Table of Contents

1. Using This Manual .................................................................................................................. 5

2. Application Infrastructure and Architecture ............................................................................. 7
   2.1. Pure Access Cloud Infrastructure ....................................................................................... 8
   2.2. Pure Access Manager Infrastructure ..................................................................................... 9
       2.2.1. Pure Access Manager System Requirements ............................................................. 10
   2.3. Platform Update Process .................................................................................................... 11
       2.3.1. Pure Access Cloud ....................................................................................................... 12
       2.3.2. Pure Access Manager ................................................................................................. 13

3. Setup and Configuration ........................................................................................................... 14
   3.1. Network Configuration ......................................................................................................... 15
       3.1.1. IP Addressing ............................................................................................................. 16
       3.1.2. Basic Firewall Information .......................................................................................... 17
       3.1.3. Best Practices ............................................................................................................ 19
           3.1.3.1. Additional Network Troubleshooting ................................................................. 20
   3.2. Configuring ISONAS Devices ............................................................................................... 23
       3.2.1. Using the Configuration Tool ...................................................................................... 24
           3.2.1.1. Advanced Configuration ..................................................................................... 27
           3.2.1.2. Reviewing Network Config Settings ..................................................................... 31
           3.2.1.3. Connectivity Test ............................................................................................... 35
       3.2.2. Discovering Units ......................................................................................................... 37
           3.2.2.1. Find device by IP .................................................................................................. 39
   3.3. Updating Firmware .............................................................................................................. 41
   3.4. Wiring and Hardware Installation ......................................................................................... 44
       3.4.1. RC-04 Installation Guide .............................................................................................. 45
       3.4.2. IP-Bridge Installation Guide ......................................................................................... 46
           3.4.2.1. IP-Bridge Status Light Indicators ........................................................................... 47
       3.4.3. RC-03 Installation Guide .............................................................................................. 49
           3.4.3.1. RC-03 Jumper Configurations .............................................................................. 50
       3.4.4. ASM Status Light Indicators ....................................................................................... 54

4. Getting Started in Pure Access ............................................................................................... 55
   4.1. Crystal Migration Cookbook ............................................................................................... 56
       4.1.1. Database Export Methods ............................................................................................ 58
           4.1.1.1. Exporting DBCrystal Database (v20.11.02 or later) ............................................ 59
           4.1.1.2. Exporting DBCrystal Database (alternate method 1) ........................................... 62
           4.1.1.3. Exporting DBCrystal Database (alternate method 2) ........................................... 64
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2. Pure Access Cloud</td>
<td>66</td>
</tr>
<tr>
<td>4.2.1. Logging into a Pure Access Cloud tenant</td>
<td>67</td>
</tr>
<tr>
<td>4.2.2. Tenant Name</td>
<td>69</td>
</tr>
<tr>
<td>4.2.3. Cannot Log into Pure Access Tenant</td>
<td>70</td>
</tr>
<tr>
<td>4.2.4. Current Version</td>
<td>72</td>
</tr>
<tr>
<td>4.2.5. RMR License</td>
<td>74</td>
</tr>
<tr>
<td>4.2.5.1. Creating Subtenants</td>
<td>75</td>
</tr>
<tr>
<td>4.3. Pure Access Manager</td>
<td>77</td>
</tr>
<tr>
<td>4.3.1. Java Memory Allocation</td>
<td>78</td>
</tr>
<tr>
<td>4.3.2. SMTP Configuration (Pure Access Manager)</td>
<td>79</td>
</tr>
<tr>
<td>4.3.3. Configuring Pure Access Manager for SSL</td>
<td>84</td>
</tr>
<tr>
<td>4.4. Bitmasking</td>
<td>85</td>
</tr>
<tr>
<td>4.4.1. Verifying the Currently Set Bitmask</td>
<td>86</td>
</tr>
<tr>
<td>4.4.2. Discover the Appropriate Bitmask</td>
<td>87</td>
</tr>
<tr>
<td>4.4.3. Setting a Bitmask</td>
<td>90</td>
</tr>
<tr>
<td>4.4.3.1. Pushing the Current Bitmask Setting to All Readers</td>
<td>91</td>
</tr>
<tr>
<td>4.4.3.2. Pushing Bitmask Setting to All Readers (PAM)</td>
<td>93</td>
</tr>
<tr>
<td>4.4.4. Setting an External Keypad Site Code</td>
<td>94</td>
</tr>
<tr>
<td>4.4.4.1. Configuring Keypad Site Code on an R-1 Reader</td>
<td>96</td>
</tr>
<tr>
<td>4.4.5. Custom Bitmasking</td>
<td>97</td>
</tr>
<tr>
<td>4.4.6. HID iClass Credentials</td>
<td>105</td>
</tr>
<tr>
<td>4.5. Areas</td>
<td>106</td>
</tr>
<tr>
<td>4.5.1. Why Use Areas?</td>
<td>107</td>
</tr>
<tr>
<td>4.5.2. How to Configure Areas</td>
<td>109</td>
</tr>
<tr>
<td>4.5.2.1. Assigning Dashboards to an Area</td>
<td>112</td>
</tr>
<tr>
<td>4.5.2.2. Assigning Groups to an Area</td>
<td>113</td>
</tr>
<tr>
<td>4.5.2.3. Assigning Access Points to an Area</td>
<td>115</td>
</tr>
<tr>
<td>4.5.2.4. Assigning Users to an Area</td>
<td>116</td>
</tr>
<tr>
<td>4.5.2.5. Assigning Schedules to an Area</td>
<td>117</td>
</tr>
<tr>
<td>4.5.2.6. Assigning Weekly Rules to an Area</td>
<td>118</td>
</tr>
<tr>
<td>4.5.2.7. Assigning Events to an Area</td>
<td>119</td>
</tr>
<tr>
<td>4.5.3. Managing Area Administrators</td>
<td>120</td>
</tr>
<tr>
<td>4.5.3.1. Adding Administrators to an Area</td>
<td>121</td>
</tr>
<tr>
<td>4.5.3.2. Setting Access Privileges for Area Administrators</td>
<td>124</td>
</tr>
<tr>
<td>4.5.3.3. Removing Administrators from an Area</td>
<td>126</td>
</tr>
<tr>
<td>4.6. Migrating from One Tenant to Another</td>
<td>128</td>
</tr>
<tr>
<td>4.7. Backup and Restore Process (Pure Access Manager)</td>
<td>130</td>
</tr>
<tr>
<td>4.8. Active Directory Integration</td>
<td>131</td>
</tr>
<tr>
<td>4.8.1. AD Connect Prerequisites</td>
<td>132</td>
</tr>
</tbody>
</table>
5. Managing Users ................................................................................................................................................. 141

5.1. How to Add a User in Pure Access .................................................................................................................. 142

5.1.1. Importing Users ........................................................................................................................................... 145

5.2. User Profiles ...................................................................................................................................................... 148

5.2.1. Adding Credentials ...................................................................................................................................... 150

5.2.1.1. Badge ....................................................................................................................................................... 152

5.2.1.2. Keypad Entry .......................................................................................................................................... 153

5.2.1.3. Mobile/Bluetooth .................................................................................................................................. 154

5.2.1.3.1. Using the Mobile Credential to Unlock a Door ................................................................................. 158

5.2.1.4. Enrolling by Presentation ....................................................................................................................... 159

5.2.1.5. Additional Credential Settings .............................................................................................................. 160

5.2.1.5.1. Time Limit ......................................................................................................................................... 161

5.2.1.5.2. Count Limit ....................................................................................................................................... 162

5.2.1.6. Special Credential Properties .............................................................................................................. 163

5.2.1.6.1. Toggle Credential ............................................................................................................................. 164

5.2.1.6.2. Master Credential .......................................................................................................................... 167

5.2.1.7. Deactivating a User Profile .................................................................................................................. 170

5.2.1.7.1. Viewing Deactivated Users ........................................................................................................... 172

5.2.1.7.2. Reactivating a User Profile ............................................................................................................ 173

5.2.2. Adding a Profile Picture ............................................................................................................................. 175

5.2.3. Adding Users to Groups ............................................................................................................................. 178

5.2.4. User Defined Fields ................................................................................................................................... 185

5.2.5. Updating Readers ....................................................................................................................................... 187

5.2.6. Deactivating Credentials .......................................................................................................................... 188

5.2.7. Reactivating Credentials ........................................................................................................................... 189

5.3. Web Access and Administrator Privileges ....................................................................................................... 190

5.3.1. Setting up Web Access for a User .............................................................................................................. 191

5.3.2. User Roles .................................................................................................................................................. 193

5.3.3. Accepting the Web Access Invitation ..................................................................................................... 194

5.3.4. Removing Web Access Privileges ............................................................................................................ 198

5.4. Custom Rules for Individual Users .................................................................................................................. 199

9.1. History Report ............................................................................................................................. 290
9.2. Users Report ................................................................................................................................. 293
9.3. Access Points Report .................................................................................................................... 297
9.4. Schedules Report .......................................................................................................................... 301
9.5. Holidays Report ............................................................................................................................ 302
9.6. Attendance Report ........................................................................................................................ 303
9.7. Permissions Report ....................................................................................................................... 304
9.9. Scheduled Reports ....................................................................................................................... 307

10. Alerts and Notifications .................................................................................................................. 314
    10.1. Alert Types and Setup Procedure ............................................................................................ 315
        10.1.1. Unauthorized Open ...................................................................................................... 316
        10.1.2. Extended Open ........................................................................................................... 319
        10.1.3. Tamper .......................................................................................................................... 322
        10.1.4. AUX/REX Alarm ......................................................................................................... 324
        10.1.5. Credential Rejected, Expired, or Over Limit. ............................................................... 325

