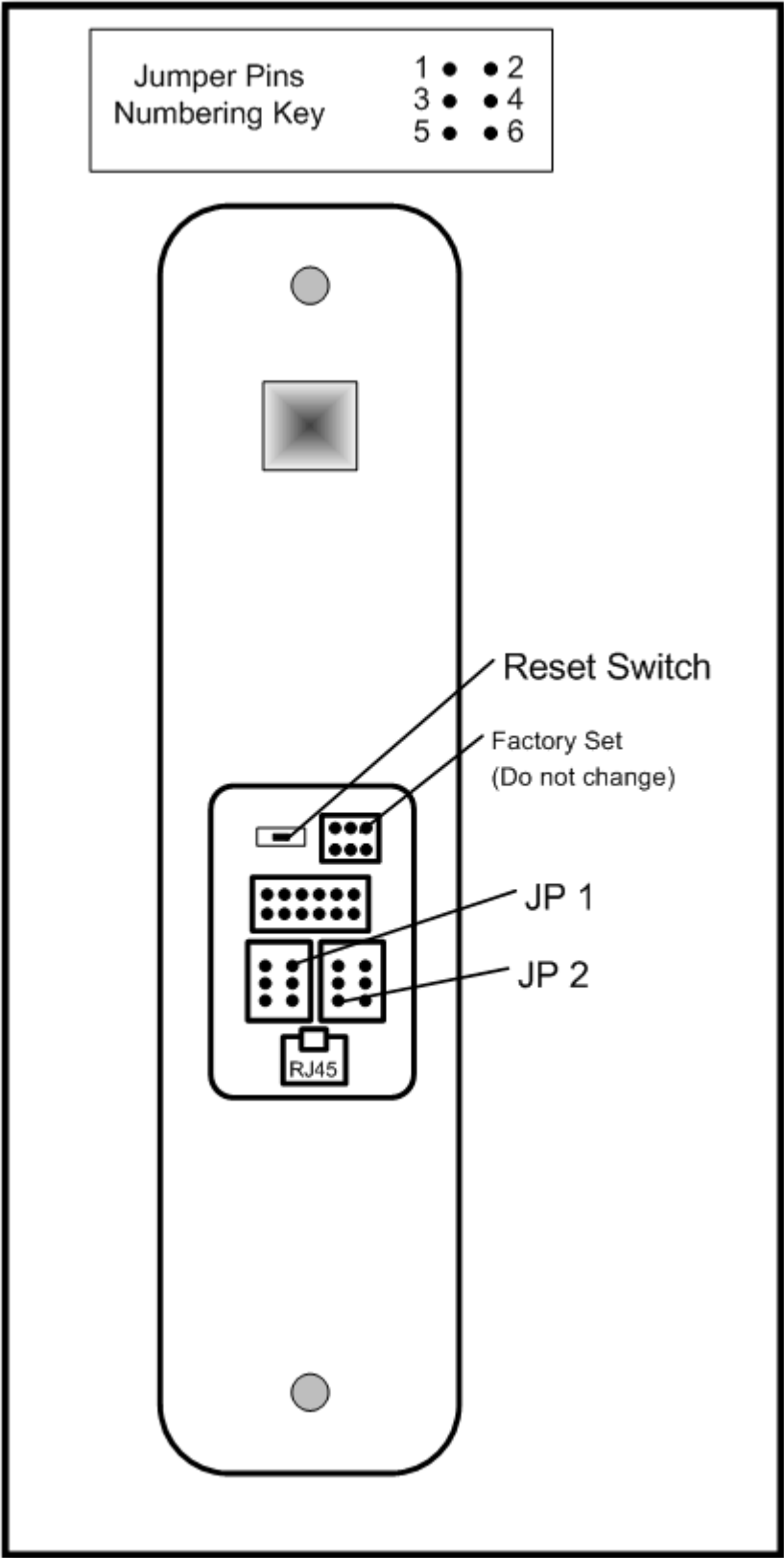
The RC-03 PowerNet reader-controller has a set of jumper pins that configure both its input power source and its lock control circuit. The device can be configured for power to be supplied to it through the 12 conductor pigtail (either 12VDC or 24VDC) or through the RJ45 connector (Power Over Ethernet).

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.


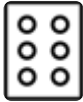
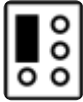

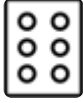
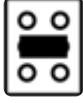


The below image shows the components on the back of the RC-03:



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](#)

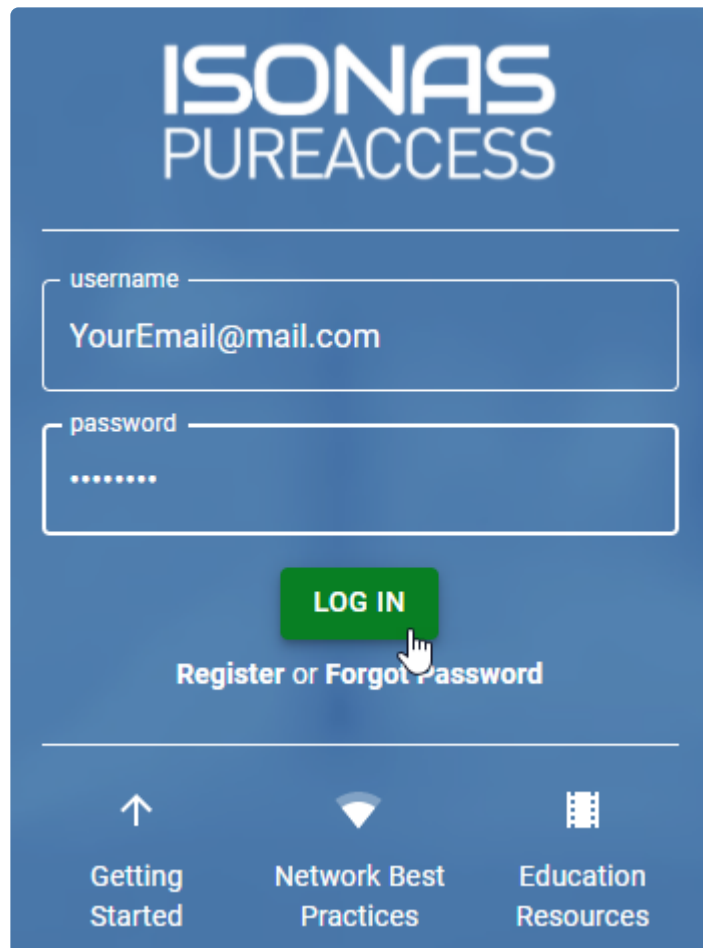
5.1. Pure Access Cloud

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://app.pureaccess.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?

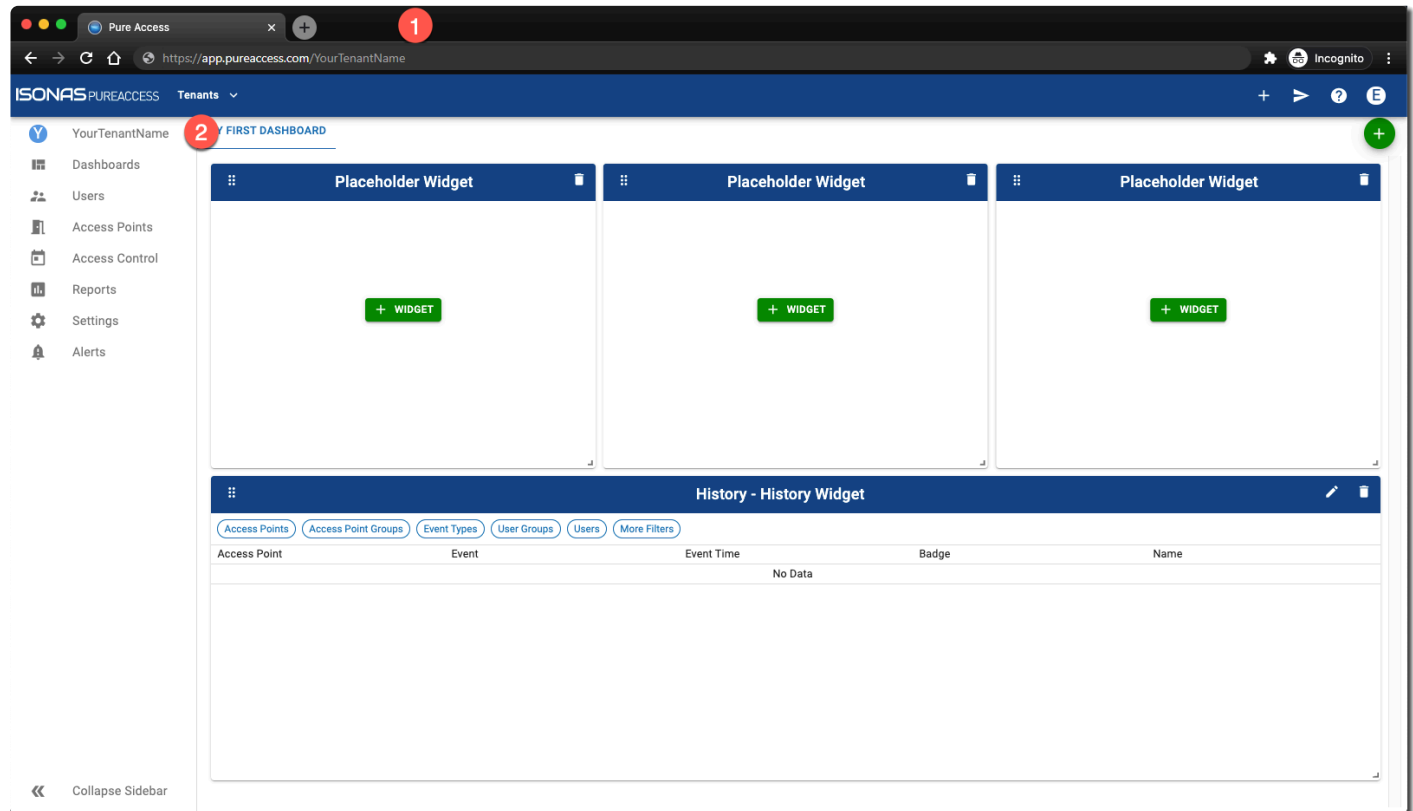
For security, we are not able to reset passwords upon request. You can reset your password by clicking on the **“Forgot Password”** link from the login page. See [next page](#) for instructions.

5.1.2. Tenant Name

What's my tenant name?

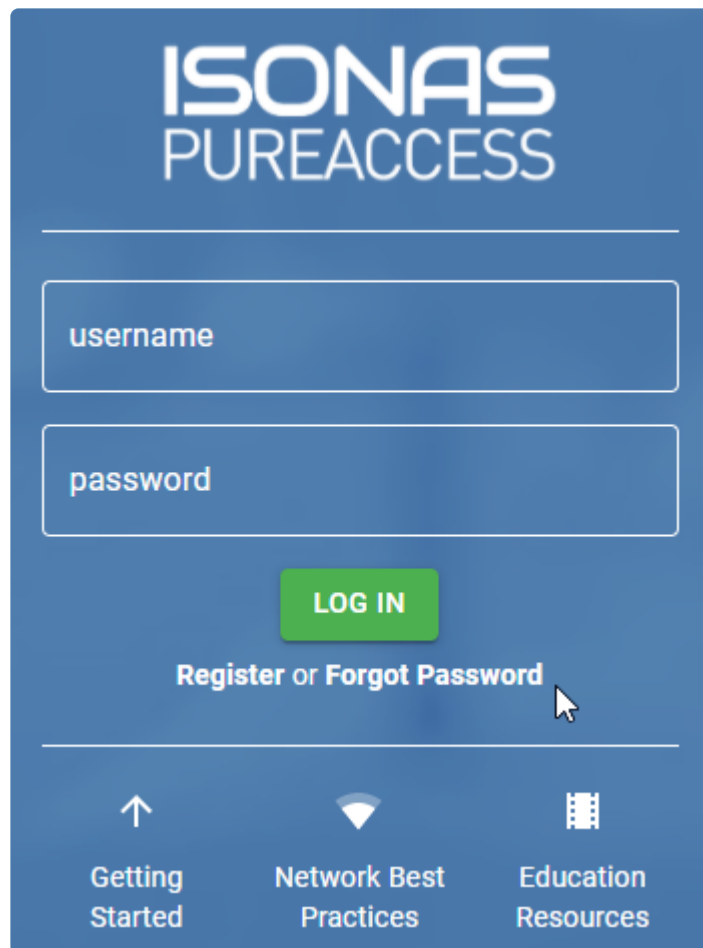
You can find the name of your tenant from two places:

1. In your address bar, immediately after “app.pureaccess.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.



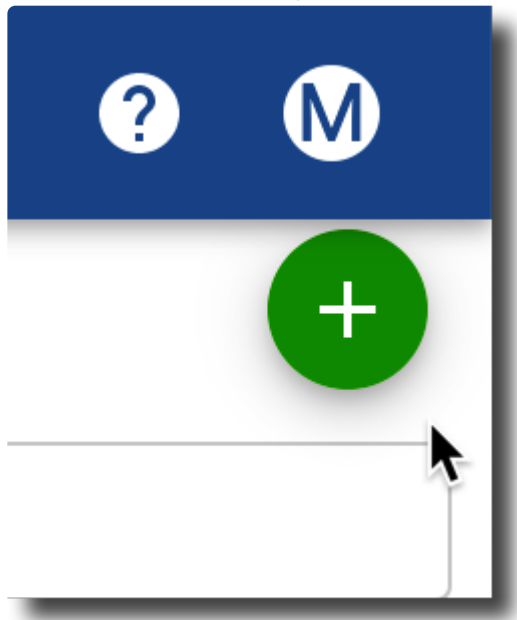
We advise against using a parent tenant for access control. Please create a new subtenant to be used for this purpose.

5.1.4.1. Creating Subtenants

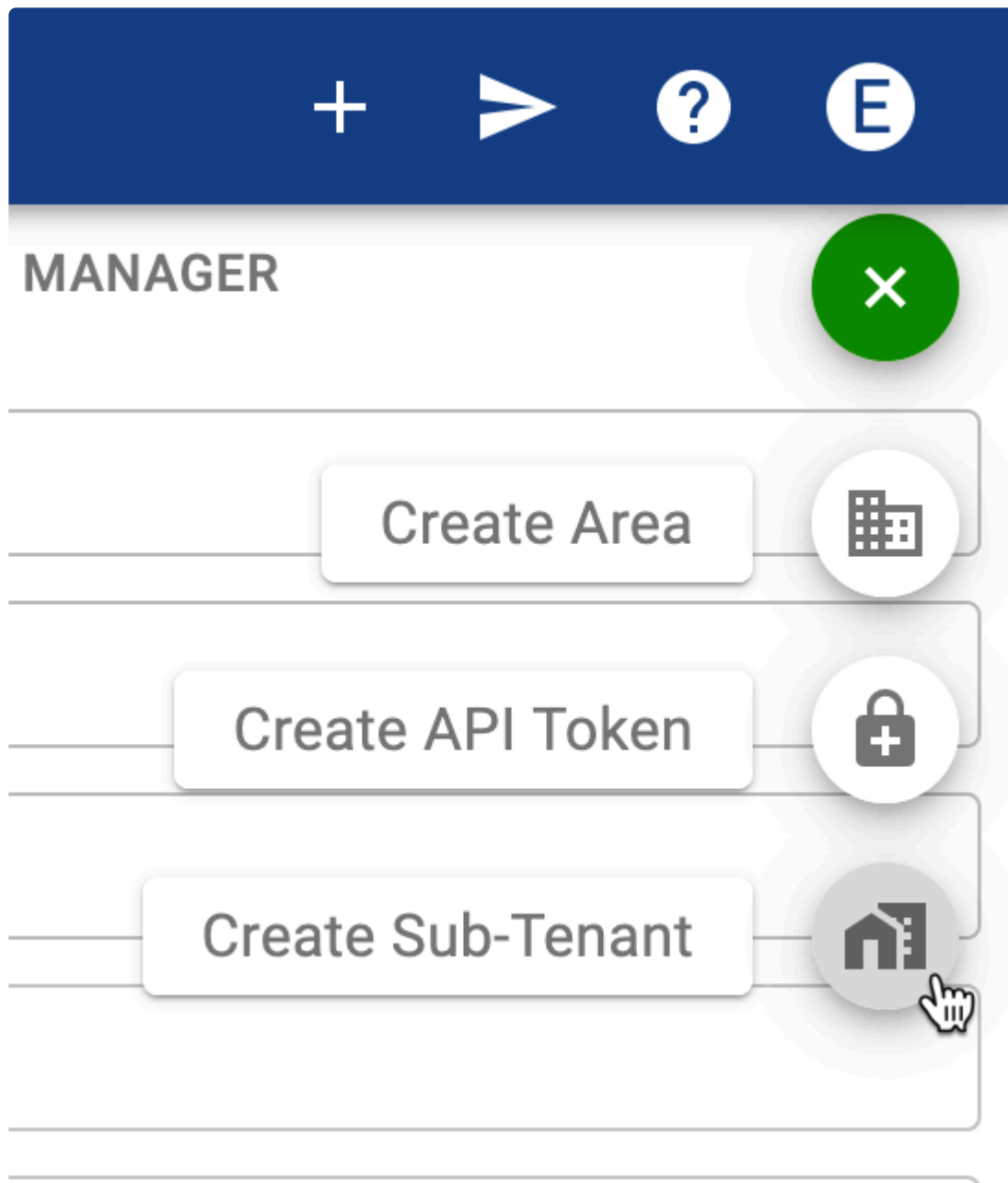
1. Navigate to **Settings**.



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 form titled "Create Tenant" with a dark blue header. The form contains several input fields arranged in two columns. The first column includes "Tenant Name", "Timezone" (a dropdown menu currently showing "(UTC-07:00) Mountain Time (US & Canada)"), "Administrator Email", "Street", and "City". The second column includes "Company Name", "Contact Name", "State/Province", "Zip/Postal Code", and "Phone number". At the bottom right of the form, there are two buttons: "CANCEL" and "CREATE". A mouse cursor is hovering over the "CREATE" button.

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

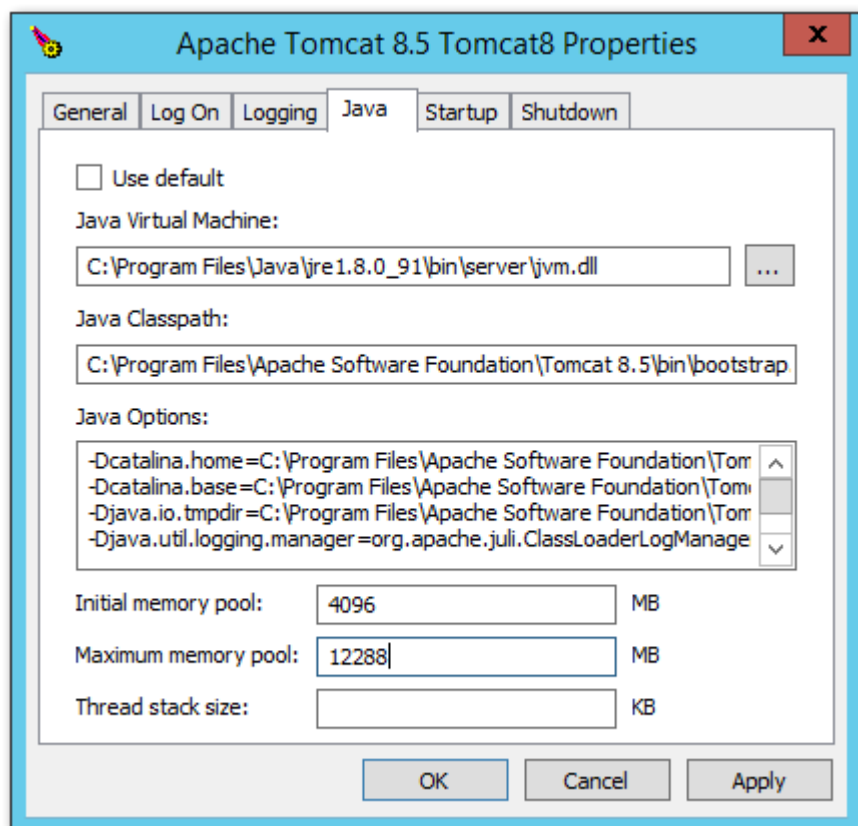
- Make sure this is a fresh installation of Windows.
 - There are many prerequisite software packages that Pure Access needs in order to function. If one of these pieces of software is already installed on the system but it is an incompatible version or if there is something using the same network ports 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

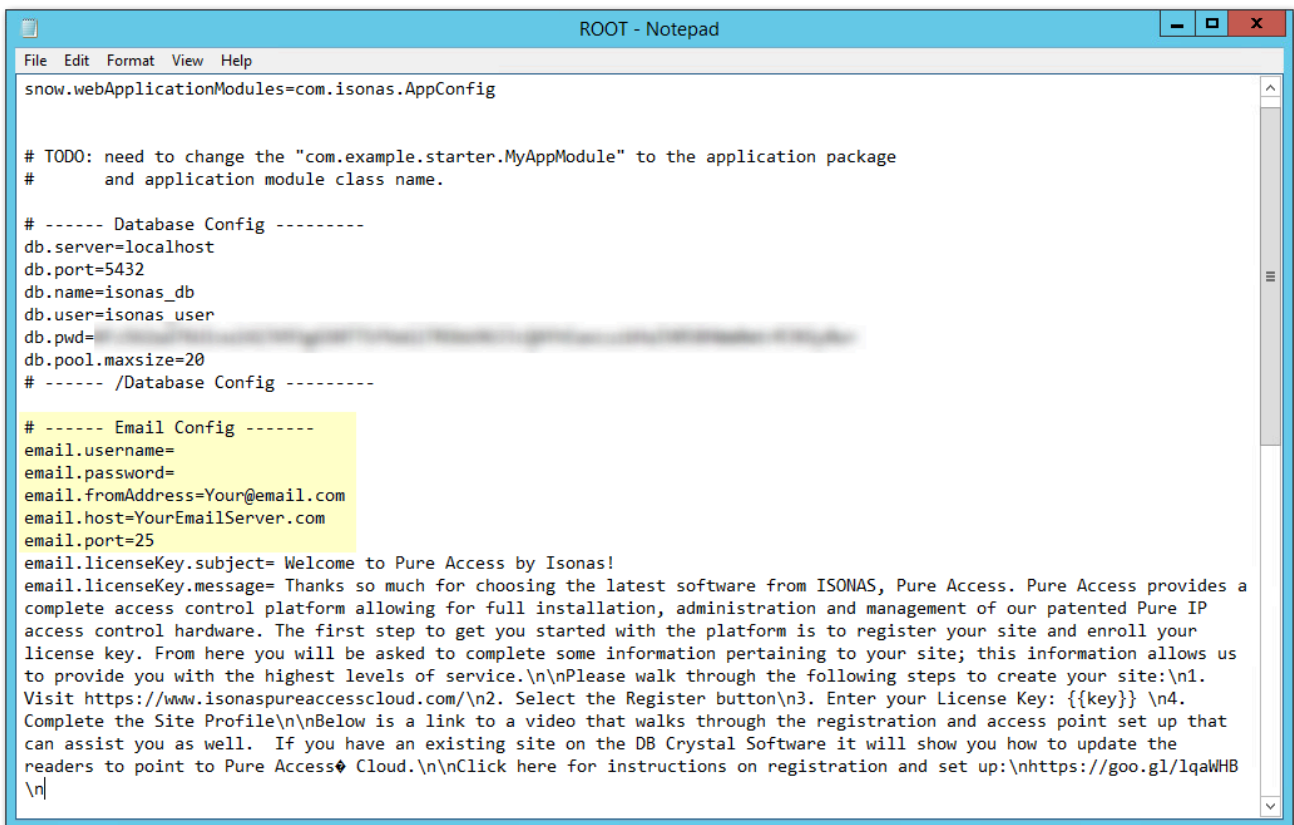


5.2.2. SMTP Configuration (Pure Access Manager)

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.\n\nPlease walk through the following steps to create your site:\n1.
Visit https://www.isonaspureaccesscloud.com/\n2. Select the Register button\n3. Enter your License Key: {{key}} \n4.
Complete the Site Profile\n\nBelow 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.\n\nClick here for instructions on registration and set up:\nhttps://goo.gl/lqaWHB
\n

```

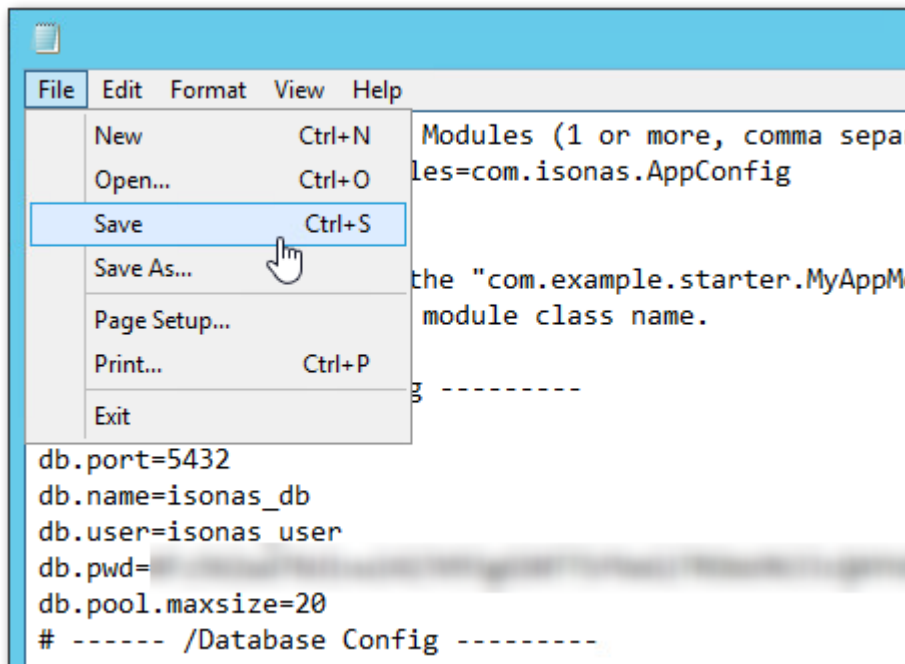
4. Additionally, you need to set the **email.file.base.path** value so that the hyperlinks within emails can direct users to the correct system. By default, this is set to **https://isonaspureaccesscloud.com**, but must be changed to the **PAM server's IP address or hostname**:

```
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 access point groups, weekly rules, etc.

1. Re-create your access point groups.
2. Re-create your weekly rules.
 - 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.
 - b. Also 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.
3. 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 migrate access points one at a time.
 - b. Once added to the new tenant, [update access points](#) and then verify that a credential is operational before proceeding.
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. PANRServ

[PANRServ Installation and Setup](#)

5.5.2. 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](#)

5.5.3. Milestone XProtect

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

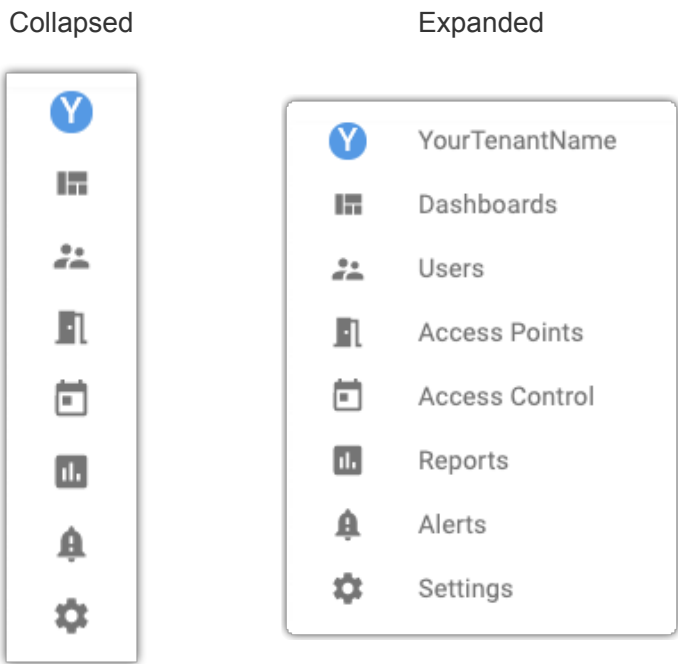
1. [ISONAS Pure Access + Milestone XProtect installation instructions](#)
2. Installation files:
 - a. [Pure Access Cloud](#)
 - b. [Pure Access Manager](#)

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.



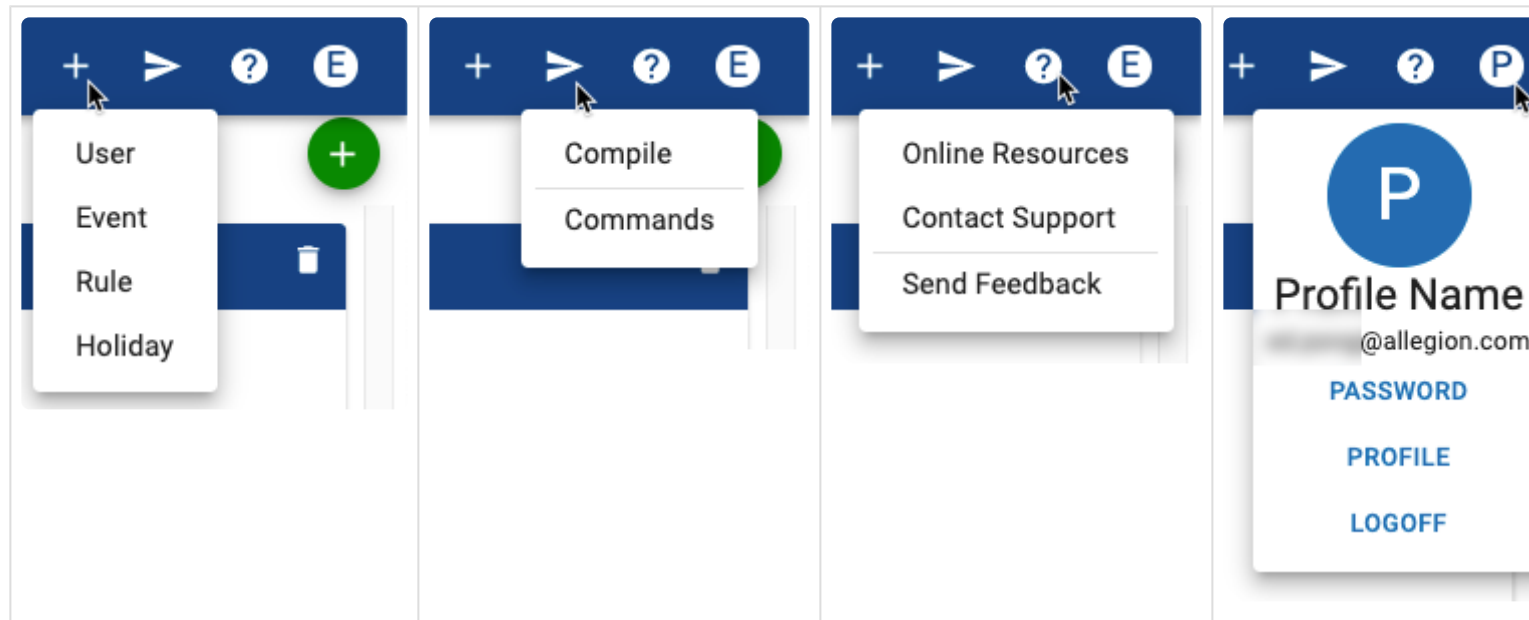
Context Menu

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



Quick Links

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



6.1. App Bar

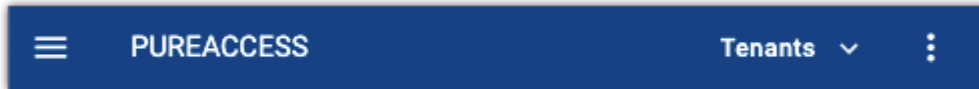
The **App Bar** in Pure Access Cloud contains buttons that allow web access users to perform operations within their tenant. This will appear slightly different depending on whether the application is being displayed in a web browser versus a mobile device.

App Bar on a Web Browser



App Bar on a Mobile Device

Default view:



Select  to view actions:



The actions that can be performed are:

- [Tenant Select](#)
- [Quick Add](#)
- [Send Commands](#)
- [Help](#)
- [User Profile](#)

6.1.1. Tenant Select

If a web access user has an account in multiple tenants, the **Tenants** selector will be available.



Tenants ▼

Simply click or tap then make a selection from the list to be redirected to that tenant.




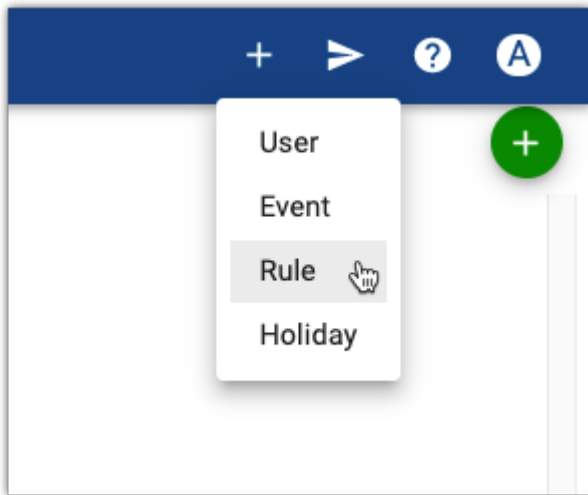
ISONAS PUREACCESS

Tenants ▼

6.1.2. Quick Add




To quickly add a **User**, **Event**, **Rule**, or **Holiday**; simply select the  from the App Bar, then choose what you'd like to create from the list.



6.1.3. Send Commands


There are multiple commands that can be sent to readers from the App Bar. A **Compile** command will need to be sent to your devices when changes are made to users, rules, or access points.

An **Admit**, **Lock Down**, **Schedule**, or **Unlocked** command can be sent to individual access points, access point groups, or all devices by selecting  then “**Commands**.” See below for more information.

Sending a Compile

When a change that requires a compile is made, the send command button will display a red notification badge.



1. Click  from the App Bar
2. Select **Compile**
3. (optional) Verify compile was sent successfully using a History widget or report



Note that single changes to a user no longer require a full compile to be sent thus the notification badge *will not* be displayed.

Sending a compile requires that the web access user has 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

Sending Additional Commands



1. Click  from the App Bar


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
 - **Lock**: locks the access point or access point group (Engage devices only)
 - **Clear Tamper**: clears a tamper alarm on an access point (Engage devices only)
-

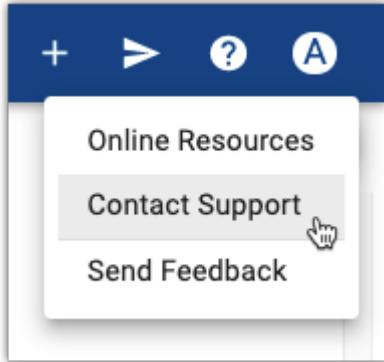
Sending command via the App Bar requires that the web access user has one (or more) of the following permissions:

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

6.1.4. Help Button



For assistance, the  can be selected to access the user manual (**Online Resources**), find contact information to reach technical support (**Contact Support**), or to check our product portal where one can view upcoming features and/or submit feature requests (**Send Feedback**).



6.1.5. User Profile

Selecting the letter at the far right of the App Bar will open actions that can be performed to the logged in user's profile. This will be the first letter of your first name.

From here you can change your password, edit your user profile, or log out of the tenant.





6.2. 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.

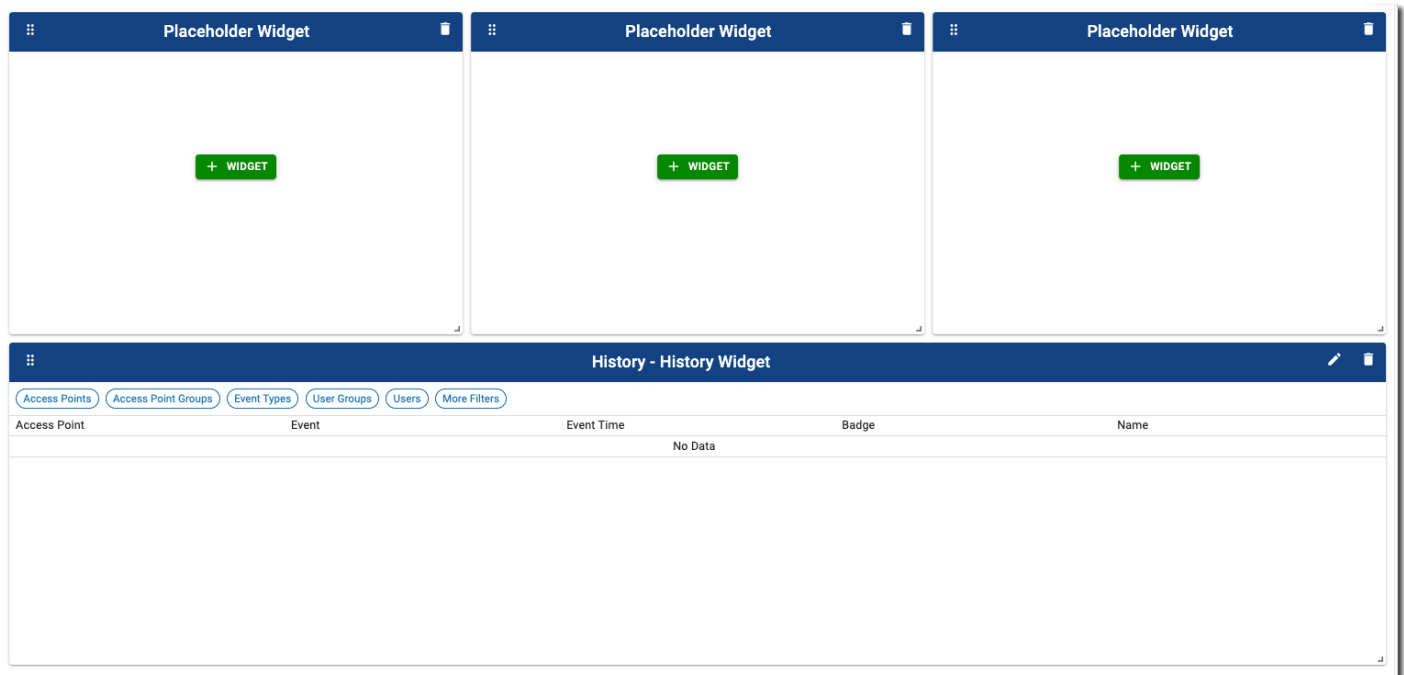
You can create an unlimited number of dashboards for various applications.

6.2.1. 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](#).



6.3. 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.

6.3.1. 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.

6.3.1.1. 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





		<i>Unlatch.”</i>
	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.

6.3.2. 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 .
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  in each filter box.




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

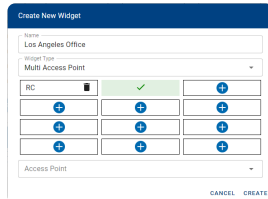
You can also control the Access Point in the widget by using the drop-down box and  button in the lower right corner of the widget. Actions include:



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


6.3.3. 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 .

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

6.3.4. 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 .
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.

6.3.5. 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 .
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.

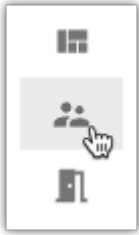
6.3.6. User Profile Widget

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 .
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  in each filter box.

7. Users

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



2. All active users in your system will be displayed

Name	Web Access	Edit Access	Manage User	Last Update	Action
John Doe	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User
Jane Smith	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User
John Doe	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User
Jane Smith	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User
John Doe	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User
Jane Smith	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User
John Doe	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User
Jane Smith	Yes	Yes	Yes	2021-11-10 12:34:56	Deactivate/Activate User

- After selecting one or more check boxes next to user(s), the following buttons will appear at the top:

ADD TO GROUP

- : Select a group from the drop-down and then click



SAVE

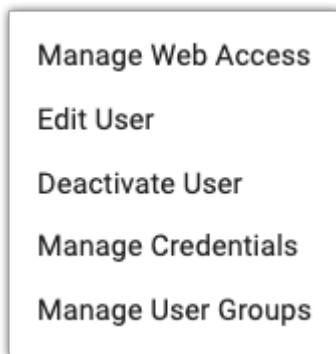
ACTIVATE

- : The user(s) will be activated

DEACTIVATE

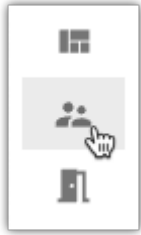
- : The user(s) will be deactivated

- Select  to the left of a user's name to display the following additional details: **User Group**, **Rules**, **Credentials**, and **Web Access** (if applicable)
- Select  to show the menu for [Manage Web Access](#), [Edit User](#), [Deactivate/Activate User](#), [Manage Credentials](#), and [Manage User Groups](#)

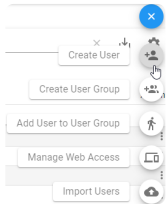


7.1. Create User

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](#).




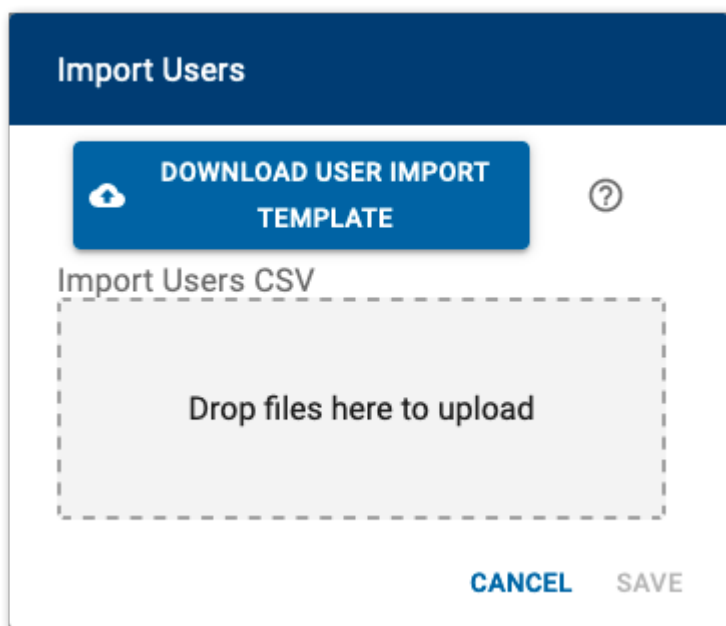
7.1.1. Importing Users

Summary

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

There are different methods and template files depending on the Pure Access environment being used:

1. For **Pure Access Cloud** using only legacy devices, the template file can be found within the application by navigating to **Import Users** from the quick dial  on the Users page:



2. For **Pure Access Cloud** that is linked with Engage (using Schlage devices), the template file can be found in [this article](#).
3. For **Pure Access Manager** (on premise), [this template](#) must be used. See article below for formatting instructions.

Environments

Click on one of the links below to find instructions on how to configure and upload a user import:

- My tenant is in Pure Access Cloud and [only contains legacy devices](#).
- My tenant is in Pure Access Cloud and [it is linked with Engage](#).
- My tenant is in [Pure Access Manager](#).


7.1.1.1. Importing Users into Pure Access Cloud (non-Engage tenant)

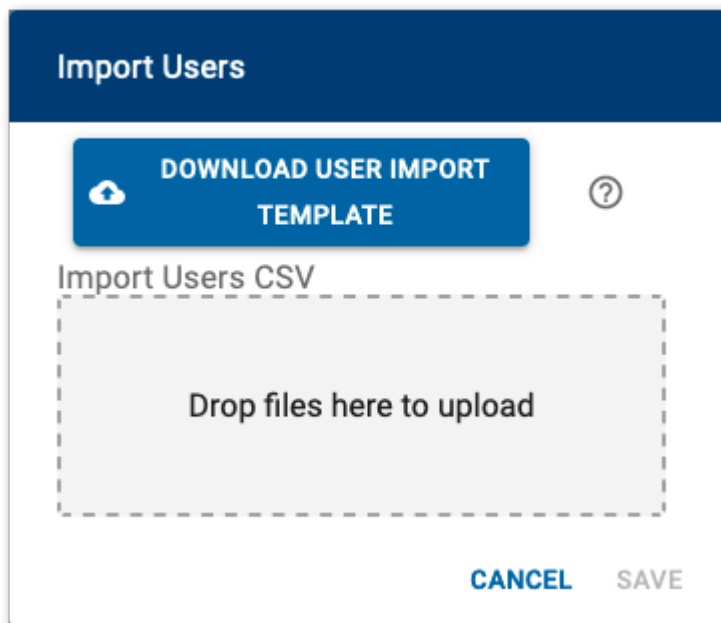
Before continuing, please note that the **formatting** of the template file, including proper **capitalization**, is very important.

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 **will cause the import to fail**.*

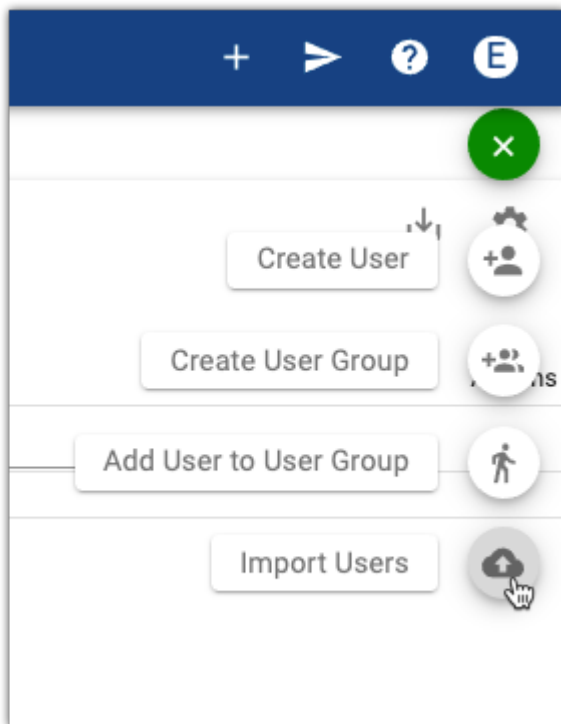
Instructions

1. From the **Users** page, hover over the  quick dial then select **Import Users**
2. Click “**DOWNLOAD USER IMPORT TEMPLATE**”



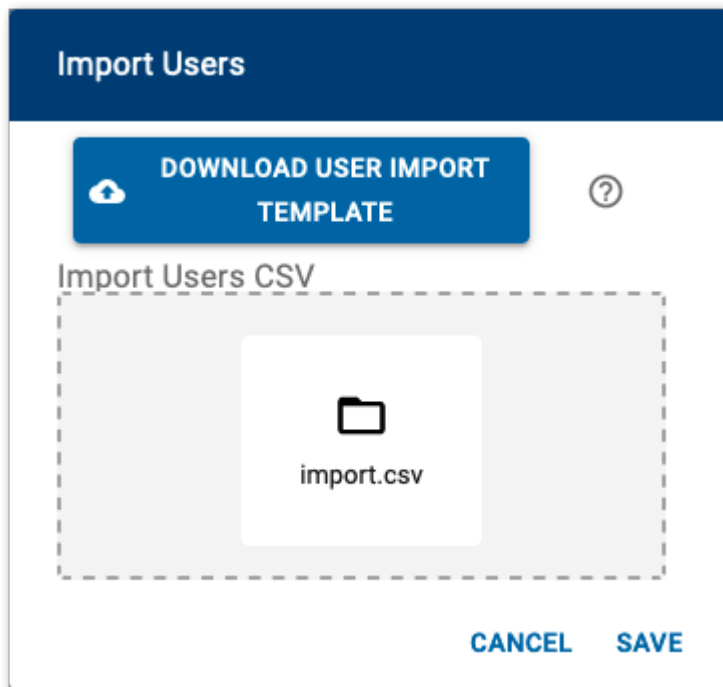
- a. Note that row 1 (containing the column headers) *must remain as is* for the import to be successful
3. Open the template CSV file and input the users' information
 - The required fields are: **LastName** and **FirstName**
 - a. In a tenant that is not linked with Engage, the **Badgeld** column should contain either the hot-stamped number printed on the user's [badge](#), a [keypad code](#), or a [mobile/bluetooth Device ID](#) number.

- To import multiple credentials for a single user, they will need more than one row in the CSV (one row for each credential being added)
 - 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
 - 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 the *All Users* and *Managers* groups, the cell would contain: **All Users;Managers**
 - Note: If the **UserGroups** field is not populated or if there is a typo, the user(s) will not be assigned to a group
4. 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. If an **AreaName** cell is populated with an area that does not exist in Pure Access, the user will be placed into *COMMON*.
 - b. Populate the **AreaName** column
 - c. Ensure that the capitalization and punctuation match the area(s) in Pure Access
5. The columns titled **CountLimitFlag**, **RemainingUses**, and **ExpirationDate** do not require data for the import to be successful. These columns must remain in the CSV for the import to function, however.
- a. If you wish to set an **ExpirationDate** on one or more credentials, you can do so using the date format: *yyyyMMdd*
 - **Example**: April 1st, 2022 would be *20220401*
 - b. If you wish to set a count limit on one or more credentials, **CountLimitFlag** will need to be true (the cell will need to contain a “t”) and the **RemainingUses** cell will be the number of times the credential can be presented before it is deactivated
6. If it had been closed, once again select the **Import Users** button from the **Users** page

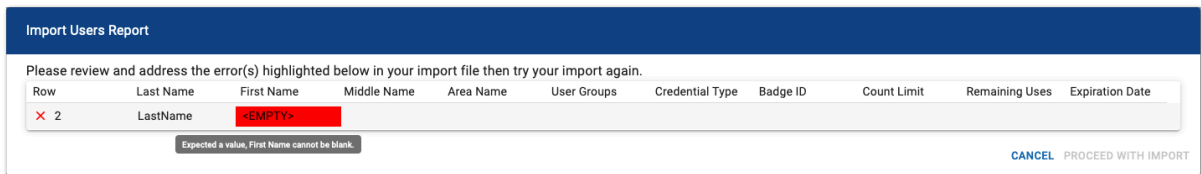


7. Drag the .csv file into the upload area then click

SAVE



8. Validation will be run against the uploaded file
- If any errors are found, a table will be displayed to give feedback on the exact issues found with the import. When you hover on the red cell with your mouse, you will be able to see helpful tips on the exact error found.



Import Users Report

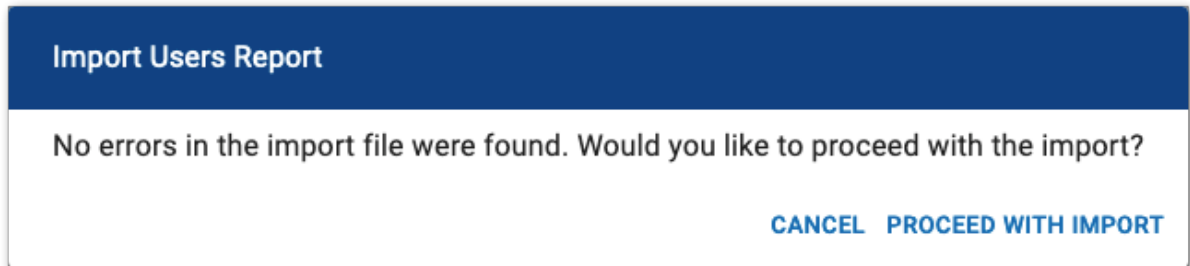
Please review and address the error(s) highlighted below in your import file then try your import again.