11. Custom Rules .................................................................................................................................. 326
    11.1. Creating a Custom Rule ......................................................................................................... 327
    11.2. Changing a Custom Rule ...................................................................................................... 332

12. Two-Factor Authentication ............................................................................................................. 333
    12.1. Card/PIN ............................................................................................................................... 334
    12.2. Two User .............................................................................................................................. 335
    12.3. Two-User – Card/PIN .......................................................................................................... 336
    12.4. Configuration Process ......................................................................................................... 337
        12.4.1. General Settings Page ............................................................................................... 338
        12.4.2. Adding Two-Factor PINs ......................................................................................... 340
        12.4.3. Adding Two-Factor Rules ....................................................................................... 342
    12.5. Two-Factor History Events ................................................................................................. 343

13. Still Need Help? .............................................................................................................................. 345
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:**
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. 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)
2.1. Pure Access Cloud Infrastructure

ISONAS PURE ACCESS CLOUD INFRASTRUCTURE
2.2. Pure Access Manager Infrastructure
2.2.1. Pure Access Manager System Requirements

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

OR

- Virtual Environment with a Hypervisor download
- At least 80GB of disk space available from the VM
2.3. Platform Update Process

The following pages will explain the update process for Pure Access Cloud and Pure Access Manager.
2.3.1. 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 two-week notification prior to release so you are aware of the update. In this notification, you will receive the release notes giving you visibility to the changes. All updates take place during off hours to reduce any potential interruption to your system.

(See next page for 2.3.2. Pure Access Manager >>)
2.3.2. Pure Access Manager

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

Pure Access Manager feature updates are available to customers who have purchased a software upgrade program. Please contact our sales team for more information on this program.

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.
3. 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.
3.1. Network Configuration

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](#)
3.1.1. 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
3.1.2. 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.

![Figure 1 - RC-03 Example Connection](image)

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.

![Figure 2 – IP-Bridge Example Connection](image)
Figure 3 – Reader-controller Connections
3.1.3. Best Practices

Network

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

Port Speeds

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

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

Firewall

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

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

General

- Do you have **port 55533** open to the internet or at least open to **isonaspureaccesscloud.com**?
  - If you are using the on-premise version of Pure Access, is port 55533 open across your enterprise?
- How is your latency? If the latency to the **isonaspureaccesscloud.com** site is greater than 100ms, you may see minor issues. If greater than 200ms there could be larger communication problems.
  - You can use a site like **SpeedTest.net** 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):
• If you are unable to discover a unit, plug the reader into an unmanaged PoE switch connected to your PC and try again.
  ◦ Alternatively, you can use a PoE injector and a crossover cable to connect the reader directly to a PC.
• If using DHCP, try to statically set a reader's IP to an available address instead. Setting the reader to a static IP will let us know if DHCP is preventing the connection.
• If running Pure Access Cloud, try bypassing the DNS.
  ◦ To do this, you will need to configure the reader(s) using the Cloud server's IP – 52.38.127.152 – as the host address (click “Specify Host IP Address” in the configuration tool).
  ◦ Alternatively, you can find the public IP address of our Cloud environment via command prompt by typing nslookup isonaspureaccesscloud.com then hitting enter.
  ◦ If the device is able to connect this way, we know there is a DNS issue.
• If running Pure Access Manager (on-premise), ensure that the Windows Firewall is not blocking the connection. You may want to disable the firewall entirely to test.
• Run a packet capture application such as Wireshark to determine where/when the data is dropping.

Physical Issues

• If possible, power-cycle the switch where the affected device(s) are connected.
• Verify that the CAT cable connected to the device is not faulty. It may be best to try another cable entirely.
• Verify that the PoE port on the switch is fully operational.
  ◦ If you are able to test the port with a spare reader (or swap this port with the port of a functional reader), that can be useful in narrowing down the root of the issue.
  ◦ For issues related to powering on the device, a PoE tester is useful determining whether or not
the port is supplying the proper voltage.
3.2. 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
3.2.1. Using the Configuration Tool

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

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

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

If you are not able to find the devices on the network, see the Discovering Units section.
If the devices were discovered, proceed to Advanced Configuration to continue setting up the controllers.
3.2.1.1. Advanced Configuration

Clicking on [Advanced Settings] will bring up the options needed to fully configure a device.

The options now available allow you to change where the device(s) will be attempting to connect as well as the ability to set the readers to either DHCP (preferred) or static IP addresses.
Establishing a connection to Pure Access:

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

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

3. For **Pure Access Manager**, you must click “**Specify Host IP Address**” and then input the server’s IP in the “**IP Addr**” field.

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.

![ISONAS Configuration Tool]

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.
3.2.1.2. Reviewing Network Config Settings

To see the current configuration of a device:

1. Discover the unit on the subnet
2. Highlight it from the discovered units field
3. Click on "Advanced Settings"
4. Click "Show Reader Info"
Once the “Show Reader Info” box is clicked, a “Current Information” window will appear displaying the
configuration settings of the device.

How the device is currently configured
With the **Current Information** window open, you can simply highlight another device in the config tool to quickly display its settings. This is a handy way to compare the configuration settings of multiple units.
3.2.1.3. 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 connectivity test will run a series of four tests:

- **Test 1**: Pings the specified DNS server (Google DNS by default) 4 times and averages the response time to confirm DNS connectivity
- **Test 2**: Finds routing info for ISONAS Pure Access Cloud using the specified DNS server (Google DNS by default)
- **Test 3**: Tests connectivity to ISONAS Pure Access Cloud by pinging the environment 4 times and averaging the response times.
- **Test 4**: Simulates a device connection by ensuring a simulated ISONAS device can make a connection to Pure Access through port 55533.
The results of the test can be clicked on to display more information. Alternatively, one can export or print the results of the test for further review.

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

If no devices appear after clicking the `Discover Units` 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
3.2.2.1. 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.
3.3. 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.
3. Once devices have been discovered, click Update Firmware to open the firmware update window.
4. Select your device’s model from the “Select Model” drop-down menu.

![Select Model]

5. Use the check-boxes to select the device(s) that need to be updated.
   a. For RC-03’s and IP-Bridges: Select Update ColdFire as well as Update Coprocessor. Both of these will need to be updated.
   b. For RC-04’s: Select Update ColdFire. See note below for more information.
6. Click 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”.

! Isonas Pure Access Manual - 1
Page 41 of 345
8. Once the firmware files have been selected, click **Prepare Devices** 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.
9. Click Update 

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.

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.
3.4. 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.
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.
3.4.2. 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.
3.4.2.1. 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.

<table>
<thead>
<tr>
<th>IP-Bridge Status</th>
<th>LED “A” Color</th>
<th>LED “B” Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-Bridge is not powered on</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Power Turned On – Waiting in Boot Loader mode (~10 sec)</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Performing All IP work, all mode, duration depends on settings</td>
<td>Amber</td>
<td>Red</td>
</tr>
<tr>
<td>IP Work completed (except long DNS lookups), ports/DNS</td>
<td>Red</td>
<td>Amber</td>
</tr>
<tr>
<td>Startup Complete – Errors reported</td>
<td>Green</td>
<td>Amber</td>
</tr>
<tr>
<td>Startup Complete – No issues reported</td>
<td>Green</td>
<td>Off</td>
</tr>
<tr>
<td>IP-Bridge is on and in a normal state</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Status</td>
<td>Red</td>
<td>Green</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>No Door (2-door Bridge)/Deactivated Door</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Normal Operation</td>
<td>Red</td>
<td>Off</td>
</tr>
<tr>
<td>Door is unlocked</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Door is unlocked for the latch interval</td>
<td>Green</td>
<td>Off</td>
</tr>
<tr>
<td>Door is in the Lockdown state</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Waiting in Startup or Performing Boot Load</td>
<td>Amber</td>
<td>Amber</td>
</tr>
<tr>
<td>Waiting to be activated or door process issue</td>
<td>Off</td>
<td>Amber</td>
</tr>
</tbody>
</table>
3.4.3. 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.
3.4.3.1. 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 accidently 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:

<table>
<thead>
<tr>
<th>Feature</th>
<th>JP 1 Jumpers</th>
<th>JP 2 Jumpers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Power – 12VDC through Pigtail</td>
<td>1 to 3</td>
<td></td>
</tr>
<tr>
<td>Input Power – 24VDC through Pigtail</td>
<td></td>
<td>3 to 5 &amp; 4 to 6</td>
</tr>
<tr>
<td>Input Power – PoE through RJ45 connector</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Input Power – PoE through RJ45 connector (See Note 1)</td>
<td>1 to 3</td>
<td></td>
</tr>
<tr>
<td>Input Power – No effect, place-holder for extra jumper</td>
<td>2 to 4</td>
<td></td>
</tr>
<tr>
<td>Lock’s power/signal is externally supplied on the pigtail’s pink wire</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Supply internal 12VDC to relay common (See Note 2)</td>
<td>1 to 3</td>
<td></td>
</tr>
<tr>
<td>ISONAS External Door Kit being used</td>
<td>3 to 4</td>
<td></td>
</tr>
<tr>
<td>Connect GROUND to relay’s common contact</td>
<td>3 to 5</td>
<td></td>
</tr>
</tbody>
</table>
**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.*
3.4.4. 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.