Row	Last Name	First Name	Middle Name	Area Name	User Groups	Credential Type	Badge ID	Count Limit	Remaining Uses	Expiration Date
2	LastName	<EMPTY>								

Expected a value, First Name cannot be blank.

[CANCEL](#) [PROCEED WITH IMPORT](#)

- i. Use this feedback to address any issues found directly in the CSV file. Once done, click [CANCEL](#) and then attempt to import the file again starting from Step 1 above.
- b. If no errors are found, click [PROCEED WITH IMPORT](#)

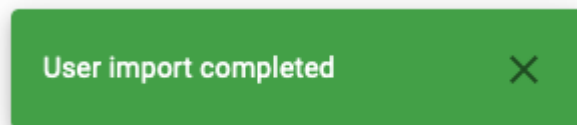


Import Users Report

No errors in the import file were found. Would you like to proceed with the import?

[CANCEL](#) [PROCEED WITH IMPORT](#)

- i. Depending on the size of the import, it could take from a few seconds to a few minutes to complete the user import. You can continue to use the application while the import is processed in the background. You will see a snackbar notification to let you know once the import has completed.



User import completed [×](#)

✿ 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.

7.1.1.2. Importing Users into Pure Access Cloud (Engage linked tenant)

When a tenant is linked with Engage, all of the steps from [the previous article](#) still apply. There is, however, additional credential information that must be taken into consideration so that the badges/fobs can be added successfully.

In the [user import template CSV](#), the additional parameters are:

- **CardFormat** (column F)
- **Hotstamp** (column G)
- **FacilityCode** (column I)
- **IssueLevel** (column J)

The required fields for adding credentials to an Engage linked tenant are dependent upon the card format(s) that are being imported.

The chart below can be used to assist with filling out the user import CSV file:

Card Format Name	CardFormat	CredentialType	Hotstamp	Badgeld	FacilityCode	IssueLevel
26A (26 bit)	2	1		[REQUIRED]	[REQUIRED]	
28G	27	1		[REQUIRED]	[REQUIRED]	
28H	28	1		[REQUIRED]		
32K	36	1		[REQUIRED]	[REQUIRED]	32
32X	30	1		[REQUIRED]		
33D	25	1		[REQUIRED]	[REQUIRED]	
34N	33	1		[REQUIRED]	[REQUIRED]	
34S	41	1		[REQUIRED]	[REQUIRED]	
35C	13	1		[REQUIRED]	[REQUIRED]	
35X	42	1		[REQUIRED]	[REQUIRED]	
36B	38	1		[REQUIRED]	[REQUIRED]	
36C	39	1		[REQUIRED]	[REQUIRED]	
36L	34	1		[REQUIRED]	[REQUIRED]	

36M	37	1		[REQUIRED]	[REQUIRED]	
36X	40	1		[REQUIRED]	[REQUIRED]	
37B	35	1		[REQUIRED]	[REQUIRED]	
37H	21	1		[REQUIRED]		
37P	32	1		[REQUIRED]	[REQUIRED]	
37X	19	1		[REQUIRED]	[REQUIRED]	
40X	31	1		[REQUIRED]	[REQUIRED]	
48X	26	1		[REQUIRED]	[REQUIRED]	[REQUIRED]
ISONAS Prox	43	1		[REQUIRED]		
ISONAS HID	22	1	[REQUIRED]			
EV2	29	1		[REQUIRED]		
Keypad		2		[REQUIRED]		
Isonas Mobile		3		[REQUIRED]		
Schlage Mobile		4		[REQUIRED]	110000	20

7.1.1.3. Importing Users into Pure Access Manager

Before continuing, please note that the **formatting** of the template 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.

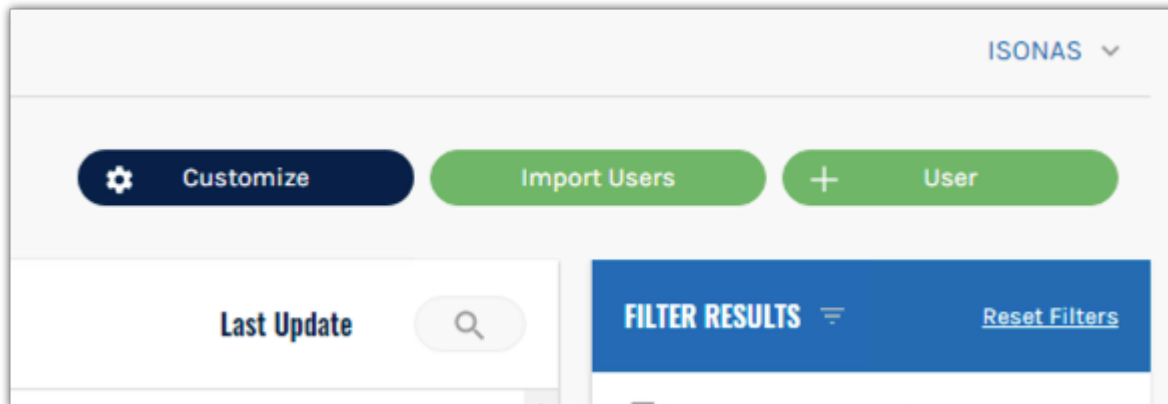
Note: *Modifying and/or removing any of the column headers from the template **will cause the import to fail**.*

Instructions

1. Download [this CSV template](#)
 - a. Note that row 1 (containing the column headers) *must remain as is* for the import to be successful
2. Open the template CSV file and 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 Device ID](#) 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 being added)
 - 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. If areas are being used in this tenant, please review the following formatting and notes:
 - i. Ensure that the area(s) **already exist** in Pure Access. The user import **will not** create new areas. If an **AreaName** cell is populated with an area that does not exist in Pure Access, the user will be placed into *COMMON*.
 - ii. Populate the **AreaName** column
 - iii. Ensure that the capitalization and punctuation match the area(s) in Pure Access
 - d. The columns titled **CountLimitFlag**, **RemainingUses**, and **ExpirationDate** do not require data for the import to be successful. These columns must remain in the CSV for the import to function, however.
 - i. If you wish to set an **ExpirationDate** on one or more credentials, you can do so

using the date format: *yyyyMMdd*

- **Example:** April 1st, 2022 would be *20220401*
- ii. If you wish to set a count limit on one or more credentials, **CountLimitFlag** will need to be true (the cell will need to contain a “t”) and the **RemainingUses** cell will be the number of times the credential can be presented before it is deactivated
- e. Once completed, the CSV file will need to be [zipped](#)
- f. Click the **Import Users** button from the **Users** page



- g. Navigate to and select the zipped .csv file (.zip file) then click **Open**



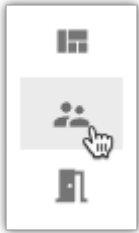
If the import fails, please ensure that no changes have been made to row 1 of the CSV. Pure Access is looking for specific data so these fields must remain **exactly** as they are found in the template.




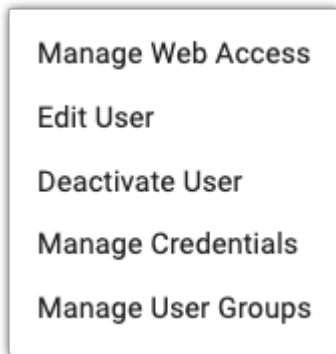
For Pure Access Manager 2.12.2 and lower, **CountLimitFlag** will be **CountLimit** (as provided in the template). The ability to add users to groups via user import was added into Pure Access in version 3.1 and is not available in any version of PAM.


7.2. Edit User

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



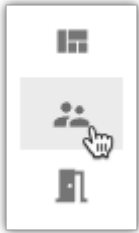
2. Select  next to the User you want to edit and then choose **Edit User**.



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

7.3. User Search and Filters

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



2. Near the top of the screen will be a search bar and filter options



3. **Search** can be used to find a user from their:
 - a. Name
 - b. Web access username
 - c. Credential information
 - d. User defined field information
4. To filter the user list down, first click one of the following chip filters to expand the selection:
 - [User Groups](#)
 - **Users**
 - [Web Access](#)
 - [User Status](#)
 - [Credential Status](#)
5. Once expanded, select the appropriate check boxes for which you would like to filter results then click **SAVE** to apply changes

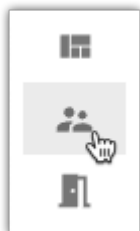
The screenshot shows a web interface for managing user groups. At the top, there are three tabs: 'User Groups - 2', 'Users', and 'Web Access'. Below the tabs is a search bar labeled 'Search'. A list of user groups is displayed with checkboxes: 'Select All', 'Active Contractors', 'Administrators' (checked with a green checkmark), 'All Contractors', 'All Users', and 'IT'. A mouse cursor is hovering over the 'IT' checkbox. At the bottom left is a blue 'CLEAR' button, and at the bottom right is a blue 'SAVE' button.

- Alternatively, click [CLEAR](#) to remove all filters for the selected category

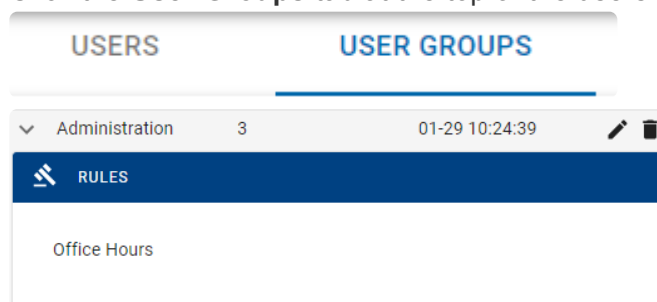
7.4. User Groups




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:



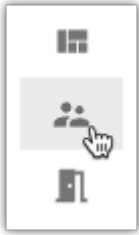
2. Click the **User Groups** tab at the top of the users list.





- 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.

7.4.1. 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  .

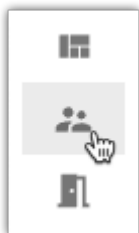
7.4.2. Manage User Groups


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.

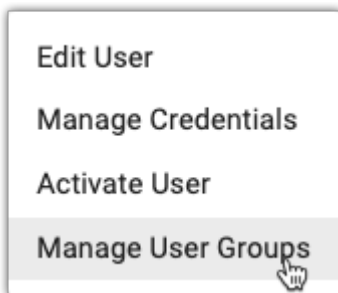
There are several ways to change which user groups a user is included in:

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.

Manage User Groups: Test, 01

User Group —
Standard Users, All Users, All Contractors, Administrators ▼

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

CANCEL SAVE

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

Manage User Groups: Test, 01

User Group —
Standard Users, All Users, All Contractors, Administrators ▼

Search

☐ Select All

☐ IT

☒ Administrators

☒ All Contractors

☐ Active Contractors

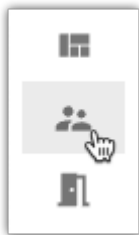
☐ Terminated


SAVE

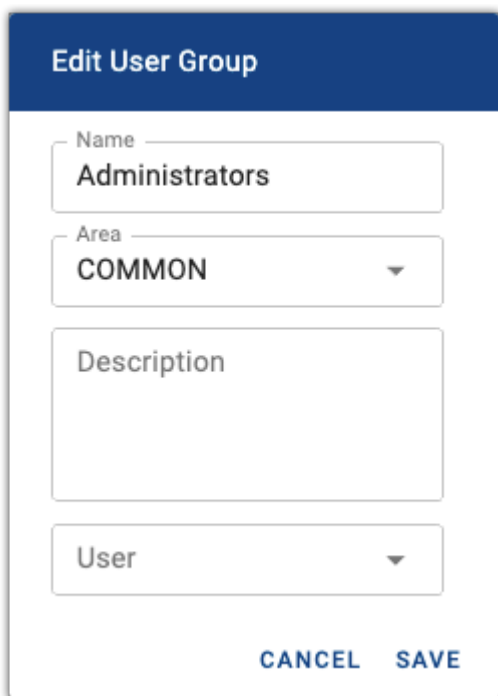
6. Click **SAVE**

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

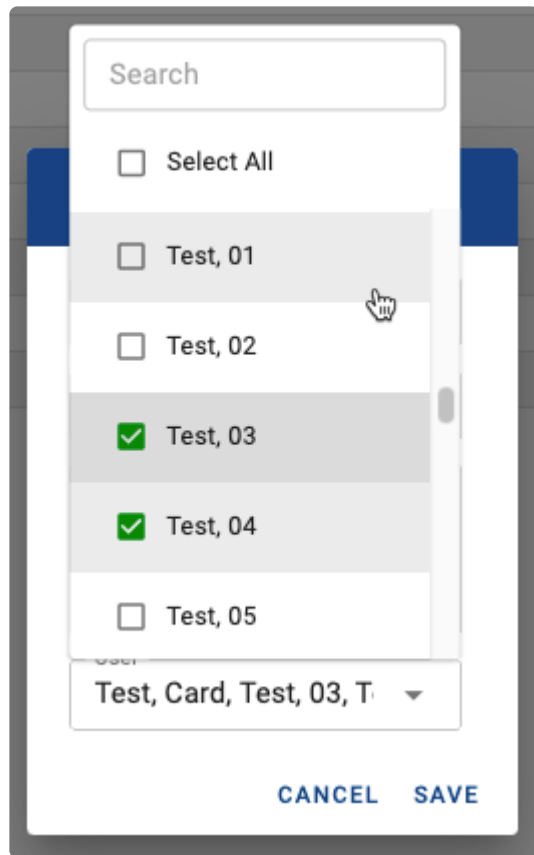
1. Click the **Users** tab on the left side navigation:



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

A dialog box titled "Edit User Group" with a blue header. It contains four input fields: "Name" with the value "Administrators", "Area" with the value "COMMON" and a dropdown arrow, "Description" which is empty, and "User" with a dropdown arrow. At the bottom, there are two buttons: "CANCEL" and "SAVE".

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



5. Click 

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:

ISONASPUREACCESS

Tenants

E

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

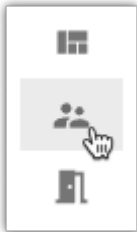
03-01 16:02:45


7.5. Manage Credentials

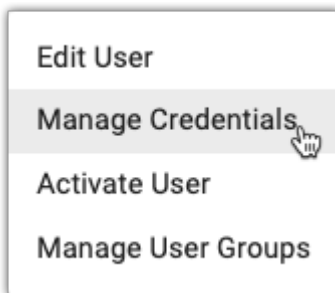
This article contains information on how to add credentials to a user as well as how to modify existing credentials.

Navigating to the *Manage Credentials* dialog:

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

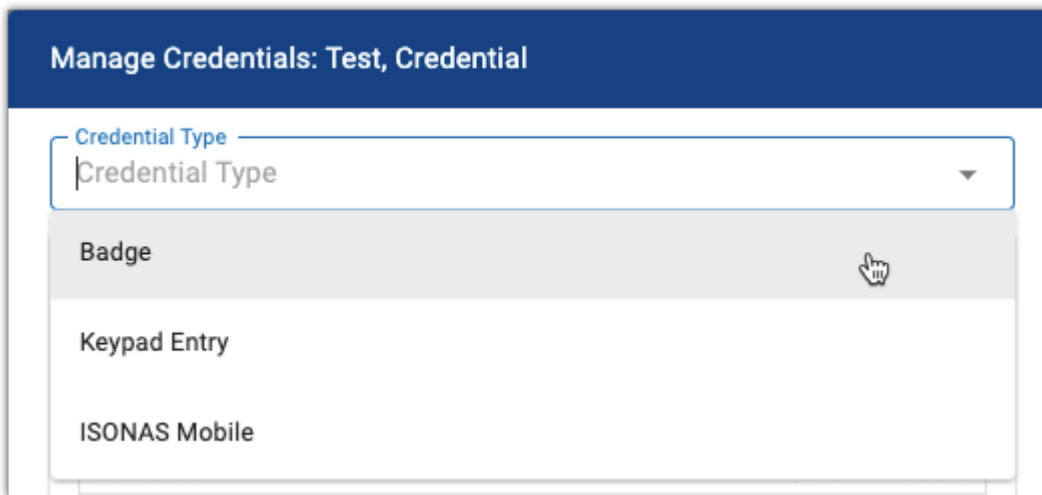


2. Click  next to the user for which you will need to add/modify a credential, then choose **Manage Credentials**:



Adding a credential (overview):

1. Choose the credential type from the drop-down list



2. For a badge or mobile credential, choose one of the following methods:

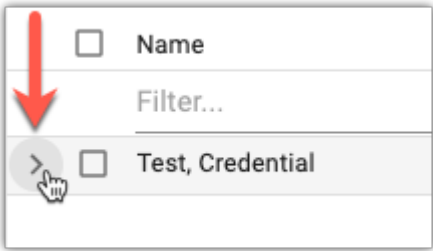
- a. *Enroll Manually*
 - b. *Enroll By Presentation*
- 3. For a keypad credential, choose one of the following methods::
 - a. *Enroll Manually*
 - b. *Generate Random PIN*
- 4. Input credential value (required) and add [special properties](#) (optional)
- 5. Click SAVE



For more information on adding credentials, click on one of the credential types from the table below.

Modifying a credential:

- 1. **Method 1:** *Manage Credentials* action
 - a. Navigate to the *Manage Credentials* dialog for a user (see above for instructions)
 - b. Next to the credential you wish to modify, select the
- 2. **Method 2:** *User Details*
 - a. Navigate to the user and select the arrow to display additional details



- b. Under the “**Credentials**” section, select the credential that needs to be modified
- 3. Make the desired changes
- 4. Click SAVE

Credential Types						
Type	Format	Facility Code	Issue Level	Hot Stamp	Badge ID	Special Properties
Badge	26A, 37X,	X			X	Master ,

	33D, 48X, 28G, 40X, 37P, 34N, 36L, 37B, 36M, 36B					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				
ISONAS Mobile	Device ID					
Schlage Mobile	Mobile Phone Number					

7.5.1. Badge

There are two methods of adding a badge/fob to a user: manually and by presentation


In a tenant not linked with Engage:

Enrolling Manually

In order to add a badge manually, you will first need to ensure that the [bitmask](#) on the tenant is set correctly.

! If badges have already been enrolled and are fully operational, please note that **changing the bitmask** may result in these existing credentials being declined. If this occurs, one will need to either set the bitmask back to the original setting or existing credentials will need to be re-enrolled with the new mask.

If the bitmask is set correctly:

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**Badge**” from the **Credential Type** dropdown
3. Select “**Enroll Manually**”
4. Input the hot stamped number from the card/fob into the **Badge ID** field (required)
 - Add [special properties](#) (optional)
5. Click 

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

Enrolling By Presentation

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**Badge**” from the **Credential Type** dropdown
3. Select “**Enroll By Presentation**”
4. Present an unenrolled badge/fob to a connected reader
 - The raw data and badge ID of **the most recently declined card*** will populate:
5. From the “Access Point” drop-down menu, select the access point where the credential had been

presented then click

READ

- Add [special properties](#) (optional)

6. Click

SAVE

* The declined credential will clear after 15 minutes. *

In a tenant linked with Engage:

Enrolling Manually

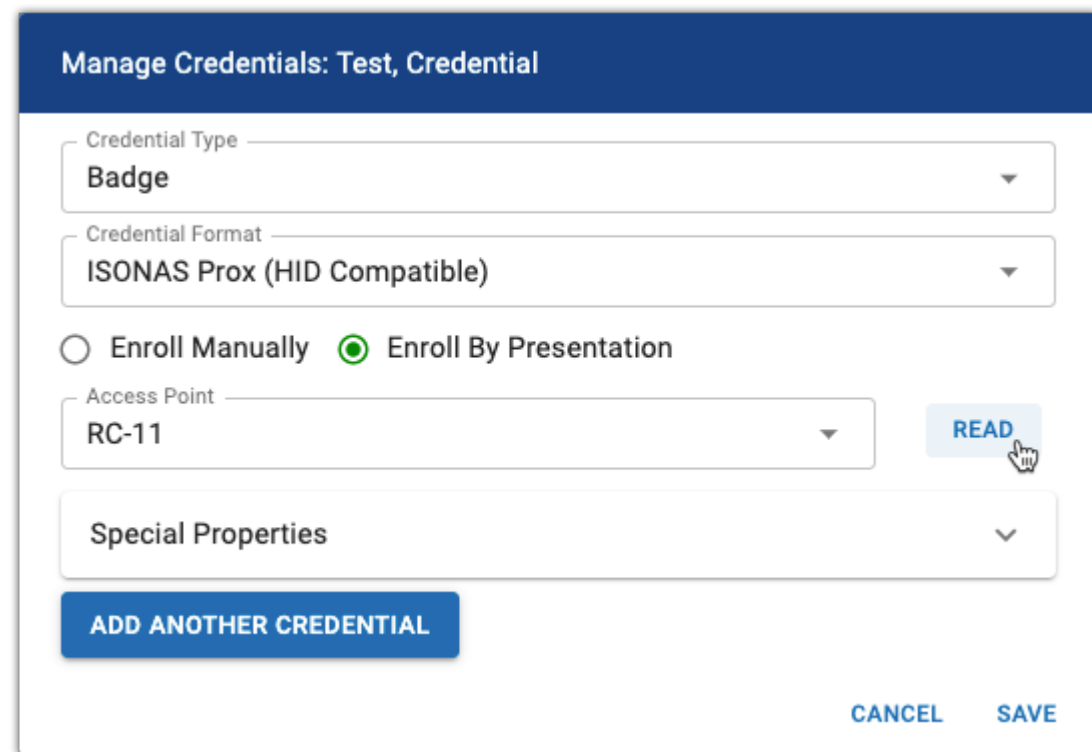
1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**Badge**” from the **Credential Type** dropdown
3. Select the **Credential Format** of the badge/fob that is being enrolled
4. Select “**Enroll Manually**”
5. Input the hot stamped number from the card/fob into the **Badge ID** field (required)
 - Add [special properties](#) (optional)

6. Click [SAVE](#)

Enrolling By Presentation

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**Badge**” from the **Credential Type** dropdown
3. Select the **Credential Format** of the badge/fob that is being enrolled
4. Select “**Enroll By Presentation**”
5. Present an unenrolled badge/fob to a connected reader
 - The raw data and badge ID of *the most recently declined card** will populate:
6. From the “Access Point” drop-down menu, select the access point where the credential had been

presented then click [READ](#)



Manage Credentials: Test, Credential

Credential Type —
Badge

Credential Format —
ISONAS Prox (HID Compatible)

☐ Enroll Manually ☒ Enroll By Presentation

Access Point —
RC-11

[READ](#)

Special Properties —

[ADD ANOTHER CREDENTIAL](#)

[CANCEL](#) [SAVE](#)


- Add [special properties](#) (optional)

7. Click [SAVE](#)



7.5.2. Keypad Entry

If you have a keypad device and would like to assign an entry code to a user, you can do so manually or you may generate a randomized PIN.