<table>
<thead>
<tr>
<th>Pure IP Reader Controller Locked</th>
<th>Pure IP Reader Controller Unlocked</th>
<th>Lock State when Pure IP Reader Controller is Unlocked</th>
<th>Description or Item to Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>GREEN</td>
<td>Normal Operation</td>
<td></td>
</tr>
<tr>
<td>Flash Amber</td>
<td>Flash Amber</td>
<td>No Operation</td>
<td>Yellow wire may be disconnected.</td>
</tr>
<tr>
<td>OFF</td>
<td>Flash Amber</td>
<td>No Operation</td>
<td>White wire may be disconnected.</td>
</tr>
<tr>
<td>OFF</td>
<td>Flash Amber</td>
<td>No Operation</td>
<td>Invalid encryption key received from Pure IP Reader-Controller.</td>
</tr>
<tr>
<td>OFF</td>
<td>OFF</td>
<td>No Operation</td>
<td>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.</td>
</tr>
</tbody>
</table>

Isonas Pure Access Manual - 1
Page 54 of 345
4. Getting Started in Pure Access

1. Migrating from Crystal to Pure Access
2. Logging into a Pure Access Cloud tenant
3. Bitmasking
4. Configuring Areas (optional)
5. Managing Users
6. Managing Access Points
7. Configuring Schedules, Weekly Rules, and Events
8. Setting up Dashboard Widgets
4.1. Crystal Migration Cookbook

Migration Planning

Make sure to have a migration plan in place:

- Know which doors you will be moving and when.
- Create access point groups that are near each other so the move can be easier and controlled.
- Make sure everyone involved knows that, during the migration, there may be a need to manage multiple systems simultaneously.
  - i.e. Until all doors are moved, you will have to manage both DB Crystal and Pure Access.
- Consider how you will layout doors and door groups in your new system. It’s a completely different software so this is an opportunity rearrange or clean up the system.

Ask for help planning! ISONAS Support has migrated hundreds of sites and we are here to help. Email support@isonas.com or book an appointment and request a migration planning session to make sure all your bases are covered.

Initial Steps

1. Export the Crystal database and send to support@isonas.com. Once this information is sent in, please allow up to 48 hours for the data to be re-configured and tested to work in the new system.
   a. What does the export contain?
      - **Answer:** Users, credentials, user groups, access points, shifts (schedules), and holidays.
      - **Note:** Depending on the database export method used, access points may not be translated correctly. If this happens, we will remove them from the import to avoid additional labor on your end. IP Bridges always need to be re-added manually regardless of the export method that was used, so we also do not import these into Pure Access.
   b. What will not be imported into Pure Access?
      - **Answer:** Access point groups, rules, and images.
      - Why?
        - Pure Access handles access point groups and rules in a different manner than Crystal. Since the data does not translate properly, they cannot be imported.
        - The way images are stored in Crystal is not compatible with Pure Access. The import will attempt a conversion, however, in most cases it will not work.

2. If you are using Pure Access Manager, first review the system requirements then download and install the latest release.
3. Schedule a migration time with support@isonas.com.

4. For either Pure Access Manager or Pure Access Cloud, we will assist you in importing the data and migrating some access points to make sure the process is going smoothly. At any time during the migration, you can reach support by calling (800) 581-0083 option 2 or by emailing support@isonas.com. Alternatively, you can schedule a call using our appointment booking site.

Performing the migration

![Important note] Before beginning, please note that you should never update the firmware of all devices simultaneously.

1.) Updating more than five devices at the same time is ill-advised since the increase in network traffic may cause complications/failure of the firmware to update properly.

2.) Updating the firmware will sever the connection with the Crystal system. If you run into any issues with the update, it is best to limit the impact to avoid all doors being down.

1. Configure your weekly rules.

2. Update the firmware on a single reader controller. As a best practice, we recommend beginning with the least important and/or least frequented door.
   - Note that you will need to stop the Crystal supervisor(s) [CSUP] as this connection may interfere with the firmware update.

3. Configure your device.

4. In Pure Access, locate the door and wait for it to connect.
   - Enable and test the ASM (formerly known as EDK), enable peripherals such as REX or AUX, and add the door to the appropriate access point groups.

5. Send a compile to the devices using the “Update Access Points” button at the top of the page then test a credential.

6. Repeat until the site is complete.
4.1.1. Database Export Methods

- For DBCrystal v20.11.02 or later
- Export to a .bak file. This method is for Crystal Matrix or if the above method does not work.
- Export to CSV files using the DBRM method. This method is for Crystal Matrix or if the above methods do not work.
4.1.1.1. Exporting DBCrystal Database (v20.11.02 or later)

1. Navigate to the C:\Apps\Isonas_DBCrystal directory.
2. Create a new folder called “ExportedData”
3. Run the ExportData.bat file located in the Isonas_DBCrystal Directory
4. A command prompt window will open. If the default server and SQL instance information is correct, hit enter.

5. You will then be asked for the database name. If the default is correct, hit enter.
6. You will now be prompted where the data is to be exported. This will be the folder we created earlier. Hit enter to proceed.

7. Press 2 for the SQL login option.
8. It will then ask which data should be exported. Press A for all.

After the command prompt window closes, you will see a list of .CSV files populated in the ExportedData folder that had been created in step 2. Zip up this folder and send it to support@isonas.com. From here, a help desk technician will be able to re-configure and test the database for Pure Access. Please note that this process may take up to 48 hours to complete.
4.1.1.2. Exporting DBCrystal Database (alternate method 1)

1. Download this **backup.zip** file and then unzip it onto the Crystal server.
2. Launch the **backup_db.bat** batch file.
3. From the command prompt window, input `.\IsonasExpress` then hit enter.

4. If successful, you should see something that resembles this:
5. If the step above fails, you will need to input the correct server and instance name in step 3. Your instance name can be found in parentheses next to the SQL Server Windows service:

6. The exported database can be found in the C:\Apps directory and it will be named “DBCrystalBackup.bak”

Zip up this file and send to support@isonas.com. From here, a help desk technician will be able to re-configure and test the database for Pure Access. Please note that this process may take up to 48 hours to complete.
4.1.1.3. Exporting DBCrystal Database (alternate method 2)

1. Navigate to the C:\Apps\Isonas directory* and then launch the DBRM.exe file.

2. Click on “Export” then select “CSV Files”:

3. For each tab (People, Groups, Doors, etc.), click the “Export” button in order to export the data into .CSV format.
4. Find the newly created .CSV files in the C:\Apps\isonas or C:\Apps\isonas_DBCrystal directory (you may want to sort by date). The files will look like this:

Zip up these files and send to support@isonas.com. From here, a help desk technician will be able to re-configure and test the database for Pure Access. Please note that this process may take up to 48 hours to complete.

Information above is for the legacy Crystal Matrix software. If you are running DBCrystal, the directory will be C:\Apps\isonas_DBCrystal and the file to launch will be called DBDBRM.exe.
4.2. 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
4.2.1. Logging into a Pure Access Cloud tenant

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

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

What’s my tenant name?

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

1. In your address bar after the # (see image below)
2. At the upper right corner of the page, below your user profile image
4.2.3. 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.

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.
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.
4.2.4. Current Version

When logged into Pure Access, you can see the current version of the software at the bottom right corner of the page:

To view the current release notes, click on your profile picture from the upper right corner of the page, then select “Help”:
4.2.5. 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.
4.2.5.1. Creating Subtenants

1. Navigate to **Settings**.

2. Click on the **Tenant Manager** tab.

3. Click the **Tenant** button from the upper right corner of the page.

4. Fill in the **Add Tenant** window. Note that the only required field is “Tenant Name”.
5. Click **Add**

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.
4.3. 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.
4.3.1. 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
4.3.2. 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 Notepad as an administrator:
3. Drag-and-drop the `ROOT.properties` file into the empty document so that it can be modified:
4. With **ROOT.properties** open in Notepad, change the “Email Config” section to your preferred settings:

   ```
   # ----- Email Config ----- 
   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   Please walk through the following steps to create your site:1. Visit https://www.isonaspureaccesscloud.com/v2. Select the Register button\n   Enter your License Key: {{key}} \n   Complete the SiteProfile\n   Below is a link to a video that walks through the registration and access point setup 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   Click here for instructions on registration and set up:\n   \n   email.passwordReset.message Subject: ISONAS - Password Reset Instructions 
   email.passwordReset.path = /emails/password_reset.html 
   email.alert.path = /emails/alert.html 
   email.customrule.path = /emails/customrule.html 
   email.scheduledReport.path = /emails/scheduled_report.html 
   email.pamBasePath = /isonaspureaccesscloud.com/ 
   # ----- Email Config ----- 
   ```

5. 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:
6. If running **Pure Access Manager 2.12.2**, see the bottom of this page. Otherwise, save the document and then reboot the system (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 2.12.2? 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:

```bash
# -- PDF config
pdf.logo.path=css/image/logo1.png
df.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
```

*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.*
4.3.3. 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.
4.4. Bitmasking

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](#).
4.4.1. Verifying the Currently Set Bitmask

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

2. Click the **Credential** tab under **General Settings**.
3. The set bitmask will be designated with a checkmark.

Readers are set to the 26 bit bitmask
4.4.2. Discover the Appropriate Bitmask

Verifying the correct bitmask for your credential:

1. 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.

2. In Pure Access, navigate to the **Settings > Credential** tab.
3. From the “Access Point” drop-down list, select the reader where the unenrolled badge was presented then click the **Calculate** button.
4. 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.

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.
4.4.3. Setting a Bitmask

1. Under “Bitmask Options”, select the mask determined above then click Save Changes.

![Bitmask Options](image)

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

Once saved, your readers will be updated immediately. You can now enroll credentials by typing in the badge ID manually.

⚠️ Changing your bitmask can cause all of your previously enrolled credentials to be rejected. Clicking the “Save Changes” button will affect every connected reader.
4.4.3.1. Pushing the Current Bitmask Setting to All Readers

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

![Setting Tab]

2. Click the **Credential** tab under **General Settings**.

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.
### 4.4.3.2. 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 **Save Changes** button appears), then return to the desired/original bitmask.

4. Click **Save Changes**.

5. Input your password when prompted then click **Confirm Change**.

*The selected bitmask will be pushed out to all connected devices on the tenant.*
4.4.4. Setting an External Keypad Site Code

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

2. Click the **Credential** tab under **General Settings**.

3. Input the desired 3-digit code next to **External Keypad Site Code** then click **Save Changes**.
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.
4.4.4.1. 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: `8 8 8 9 9 9`
   *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.*
4.4.5. 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.

Prerequisites:

- A web access profile with the privilege to assign credentials.
- 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:

<table>
<thead>
<tr>
<th>EVENT</th>
<th>BADGE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decline Badge Not Found</td>
<td>0000379500</td>
<td>System Admin.</td>
</tr>
</tbody>
</table>

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 a new or existing user profile, then click on the + to open the "Add Credential" window.
   b. Click the "Read From Access Point" drop-down menu and then select the name of the access point where the credential had been presented. Click "Read".
   c. 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: 0000000000001111111111111111111

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: 11111111111111111111111111111111 = 1FFFFFE
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).
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.
4.4.6. 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.
4.5. 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.
4.5.1. 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.
4.5.2. 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 Access Control page from the left navigation bar.

2. Select the Areas tab.

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

Administrators must be assigned to the area or areas of which they need to **View** or **Modify** the users, groups, schedules, rules, dashboards, etc.
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.
4.5.2.1. Assigning Dashboards to an Area

1. Navigate to the Access Control page from the left navigation bar.

2. Select the next to the name of a dashboard to edit (or create a new dashboard).
3. From the Area drop-down menu, select the area with which this dashboard needs to be associated.
4.5.2.2. 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 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.

Access Point Group

1. Navigate to the Access Control page from the left navigation bar.
2. Select the **Access Points** tab, then click on 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.
4.5.2.3. Assigning Access Points to an Area

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

2. Select the **Access Points** tab, then click on an access point to view its settings.

3. From the **Area** drop-down menu, select the area with which this access point needs to be associated.
4.5.2.4. Assigning Users to an Area

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

2. Select a user to view their profile.

3. From the **Area** drop-down menu, select the area with which this user needs to be associated.
4.5.2.5. Assigning Schedules to an Area

1. Navigate to the Access Control page from the left navigation bar.

2. Select the Schedule tab, then click on a schedule to view its configuration.

3. From the Area drop-down menu, select the area with which this schedule needs to be associated.
4.5.2.6. Assigning Weekly Rules to an Area

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

2. Select the **edit** to edit a weekly rule (or **add a new rule**).

3. From the **Area** drop-down menu, select the area with which this weekly rule needs to be associated.
4.5.2.7. Assigning Events to an Area

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

2. Select the **Calendar** tab, then **add or edit an event**.

3. From the **Area** drop-down menu, select the area with which this event needs to be associated.
4.5.3. Managing Area Administrators

1. Adding Administrators to an Area
2. Setting Access Privileges for Area Administrators
3. Removing Administrators from an Area

* Please note that a newly created user profile will inherit ALL areas that the integrator/administrator account is associated with.
4.5.3.1. Adding Administrators to an Area

1. Navigate to the Access Control page from the left navigation bar.

2. Select the Areas tab.

3. Select the area with which an administrator needs to be added.

4. Click + Users

5. Choose whether the administrator(s) need Manage or View privileges.

6. Select the administrator(s), then click Add
**Alternative Method**

From a user’s profile, another area can be selected from the drop-down menu:
Note that the currently selected area will be the user's primary area. In the following image, the user's primary area is **COMMON**: 
4.5.3.2. Setting Access Privileges for Area Administrators

1. Navigate to the Access Control page from the left navigation bar.

2. Select the Areas tab.

3. Select the area with which an administrator’s access privileges need to be modified.

4. Under the Access column, select either “View” or “Manage” next to the administrator you wish to modify.

5. Select either “View” or “Manage”.
6. Click on the green check button (✔) to confirm.

Changing the access rights for multiple administrators

1. Click Edit
2. Select the administrators you wish to edit.
3. From the “Select an action” drop-down menu, choose either “Give Users Manage Access” or “Give Users View Access”
4. Click on the green check button (✔) to confirm.
4.5.3.3. Removing Administrators from an Area

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

2. Select the **Areas** tab.

3. Select the area where the administrator(s) currently reside.

4. Click **Edit** , then select the administrator(s) who need to be removed.

5. From the “Select an action” drop-down menu, click **Remove from Area**
6. Click on the green check button (✓) to confirm.
4.6. Migrating from One Tenant to Another

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

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

1. Moving users from one tenant to another

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

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

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

1. Before proceeding, please be aware that once an access point is deleted from a tenant you will no longer be able to view reports for that device.
   a. If you need to view historical events for auditing purposes, you will want to generate and download the reports now.
2. Deactivate and then delete an access point from the old tenant.
3. Add this access point to the new tenant.
   a. It is best practice to delete the access points and then add them to the new tenant one at a time.
   b. Once added to the new tenant, update access points and then test a credential.
4. Repeat steps 2 and 3 until all of the access points have been moved over.
4.7. 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.
4.8. Active Directory Integration

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

Functionality includes:

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

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

* 51-100 license and above
4.8.1. AD Connect Prerequisites

Requirements

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

Service Account:

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

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

Directory Structure and Groups:

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

AD Connect Software:

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

Structures that will NOT work:

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

Resources:

• General Best Practices for AD
• Key Principles on OU design
• Securing Active Directory
• Design Planning
4.8.2. Installation and Configuration

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

* Still need help? Please send the adpod.log file (located in the same directory that ADConnect is installed) and a description of your issue to our support team for review.
4.8.3. 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 > General Settings > Active Directory
4. Set sync times under General Configuration.

![General Configuration](image)

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 ![Sync Active Directory](image).
   - Please note that this may take some time to complete if this is the first time syncing. If there doesn't appear to be activity after 10 minutes, refresh the page and try to sync again.
   - If the above did not work, restart the Isonas AD Connect Windows service and try again.

Still need help? Please send the adpod.log file (located in the same directory that ADConnect is installed) and a description of your issue to our support team for review.
4.9. 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.
4.9.1. 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 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.
4.9.2. 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.

![API Tokens Page](image)

To assign a token, click the + button. You can assign both a name and an optional expiration date for your new token. By default, all new tokens will only provide read only access.

You can create a token with both read a write access by unchecking the “Read Only” checkbox.
You *must* export a token before saving it as the Token ID and Token Value are **NOT** stored in Pure Access for security reasons. The export button will generate a .CSV file with all of the necessary information about the token.
4.9.3. 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 calls per minute. If you think you might exceed this limit, please contact Isonas support.

Resources

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

https://app.swaggerhub.com/apis/isonaspureaccess/api-v2/1.0.2
5. Managing Users

1. Adding user profiles
2. Granting web access and administrator permissions
3. Adding credentials:
   a. Badge or Keypad
   b. Mobile/Bluetooth
4. User Groups
5. Custom Rules
6. Deactivating a User Profile
5.1. How to Add a User in Pure Access

1. Click the “Users” tab on the left side navigation:

2. This brings you to a full summary page of all active users in your system. From here you can take actions on individual users by selecting their name or take actions on multiple users by selecting the check boxes then drop-down menu:

3. You will see all users by default but can filter the list to only users who meet specific criteria:
4. By choosing the carrot icon after you have selected a user profile, you can take actions on the user(s):
5. To add a new user, click the **User** icon at the top right corner of the window.
5.1.1. Importing Users

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

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

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

Instructions

1. For Pure Access Cloud, download this template CSV file. For Pure Access Manager, please use this template and see the note at the bottom of this page.

2. Input the users’ information. The required fields are: LastName, FirstName, BadgeID, and CredentialType.
   
   a. The BadgeId column should contain either the hot-stamped number printed on the user’s badge, a keypad code, or a mobile/bluetooth DeviceID number.
      
      • If you intend on adding a user profile without a credential, you must have a “0” in this column or the import will fail.
      
      • To import multiple credentials for a single user, they will need more than one row in the CSV (one row for each credential they have, see Alyx Vance in the example at the bottom of this page for reference). The same required fields apply to each subsequent row that is added.
         
         ◦ Note that if the user’s first or last name does not match the original row’s data, it will create a new user profile and will not simply append the additional credential(s).
   
   b. CredentialType will need to be either a “1” (if the credential is a badge), “2” (if it’s a keypad), or “3” (for mobile/bluetooth credentials).

   c. To add users to user groups, populate the UserGroups column using the following formatting and notes:
      
      i. Ensure that the user group(s) already exist in Pure Access. The user import will not create new groups.
      
      ii. Ensure that the capitalization and punctuation of the group(s) are correct in the import. The All Users group in Pure Access must be All Users in the import.

      iii. To add a user to multiple groups, you will need to separate the names of the groups with a semi-colon (;) without spaces. For example, to add a user to All Users and to Managers, the field would look like this: All Users;Managers
• **Note:** If the **UserGroups** field is not populated, the user(s) will not be assigned to a group.