Enrolling Manually

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**Keypad Entry**” from the **Credential Type** dropdown
3. Select “**Enroll Manually**”
4. Input a PIN between 4 and 9 digits long (note that if an RC-03 or IP-Bridge v1 is connected to the tenant, the maximum value that will function is 65535)
 - Add [special properties](#) (optional)
5. Click 

Generating a Random PIN

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**Keypad Entry**” from the **Credential Type** dropdown
3. Select “**Generate Random PIN**”
4. Select a PIN length from the drop-down list (note that if an RC-03 or IP-Bridge v1 is connected to the tenant, the maximum value that will function is 65535)
5. Click  until the desired PIN is generated
 - Add [special properties](#) (optional)
6. Click 

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

7.5.3. ISONAS Mobile

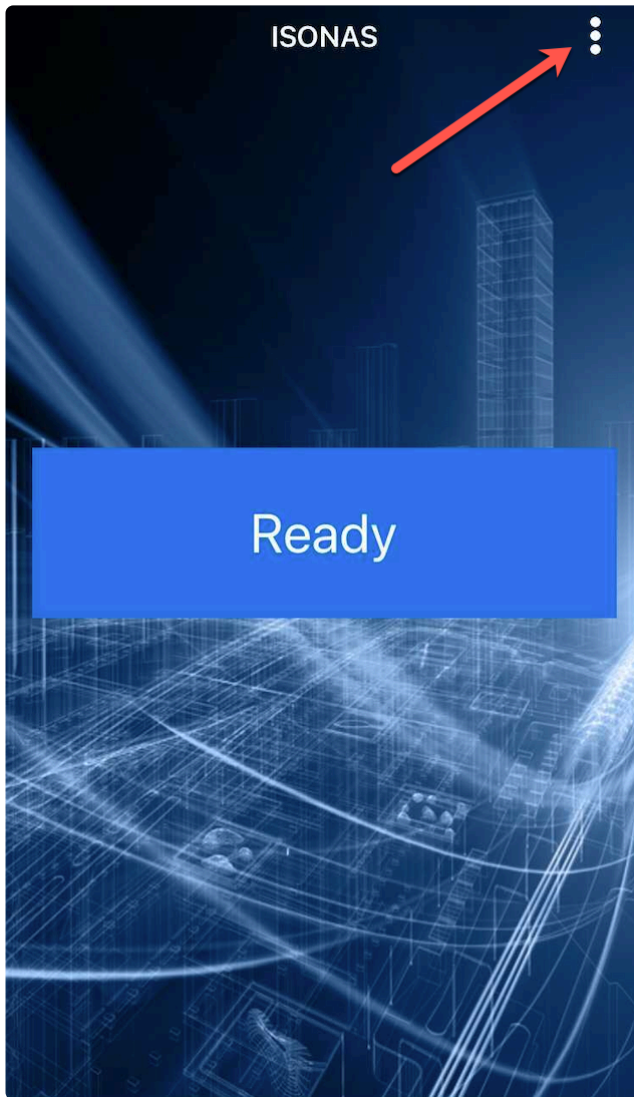
There are two methods of adding an ISONAS mobile credential to a user: manually and by presentation

Prerequisite

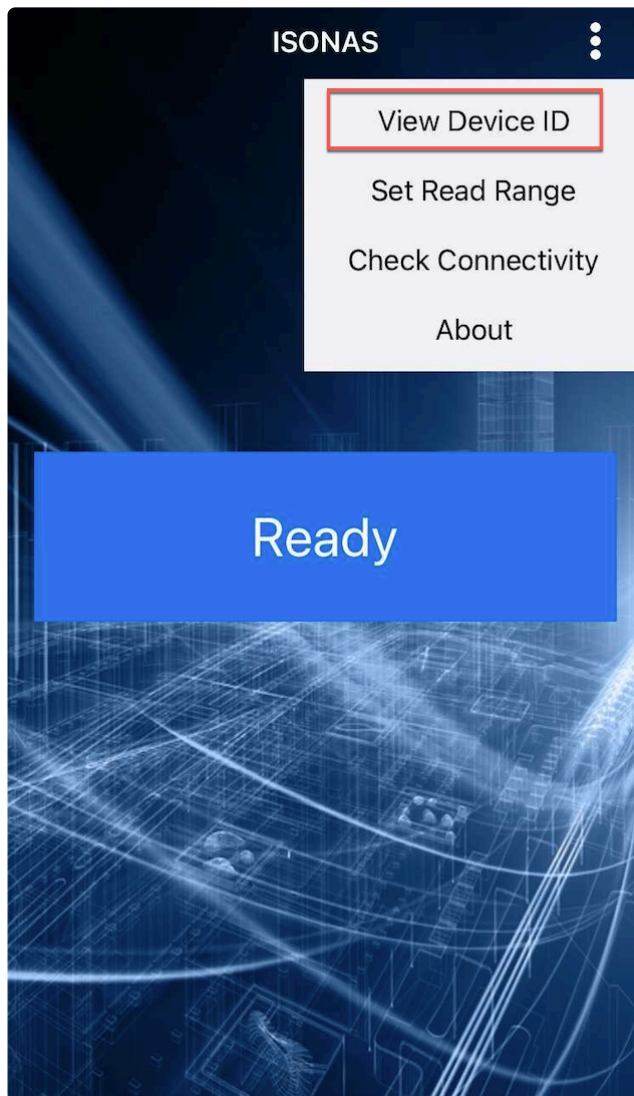
In order to use the ISONAS Mobile Bluetooth credential, you must first install the Pure Mobile app from the [iOS App Store](#) or [Google Play Store](#).

Enrolling Manually

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**ISONAS Mobile**” from the **Credential Type** dropdown
3. Select “**Enroll Manually**”
4. Find your phone’s unique Device ID from the Pure Mobile app:
 - a. Click on the three dots in the upper right corner of the **ISONAS Pure Mobile** application.



- b. Click “**View Device ID**”



- c. Input this into the “**Device ID**” field
 - Add [special properties](#) (optional)

5. Click 

Enrolling by Presentation

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Select “**ISONAS Mobile**” from the **Credential Type** dropdown
3. Select “**Enroll By Presentation**”
4. While in proximity of a compatible ISONAS device, touch “**TAP TO SEND**” in the **ISONAS Pure Mobile** application
5. From the “Access Point” drop-down list, select the access point where the credential had been

presented then click

READ

- Add [special properties](#) (optional)

6. 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.

7.5.3.1. 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

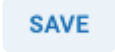
1. When a user approaches a Schlage hardware device, they *must have* **Bluetooth® Low Energy (BLE)** as well as **location services** turned on in order for the phone to communicate with the hardware.
2. Open the **Schlage Mobile** app on the mobile device.
3. When in range, touch **Tap to Unlock**.

7.5.4. Schlage Mobile



Prerequisite

In order to use a Schlage Mobile Access credential, you must first install the Schlage Mobile Access app from the [iOS App Store](#) or [Google Play Store](#).

Enrolling by Text

1. Navigate to the [Manage Credentials](#) dialog for a user
2. Choose **Schlage Mobile** from the **Credential Type** drop-down list
3. Select **Enroll by Text**
4. Enter the user's **Mobile Number** in the box
 - Add [special properties](#) (optional)
5. Click 
 - The user will receive an SMS message that directs them to download the app and register the new credential

Enrolling By Presentation

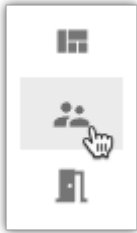
1. Navigate to the [Manage Credentials](#) dialog for a user
2. Choose **Schlage Mobile** from the **Credential Type** drop-down list
3. Select **Enroll By Presentation**
4. While in proximity of a compatible Schlage device, touch “**TAP TO UNLOCK**” in the **Schlage Mobile Access** application
5. From the “Access Point” drop-down list, select the access point where the credential had been presented then click 
 - Add [special properties](#) (optional)
6. Click 




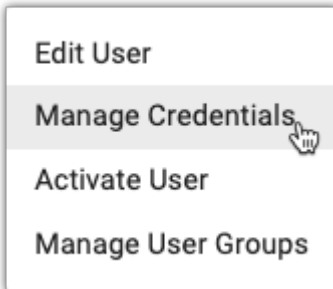
Note that Schlage Mobile Access credentials are only compatible with Schlage locks and Schlage reader controllers. These *will not* function with legacy ISONAS hardware. In order to enable this functionality, your tenant must first be linked with [Engage](#).

7.5.5. 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

A screenshot of the 'Manage Credentials: Test, Credential' window. The window has a dark blue header with the title 'Manage Credentials: Test, Credential'. Below the header, there is a 'Credential Type' dropdown menu with 'Badge' selected. Below this, there are two radio buttons: 'Enroll Manually' and 'Enroll By Presentation', with 'Enroll By Presentation' selected. Below the radio buttons, there is an 'Access Point' dropdown menu with 'RC-04' selected, and a 'READ' button to its right. Below the 'Access Point' dropdown, there is a 'Raw Data' text field containing the value '009B42E5000000000000000023229B42E5'. Below the 'Raw Data' field, there is a 'Value' text field containing the value '10175205'. Below the 'Value' field, there is a 'Special Properties' dropdown menu. Below the 'Special Properties' dropdown, there is a blue button labeled 'ADD ANOTHER CREDENTIAL'. Below the button, there is an 'Additional Credentials' dropdown menu. At the bottom right of the window, there are two buttons: 'CANCEL' and 'SAVE', with a hand cursor pointing at the 'SAVE' button.

4. Choose the **Credential Format** from the drop-down box (Engage-linked tenants only)
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 
 - a. The raw data and badge ID of *the most recently declined card** will populate:
8. Click the  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.*

7.5.6. Special Credential Properties

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

1. **[Master](#)**: The ability to unlock an access point that is in Lockdown; bypass two-factor authentication; grants 24/7 access
2. **[Toggle](#)**: The ability to unlock/lock access points for which the user has Grant Access permissions
3. **[Count Limit](#)**: used to limit how many times a credential may be used before deactivating
4. **[Time Limit](#)**: used to limit the time during which a credential will be active
5. **[Force Check-In](#)**: used to force wireless locks to [check-in](#) with Pure Access for updates

7.5.6.1. Master Credential

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

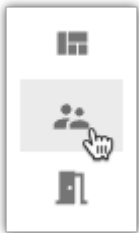
- Bypass a locked down access point
- Bypass a two-factor rule
- Provides 24/7 “Always” access to doors where user currently has Grant Access permissions




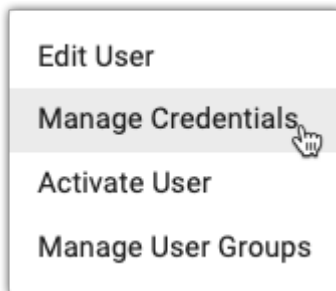
Note that a master credential *does not* provide grant access permissions to all access points in a tenant. The user profile with a master credential must have **Grant Access** permission for the access point(s) they're attempting to access otherwise they will be declined.


Adding Master Credential Special Property




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




2. Click  next to the user for which you want to add a master credential
3. Select [Manage Credentials](#)



4. Click  next to the credential for which you will be enabling the master property

1 results		
Credential	Active	Actions
 1235		

5. 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

☒

☐

☐

☐

6. Click 

7.5.6.2. Toggle Credential

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

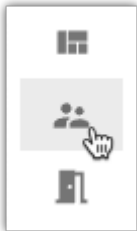
It *cannot*, however, be used to override an **Auto-Unlock** nor **Auto-Unlock w/ Badge** rule. Toggle lock can *only* reset a toggle unlock.




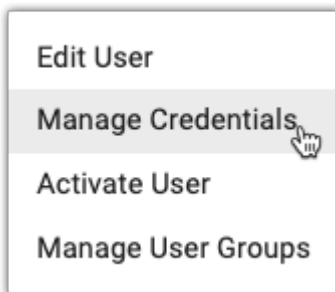
***Please note this is a function that requires the ISONAS hardware to be online and **will not** toggle the state of the device if it is not actively communicating with Pure Access.*

Adding Toggle Credential Special Property




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




2. Click  next to the user for which you want to add a toggle credential
3. Select [Manage Credentials](#)



4. Click  next to the credential for which you will be enabling the toggle property

1 results		
Credential	Active	Actions
 1235		

5. Click  next to **Special Properties** then select the slider for **Toggle Credential** to enable the toggle property

Special Properties

Master

Toggle Unlock

Count Limit

Time Limit

Toggle Access Point(s)


☐ All Access Points
 ☐ Access Point Group
 ☒ Access Point

Access Point

1163

6. Choose which access point(s) or access point group(s) the toggle credential should work with

7. 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

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



3. Click on the **Global Settings** tab
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	<input type="text" value="4"/>
Re-lock Time	<input type="text" value="23:59"/> 
Timezone	<input type="text" value="(UTC-07:00) Mountain Time (US & Canada)"/> 

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

5. Click **SAVE** and then enter your password to confirm

7.5.6.3. 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 .

Special Properties

Master

Toggle Unlock

Count Limit

Time Limit

3

?

7.5.6.4. 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

☒

Start Date

2021-01-29

End Date

2021-01-29

Start Time

08:00

End Time

05:00

7.5.6.5. Force Check-In

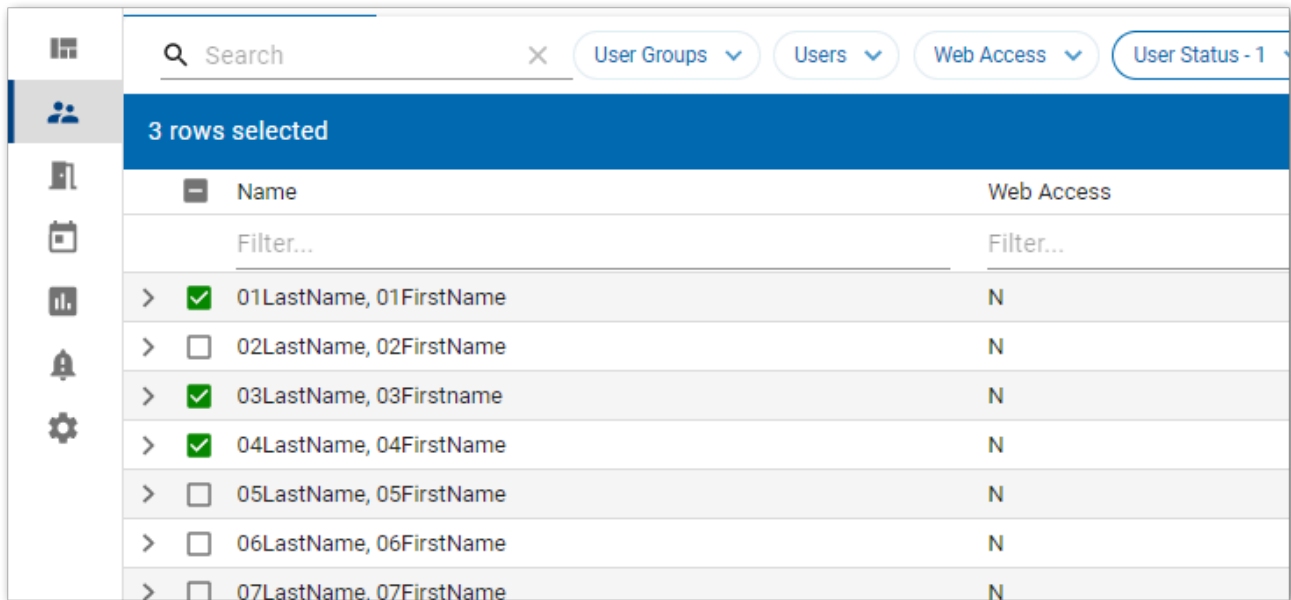
When a credential with the **Force Check-In** special property is presented to a wireless lock, the device will enable its WiFi radio to perform a [check-in](#) with Pure Access outside of the normal check-in schedule.

7.5.7. Migrate Credentials (Legacy to ENGAGE)

After linking an existing tenant (with active credentials) to ENGAGE, each credential will need to be migrated before it will function at an ENGAGE device (Schlage RC, LE, NDE, etc.).

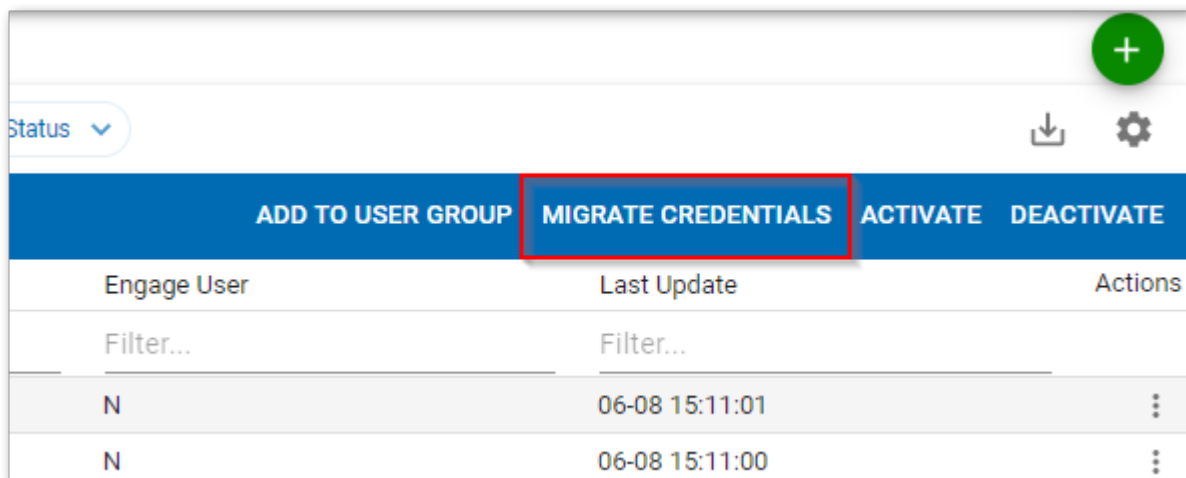
Process:

1. Navigate to the **Users** page
2. Select one or more users with legacy credentials



Name	Web Access
01LastName, 01FirstName	N
02LastName, 02FirstName	N
03LastName, 03FirstName	N
04LastName, 04FirstName	N
05LastName, 05FirstName	N
06LastName, 06FirstName	N
07LastName, 07FirstName	N

3. Click the **MIGRATE CREDENTIALS** button



Engage User	Last Update	Actions
N	06-08 15:11:01	⋮
N	06-08 15:11:00	⋮

4. Proceed through the **Credential Migration** steps

Credential Migration: 1 Credential Remaining for 01LastName, 01FirstName

Are all of this user's badges the same format?

☐ Yes ☐ No

CANCEL MIGRATE

- If migrating credentials of different formats, select “**No**” then choose the format for the respective credential(s)

Credential Migration: 1 Credential Remaining for 01LastName, 01FirstName

Are all of this user's badges the same format?

☐ Yes ☒ No

Credential Format

Search

Isonas EV2

ISONAS Prox

ISONAS Prox (HID Compatible)

26A

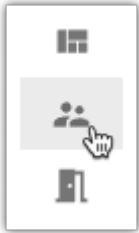
28G


Credentials

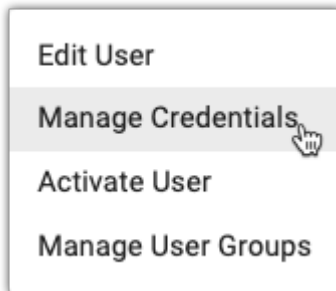
CANCEL MIGRATE

7.5.8. 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.

Manage Credentials: Adams, Eryn

Credential Type

Badge

Credential Format

48X

☒ Enroll Manually ☐ Enroll By Presentation

Issue Level

1

Facility Code

1

Badge ID

1235

☒ Active

Special Properties

ADD ANOTHER CREDENTIAL

Additional Credentials

CANCEL

SAVE

4. Click

SAVE



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

7.6. Manage Web Access

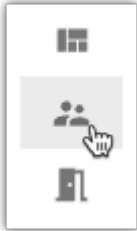
In order to log into a [Pure Access Cloud](#) tenant, your user profile will need to be configured for **web access** and have sufficient user roles assigned.


If either of these criteria are not met but your user profile *should* be able to log in, an **Integrator** or an **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 if the invitation has expired).

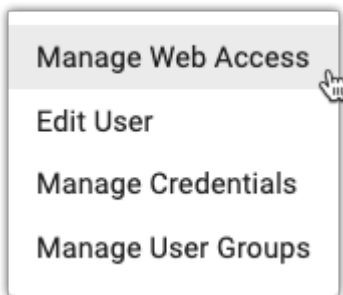
7.6.1. Setting up Web Access for a User

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

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

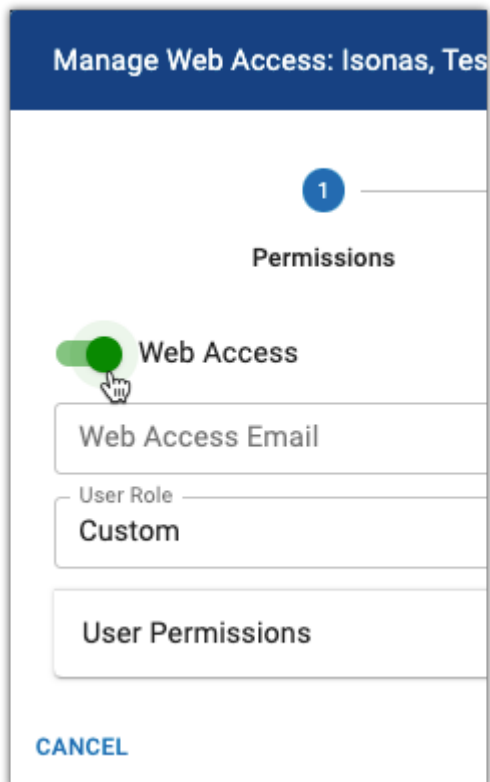


2. Select  next to the User you want to configure and then choose **Manage Web Access**



3. **Permissions:**

- a. Select the **Web Access** slider



- b. Enter the email address of the user
 - c. Choose one of the four preset roles from the [User Role](#) drop-down menu or select **Custom** to choose their permissions individually
 - i. To view/edit the specific permissions granted, click on **User Permissions**
4. Click **NEXT**
5. **Area Access:**
 - a. From the drop-down menus under the **Access** column, select the appropriate permissions for each area
6. Click **SEND INVITE**

The user will receive an invitation via email with the subject of “*Please confirm your ISONAS Pure Access account*” which must be accepted within 72 hours. The user’s web access will remain in a pending state until then (denoted by a **P** under the **Web Access** column on the Users page).

Once the user accepts the invitation and creates/confirms their password, a **Y** will be displayed in the **Web Access** column to show that they now have web access.



New users should note that ISONAS does not have the ability to re-send invitations that have expired. Users who have let their invitation expire will need an Administrator of the tenant to send them a new invitation.

7.6.2. User Roles

What do the pre-defined roles provide access to?

- **Integrator:** Provides access to view and modify all aspects of the tenant, has access to all areas, and can create sub-tenants (RMR license).
- **Administrator:** Provides access to view and modify all aspects of the tenant but is limited to a single tenant, may not have access to all areas, and cannot create sub-tenants (RMR license).
- **Human Resources:** Provides access to view tenant settings, dashboards, alerts, holidays/events, access points, rules, and reports; can modify users.
- **Operator:** Provides access to view users, holidays/events, dashboards, alerts, and reports.
- **Custom:** Individual permissions can be added or removed*.

You can view current user role permissions by selecting **User Permissions** from the **Manage Web Access** action taken on a user. Here is a list of the permissions:

- 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
- Engage (feature coming soon)

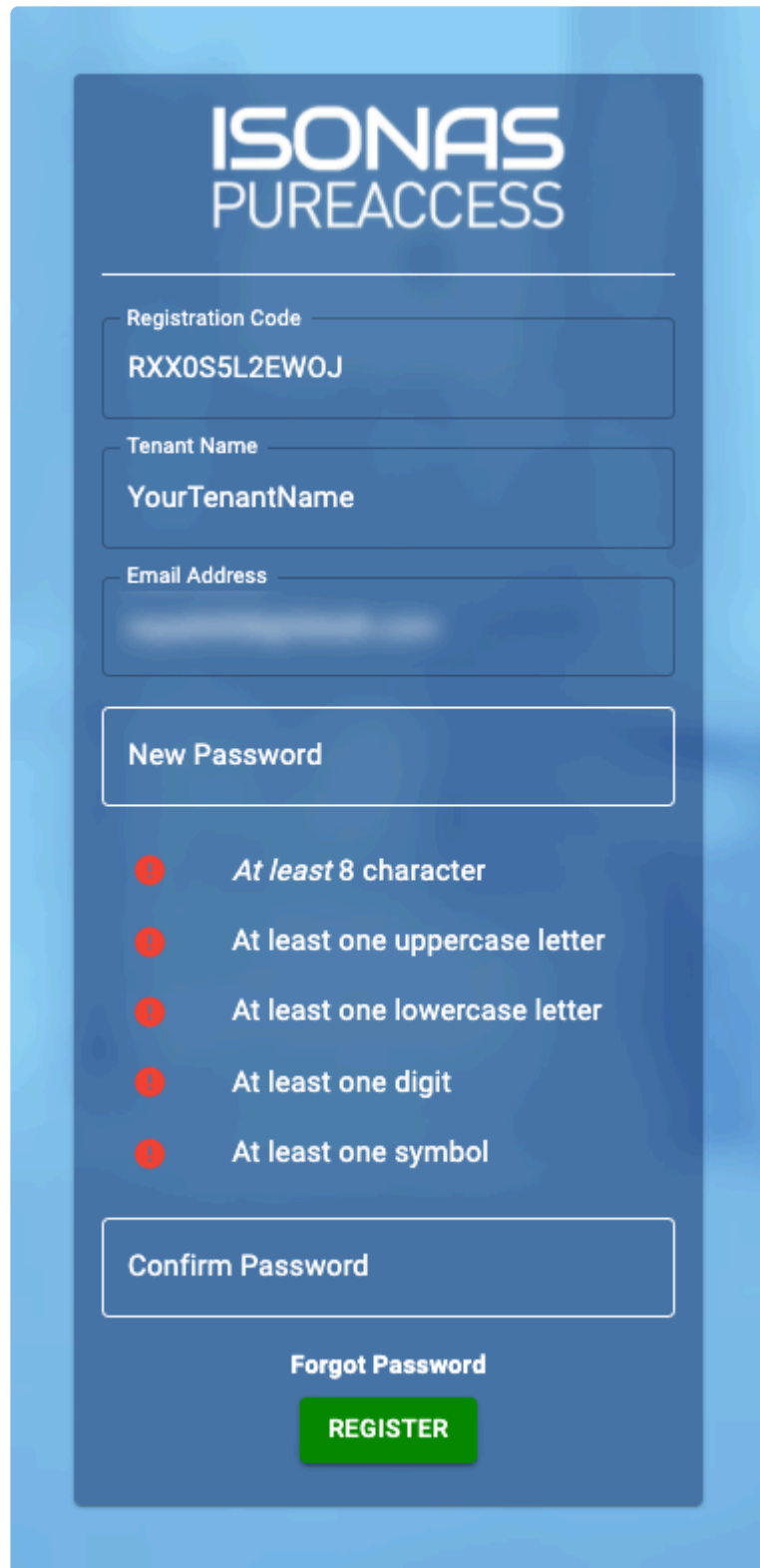


Additional information on the **Custom** user role: only web access users with modify privileges for a specific permission can grant another person view/modify access to that permission. For example, if a web access user who does not have modify access to Dashboards attempts to grant another person access to Dashboards, they will be denied.

7.6.3. 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 'ISONAS PUREACCESS' logo is displayed in white. Below the logo, there are five input fields: 'Registration Code' (containing 'RXX0S5L2EW0J'), 'Tenant Name' (containing 'YourTenantName'), 'Email Address' (containing a blurred email address), 'New Password', and 'Confirm Password'. Below the 'New Password' field, there are five red circular icons, each followed by a password requirement: 'At least 8 character', 'At least one uppercase letter', 'At least one lowercase letter', 'At least one digit', and 'At least one symbol'. Below these requirements is the '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
RXX0S5L2EW0J

Tenant Name
YourTenantName

Email Address
[blurred email address]

New Password

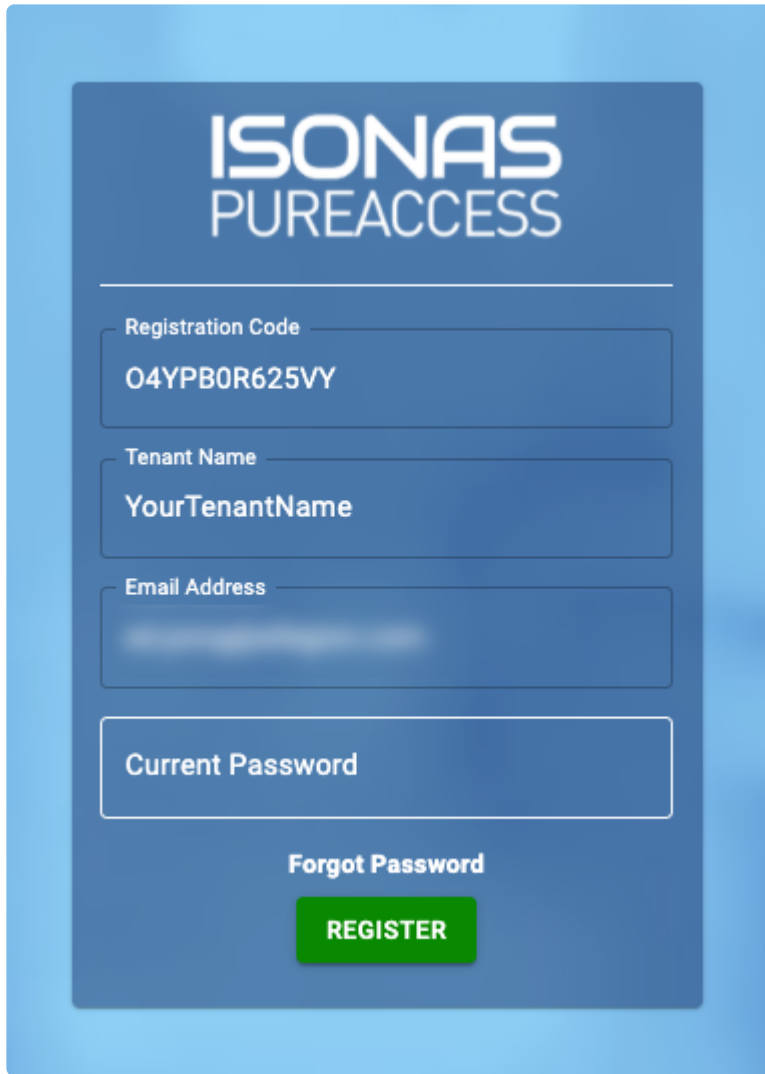
- At least 8 character
- At least one uppercase letter
- At least one lowercase letter
- At least one digit
- At least one symbol

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 blue gradient background. At the top, the 'ISONAS PUREACCESS' logo is displayed in white. Below the logo, there are four input fields: 'Registration Code' with the value 'O4YPB0R625VY', 'Tenant Name' with the value 'YourTenantName', 'Email Address' (which is blurred), and 'Current Password'. Below these fields is a link for 'Forgot Password' and a green 'REGISTER' button.

ISONAS
PUREACCESS

Registration Code
O4YPB0R625VY

Tenant Name
YourTenantName

Email Address

Current Password

[Forgot Password](#)

REGISTER

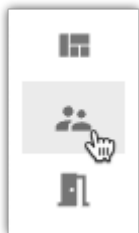
Don't know your password? You can reset it from the [Pure Access Cloud login page](#) or by [clicking here](#).


Invitation not working?

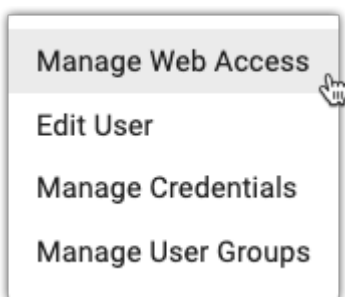
If you accept the web access invitation and it there is no space for you to enter your information, you are likely using Internet Explorer or another unsupported browser. Please retry using **Chrome** or **Firefox** instead.

7.6.4. 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

1. Click 
2. Click 

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 sub-tenants. For this reason, the user's web access will need to be removed from each sub-tenant individually.

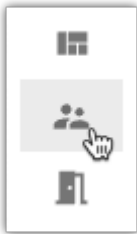
7.7. Deactivate User

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.

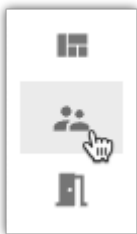
11 results	Name	Role	User Active	Registration	Last Login	Actions
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate
<input type="checkbox"/>	Admin User	Admin	Yes	2020-12-01 12:00:00	2020-12-01 12:00:00	Edit Deactivate

3. Click on **Deactivate**:

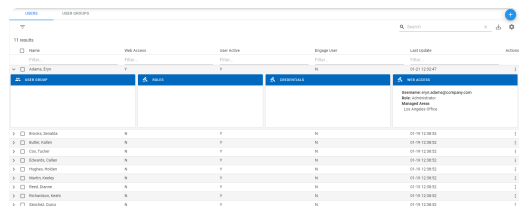


Deactivating one user:

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

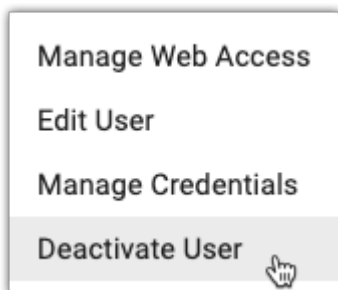


2. All active users in your system will be displayed. Click  next to the user you want to deactivate.



Name	Web Access	Edit Access	Manage User	Last Update	Action
John Doe	Yes	Yes	Yes	2023-10-24	
Jane Smith	No	No	No	2023-10-24	
...

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.

7.7.1. Viewing Deactivated Users

See [Filter Users](#).

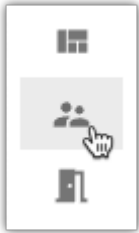
7.7.2. Activating a User Profile

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:



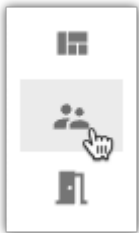
2. All active users in your system will be displayed. Select one or more users who you wish to activate.


Name	Role	User Status	Registration	Last Update	Action
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1
Banks, Brenda	N	Y	N	21-09-2020	1

3. Click on .

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**.

8. 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.


8.1. Access Point Main Page

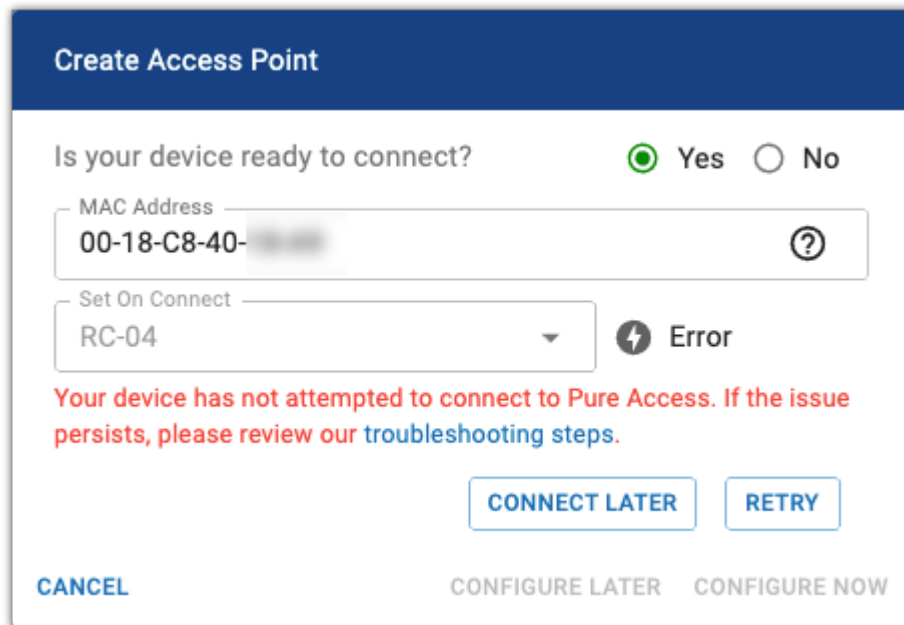
The Access Points main page shows of your access points by name, the groups they are associated with, their MAC address, status (which represents whether they had been tested), the last update (which is determined by when the settings were last changed from the AP screen), and whether or not they are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

ISONAS PUREACCESS Tenants							
ACCESS POINTS ACCESS POINT GROUPS							
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	

8.1.1. Adding a Reader Controller (legacy device)

1. Navigate to the **Access Points** page
2. Hover over the  speed dial button and then select **Create Access Point**
 - a. For a device that is plugged in and [discoverable on the network](#):
 - i. Select “Yes” to the question “Is your device ready to connect?”
 - ii. Input the MAC address of the reader controller (located on the back and side of the device)
 - iii. If the device is either not configured properly or is not currently discoverable, the following message will be displayed:



The screenshot shows a 'Create Access Point' dialog box. At the top, it asks 'Is your device ready to connect?' with 'Yes' selected. Below this, the 'MAC Address' field contains '00-18-C8-40-...' and the 'Set On Connect' dropdown is set to 'RC-04'. An error message is displayed: 'Your device has not attempted to connect to Pure Access. If the issue persists, please review our troubleshooting steps.' At the bottom, there are buttons for 'CONNECT LATER', 'RETRY', 'CANCEL', 'CONFIGURE LATER', and 'CONFIGURE NOW'.

- iii. If the device is either not configured properly or is not currently discoverable, the following message will be displayed:
 - b. For a device that is either not plugged in or not currently [discoverable on the network](#):
 - i. Select “No” to the question “Is your device ready to connect?”
 - ii. Input the MAC address of the reader controller (located on the back and side of the device)
 - iii. Choose the device type from the drop-down list (this may auto-populate with the correct type)
 - c. Input a name for the access point
 - d. Input a description (optional)
 - e. Select the relevant access point group(s) from the list (optional)

- f. Choose the Area to which this access point belongs (if applicable)
- g. Select either “**Configure Later**” or “**Configure Now**”

8.1.2. Adding a Schlage device using ENGAGE

In order to commission Schlage devices in Pure Access, you'll need the ENGAGE mobile app from the [iOS App Store](#) or the Android [Google Play Store](#).

After installing, you'll need to log into the ENGAGE mobile app using the account that had been [created or linked with the tenant](#).

Once logged in, navigate to the “**Sites**” tab where you'll find all of your linked Pure Access tenants associated with your ENGAGE account.

1. Select the site where you want to add a new ENGAGE device from the list
2. Tap the “+” button from the upper right corner of the app
3. Select the type of device you would like to add to Pure Access
 - **Note:** *Only the Schlage RC, NDE, and LE devices are currently supported in Pure Access*
4. Follow the device specific instructions to continue (NDE/LE locks will require you to physically turn and release the interior handle)
5. All devices that are powered on and not currently commissioned to an ENGAGE site will appear in the list
 - a. Select the device you'd like to commission and tap continue
 - b. You can find the serial number on the sticker under the battery cover of the device
6. For NDE/LE – select “**Use Default Settings**”
7. The ENGAGE app will now attempt to establish a Bluetooth connection to the lock
 - a. If successful, the LED on the device will start to blink
 - b. Tap “**Continue**” after confirming the correct device's LED is blinking
8. Enter a name for the device
9. If your Wi-Fi network is not yet saved in ENGAGE, select “**Add a New Network**” and enter your Wi-Fi settings
 - **Note:** *Leave your host configuration unchanged*
10. Tap “**Finish**” to complete the process of adding the Schlage device



The name you enter for the device in Pure Access is the name that will appear in the Schlage Mobile Credential for anyone in that tenant.

8.1.3. Configuring an Access Point

Configure Now

When selecting **Configure Now** (within the [Create Access Point](#) wizard), you will be immediately directed to a new dialog box where you can configure the access point and then run through tests. These options will vary depending on the device type. Here are the default configuration settings for each:

- **RC-04**

Configure Access Point - RC-04

1

2

3

4

Configure

Warning

Lock

Review

RC-04

Door Sense

Latch

Latch Interval

3

seconds

Fail Modes

Fail Safe

Tamper Sensor

ASM

REX/AUX

Beeper

Beeper Sounds

Accept Cards, Reject Cards, REX Event, Tamper Event

Keypad

Keypad Backlight

AUX/REX LED

Lock on Open

Lock On Close

CANCEL

SKIP TEST

BACK

SAVE & CONTINUE

- RC-03

Configure Access Point - RC-03 Classic

1

2

3

4




Configure

Warning

Lock

Review

RC-03 Classic



☐ Door Sense

☒ Latch

Latch Interval seconds

☒ Tamper Sensor

☐ ASM

☐ REX

☐ AUX

☒ Beeper

Beeper Sounds

☒ Keypad

☒ Lock On Close

CANCEL

SKIP TEST

BACK

SAVE & CONTINUE

- IP-Bridge

Configure Access Point - IP-Bridge v2 Door 1

1

2

3

4




Configure

Warning

Lock

Review

IP-Bridge v2 Door 1



☐ Door Sense

☒ Latch

Latch Interval seconds

☐ REX

☐ AUX

☒ Beeper

Beeper Sounds

☒ Lock On Close

CANCEL


SKIP TEST

BACK









SAVE & CONTINUE

Configure Later

To modify the configuration settings on a device:

1. Navigate to the **Access Points** page
2. Select  next to the Access Point you wish to configure, then choose **Edit Device Settings**
3. Make the desired changes, then:
 - a. You may select **SKIP TEST** to jump ahead to the last page of the wizard
 - b. Or you may select **SAVE & CONTINUE** to proceed with testing the enabled peripherals
4. Follow the prompts, then click **SAVE** when finished

8.1.3.1. Configuring the Advanced Security Module (ASM)

1. Navigate to the **Access Points** page
2. Select  next to the Access Point for which you need to configure the ASM, then choose **Edit Device Settings**
3. Toggle the **ASM** slider to the on position
 - a. **Note:** When using an ASM, the **Fail Mode** must be set to “Fail Secure”
4. Select  to proceed
5. Select the desired lock state (once testing is complete) then click either  or 
6. Follow the prompts to configure the ASM
 - a. First, factory reset the ASM by using a pin to hold the reset button down for ~5 seconds (status light will turn green)
 - b. Once the ASM has been reset, click 
 - c. An admit will be sent as a test:
 - i. The reader's LED should turn green for the duration of the latch interval
 - ii. The ASM's status light should turn green for the duration of the latch interval
 - iii. The physical lock should unlatch for the duration of the latch interval
 - d. If the admit test did not successfully unlatch the lock, click  then follow the prompts to repeat the configuration process
7. Proceed through the tests (or click , then select  when finished



If the ASM's status light is stuck green, you will need to repeat the configuration process. If the status light is turning amber during the admit test (step 6C above), the encrypted ASM code does not currently match what is set in Pure Access and the ASM configuration process must be repeated (you may need to factory reset the ASM).

8.1.3.2. Configuration Settings

Important: The following configuration settings *are not* available for every device.

- **First Person In** (Engage devices only): Unlike ISONAS legacy devices, Engage wireless locks and the Schlage RC are not able to utilize the “Auto-Unlock w/ Badge” schedule type, but they have a similar function called “[First Person In](#).”
 - In order for a credential to trigger an Auto Unlock on a device with the First Person In setting enabled, that credential must be active on the device. For wireless locks and the Schlage RC, this means that a user must have grant access privileges to the device via a schedule that is separate from the Auto Unlock rule, since Auto Unlock rules do not allow specification of users or user groups.
- **Door Sense:** enables/disables a connected door position sensor
- **Latch Interval:** duration with which the lock will remain unlatched on admit/approve
- **Tamper:** enables/disables the tamper sensor in the device
- **Tamper Sensitivity** (Engage devices only): controls the sensitivity of the tamper alarm
- **Fail Modes:** [Fail Safe](#) or [Fail Secure](#)
- **ASM:** enable this slider if access point is tied to an [Advanced Security Module](#)
- **REX:** enables/disables a connected REX (Request to Exit) peripheral
 - **REX** drop-down box: choose the action that occurs when someone triggers the REX switch
- **AUX:** enables/disables a connected AUX (Auxiliary) peripheral
 - **AUX** drop-down box: choose the action that occurs when someone triggers the AUX switch
- **Beeper:** enables/disables beeper sounds
- **Beeper Sounds:** select which events trigger the beeper to sound
- **Keypad:** enables/disables the keypad
- **Keypad Backlight:** enables/disables persistent keypad backlight
- **Keypad Back Light Timeout** (Engage devices only): the number of seconds the keypad backlight will stay illuminated after a button is pressed
- **Lock On Close:** enable this slider to lock the door when the door is closed (requires a door position sensor)
- **Lock On Open:** enable this slider to lock the door when the door is opened (requires a door position sensor)
- **Check-In Settings** (Schlage devices communicating via WiFi Only): Use this to configure the check-in frequency*. You can use a daily schedule and have the device check in anywhere from every 1

hour to every 24 hours. You can use a weekly schedule and only have the device check in at specific times on specific days of the week.




Check-In Frequency refers to how often a Schlage device will wake up and communicate with Pure Access via its WiFi connection. When a device check-in occurs it will receive updated device settings and access control configuration from Pure Access as well as report its activity history.

8.1.4. Edit Access Point

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



2. Select  next to the Access Point you wish to edit, then choose **Edit Access Point**

A form titled "Edit Access Point - RC-04" with a dark blue header. It contains several input fields: "MAC Address" with the value "00-18-C8-40-...", "Access Point Name" with the value "RC-04", a large "Description" text area, "Access Point Groups" with a dropdown menu showing "All Doors", and "Area" with a dropdown menu showing "COMMON". At the bottom left, there is a green toggle switch labeled "Active". At the bottom right, there are two buttons: "CANCEL" and "SAVE".

Edit Access Point - RC-04

MAC Address
00-18-C8-40-...

Access Point Name
RC-04

Description


Access Point Groups
All Doors

Area
COMMON

☒ Active


CANCEL SAVE

3. Here, you can see:
 - **MAC Address**
 - **Name**
 - **Description:** a helpful description of the Access Point
 - **Serial Number:** this is the serial number of the physical device (Engage devices only)
 - **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  to save your changes

8.2. Deactivate Access Point

Method 1

1. Navigate to the **Access Points** screen
2. From the access point you wish to deactivate, select the  to view more actions
3. Select **Deactivate Access Point**

Method 2

1. Navigate to the **Access Points** screen
2. From the access point you wish to deactivate, select the  to view more actions
3. Select **Edit Access Point**
4. Toggle the **Active** switch to the off position
5. Click 



Note that a deactivated access point is *still in the system*. If you would like to remove it from your tenant entirely, see this [article](#) which details how to delete an access point.



8.2.1. Viewing Deactivated Access Points

You can filter your view to only see deactivated access points using the “**Active**” filter column. Simply type “N” in the filter field to narrow the results of the access points table.

Connected	Active	Actions
Filter...	N	
No	N	⋮
No	N	⋮

8.2.2. Replacing an Access Point with Another Device

In order for a device to be replaced with another device, it will first need to be [deactivated](#).

1. Navigate to the **Access Points** screen
2. From the deactivated access point you wish to replace, select the  to view more actions
3. Select **Edit Access Point**
4. The **MAC Address** field can now be modified; input the MAC address of the device that will be replacing the old one
5. Click 



Once complete, you will need to send a compile to the device so it can be updated with the users, rules, etc.


8.2.3. Deleting an Access Point

In order for a device to be deleted from the system, it will first need to be [deactivated](#).



Please note that removing an access point from a tenant will also clear all history events from the database.



Instructions

1. Navigate to the **Access Points** screen
2. From the deactivated access point you wish to delete, select the  to view more actions
3. Select **Delete Access Point**

8.3. Access Point Groups



Access Point Groups are used to control a set of Access Points that should all behave the same way (follow the same schedules). 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.

8.3.1. Create Access Point Group



1. Navigate to the **Access Points** page
2. Select  then click **Create Access Point Group**
3. From the **Create Access Point Group** dialog:
 - a. Input a name
 - b. Select an area (if applicable)
 - c. Input a description (optional)
 - d. Select an access point or access points that should be added to the group (optional)
4. Click 

8.3.2. Add Access Point to Access Point Group

Method 1


1. Navigate to the **Access Points** page
2. Select  then click **Add Access Point to Access Point Group**
3. From the **Add Access Point to Access Point Group** dialog:
 - a. Select the desired group from the drop-down list
 - b. Select one or more access points from the drop-down list
4. Click 

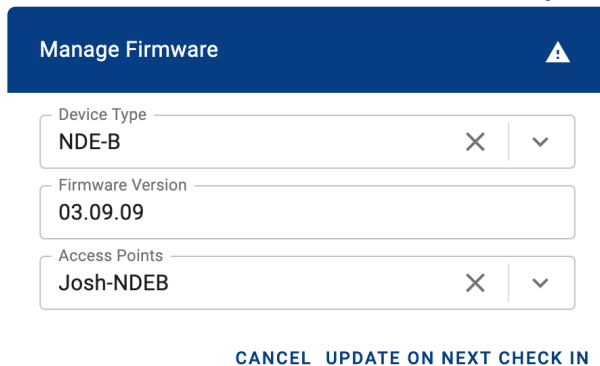
Method 2


1. Navigate to the **Access Points** page
2. From the access point you wish to add to a group, select the  to view more actions
3. Select **Edit Access Point**
4. Select an access point group or multiple access point groups from the drop-down list
5. Click 



8.4. Update Firmware for Schlage Devices

Please note that these instructions apply only to Schlage devices (e.g. LE, NDE, RC).



1. Navigate to the **Access Points** page
2. Hover over the  speed dial button and then select **Update Firmware**
 - a. Please note that if all devices are up-to-date, this option will not be available
3. Select the **Device Type** to update from the **Manage Firmware** Window
4. The **Firmware Version** should auto-populate
5. Select the device(s) to update using the **Access Points** drop-down
6. For Wireless locks NDE and LE, Select **Update On Next Check In**



Manage Firmware 

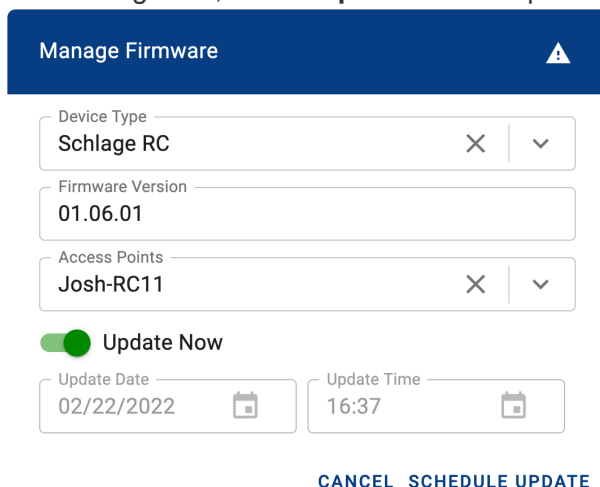
Device Type  


Firmware Version



Access Points  

[CANCEL](#) [UPDATE ON NEXT CHECK IN](#)



7. For Schlage RC, select **Update Now** or provide a date and time before selecting **Schedule Update**




Manage Firmware 


Device Type  

Firmware Version

Access Points  

☒ Update Now

Update Date 

Update Time 

[CANCEL](#) [SCHEDULE UPDATE](#)

9. Access Control

The **Access Control** section allows you to control who has access to which access points and at what time.



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

- Schedules consist of [Weekly Rules](#), [Events](#), and [Holidays](#).
- [Custom Rules](#) are if-then rules that can trigger events based on other actions/conditions.

9.1. Weekly Rules

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

By default, there are three types of weekly rules to choose from:

- **Grant Access:** provides credential access to Users/User Groups for the specified Access Point(s) or Access Point Group(s)
- **Auto-Unlock:** unlocks the Access Point(s) or Access Point Group(s) for the scheduled duration
- **Auto-Unlock w/ Badge:** once a user (with permission) has presented their credential, the Access Point(s) or Access Point Group(s) remain unlocked for the scheduled duration

Additionally, if [Two-Factor Authentication](#) is enabled on your tenant, a special rule type (**Grant Access with Two-Factor Authentication**) becomes available.



Please note that each device can only support one **Auto-Unlock w/ Badge** and one **Grant Access with Two-Factor Authentication** rule.

In order to visualize your weekly rules better, you may want to map them 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 those who need access (users and/or user groups).
3. A column for which doors they will need to access (access points or access point groups).
4. A column for the days of the week and times (scheduled times).

Example

Rule Name	Who? [<i>users/user groups</i>]	Where? [<i>access points/access point groups</i>]	When? [<i>scheduled days and times</i>]
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

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




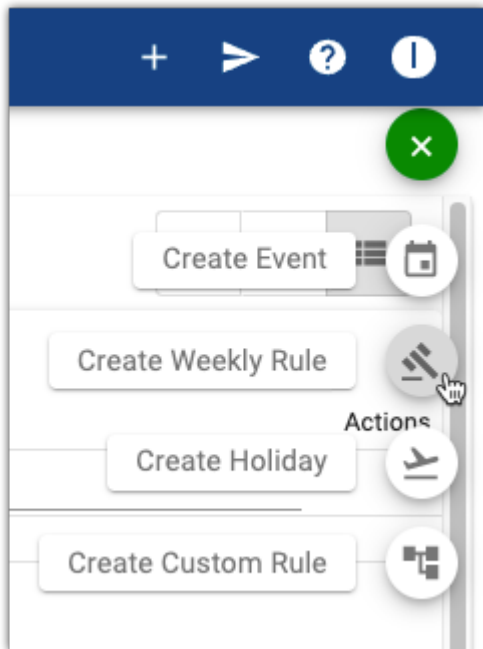
We *highly recommend* utilizing groups (for both users and access points) when configuring any weekly rule. Assigning individual people or doors to rules adds unnecessary complexities that can put a strain on the system when compiling this data to the devices.