• **Note 2:** This is for Pure Access 3.1+ only.

d. 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.
   ii. Populate the **AreaName** column.
   iii. Ensure that the capitalization and punctuation match the area in Pure Access.
   iv. **Note:** To reiterate, the import **will not** create new areas. If an **AreaName** field is populated with an area that does not exist in Pure Access, the user will be placed into **COMMON**.

e. You can ignore the columns titled **CountLimitFlag**, **RemainingUses**, and **ExpirationDate** as they are not necessary for the import to be successful. These fields must remain in the import, however.
   i. If you wish to set an **ExpirationDate** on one or more credentials, you can do so using the format: **yyyyMMdd**
   ii. **Example:** April 1st, 2020 would be **20200401**

3. Once completed, the CSV file will need to be **zipped**.

4. Click **Import Users** from the **Users** page.

5. Select the zipped import file and 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.

**Example:**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lastname</td>
<td>Firstname</td>
<td>MidName</td>
<td>AreaName</td>
<td>BadgeId</td>
<td>CredentialType</td>
<td>CountLimitFlag</td>
<td>RemainingUses</td>
<td>ExpirationDate</td>
</tr>
<tr>
<td>2</td>
<td>Bellic</td>
<td>Niko</td>
<td></td>
<td>COMMON</td>
<td>31576482</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Vance</td>
<td>Alyx</td>
<td></td>
<td>COMMON</td>
<td>45678912</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Vance</td>
<td>Alyx</td>
<td></td>
<td>COM</td>
<td>6278</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Auditor</td>
<td>Elio</td>
<td></td>
<td>COMMON</td>
<td>32165487</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Kennedy</td>
<td>Leon</td>
<td></td>
<td>COMMON</td>
<td>6E59223C32831AA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How the above import would look once in Pure Access:
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.
5.2. User Profiles

The next page that loads for you will display the information for the new user and allows you to manage their access. On the top right is a progress bar, as the grey X’s turn to green check marks, you have completed that step correctly.

1. Fill out the **First Name**, **Last Name**, and other relevant information in the empty fields provided. "**Employee ID**" and "**Alert Notification Email Address**" are optional.

2. If you want this user to receive emails for alerts that have been created, add their email address in the "**Alert Notification Email Address**" field. [Click here](#) for more information on configuring email alerts.

3. In addition, you can upload an image or photo to associate with this person. Simply click on the profile
circle and it will ask you to select an image from your files.
Once the file is loaded, select upload photo and your image will appear. Click “Save.”
5.2.1. Adding Credentials

1. To assign a credential to a user, click the + button next to the word “Credentials” on the user profile page:

![Credentials button](image)

2. A window will pop up prompting you to assign a credential to this person. This can be a Badge, Keypad Entry, or Mobile credential.
Add Credential for Marston, John

Badge

Keypad Entry

Mobile

Time Limit

Count Limit

Two-Factor Authentication

Cancel  Save
5.2.1.1. Badge

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

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

If you have a keypad device and would like to assign an entry code to a user, you will need to change the credential type from **Badge** to **Keypad Entry**:  

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

♥ To unlock a door, you will need to input star (♥) followed by the assigned keypad code then pound (#).
5.2.1.3. Mobile/Bluetooth

First, change the credential type from **Badge** to **Mobile**:

**Enrolling by Presentation**

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

**Enrolling Manually**

1. Click on the three dots in the upper right corner of the **ISONAS Pure Mobile** application.
2. Click "View device id."
3. Input this ID into the “Device ID” field on the add credential page in Pure Access.
4. Click **Save**.
5.2.1.3.1. Using the Mobile Credential to Unlock a Door

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.
5.2.1.4. Enrolling by Presentation

1. Present the credential to a reader.

2. Navigate to a user profile and then click on the + in the “Credentials” section. An “Add Credential” window will appear.

3. From the “Read From Access Point” drop-down menu, select the access point where the credential was presented.

4. Click Read. The raw data and badge ID of the most recently declined card*** will populate:

5. Next click the Save button at the bottom right corner of the pop-up window.

6. You will now see this credential listed under the “Credentials” portion of the user profile page.

7. Click Save Changes.

* The declined credential will clear after 15 minutes.***
5.2.1.5. Additional Credential Settings

In addition, you are also able to set a start and end date and time and/or a count limit to credentials.

If, for example, you have a visitor or temporary employee you can apply these limitations to their badge upon initial creation.
5.2.1.5.1. Time Limit

Add Credential for: Marston, John

- Badge ID: 591907
- Raw Data: 0009082301711111111141448187
- Read From Access Point: Employee Entry

Time Limit

- Start Date
- End Date
- Start Time
- End Time

Count Limit

Two-Factor Authentication
5.2.1.5.2. Count Limit

Add Credential for: Marston, John

- Badge ID: 591907
- Raw Data: 00090823011711111111114418187
- Read From Access Point:
  - Employee Entry
- Time Limit
- Count Limit
- Number
- Two-Factor Authentication

Save | Cancel
5.2.1.6. Special Credential Properties

There are two types of special properties which you can set for a credential:

1. **Toggle**: The ability to unlock/lock access points with which the user has Grant Access permissions to.
2. **Master**: The ability to unlock a an access point that is in Lockdown.
5.2.1.6.1. 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.**

Setting up the Toggle property for credentials in Pure Access:

1. Navigate to the user who needs to toggle doors unlocked/locked.
2. You can assign this property to new credentials or modify an existing one:
   a. [Adding a new credential](#)
   b. To edit a credential, click on the credential you wish to change and then select the icon.
3. At the top right corner of the badge enrollment is a checkbox labeled “**Special Properties.**” Select this.
4. Check the **Toggle Unlock** box to enable the toggle property.

5. A drop-down menu will populate where you can select a specific **Access Point**, **Access Point Group**, or **All Access Points** for which this credential can toggle.

6. Click the **Save** button at the lower right corner of the window.

7. Credentials that are set with the toggle feature will show a padlock icon (🔒) next to them.

**Re-Locking**

1. In order to ensure your doors are not left in a toggle unlock state accidentally, you have the ability to set a **“Re-lock”** time.
2. Navigate to the **Settings** page.
3. Under “**Global Settings**” you will see a **Re-lock Time** for the toggle unlock. Simply set this to your preferred re-lock time and if the door is in an unlock state at this time, the door will re-lock.
automatically.

![Global Settings]

4. By default this is set to **23:59**

*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.*
5.2.1.6.2. Master Credential

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

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

**Setting up the Master property for credentials in Pure Access:**

1. Navigate to the user who needs a credential(s) with master privileges.
2. You can assign this property to new credentials or modify an existing one:
   a. [Adding a new credential](#)
   b. To edit a credential, click on the credential you wish to change and then select the 🏷️ icon.

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.
3. At the top right corner of the badge enrollment is a checkbox labeled "Special Properties." Select this.

4. Check the Master Credential box to enable the master property.
5. Click the **Save** button at the lower right corner of the window.

6. Run a compile by clicking the “**Update Access Points**” button to inform the devices this credential now has additional access rights.
5.2.1.7. Deactivating a User Profile

If you have a person with 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 a user from the Users page:

1. Click the “Users” tab on the left side navigation:

2. Select one or more users who you wish to deactivate, then click on the carrot (drop-down menu):

3. Click on “Deactivate Users”: 
Deactivating a user from a user profile page:

1. Navigate to the user profile of the person you wish to deactivate.
2. Click from the upper right corner of the page:

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.
5.2.1.7.1. Viewing Deactivated Users

On the right-hand side of Users page, you will see a “User Status” filter.

By default, inactive users are not included in the user list and can be shown by checking the “Inactive” box:

You can also uncheck the “Active” box to hide all active users.
5.2.1.7.2. Reactivating a User Profile

Reactivating a user from the Users page:

1. Click the “Users” tab on the left side navigation:

2. Select one or more users who you wish to activate, then click on the carrot (drop-down menu):

3. Click on “Activate Users”: 
Reactivating a user from a user profile page:

1. Navigate to the user profile of the person you wish to activate.
   a. See Viewing Deactivated Users for more information.

2. From the user profile, click Activate from the upper right corner of the page:
5.2.2. Adding a Profile Picture

1. Navigate to the user’s profile.

2. Click on the empty profile image to the left of the user’s name.

3. From the Add Profile Picture window, click **Choose Photo** then navigate to the image you wish to upload. Once selected, click **Upload Photo**.
4. Click **Save**

5. From the upper right corner of the page, click **Save Changes**

The profile picture should now appear on the user's page, at the upper right corner of Pure Access (if user is logged in), and in widgets.
5.2.3. Adding Users to 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 multiple ways of adding users to a group.

**From a user’s profile:**

1. Navigate directly to a user’s profile page and then click the icon next to “Groups”:

   ![Image of user profile with Groups icon highlighted]

2. Select the group(s) this person should be placed in from the drop-down menu.
3. Click the button.
4. Click “Save Changes” at the upper right.
5. You will find that the “Group Rules” column on the user profile page has been auto-populated with the proper weekly rule associations.

*Alternatively, you can remove users from groups by unchecking them from the drop-down list.*

**From the Users page:**

1. Click the “Users” tab on the left side navigation:
2. Select the user(s) you would like to add to a user group.

3. Select the drop-down menu where it displays the number of selected users, then click “Add Users to Group”.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Martin, John</td>
<td>All Users</td>
</tr>
<tr>
<td>Valentine, JR</td>
<td>All Users</td>
</tr>
</tbody>
</table>
4. Select the group(s) you wish to add the user(s) to.
5. Click **Save**

**From a user group’s page:**

1. Navigate to the Users page.

2. Select the **User Groups** tab.
3. Click the group where users need to be added.
4. Click **Add Users**

5. Select the users who need to be added then click **Add**
6. Click the **Save Changes** button.

See [Creating User Groups](#) for more information.
5.2.4. User Defined Fields

Pure Access has the ability to add additional fields to a user 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 a user’s profile:

1. Go to the Settings tab on the left hand side, then select User Defined Fields from the secondary navigation. There are 10 available fields you can add to a user profile.

2. Simply enter the field name you would like to use.

3. These fields will now all appear on the user profile page.
5.2.5. Updating Readers

Once a user has been added and their profile configured, the access points will need to be sent this information.

Clicking on Changes made. Update Access Points. at the top of the page will send a compile to the readers which updates the users, rules, and any other changes made.

This will be signified in the Pure Access history as Compile Send and Compile Complete (or Compile Failed) events.

Note that it is not necessary for an update to be pushed after every change that’s made and we advise against this practice.
5.2.6. Deactivating Credentials

You can deactivate a credential by doing the following:

1. Navigate to the user’s profile.
2. Select the credential you wish to deactivate.
3. Click the icon that resembles a stop sign/pause button ( ⏳).
4. Click Save Changes.

5. In order to send these changes to all readers, click at the top of the page to send a compile.

* Once deactivated, a credential can then be re-used on another user’s profile.
5.2.7. Reactivating Credentials

You can reactivate a credential by doing the following:

1. Navigate to the user’s profile.
2. Select the credential you wish to activate.
3. Click the icon that resembles a play button (○).
4. Click "Save Changes".
5. In order to send these changes to all readers, click "Changes made. Update Access Points." at the top of the page to send a compile.
5.3. Web Access and Administrator Privileges

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

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

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

An appropriate user role will need to be defined so that they have sufficient view or manage permissions. The predefined roles are: Administrator, Operator, Human Resources, and Cardholder.

The default Cardholder role is not sufficient for web access privileges as this does not grant any view nor manage access.

Granting Web Access rights:

1. From the user’s profile page, click the "Web Access" checkbox under the "First Name" field.
2. To invite a web access user, enter their email address and click "Invite Web User." The user will receive an email from Pure Access with an invitation link. From this link, users will review the tenant information and then create or confirm their password. Invitation emails will expire if not activated within 72 hours.
3. Select the "Edit User Role" button and then you can specify the user role from the drop down options.
Phone numbers for web access users are only used for the purpose of identity verification when contacting support.
5.3.2. User Roles

What do the pre-defined roles provide access to?

- **Administrator**: Provides access to view and modify all aspects of the system.
- **Operator**: Provides access to view only alerts, users, schedules, holidays/events, and dashboards.
- **Human Resources**: Provides access to view system settings and to modify users, schedules, holidays/events, and access points.
- **Cardholder**: Does not provide any view nor manage permissions. These are standard users with no administrator permissions.

You can view which permissions, specifically, a role has access to by selecting the role, choosing a role from the drop-down menu, then by scrolling through the list:

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

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

If you do not have web access configured for a tenant on Pure Access, it will ask that you create a new password:
If you already have web access to another tenant, it will ask that you simply confirm your existing password:
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 looks like the following screenshot, you are likely using Internet Explorer or another unsupported browser.
Please retry using Chrome or Firefox instead.
5.3.4. Removing Web Access Privileges

1. From the user's profile page, click **Remove Web Access**.

2. The below dialogue will appear:

   ![Remove Access Dialogue]

   **Are you sure that you wish to remove web access for this user?**

   - **Cancel**
   - **Remove Web Access**

3. Click **Remove Web Access**.

**Alternative**

If you simply **deactivate a user's profile** or set their **user role** as “Cardholder,” they will no longer be able to log into the tenant.

With this method, the user’s web access can be reinstated at a later date without them needing to accept the web access invitation again.

---

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

You can click the button next to “Custom Rules” at the lower right portion of a user profile page to configure a Grant Access or Auto-Unlock w/ Badge rule for this person.

After clicking the button, you’ll see a popup window showing the list of available shifts, access points/access point groups, and users to configure your “Custom Rule.”

You need to specify all three pieces (who, where, and when) in this window. Naming the rule and specifying the rule type is also required before you can add it (same as a weekly rule).
6. Managing 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.
6.1. Access Point Main Page

From here you can view all 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.
6.1.1. Access Point Settings

If you need to make any changes to the settings or retest an access point after you have finished the initial configuration, simply select the access point from the main Access Control page, then scroll down to the Settings.

- The header of the access point shows the name, MAC address, the model, which area the access point is assigned to as well as the credential bitmask.
- The area will default to common unless you utilize areas and change this.
- Latch Interval: this determines the length of time the latch will remain open. The maximum interval is 255 seconds.
- Lock Type will determine fail safe or fail secure. All RC04’s lock type will be configured from the software due to the solid state relay. RC03’s will be determined by the way the device is wired to the lock.
- Tamper can be set to enabled or disabled and will allow you to trigger alarms if the device is physically interfered with.
- To enable the Door Sense select the Enable button and then to retest the door sense select the test button and this will guide you through the test.

The diagram shows the settings section of the Isonas Pure Access software with detailed labels for each setting.
**Settings Continued**

**AUX/REX:**
- REX/AUX
- REX w/o Unlatch
- AUX
- AUX w/o Unlatch

**Beepers Sounds:**
- Accept Card
- Reject Card
- Grant Access
- REX Event
- Tamper Event

**Keypad:**
- Enable
- Disable

**Backlight:**
- Enable
- Disable

**AUX/REX LED:**
- Enable
- Disable

**Lock On Open:**
- Enable
- Disable

**Lock On Close:**
- Enable
- Disable

---

**On the RC04 there is a single wire for REX or AUX. To determine the use of this wire you simply select from this drop down. If you need REX without unlatch or AUX without unlatch set that here as well.**

**Keypad:** This will be automatically enabled and you can disable this if you choose. All keypads are also backlit and you can enable/disable that off if you choose.

**AUX/REX LED:** This allows you to enable or disable the LED upon a REX or AUX event. So if you prefer for the LED to not flash green you would disable this function.

**Beepers Sounds:** You can set which actions will trigger a beep from the reader.
6.1.1.1. Configuring the Advanced Security Module (ASM)

1. Navigate to **Access Control**.

2. Select the access point which needs to have the ASM configured.

3. From the access point’s page, scroll down to **Settings** then click **Enable** to begin the configuration process.

4. Follow the prompts:
   a. Click **Ready** to begin or **Cancel** to exit.
b. If this lock has an ASM, click “Yes” to proceed or “No” to exit.
   • At this time, if you have not factory reset the ASM you may do so (using a paperclip, hold the reset button for approximately 5 seconds until the left LED turns green), then click
     ![Yes button](image1)
     to test the lock.

   • Factory resetting the ASM in the previous step is not a requirement to proceed. If you are having difficulties with the configuration, however, it would be best to not skip the step.

5. Pure Access will send an **unlock** command followed by a **lock** command as a test. You will want to ensure that the lock physically follows the correct behavior before proceeding.
6. If this test has been successful, click **Yes** to proceed, **No** to exit, or **Repeat Test** to try again.

7. Once completed, you will be asked if you would like to change the ASM code.

8. The ASM configuration will proceed with a second lock test to ensure proper functionality. Follow the prompts:

   - Answering **Yes** will randomly generate and assign a code to the ASM and to the reader controller. This is the more secure option.
   - Clicking **No** will keep the default ASM code and the configuration will end. This is not advised.
9. If this test completed successfully, click Yes and your ASM should now be configured.

Here is the above process from start to finish assuming everything has been wired correctly at the door:
Enabling this feature will cause the test to start when you click 'Ready'. This may cause the door to unlock regardless of the current schedule.

Cancel  Ready
6.2. Adding an RC-04 Access Point

1. From the main page, select the Access Points tab on the left and then select the Access Points tab. On this screen you will see any active access points and access point groups.

2. To add a new Access point, simply select the add access point button on the far right of the screen.

3. Once clicked, the access point configuration wizard will appear. The access point wizard will allow you to enroll the device into the software, but also test and verify the wiring at the door for the REX, door sense, and Advanced Security Module (ASM). This feature was designed to allow technicians in the field to use their mobile device to enroll hardware as well as test all physical wiring while on site.

4. To enroll the device’s MAC address, simply type in the 12 digit MAC ID which can be found printed on the back and side of the reader:
5. Once you have entered the MAC address, the device will begin negotiating the connection. The device model will populate in the upper right hand corner. While you are waiting for the device to connect you can enter the Access Point Name as well as the Access Point Group.
**Please Note: you must move your cursor into the next field in order for the device to begin negotiating the connection!**

6. Once the device has connected, you will see the word **Connected** on the left. Now you can move on to the door wiring tests and configuration by selecting the **Next** button at the bottom. This is not required to complete the connection of the access point, but recommended to ensure the physical setup is correct. If you decide not to complete the tests, you can simply select the **Finish Later** button.
7. The next step in the wizard will ask you which peripherals you have connected to the hardware and allows you to set the **Beeper** and/or **Tamper Sensor**. Simply select or deselect the items you are using. The request to exit will be tested in a later test and by default is automatically turned on.
8. Next you'll run through the lock test where indicate how the lock is wired. The ISONAS RC-04 has a solid state relay and the fail-safe/secure configuration is set via software.