9.1.1. Create Weekly Rule

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



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



3. Enter a **Name**, **Description** (optional), select a **Rule Type**, and choose an **Area** (if applicable); then click 

Create Weekly Rule

1 — 2 — 3 — 4
Details Who Where When

Name
All Employees - Front Doors - Office Hours

Description
Daily badge access during office hours

Rule Type
Grant Access

Area
COMMON

☐ Two Factor Authentication

☒ Active

CANCEL BACK NEXT

4. Choose the [User Group](#) or [Users](#) who should be included, then click

NEXT

Create Weekly Rule

✓ — 2 — 3 — 4
Details Who Where When

User Group
All Users

User
User

CANCEL BACK 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

Create Weekly Rule

Progress: Details (✓) — Who (✓) — **Where (3)** — When (4)

Access Point Group: **Front Doors**

Access Point:

CANCEL **BACK** **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

Note: This option is not available for 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

Create Weekly Rule

✓

✓

✓

4

DetailsWhoWhereWhen

Date Type

☒ Non-Holiday ☐ Holiday ☐ Always

Days

☐ 7 Days a Week ☒ Monday - Friday ☐ Custom Days

Times

☐ 24 Hours a Day ☐ 8:00AM to 5:00PM ☒ Custom Times

Start Time
06:00

End Time
18:00

CANCELBACKCREATE

- Alternatively, select **Custom Days** and/or **Custom Times** for a more granular schedule

Create Weekly Rule

✓

✓

✓

4

DetailsWhoWhereWhen

Date Type

☒ Non-Holiday ☐ Holiday ☐ Always

Days

☐ 7 Days a Week ☐ Monday - Friday ☒ Custom Days

Times

☐ 24 Hours a Day ☐ 8:00AM to 5:00PM ☒ Custom Times

<input checked="" type="checkbox"/> Sunday	Start Time 10:30	End Time 15:00
<input type="checkbox"/> Monday	Start Time 06:00	End Time 18:00
<input checked="" type="checkbox"/> Tuesday	Start Time 08:00	End Time 17:30
<input checked="" type="checkbox"/> Wednesday	Start Time 06:00	End Time 18:00
<input checked="" type="checkbox"/> Thursday	Start Time 08:00	End Time 17:30
<input checked="" type="checkbox"/> Friday	Start Time 06:00	End Time 18:00
<input type="checkbox"/> Saturday	Start Time	End Time

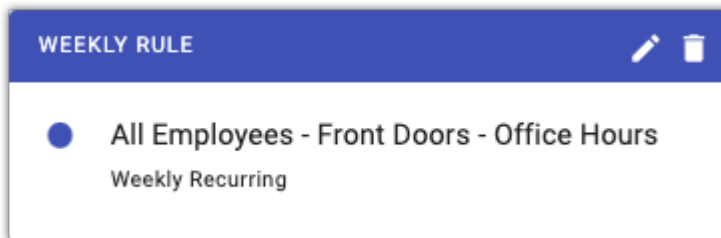
[CANCEL](#)[BACK](#)[CREATE](#)


9.1.2. Edit Weekly Rule

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




2. Find the rule you wish to edit and click on it to bring up the information pop-out, then click 




- Alternately, if you are in list view, click  next to the rule you want to edit and then choose **Edit**
- You can also **Deactivate** or **Delete** a rule using these additional actions

3. Edit the rule as necessary

- Click  to move to the next screen
- You can skip to any of the pages by clicking either **Details**, **Who**, **Where**, or **When**





4. Click  when you are finished

9.1.3. Deactivate Weekly Rule

List View

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






2. Click  to enter list view
3. In-line with the rule you wish to deactivate, click  to open the action options
4. Select **Deactivate**

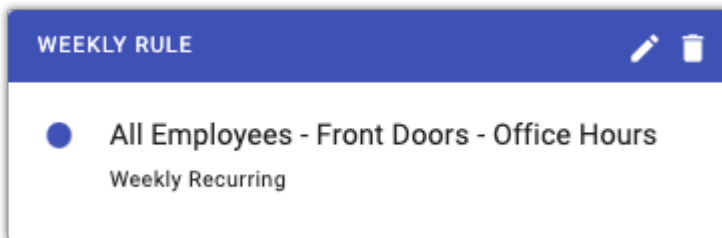
Weekly/Monthly View

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



2. From either the **monthly view** () or **weekly view** (), locate the rule you wish to deactivate

3. Click on the rule to bring up the information pop-out, then click 



4. Select **Details**

Edit Weekly Rule

1

2

3

4

Details

Who

Where

When

Name

All Employees - Front Doors - Office Hours

Description

Daily badge access during office hours

Rule Type

Grant Access

Area

COMMON

☐ Two Factor Authentication

☐ Active

CANCEL

BACK

NEXT

5. Toggle **Active** to the off position

9.2. 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 a minimum of one minute up to an entire day.

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 credential has been presented
- **Lock Down:** puts an access point or access point group into lockdown


✿ An **Event** cannot currently span multiple days.

! Please note that the “**Auto-Unlock w/ Badge**” event type is not supported by Engage devices.

9.2.1. Create Event

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



2. Hover over the  quick dial and then choose **Create Event**
3. Enter the details into the **Create Event** dialog

Create Event

Name

Basketball Game

Description

Senior semi-finals

Date

06/06/2022

☐ All Day

Start Time

18:00

End Time

21:00

☒ Access Point Group ☐ Access Point

Access Point Group

Gym Doors

Event Type

Auto-Unlock w/ Badge

☒ User Group ☐ User

User Group

Faculty

CANCEL

CREATE

- **Name:** name of the event
- **Description:** a description of the event (optional)
- **Area:** choose an area (if applicable)

- **Date:** the day the Event should be active
- **Start Time/End Time** or **All Day** toggle: the start and end times for the event or toggle the event to last all day
- **Access Point Group** or **Access Point** radio buttons: choose one of the radio buttons, as appropriate
- **Access Point Group** or **Access Point** drop-down: choose the appropriate access point(s) or group(s)
- **Event Type:** choose the appropriate [Event Type](#)




4. Click

CREATE

9.2.2. Edit Event

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



2. Find the event you wish to modify:
 - a. From the weekly or monthly calendar views, click on the event to bring up the information pop-out, then click 
 - b. From the list view, select the  under **Actions** then click “Edit”
3. Make the desired changes in the **Edit Event** dialog
4. Click  when finished

9.3. 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.*”




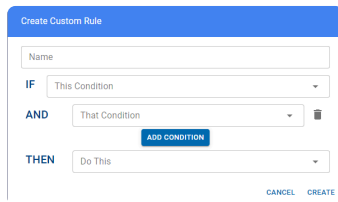
Custom Rule functionality requires an active connection to the Pure Access software. If an ISONAS device is offline or disconnected, custom rules associated with this device will not be triggered.

9.3.1. Create Custom Rule

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



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



- 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 

* 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.

9.3.2. 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

9.4. 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 to run “Always”, the door will follow this rule on days set as a **Holiday** in the tenant.




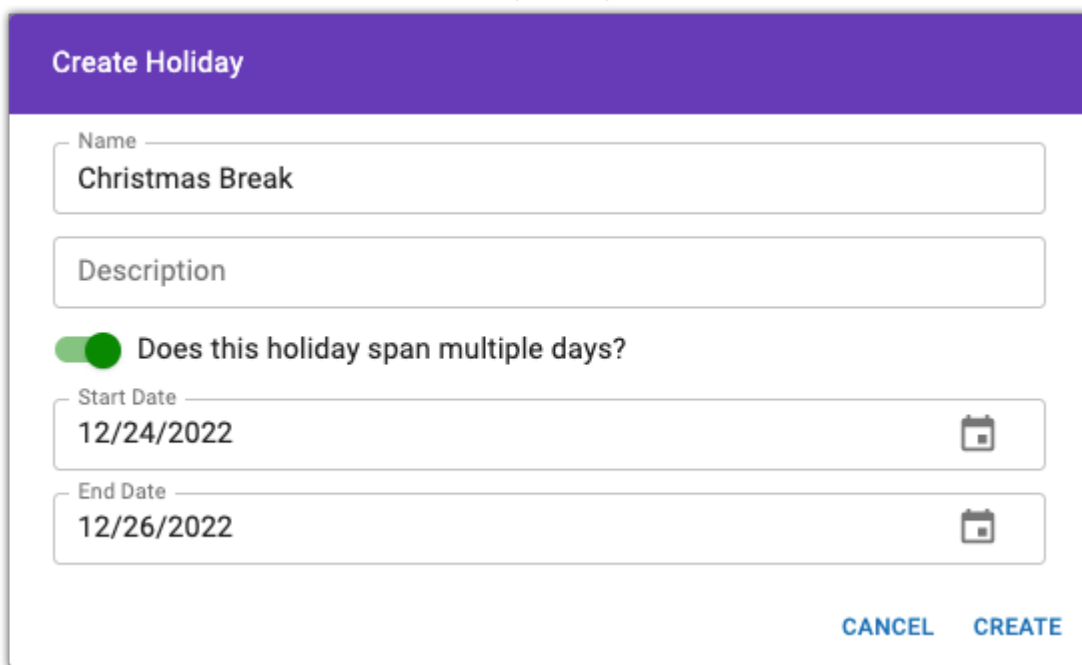
Holidays are not supported by **Engage** devices and cannot be used within Engage-enabled tenants at this time.

9.4.1. Create Holiday

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



2. Hover over the  quick dial and then choose **Create Holiday**
3. Enter the details into the **Create Holiday** dialog



- **Name:** name of the holiday
- **Description:** a description of the holiday (optional)
- Toggle 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 





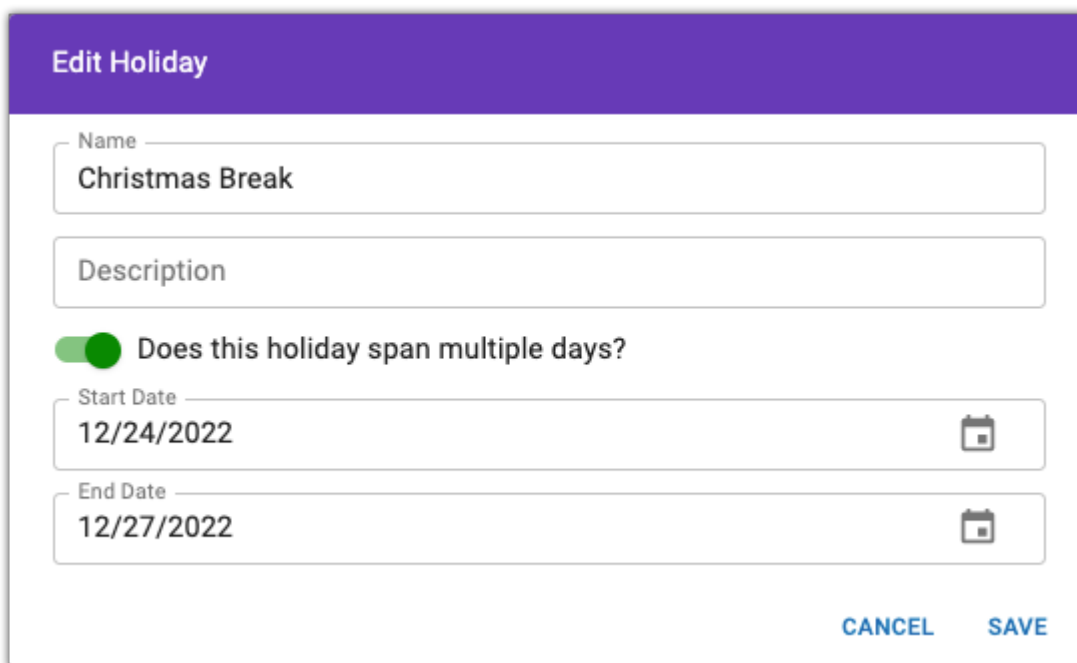
Holidays are not supported by **Engage** devices and cannot be used within Engage-enabled tenants at this time.

9.4.2. Edit Holiday

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



2. Find the holiday you wish to modify:
 - a. From the weekly or monthly calendar views, click on the holiday to bring up the information pop-out, then click 
 - b. From the list view, select the  under **Actions** then click “Edit”
3. Make the desired changes in the **Edit Holiday** dialog



4. Click  when finished



Holidays are not supported by **Engage** devices and cannot be used within Engage-enabled tenants at this time.

9.5. 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.

10. Reports

There are a variety of reports that can be utilized within Pure Access. Depending on the report being run, they can be sorted by start date and end date, filtered by users, access points, event types, badge information, and/or areas.

All reports can be exported as a .PDF or .CSV for further analysis. In addition, each column can be sorted alphabetically (ascending/descending) by selecting the headers.

1. Navigate to the **Reports** page



2. Choose the report you wish to view from the **Report** drop-down menu
3. Set any desired filters (optional)

4. Click 

5. To download this information, 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](#)

10.1. Access Point Groups Report

An **Access Point Groups** report displays which access points are members of which groups.

This report contains the following information:

- *Name of access point group*
- *Name of access points*
- *MAC address*
- *Test status (complete/incomplete)*

This report can be filtered by:

- *Access Point Groups*
- *Areas*

Note: The downloaded report will also include the description of each access point from the “Description” field of the access point’s properties.



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.2. Access Point Permissions Report

The **Access Point Permissions** report displays the users and rules assigned to individual access points.

This report contains the following information:

- *Name of access point*
- *Users*
- *Rule name(s)*

This report can be filtered by access point(s) and user(s).



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.3. Access Points Report

The **Access Points** report provides a list of doors within the tenant.

This report contains the following information:

- *Name of access point*
- *MAC Address*
- *Whether tests have been completed*
- *Description (can be changed from the access point's properties)*

This report can be filtered by access point(s).



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.4. History Report

The **History** report allows you to review status updates and events that had an affect on doors within the tenant.

This report contains the following information:

- *Access Point name*
- *Name of user (if applicable)*
- *Time of the event*
- *Type of [event](#)*
- *Credential (if applicable)*

This report can be filtered by:

- *Date Range (by default, displays from yesterday's date at 06:00 to tomorrow's date at 05:59)*
- *Access Points*
- *Access Point Groups*
- *Event Types*
- *User Groups*
- *Users*
- *More Filters (option to **Show System Administrator**; enabled by default)*



Only the first 100 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.5. Holidays Report

The **Holidays** report provides an overview of all currently scheduled holidays in the system.

This report contains the following information:

- *Holiday name*
- *Start date*
- *End date*
- *Description (can be changed by editing the holiday under Access Control)*

You can use the date range filter to display all past, current, or future holidays to ensure you have all appropriate holidays in place. By default, displays entire history to current date.



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.6. User Attendance Report

The **User Attendance** report displays the “Time In” and “Time Out” activity for users. This reflects the time in which the user first badged in for the day and then the final time their credential was presented (it *does not* take into account times where the credential was presented between the first and last).

This report contains the following information:

- *Name of user*
- *Time in*
- *Time out*
- *Total (amount of time)*

This report can be filtered by:

- *Date (displays today’s date by default)*
- *Users*

Example

If a user enters at 8:05AM, exits at 12:03PM, comes back at 1:01PM, and then out again at 4:59PM – the report will reflect an 8:05AM “Time In” and a 4:59PM “Time Out” and show the total time of 8h 54m.



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.7. User Export Report

The **User Export** report allows you to review and/or export user data in PDF/CSV format.

This report contains the following information:

- *First Name*
- *Last Name*
- *When the user was created (date and time)*
- *Email address (notification email)*
- *Area*
- *Employee ID*
- *User defined fields*

This report can be filtered by date range (according to when users were created in the tenant, by default displays entire history to the current date) and by user(s).



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

Pure Access Manager

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										

10.8. User Group Attendance Report

The **User Group Attendance** report displays the “Time In” and “Time Out” activity for users by User Group. This reflects the time in which the user first badged in for the day and then the final time their credential was presented (it *does not* take into account times where the credential was presented between the first and last).

This report contains the following information:

- *User group name*
- *Name of user*
- *Time in*
- *Time out*
- *Total (amount of time)*

This report can be filtered by:

- *Date (displays current date by default)*
- *User Groups*

Example

If a user enters at 8:05AM, exits at 12:03PM, comes back at 1:01PM, and then out again at 4:59PM – the report will reflect an 8:05AM “Time In” and a 4:59PM “Time Out” and show the total time of 8h 54m.



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.9. User Group Permissions Report

The **User Group Permissions** report displays the weekly rules and doors that are assigned access to specific user groups.

This report contains the following information:

- *Name of user group*
- *Access point name(s)*
- *Rule name and type*
- *Day(s) rule is active*
- *Start time of the rule(s)*
- *End time of the rule(s)*

This report can be filtered by user group(s).



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.10. User Groups Report

A **User Groups** report displays which users are members of which groups.

This report contains the following information:

- *Name of user group*
- *Name of user*
- *Email login (web access username, if applicable)*
- *Badge ID*
- *Credential status*

This report can be filtered by:

- *User Status*
- *Credential Status*
- *User Groups*



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

10.11. User Permissions Report

The **User Permissions** report displays individual users who are assigned directly to rules.

This report contains the following information:

- *Name of user*
- *Access point name(s)*
- *Rule name and type*
- *Day(s) rule is active*
- *Start time of the rule*
- *End time of the rule*

This report can be filtered by users.



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.



If you have set up all rules by user group (recommended), this report will not display data.

10.12. Users Report

A **Users** report allows you to review user information and their assigned credentials.

This report contains the following information:

- *Name of user*
- *Email login (web access username, if applicable)*
- *Badge ID*
- *GUID*
- *Credential status*
- *Special properties (if applicable)*
- *Count limit (if applicable)*
- *Credential expiration (if applicable)*

This report can be filtered by:

- *User Status*
- *Credential Status*
- *Users*



Only the first 50 results will be displayed when the report is run. To view all results, the report must be downloaded as a PDF or CSV.

11. 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](#)

11.1. 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

11.2. Integrator Information

This information should be kept up-to-date.

11.3. 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](#)

11.3.1. 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.

11.3.1.1. 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.

11.3.1.2. 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.

11.3.1.3. 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.

11.3.1.4. Configuration Process

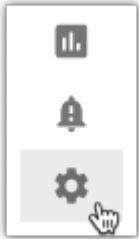
To configure and use two-factor authentication, you must:

1. Enable two-factor authentication from the **Settings** page (under the **Global Settings** tab)
2. Set up [two-factor credentials](#) (for any Card/PIN configuration)
3. Set up a [two-factor rule](#)

11.3.1.4.1. Enable Two-Factor Authentication

Before configuring two-factor credentials and rules, you must first choose a global two-factor setting to enable.

1. Navigate to the **Settings** page by clicking the **Settings** button on the left navigation bar.



2. Click the “**Global Settings**” tab.
3. Under the **Two-Factor Authentication** heading, you can choose from the three [two-factor modes](#) or globally disable two-factor.
4. Enter the number of seconds to wait for the second credential into the **Two Factor Timeout** box.
 - Default is ten (10) seconds. This can be set between five and 30 seconds.

When first enabling two-factor authentication, ensure your devices are on up-to-date firmware.

Two Factor is available for the following firmware versions:

- RC-04 – Coldfire v75.06 / WL v1.8 / BLE v1.6 (or greater)
- RC-03 Rev M/N – Coldfire v63.01 / PIC v33.03 (or greater)
- IP-Bridge v2.0 – All firmware versions

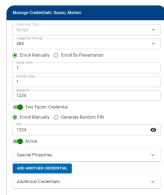


Before globally disabling two-factor, you'll need to ensure that all two-factor rules are removed from Pure Access.

11.3.1.4.2. Adding Two-Factor PINs

If you've chosen either the **Card/PIN** or **Two-User – Card/PIN** modes, you'll need to configure two-factor credential PIN's.

To start, navigate to the users page and select the user you would like to create a two-factor PIN for. Once selected, you can either update an existing badge to add a two-factor PIN or configure a new badge/mobile credential and two-factor PIN:



Two-factor PIN's must consist of between 4 and 9 digits. Cards that have been configured with a PIN will still work as a normal badge when accessing a non two-factor access point.

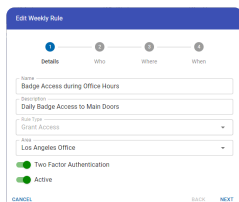


To enhance the security of the two-factor system, you will be unable to reveal the configured PIN once it has been saved.

11.3.1.4.3. Adding Two-Factor Rules

Once two-factor authentication is globally enabled, navigate to the [Weekly Rules](#) page by clicking the **Access Control** button on the left navigation bar. From here you can either edit an existing rule or add a new rule to use two-factor authentication.

To enable two-factor authentication on a rule, simply enable the slider on any **“Grant Access”** rule type:



In the event that there are rules with overlapping schedules, the two-factor rule will always take precedence over the standard rule.



Only the **“Grant Access”** rule type supports two-factor authentication.

11.3.1.5. 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	<i>Denied – Timeout</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 Timeout	(2)	
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.

11.4. Areas

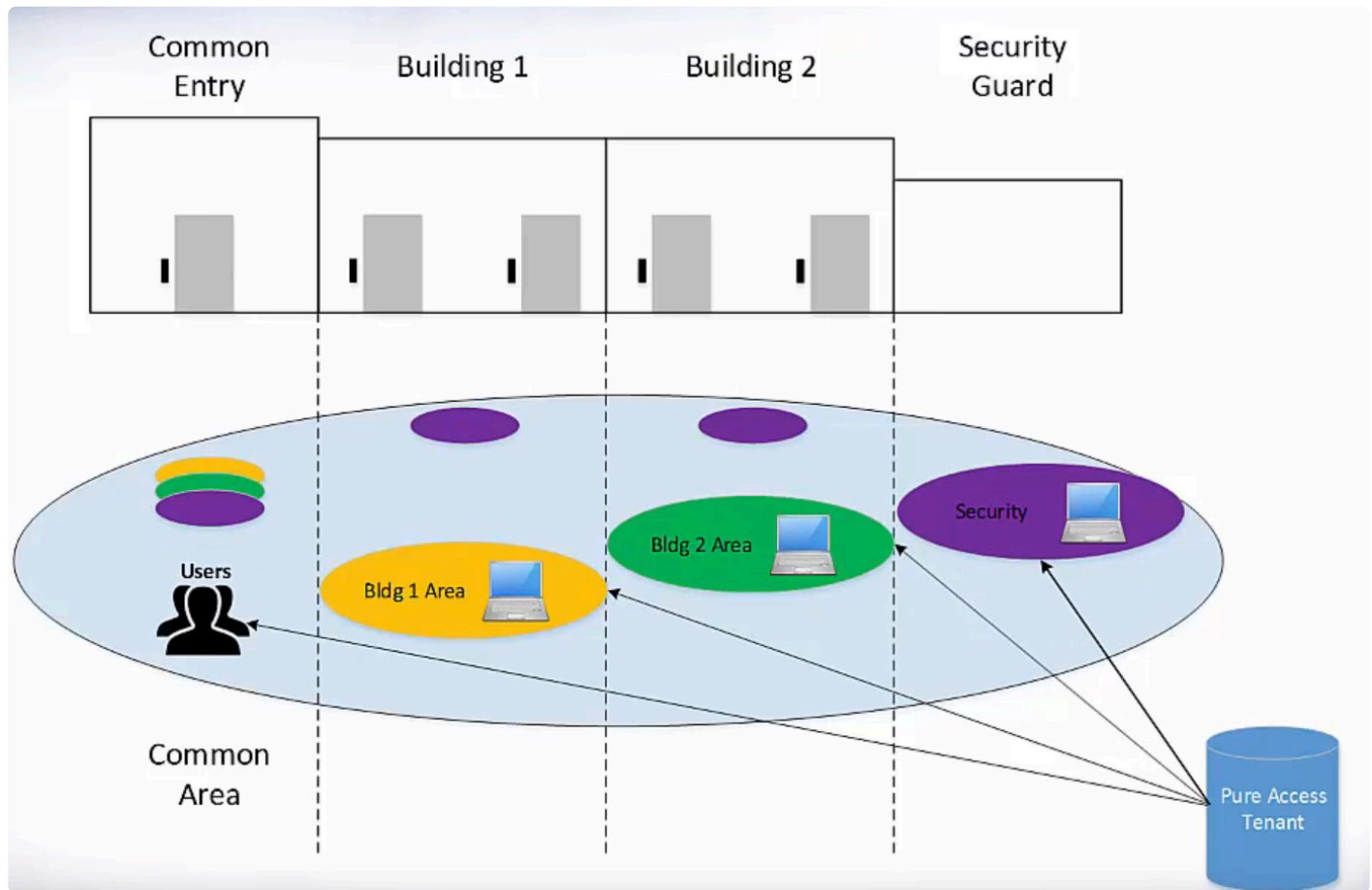
Areas are “containers” which are used to segment a Pure Access tenant for **administration purposes**.

- 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.

11.4.1. 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.

11.4.2. 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.