9. The second item it will ask you about is the ASM (formerly called an External Door Kit or EDK). Simply select whether or not one is in use at this door.
10. If you have manually reset the ASM/EDK back to its factory default settings, select “Yes” otherwise select “No.”

**Tip: To factory reset the ASM/EDK, simply take a paperclip to the small hole on top and hold it down for 15 seconds.**

11. Next the software will test the lock. If everything is wired properly, you should hear the latch click and see the door unlock.
12. The door sense test will ask you to open then close the door to test the sensor. If successful, you can hit “Next” to move on.
Door Sense Test

Open the door...
13. The badge test will allow you to ensure that the devices are reading credentials successfully (note that the badge will not provide access until it has been enrolled and the appropriate rules have been created). To begin the test, hit “Ready” then present your badge when prompted.
14. Next the wizard will provide the ability to update settings on your device. You can set the latch interval, the tamper sensor and which actions should initiate a beeper sound. You can change all of these items to configure the door as you prefer.
15. When you are finished, hit the “Settings Complete” button. This will take you to the last screen of the configuration wizard notifying you that the door is still unlocked. This is the case so you cannot be locked out while you’re programming the door prior to the system going live.

16. To set the door to a locked state, simply hit the “Lock” button. If you prefer to leave it unlocked, select “Unlock.” If you select “Unlock,” you will need to lock the door from the Pure Access software once you’re ready to do so.
Testing caused the latch to be unlocked. Do you want to leave this Access Point unlocked right now?
6.3. Adding an RC-03 Access Point

Instructions for the RC-03 are very similar to the RC-04 but with the following differences.

1. The enrollment process is the same as with the RC-04. You will enter the MAC address, name the door, and move through the tests.
2. One difference with the RC-03 is that there is both a REX wire and an AUX wire so you will see those as separate selections on the peripherals section.

3. On the RC-03 there is a typical Form C relay, unlike the RC-04 that has a solid state relay. Therefore, the RC-03’s fail-safe or fail-secure configuration is done via the hardware/wiring and not set in the software like with the RC-04. For this reason you will not see the “Lock Type” setting for the RC-03.
For a more comprehensive installation guide, please review [this article](#) from the **Setup and Configuration** section.
6.4. Adding an IP-Bridge

The process for adding an IP-Bridge is very similar to adding the RC-04 and RC-03. The IP-Bridge can control 2 or 3 doors and those doors are configured with the same MAC address.

1. Begin by entering the MAC address for the IP-Bridge. The configuration wizard will recognize the device as an IP-Bridge and populate the number of doors on the bridge to configure. Simply add the names of the 2 or 3 access points based on your IP-Bridge. Below is a 2 door scenario which is why the third door is showing "Not Communicating."

2. The configuration will then walk you through the setup for each door associated with the IP-Bridge. This is the same setup process as the RC-03. Once you hit "Settings Complete" on the first door, the wizard will prompt you to start the second door’s tests.
Configuration section.
6.4.1. Viewing/Managing Doors on an IP-Bridge

1. From the **Access Points** page, navigate to the bridge you wish to manage.

2. From the **Model** column, click on “IP-Bridge 1.0” or “IP-Bridge 2.0” depending on your model number.

3. Listed will be the currently added access point(s) as well as the option to add an access point.

   a. Clicking on the name of an access point (in this case, *Side Entry (left) [1]*) will take you to the access point’s page.

   b. Clicking on *Add Access Point* will launch the **Add New Access Point** modal.
6.5. Access Point Door Status

The status bar on the right hand side of the screen will show the current status of the door. If it is connected as well as the whether the door is locked or unlocked.

⚠️ **Please Note: This setting is not an override setting. You are not able to override the state of the door from locked to unlocked.**
6.6. Deactivating an Access Point

You can deactivate an access point by navigating directly to it from the main access point page (by clicking on the AP’s name) and then by clicking the “Deactivate” button from the upper right:

Alternatively, you can select one or more access points from the main Access Points page, click on the drop-down menu, then select “Deactivate Access Points”:

Note that a deactivated access point is still in the system. If you would like to remove it from your tenant entirely, see below for instructions on how to delete an access point.
### Deactivate Access Points

In the ISONAS Pure Access software, to deactivate access points:

1. Navigate to the Access Points section.
2. Select the access point(s) you wish to deactivate.
3. Right-click and choose **Deactivate Access Points** from the context menu.

**Note:** You can also activate or change the status of access points by selecting the desired action from the context menu.
6.6.1. Viewing Deactivated Access Points

You can view deactivated access points by clicking on “Show Deactivated Access Points” from the upper right corner of the main access point page:
6.6.2. Replacing an Access Point with Another Device

Once an access point has been deactivated, you will be able to use the button on the access point’s page to swap it with another device:

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

* If the new access point is having difficulty connecting, ensure the device has been configured properly.
6.6.3. 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 deactivated access point’s page.
2. Click **Delete**
3. From the confirmation prompt, click **Yes** to finalize the action:
Are you sure you want to delete this access point? This cannot be undone and all associated rules, dashboard panels, and permissions will also be deleted.

No  Yes
7. Weekly Rules, Schedules, and Events

Weekly Rules provide access to a user with a credential (Grant Access), unlock doors on a schedule (Auto-Unlock), or unlock a door on a schedule after a user with access has badged in (Auto-Unlock w/ Badge).

There are three items that are critical to creating these rules:

WHO will have access, WHERE will they have access, and WHEN will they have access.

1. WHO – Users and User Groups
2. WHERE – Access Points and Access Point Groups
3. WHEN – Weekly Schedules

• A User is a person in the system that has credentials and rules assigned to them. For example: John Doe is a user, his credential is Badge 35350, and he is a member the “Managers” User Group.
• An Access Point is a reader controller or port on an IP-Bridge. Access Points can be added to Access Point Groups for easy administration.
• Finally, a weekly schedule consists of the the time and days with which users will have access or an access point(s) will be unlocked.

* When creating rules, it is best practice to use groups whenever possible. It is significantly easier to manage a single group containing one hundred users than to manage the same one hundred users individually. This can also be said for access points.
7.1. Types of Rules in Pure Access

There are three types of weekly rules:

1. Grant Access
2. Auto-Unlock
3. Auto-Unlock w/ Badge
7.1.1. Grant Access

Grant Access is the most common rule type. This rule provides access to a group of Users (WHO) to a group of Access Points (WHERE) during a Schedule (WHEN).
7.1.2. Auto-Unlock

An Auto-Un{
lock} rule will keep one or more Access Points or Access Point Groups (WHERE) unlocked for
the duration of a Schedule (WHEN).
7.1.3. Auto-Unock w/ Badge

An Auto-Unock w/ Badge rule will keep one or more Access Points or Access Point Groups (WHERE) unlocked for the duration of a Schedule (WHEN) after a user with permissions has presented their credential (WHO).
7.2. Weekly Rules

In preparing to create a weekly rule, you will want to determine WHO will need access to which doors (WHERE) during which schedule (WHEN).

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

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

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

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

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

In the following steps, we will review a tenant in Pure Access who needs to create a rule for their cleaning crew that works in the evenings and on Saturdays.

It has been identified that anyone who is part of the cleaning crew will need access to specific doors on Monday through Friday from 5:30 PM to 11:30 PM as well as Saturday from 8:00 AM to 5:00 PM.

For this example we will cover:

1. Configuring user groups (WHO)
2. Configuring access point groups (WHERE)
3. Configuring schedules (WHEN)
4. Creating weekly rules
7.2.1. Step 1 – Configuring User Groups (WHO)

User Groups are used to organize users and efficiently manage access permissions via Weekly Rules. Those placed in the same user group will have identical access privileges once said group is assigned to a rule.

A group can be associated with a rule with or without users in it (the users can be added at any time). Once users have been placed in their appropriate groups, they will automatically inherit the rules that have been configured, if any.

1. Navigate to the Users page:

2. Select the “User Groups” tab.

3. Click the button at the upper right.

4. Name the group, then either Add Users or simply click the button.
*Note:* A user group can be created without adding users.

Adding the “Cleaning Crew” user group:

1. **Naming the user group**

2. **Adding users to the ”Cleaning Crew” group**
**Users listed in the group**

<table>
<thead>
<tr>
<th>Name</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drake, Nathan</td>
<td>Cleaning Crew</td>
</tr>
<tr>
<td>MacFarlane, Bonnie</td>
<td>Cleaning Crew</td>
</tr>
</tbody>
</table>
7.2.2. Step 2 – Configuring Access Point Groups (WHERE)

Access Point Groups are used to organize your doors and efficiently manage access permissions via Weekly Rules.

An access point group can be associated with a rule with or without doors in it (these can be added at any time). Once the access points have been placed in the appropriate groups, they will automatically inherit the rules that have been configured, if any.

1. Navigate to the Access Control page.

2. Select the “Access Point Groups” tab.

3. Click the Access Point Group button at the upper right.

4. Name the group, then either Add Access Points or simply click the Save Changes button.

Note: An access point group can be created without assigning access points.
Adding the “Cleaning Crew Doors” access point group:

Naming the access point group

Adding access points to the “Cleaning Crew Doors” group
Access points listed in the group
7.2.3. Step 3 – Configuring Schedules (WHEN)

Schedules determine when users will have access to doors (Grant Access or Auto-Unlock w/ Badge rules) or when doors will be unlocked (Auto-Unock rule).

1. Navigate to the Access Control page.

2. Select the “Schedule” tab.

3. Click the button at the upper right.

4. Name the schedule. Adding a description is optional.

5. Choose a schedule type:
   a. **Non-Holiday**: This schedule will not run on days set as a “Holiday” on the calendar.
   b. **Holiday**: This schedule will only run on days set as a “Holiday” on the calendar.
   c. **Always**: This schedule will run on both “Non-Holiday” days as well as on days set as a “Holiday” on the calendar.