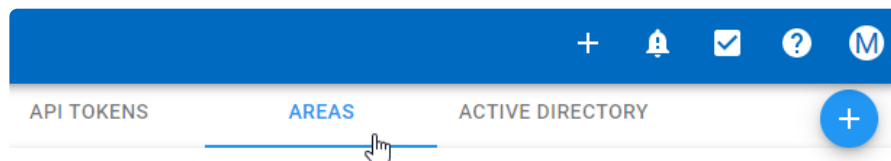
Once another area is added to the system, the areas feature will be turned on and everything created in the system will need to be designated to an area.

Creating an Area

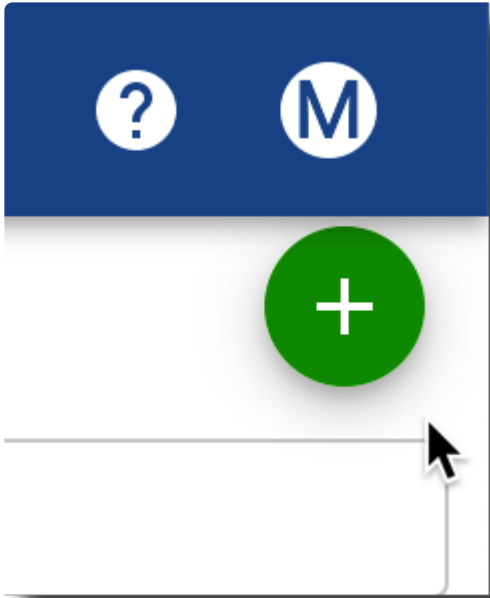
1. Navigate to the **Settings** page from the left navigation bar.



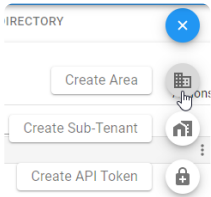
2. Select the **Areas** tab.



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.

Create Area

1

2

Area

Area Access

Area Name

Los Angeles Office

Timezone

(UTC-08:00) Pacific Time (US & Canada)

CANCEL

BACK


NEXT

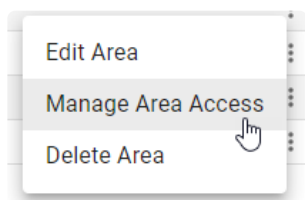
For the below example, we've created three new areas in addition to COMMON – *Los Angeles Office*, *New York Office*, and *Security Center*.

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			

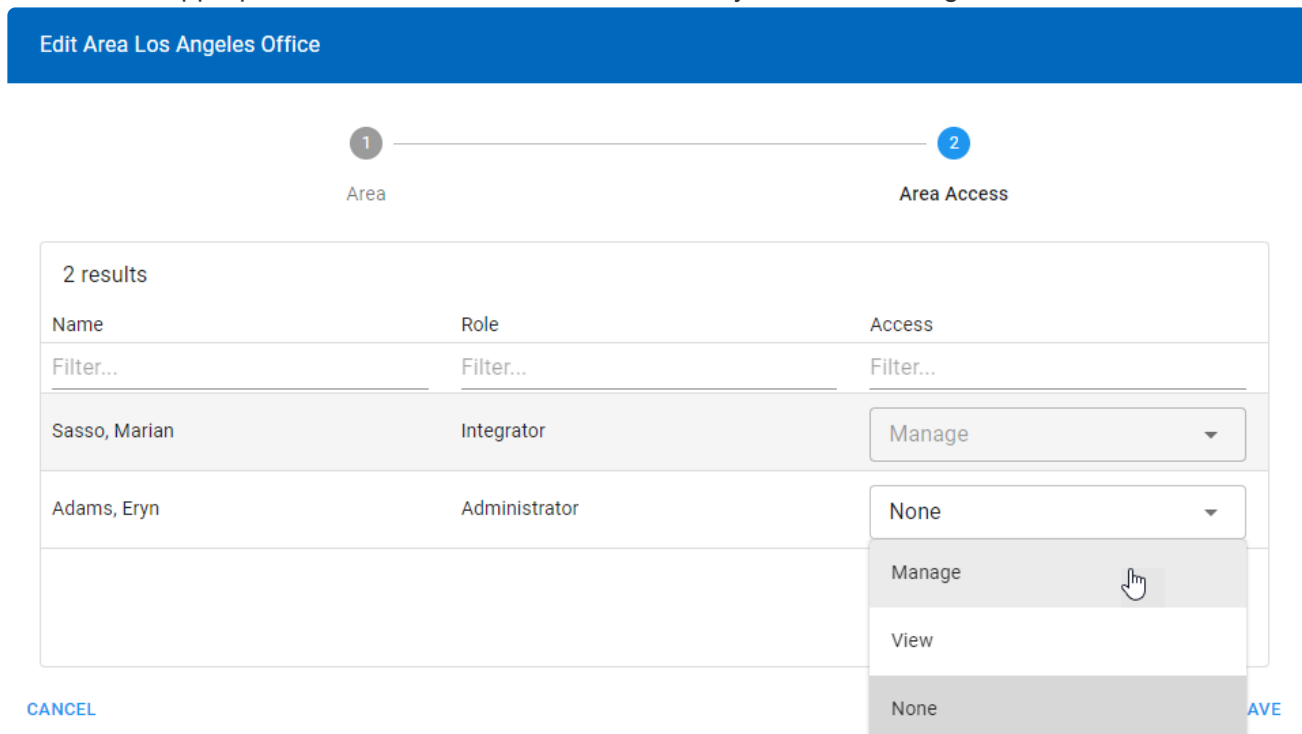
Assign Administrators to an Area

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.

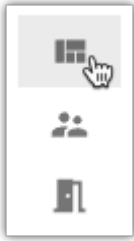



* Users must have web access granted before they can be assigned as an administrator. See [Setting Up Web Access for a User](#).

* 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.

11.4.2.1. Assigning Dashboards to an Area

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

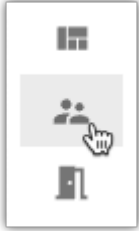



2. Hover over the name of the dashboard you want to edit and choose  (or [create a new dashboard](#)).
3. From the **Area** drop-down menu, select the area with which this dashboard needs to be associated.

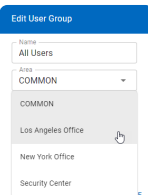
11.4.2.2. Assigning Groups to an Area

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.




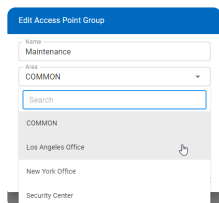
4. Then click .

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 .


11.4.2.3. 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 .


11.4.2.4. Assigning Users to an Area

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


11.4.2.5. Assigning Holidays to an Area

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

11.4.2.6. Assigning Weekly Rules to an Area

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

11.4.2.7. Assigning Events to an Area




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

11.4.3. 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 .

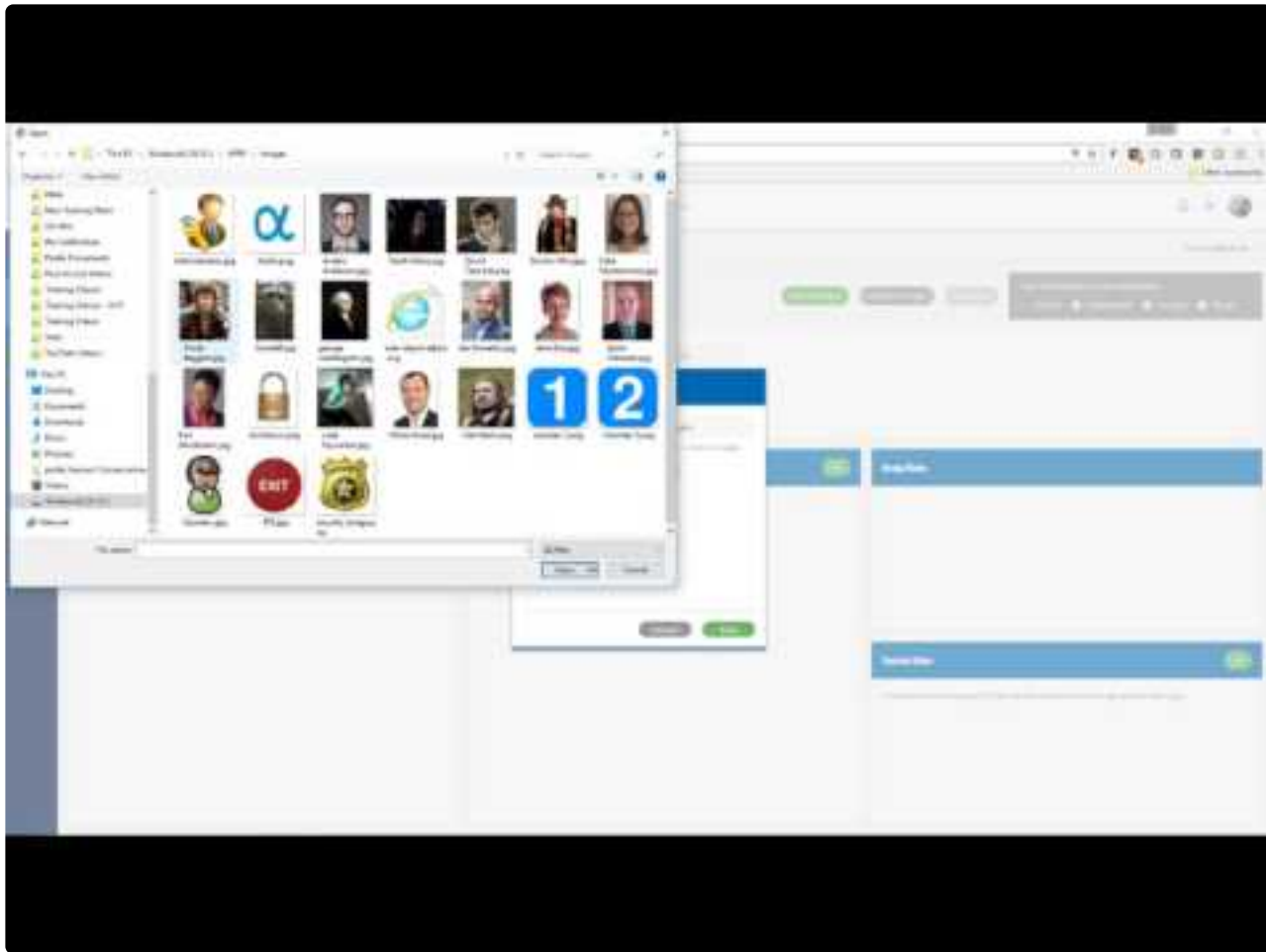


Please note that a newly created user profile will inherit ALL areas that the integrator/administrator account is associated with.

11.5. Credential

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

11.5.1. Bitmasking



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

Resources

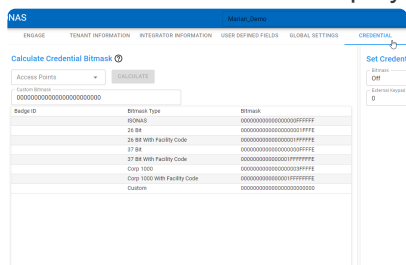
- Verifying the [currently set bitmask](#).
- [Discover and set](#) a bitmask.
- [Pushing bitmask settings](#) to all readers.
- [Pushing bitmask settings](#) to all readers in PAM 2.12.2 or below.
- Setting an [external keypad site code](#).
 - Configuring [site code on an R-1 reader](#).
- Creating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

11.5.1.1. 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.



11.5.1.2. Identifying Credential Data

1. Present an unenrolled badge/fob to a reader. You should see a  **Decline Badge Not Found** event in the history.
2. Navigate to the **Settings** tab:



3. Click the **Credential** tab under **Settings**.
4. From the right, use the *Access Point* drop-down menu to select the reader where the credential had been presented:

Calculate Credential Bitmask ⓘ

Front Door

Custom Bitmask
00000000000000000000000000000000

Badge ID	Bitmask Type	Bitmask
	ISONAS	00000000000000000000000000000000
	26 Bit	00000000000000000000000000000000
	26 Bit With Facility Code	00000000000000000000000000000000
	37 Bit	00000000000000000000000000000000
	37 Bit With Facility Code	00000000000000000000000000000000
	Corp 1000	00000000000000000000000000000000
	Corp 1000 With Facility Code	00000000000000000000000000000000
	Custom	00000000000000000000000000000000

CALCULATE

5. Click
6. This will display how the credential is being read for each of the bitmask settings:

Calculate Credential Bitmask ⓘ

Front Door

Custom Bitmask
00000000000000000000000000000000

Badge ID	Bitmask Type	Bitmask
6250155	ISONAS	00000000000000000000000000000000
44885	26 Bit	00000000000000000000000000000000
11513685	26 Bit With Facility Code	00000000000000000000000000000000
503637	37 Bit	00000000000000000000000000000000
716156757	37 Bit With Facility Code	00000000000000000000000000000000
1027925	Corp 1000	00000000000000000000000000000000
716156757	Corp 1000 With Facility Code	00000000000000000000000000000000
	Custom	00000000000000000000000000000000

If the badge ID printed on the credential *does not appear on this list*, there are two options for enrolling the credential:

- [Enroll by presentation](#)
- 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.

11.5.1.3. Discover the Appropriate Bitmask

Verifying the correct bitmask for your credential:


- Present an unenrolled badge to a reader.
 - Note:** The badge must be **unenrolled** and get rejected. You should see a “**Decline Badge Not Found**” event with the name “**System Admin**” in the history.
 - The badge data will remain in the system for 15 minutes or until another unenrolled credential is presented to this reader.

- In Pure Access, navigate to the **Settings > Credential** tab.

- From the “Access Point” drop-down list, select the reader where the unenrolled badge was


presented then click .

Calculate Credential Bitmask ⓘ

Front Door		
Custom Bitmask	000000000000000000000000	
Badge ID	Bitmask Type	Bitmask
	ISONAS	000000000000000000000000
	26 Bit	000000000000000000000000
	26 Bit With Facility Code	000000000000000000000000
	37 Bit	000000000000000000000000
	37 Bit With Facility Code	000000000000000000000000
	Corp 1000	000000000000000000000000
	Corp 1000 With Facility Code	000000000000000000000000
	Custom	000000000000000000000000

- The “**Badge ID**” column will populate. If one of these numbers matches what is printed on the badge, this is the bitmask that should be set on the readers.

Calculate Credential Bitmask ⓘ

Front Door		
Custom Bitmask	000000000000000000000000	
Badge ID	Bitmask Type	Bitmask
6250155	ISONAS	000000000000000000000000
44885	26 Bit	000000000000000000000000
11513645	26 Bit With Facility Code	000000000000000000000000
593637	37 Bit	000000000000000000000000
716156757	37 Bit With Facility Code	000000000000000000000000
1027925	Corp 1000	000000000000000000000000
716156757	Corp 1000 With Facility Code	000000000000000000000000
	Custom	000000000000000000000000

If there is **no matching badge ID** in step 4, you will either need to calculate a [custom bitmask](#) in order to manually enroll these credentials or you are using a high frequency credential and will need to [enroll them by presentation](#).

11.5.1.4. 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**.

Set Credential Bitmask ?

Bitmask
26 Bit

Search

ISONAS

26 Bit

26 Bit With Facility Code

37 Bit

37 Bit With Facility Code

SEND BITMASK TO ALL READERS

CANCEL 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.

11.5.1.4.1. Pushing the Current Bitmask Setting to All Readers

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



2. Click the **Credential** tab.



CREDENTIAL

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](#).

11.5.1.4.2. 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.

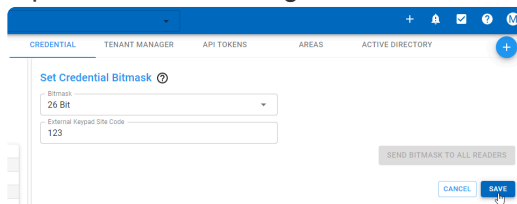
11.5.1.5. Setting an External Keypad Site Code

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 **SAVE**.



* 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.

11.5.1.5.1. 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 0 0 1.

11.5.1.6. 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.

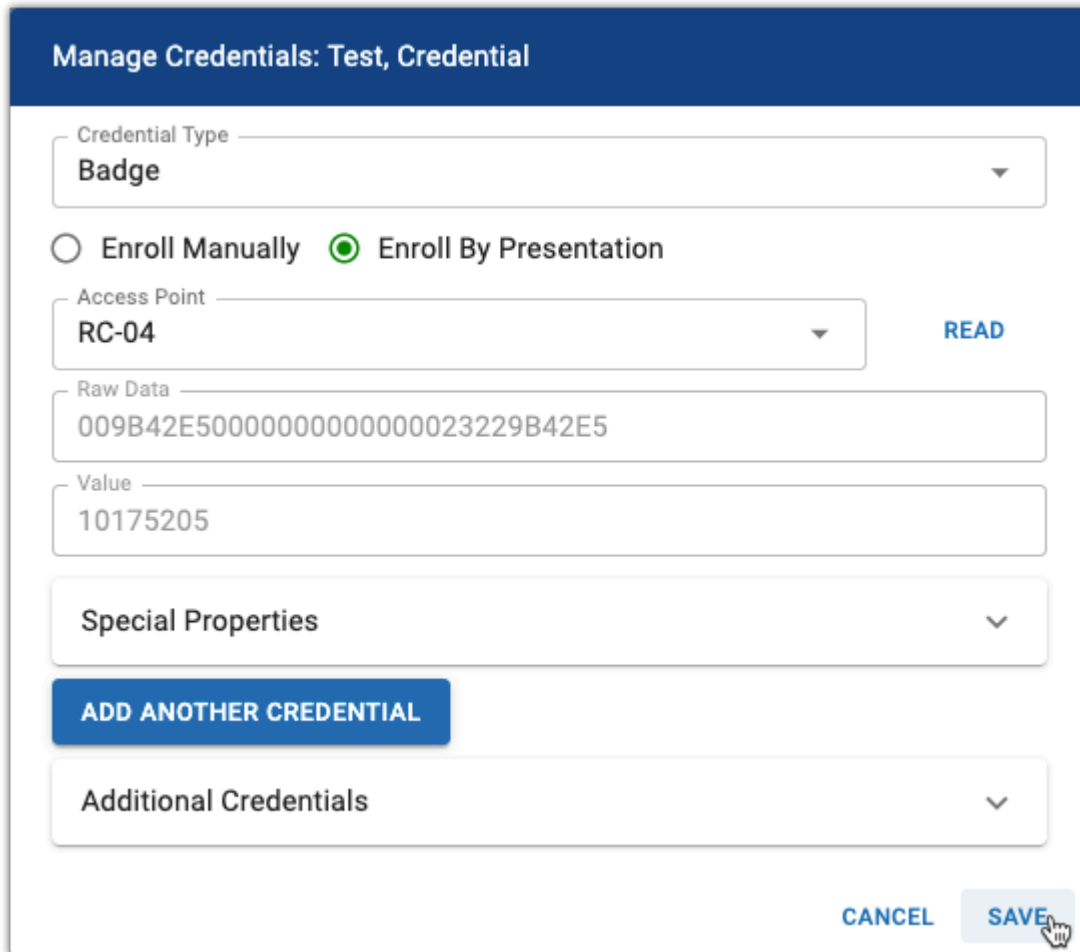
1. Present the unenrolled credential to a reader to produce a “**Decline Badge Not Found**” event in the dashboard history. Take note of the value under the “BADGE” column:

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**”:



Manage Credentials: Test, Credential

Credential Type **Badge**

☐ Enroll Manually ☒ **Enroll By Presentation**

Access Point **RC-04** **READ**

Raw Data **009B42E5000000000000000023229B42E5**

Value **10175205**

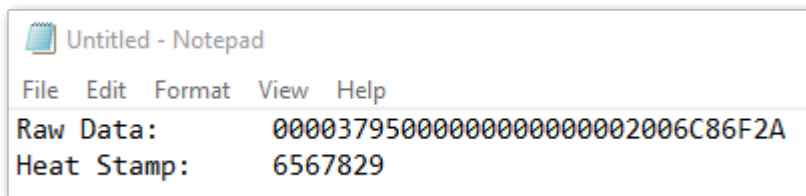
Special Properties

ADD ANOTHER CREDENTIAL

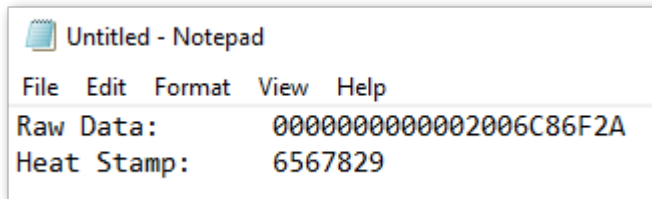
Additional Credentials

CANCEL **SAVE**

- 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:



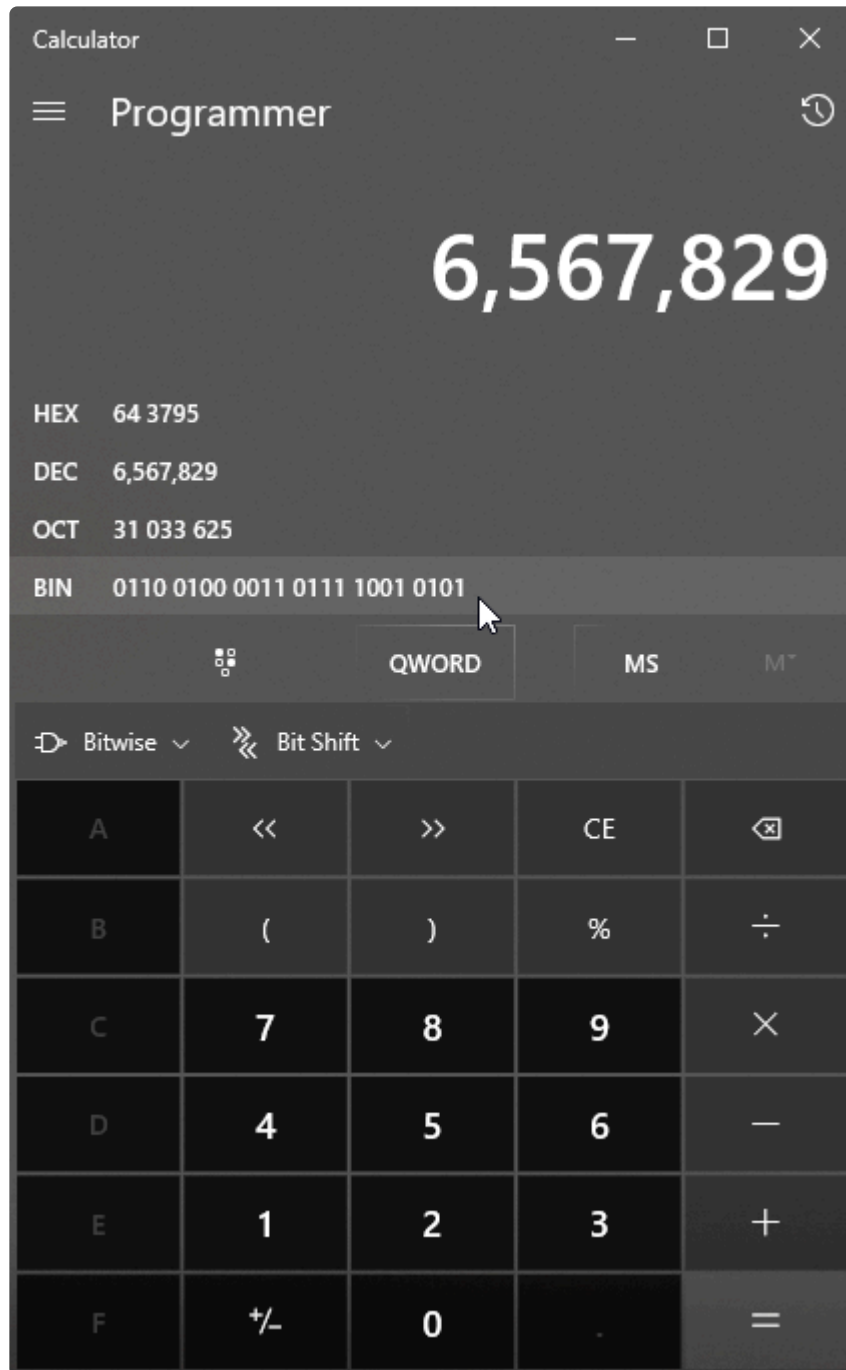
Converting data to binary:

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).

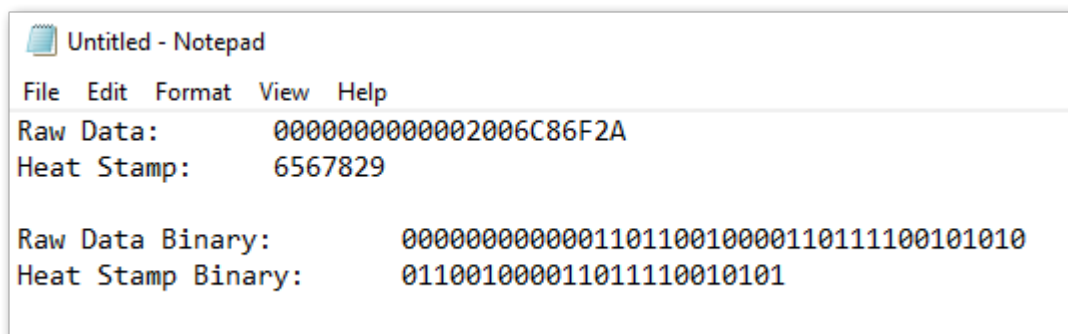
1. Copy the raw data value from Notepad and paste it into the calculator, then click "**BIN**" (binary).



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:	000000000000110110010000110111100101010
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:	000000000000110110010000110111100101010
Heat Stamp Binary:	011001000011011110010101
Wanted Bits:	00000000000001111111111111111111111110

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:



7. This value is our custom bitmask.


```
Wanted Bits: 111111111111111111111110 = 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):

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



2. Select **Credential** from the secondary navigation.
3. Under **Set Credential Bitmask**:
 - a. Select **Custom** from the **Bitmask** drop-down box.
 - b. Paste the value from above into the **Custom Bitmask** box.
 - c. Enter the **External Keypad Site Code**.
4. Click **SAVE** and then **SEND BITMASK TO ALL READERS**.

Set Credential Bitmask 

Bitmask

Custom

Custom Bitmask

000000000000000000000001FFFFFFF

External Keypad Site Code

123

SEND BITMASK TO ALL READERS

CANCEL

SAVE

To test your custom bitmask: enroll the credential to a user [via presentation](#), send an update to your access points, then present the credential to a reader.

11.5.1.7. 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.

11.6. 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 **SAVE**.
5. These fields will now all appear on the [user profile page](#).

11.7. 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](#).

! **NOTE:** AD Connect software is **NOT** compatible with ENGAGE devices (Schlage RC, NDE, LE). Please see the [AD Connect Limitations and Requirements](#) page for additional information.

* 51-100 license and above

11.7.1. AD Connect Limitations and Requirements

ENGAGE Device Limitations

ISONAS devices require a bitmask to be set at the device level such that only a single credential format can be used on each device. You can learn more about how Pure Access handles bitmasking [here](#). For credentials being enrolled on ISONAS devices, only the Badge ID is required (this is how the AD Connect integration currently functions). If the bitmask is set correctly, the device then delegates to Pure Access for backfilling data such as the credential facility code or issue level when the badge is scanned for the first time.

In contrast, ENGAGE devices (Schlage RC, NDE, LE) rely on the credential records themselves to specify a specific bit format and all of the data associated with that bit format. You can see the data required for each card format on the [Importing Users into Pure Access Cloud](#) page. Because of this distinction, **AD Connect does not support integration with ENGAGE devices at this time.**

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.

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.

Resources:

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

11.7.2. 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 AD Connect 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://app.pureaccess.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 AD Connect is installed) and a description of your issue to our [support team](#) for review.

11.7.3. 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 AD Connect is installed) and a description of your issue to our [support team](#) for review.

11.8. 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.


11.8.1. 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.

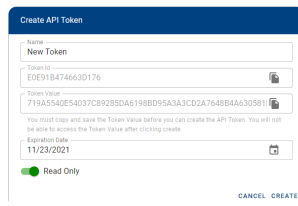
Authentication to the API is performed via [HTTP Basic Auth](#). Provide your API ID and token pair (TokenID:TokenValue) as the basic auth username value. You do not need to provide a password.


11.8.2. 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 and 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**.

11.8.3. 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>

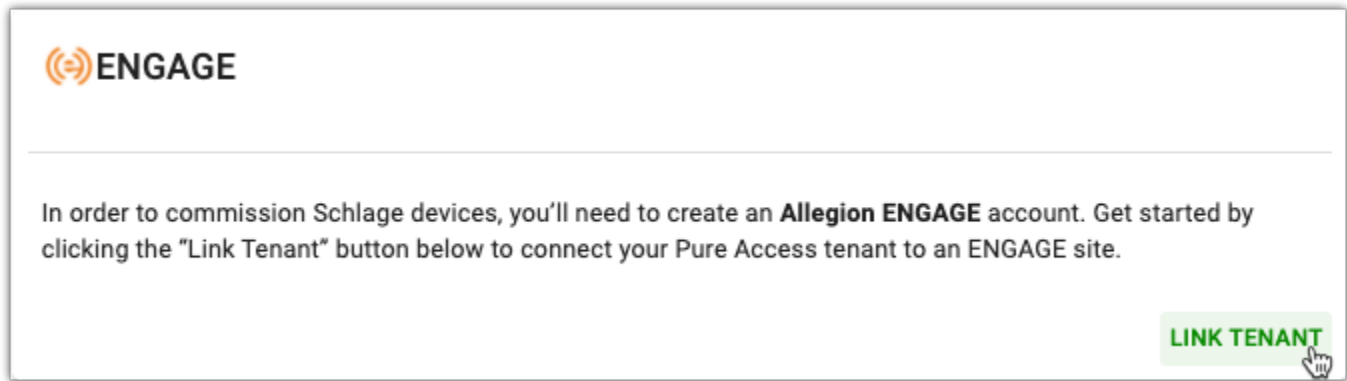
11.9. ENGAGE

The Allegion ENGAGE™ ecosystem is a mobile application that delivers simple and convenient commissioning services for Schlage devices. In order to use Schlage devices (such as NDEB, LEB, and the Schlage RC), you'll need to link your Pure Access tenant to ENGAGE.

11.9.1. Linking to ENGAGE

Overview

In order to [add ENGAGE devices](#) to your Pure Access tenant, you must first establish a relationship between the tenant and an ENGAGE site by linking them together.



! Linking to ENGAGE will permanently change the way your tenant functions to ensure the most consistent experience possible across all device types.

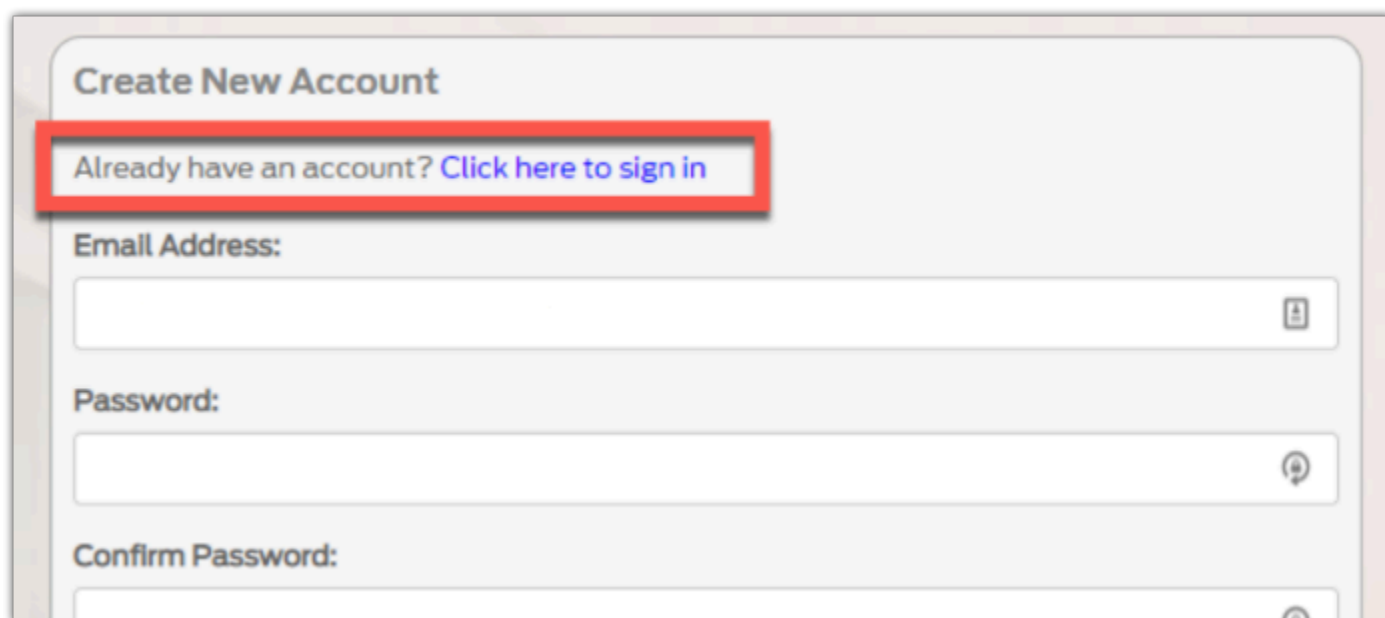
Once your tenant is linked with ENGAGE, there are a number of changes that will be enforced globally within Pure Access:

- Enrolling any new credentials will require the credential to be a known credential format.
- **Holidays** and the "Holiday" date type within schedules can no longer be created/used.
- You can no longer enroll by presentation on legacy ISONAS devices (RC-04, RC-03, and IP-Bridge). Enrollment by presentation will *only* be supported by a Schlage RC after linking.

Instructions

1. Once you click **Link Tenant**, an email invitation will be sent to the email address of the currently logged in web access user
2. Click on the link in the invitation email and proceed to the ENGAGE account creation screen
3. If you do not have an account:
 - a. Continue to fill out the new account form and click submit
4. If you already have an ENGAGE account associated with your email address:
 - a. You can add the new Pure Access tenant to this account by clicking the link at the top of the

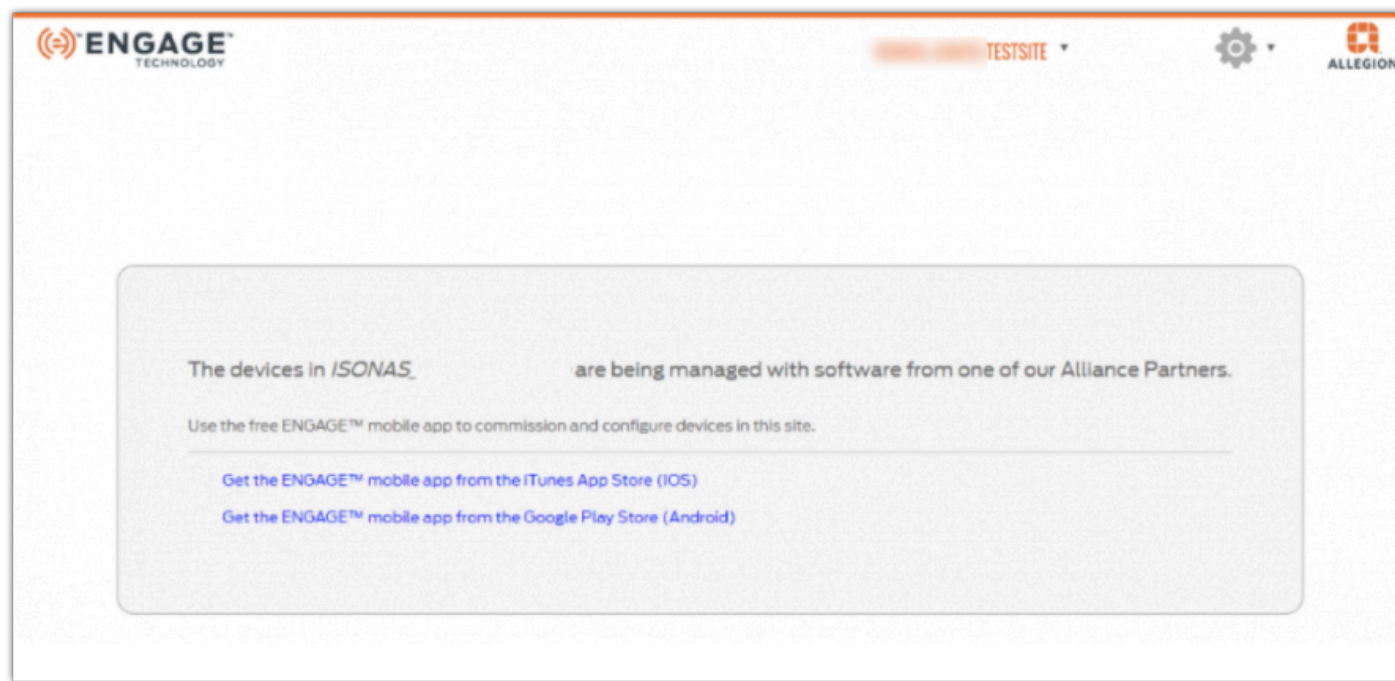
new account registration form



The image shows a 'Create New Account' registration form. At the top, the title 'Create New Account' is displayed. Below it, a red rectangular box highlights the text 'Already have an account? [Click here to sign in](#)'. The form contains three input fields: 'Email Address:', 'Password:', and 'Confirm Password:'. Each field has a small icon on the right side of the input box, likely for password strength or visibility toggles.

There is an additional email to confirm your email address for account verification. To confirm your account is working properly, you can login with the username and password you just created.

If successful, you will see the following screen confirming you are ready to login to the ENGAGE mobile app for [device commissioning](#):



11.9.2. Inviting Users to ENGAGE

Preconditions:

1. The Pure Access Tenant must have already been linked to ENGAGE.
2. Users must have web access permissions before they can be invited to ENGAGE.

Inviting Pure Access Users to ENGAGE

1. In the Pure Access application, Navigate to Settings > ENGAGE.
2. Identify the User to invite to ENGAGE. Under the 'Actions' column, press the 'Invite User' envelope button to send the invite.
 - a. Please note that this invitation will expire in 7 days.
3. The user will receive an email invitation to manage the ENGAGE site, and should select 'Accept This Invite'.
4. The user will be prompted to sign in with an existing ENGAGE account or create a new one. Creating a new account will require verification, which is another automated email sent following the account setup process.
5. Now that the invitation process is complete, the user should be able to sign in to the ENGAGE mobile app to manage the linked site!

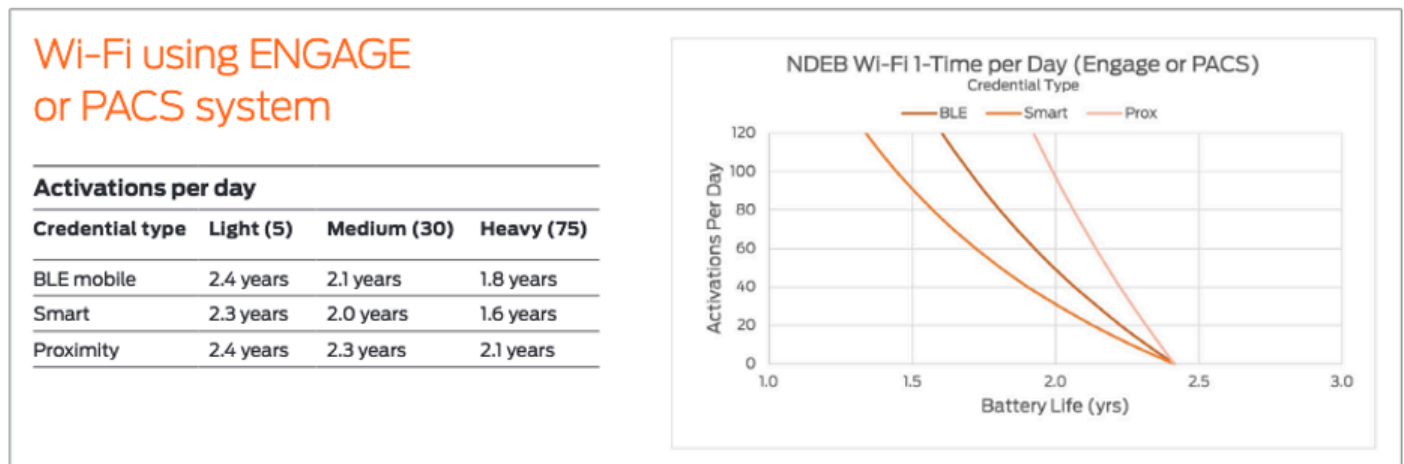
11.9.3. Wireless Device Check-In

The addition of Schlage NDE and LE wireless locks introduced a new device communication pattern to Pure Access. In contrast to the ISONAS line-powered reader controllers with a realtime connection, these wireless locks rely on batteries for power and periodic updates over WiFi to communicate with Pure Access.

The battery life of wireless devices is a function of two main variables:

1. How frequently credentials are presented to the device
2. How frequently the device wakes up to establish a WiFi connection to transmit data back to the host software

By default, wireless devices will wake up their WiFi radios and communicate with Pure Access once every 24 hours. This frequency is used to determine the battery life graphs in the following charts:



Pure Access also allows end users to configure the devices' check-in frequency and schedule in the device settings. This check-in frequency has a predictable and direct effect on battery life. Having a device check in via WiFi twice per day (or every 12 hours) will result in approximately half the expected battery lifetime (i.e. 1 year instead of 2 years) than the default once-per-day setting.

When a device check-in occurs, the device receives updated device settings and access control configuration *from* Pure Access and provides activity history *to* Pure Access.

Outside of specific user interaction, there is only one scenario in which the device will establish a WiFi connection to Pure Access outside what has been configured in Pure Access. If alerts are enabled for the tenant in Pure Access, the device will establish a WiFi connection to Pure Access and report alert information if certain alert conditions are met, including; *Extended Open*, *Forced Door*, and *Tamper Alerts*.

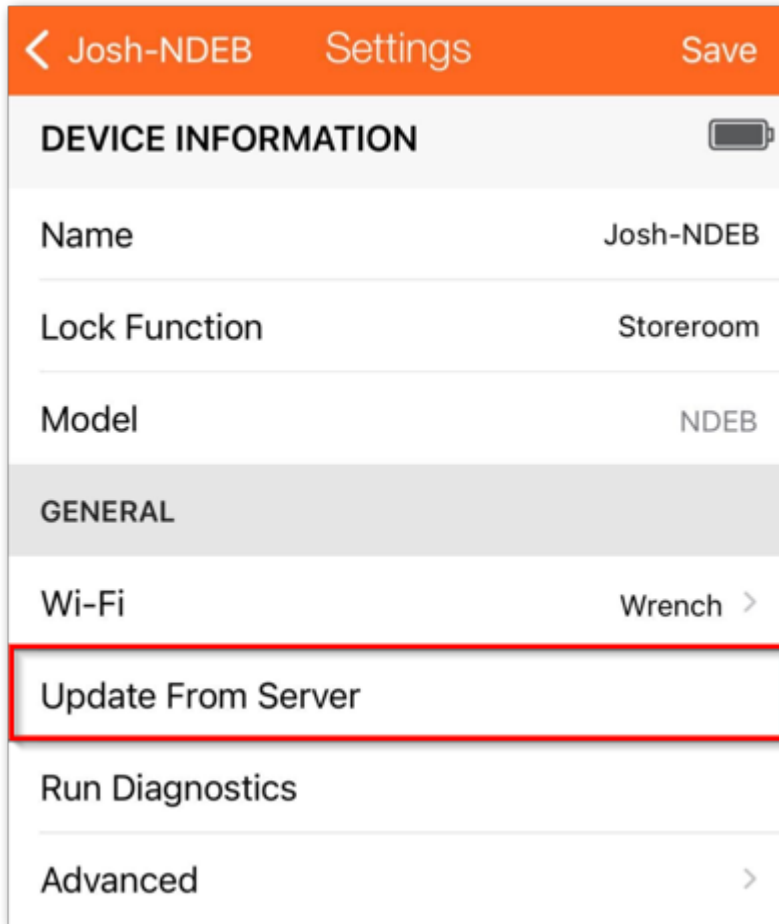
Due to the limited check-in frequency configured to preserve battery life, there may be times that you need to update a device immediately, outside of the normally scheduled recurring check-ins. This process is

referred to as a [Force Check-In](#).

11.9.3.1. Force Wireless Device Check-In

When a device check-in is desired outside of the normal check-in schedule, administrators have two ways to force a check-in:

1. Use the ENGAGE mobile app to connect to the lock and tap the **“Update From Server”** button to force the lock to update over WiFi.



2. Present a credential with the [Force Check-In special property](#) at the device.

* Force Check-In is a [credential special property](#) that can be enabled on any credential type available in Pure Access. In order for this credential special property to work, the device must first update with Pure Access to add the credential to its database. This can either be accomplished by waiting for the next scheduled check-in or using the ENGAGE mobile app to force one.

12. 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	DOWNLOAD
10 results					
<input type="checkbox"/>	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"/>	Front Door	02-23 11:13:57	Credential Rejected	Acknowledged	✓
<input type="checkbox"/>	Front Door	02-21 17:43:09	Custom Rule	Acknowledged	✓
<input type="checkbox"/>	Front Door	02-19 07:57:11	Custom Rule	New	✓
<input type="checkbox"/>	Front Door	02-17 16:41:52	Extended Open	New	✓
<input type="checkbox"/>	Front Door	02-17 16:41:50	Unauthorized Open	New	✓
<input type="checkbox"/>	Front Door	02-17 16:41:48	Tamper	New	✓
<input type="checkbox"/>	Front Door	02-17 16:41:47	REX Alarm	New	✓
<input type="checkbox"/>	Front Door	02-03 17:58:19	Credential Rejected	Acknowledged	✓
<input type="checkbox"/>	Front Door	02-03 17:58:12	REX Alarm	Acknowledged	✓

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 **DOWNLOAD**.

12.1. 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](#)

12.1.1. 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](#).

12.1.2. 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](#).

12.1.3. 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.

12.1.4. 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](#).

12.1.5. 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.

12.2. 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 .

13. Glossary

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

13.1. Admit

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

13.2. ASM

ASM: Advanced Security Module

13.3. AUX

AUX: Auxilliary Input

13.4. Compile

Compile is the action of updating access points.

13.5. Door

“Door “ is synonymous with “Access Point”.

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

13.6. 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.

13.7. 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.

13.8. 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.

13.9. Lock Down

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

13.10. REX

REX: Request for Exit

13.11. Secured

Secured is another word for locked.

14. Appendix A: Linking ENGAGE Site to Pure Access

✱ If you are using a Schlage RC only system, this does not apply.

✱ If you are using an ISONAS Only system with RC-03, RC-04, and IP Bridges, before you link an ENGAGE site to Pure Access Cloud, please read the below information to make an informed decision to proceed. [Making the Transition to Isonas Pure Access Cloud 4.0](#) is a video you may want to be familiar with.

[ISONAS + Schlage Device Environment – Customer Pre-‘ENGAGE’ Questionnaire](#)

Commissioning Hardware

All Schlage devices: RC, NDEB, and LEB will be commissioned to an ENGAGE site that is created in the Pure Access Cloud account.

All legacy RC-04 and IP Bridges will be commissioned direct to Pure Access Cloud via the ISONAS configuration tool.

Programmers

Once you link an Engage site to a Pure Access Cloud account, the only enrollment reader option is the new Schlage RC line. The MT20 series will no longer work.

Credential Migration

This step is necessary because credential data is stored differently in the Schlage RC, NDEB, and LEB than the RC-04. It is the step that caused the most issues because warnings are bypassed...see the best practice. The credential migration converts existing credentials into the proper format that is required by the Schlage RC, NDEB, and LEB.

The existing credentials will not work on the new Schlage RC hardware until migrated. You will need need to know if a different formatted credential is introduced to the system that will require bit mask settings to be pushed out to the legacy ISONAS hardware, to read the new credentials. If so, the new credentials will not work on the legacy hardware until bit mask is updated.

✱ Best practice is to run a user report before linking an ENGAGE site to Pure Access Cloud to

have the credential information readily for all users in the system. For each card format in the ISONAS software you must have the Card Format, ID Numbers, and Facility code. Without these items, the conversion will get challenging. With this information, technical support can assist with understanding the existing credentials formats in Pure Cloud before starting the migration process. Click the link below for a video on linking the accounts.
[Expanding Your Pure Access Cloud Business with Schlage's Wi-Fi Locks](#)

Physical Credential Parity

If it is desired that the stamped ID value on the credential matches the way the ID is enrolled, the following information is vital to understand.

The RC-04 only supports three message formats:

1. The ISONAS proximity credentials and ISONAS smart credentials by default (no bitmask setting required),
2. One custom format which requires the bitmask setting to be set.
3. If the customer is using the HID / ISONAS reader compatible credentials listed in the ISONAS price book, the bit mask setting labeled ISONAS will be selected under the Pure Access Cloud settings/credential tab.

The Schlage RC, NDEB, and LEB supports up to 21 additional message formats, plus the three formats in the ISONAS price book for a total of 24.

The above example is illustrated to advise that a customer cannot simply start buying open market 26-bit credentials and expect the stamped ID value to match the enrolled value on the credential.

Why? Because the 26-bitmask setting would be required to be set, but as noted above, the ISONAS bitmask setting has already been taken. Best practice is to continue to use the HID/ISONAS credentials for credential parity across both legacy RC04 and Schlage hardware.

The 26-bit credential could be enrolled by presentation to a card reader; however, the stamped ID value will not match the enrolled ID value in Pure Access Cloud.

If the customer is using the ISONAS smart card credential, Allegion owns the custom key and the Schlage RCs can be loaded with the ISONAS configuration: CE-5901-0402 to read the secure sector data of the ISONAS smart card. However, since the ISONAS smart card employs the EV2 technology, this chipset has been discontinued by Allegion due to inconsistent read performance issues, especially with battery operated NDEB or LEB locks. Another option is to have customer purchase Allegion EV1 or EV3 credentials with the ISONAS key for better read performance and backward compatibility to the RC-04.

Mobile ID Credential Parity

- The ISONAS mobile credential only works with the R-1(attached to an IP Bridge) and RC-04.
- The Schlage mobile credential only works on the Schlage RC, NDEB and LEB.
 - However, both mobile ID apps can reside on the same phone and both mobile IDs can be tied to a cardholder record.
 - User will have to select the proper app based on the RC model at the door to deliver the mobile ID to the reader / controller.

Holidays

The NDEB and LEB locks do not support holiday feature as known in ISONAS. All holidays will need to be deleted and set up as events in Pure Access Cloud.



Best practice is to run a holiday report to allow holidays as events after linking Pure Access Cloud to an ENGAGE site.

Active Directory

- Active Directory is supported if you want to import user first and last name or other non-credential data. If credential data is a requirement, Active Directory is not supported at this point.

RC Differences

- The RC-04 has an 8-wire pigtail and the Schlage RC has a 12- wire pigtail. The adapter cable is still in development and not released. Q4 2024 is the anticipated timeframe.
- The Schlage RC added a separate AUX input, two AUX outputs, and RS 485 connection but Pure Access Cloud software at present build does not support the AUX outputs or RS 485 connections.