6. Set the days of the week as well as the times in which this schedule will run. Click .
In the above example, rules configured with this schedule will not run on holidays since the schedule type is set to “Non-Holiday”. If these users should also have access during “Holidays”, the schedule type should instead be set to “Always.”
7.2.4. Step 4 – Creating Weekly Rules

Now that the Groups and Schedules have been created, you can put all of them together to create your rules.

1. Click on the “Access Control” tab.

2. From the Weekly Rules tab, select the + Weekly Rule button.

3. From the Add Weekly Access Point Rule pop-up:
   a. Name your rule (it is recommended that the name is descriptive).
   b. Select a rule type.
   c. Set the WHEN, WHO, and WHERE parameters by dragging and dropping your schedule, user group(s), and access point group(s) from the left to the right.
4. Click **Add**.

This Weekly Rule will grant our “Cleaning Crew” (user group) access to the “Cleaning Crew Doors” (access point group) from Monday through Friday, 5:30pm to 11:30pm, and Saturdays from 8:00am to 5:00pm (per the “Cleaning Crew Hours” schedule).
To edit a rule, you simply select the three dots (⋯) on the right hand side of the rule:
7.2.4.1. Deactivate a Weekly Rule

**Method 1**

1. Navigate to the access control tab:

2. Select the rule or rules you wish to deactivate, then use the drop-down menu at the top to select "Deactivate Selected Rules":

3. Confirm your decision by clicking **Deactivate**:
Method 2

1. Navigate to the access control tab:

2. For the rule you wish to deactivate, click on the three dots to the right to open up the edit window.

3. At the bottom of this window, click **Deactivate**.
4. Confirm your decision by clicking **Deactivate** again:
You are about to deactivate this rule. You will need to update access points for this change to take effect. Do you wish to continue deactivating this rule?

Cancel  Deactivate
7.2.5. Frequently Asked Questions

My schedule needs to span across midnight, what do I do?

You will need to create two schedules. One ending at 23:59 and the second one starting at 00:00.

I created a weekly rule but it’s not working!

Remember to click the button at the top of the page.
7.3. Scheduled Events and Holidays

In addition to your normal weekly schedules, you may wish to set up special events or holidays on the calendar.

When a day is set as a Holiday, your standard weekly rules configured with a “Non-Holiday” schedule will be overridden.

A day set as a Holiday on the calendar will not override a rule configured with an “Always” schedule.

Events are used to override weekly rules. The actions an event can take are:

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

For the most consistent performance, please ensure your hardware is on the latest firmware.
7.3.1. Setting up a Holiday in the Calendar

1. Navigate to **Access Control**, then select the “**Calendar**” tab:

2. There are two ways to add a “**Holiday**”:
   a. Select **+Holiday** from the upper right corner of the page.
   b. Navigate to and click on the day, then select the **+Holiday** button.
3. Give your holiday a name, set the date(s), then hit the **Save** button.
View or modify a holiday:

Select the month (and year) from the navigation bar on the right, then click on the name of the holiday you’d like to view/edit:
Holidays are designated by an  icon. When selected, you will be met with a window similar to the Add Holiday pop-up as shown in Step 3 above.

You can also view created holidays directly on the calendar:
Need access on a Holiday?

If you require access to the building on days set as a **Holiday**, you'll simply need to use a rule following the "**Holiday**" schedule type.

Here’s an example of a schedule configured for Black Friday where the doors need to be unlocked from 5:00am to 10:00pm:

![Calendar with Black Friday highlighted]

**Note:** On days set as a **Holiday**, all rules following a “Non-Holiday” schedule will be overridden.
Rules associated with this “Black Friday 2019” schedule will only run on days set as a Holiday. You cannot designate specific dates in weekly rules so this rule would need to either remain deactivated or should not be created until necessary.
7.3.2. Creating an Event in the Calendar

1. Navigate to **Access Control**, then select the “**Calendar**” tab:

   ![Calendar tab selected](image)

2. There are two ways to add an “**Event**”:
   a. Select **+ Event** from the upper right corner of the page.

   ![Add Event button](image)

   b. Navigate to and click on the day, then select the **+ Event** button.
3. Give your event a name, set the date, start time, and end time.
4. Choose the access point or access point groups that will be affected.
5. Select whether the door/doors need to be **locked**, **unlocked**, **unlocked with a badge**, or **locked down**.

   *Note: For the **Auto-Unlock w/ Badge** type, you will also need to select the user(s) who will be allowed to unlock the access point(s) selected.*

6. Hit the **Save** button.
**View or modify an event:**

Select the month (and year) from the navigation bar on the right, then click on the name of the event you’d like to view/edit:
Events are designated by an 📍 icon. When selected, you will be met with a window similar to the **Add Event** pop-up as shown in Step 3 above.

You can also view created events directly on the calendar:
8. Dashboard Widgets

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.
8.1. How to set up a Dashboard

1. 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.
2. Type the name of the new dashboard then select General (to use widgets) or Floor Plan.
3. If Areas are configured, you will need to choose the area with which this dashboard will be visible.
4. Finally assign this dashboard to a User Group or, if everyone with web access should be able to see the dashboard, select “Default (All users)”.

![New dashboard window with Areas](image)

*Different users can be set to view/manage specific dashboards and activities. For example, a web access user defined as an Operator can only view the dashboard specific to the “Operator” role (usually the admit button).*

If you select the General view, you will have the option to customize the dashboard layout with up to three widgets. Below this is a history view that shows the most recent events/activity in list form.
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.
8.1.1. Setting up a Single Access Point Widget

If one door needs to be monitored 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 anywhere on one of the three Custom Widget panels, then select “SINGLE ACCESS POINT” from the list. Click Next.

2. Choose the access point you would like to manage and deselect any unnecessary history events. Click Done.
a. From here you can view the access point’s history.

b. You can unlock the door for the duration of this access point’s latch interval (by default this is set to 3 seconds). Do this by pushing ![Admit Button](image).

c. You can also use the drop-down menu to push commands to the access point. The commands are:

   i. **Schedule**: sets the door back to the schedule it should be following.
   
   ii. **Unlocked**: unlocks the door until it is set back to **Schedule**.
   
   iii. **Locked Down**: locks this access point down.
Below is a further description of the single access point dashboard and the notifications.
Door Status Shows the schedule the door is following.

Schedule, locked or Unlocked shows the state of the door lock.

The Admit button allows you to take actions on the door.

The icon on the right side also shows you the type of event.

Shows the latest activity, person and time stamp of activity.

If a door sensor is present, the state of the door will be displayed.
8.1.2. Setting up a Multiple Access Point Widget

To manage up to 12 readers at once (up to 36 per dashboard), you can use a “Multiple Access Point” widget. Unlike the Single Access Point widget, this will not show history events.

1. Click anywhere on one of the three Custom Widget panels, then select “MULTIPLE ACCESS POINT” from the list. Click Next.

2. Click one of the 12 + buttons. Choose the access point you would like to manage from the dropdown menu, then click Done.
a. You can unlock a door for the duration of the access point’s latch interval (by default this is set to 3 seconds). Do this by selecting an access point, then by pushing

b. You can also select one or more doors then use the drop-down menu to push commands. The commands are:
   i. **Schedule**: sets the door back to the schedule it should be following.
   ii. **Unlocked**: unlocks the door until it is set back to **Schedule**.
   iii. **Locked Down**: locks this access point down.
8.1.3. Setting up a 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.

1. To set up the main history widget (at the bottom of the page), simply select the tool icon (⚙️) from the right-hand side.

2. From here you can configure the users, access points, event types, and badge ID's you would like to see in this view.
   First choose the category (i.e. users or access points) from the left-hand side. The full list of items from that category will appear to the right:

   The start date and start time are optional parameters.

3. Click Done.

On the widget you will see: the access point, the time and date stamp of the event, the specific event, the badge ID (if applicable), and the name of the person the event is associated with.
You can expand the view of the dashboard by selecting the arrows (▲) next to the settings button (⚙️). This will expand the view to be the complete screen allowing you to see more of the history. To minimize the view, simply select the arrows again.

**Adding an additional history widget:**

1. Click anywhere on one of the three **Custom Widget** panels, then select “HISTORY” from the list.

   ![Widget Selection](image-url)

   - SINGLE ACCESS POINT
   - MULTIPLE ACCESS POINTS
   - HISTORY
   - ACCESS POINT ADMIT
   - LOCKDOWN ACCESS POINTS
   - USER PROFILES

   Click **Next**.
2. Configure the date and time range you would like to view history for (if left blank this will display the previous 24 hours).

3. From the drop-down menu (beginning with Date/Time), select the category you would like to modify then deselect anything you would not like to view events for.

4. Click **Done**.
# 8.1.3.1. Standard History Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Schedule</strong></td>
<td>Device has been set to return to the scheduled weekly rules.</td>
</tr>
<tr>
<td>Approve</td>
<td>User presented a credential that has been accepted.</td>
</tr>
<tr>
<td><strong>Admit</strong></td>
<td>An admit has been sent from a dashboard widget.</td>
</tr>
<tr>
<td>Unlocked</td>
<td>An access point was set to an unlocked state from the dashboard.</td>
</tr>
<tr>
<td>Auto-Unlock</td>
<td>An auto-unlock schedule has started.</td>
</tr>
<tr>
<td>Badge Unlock</td>
<td>An <a href="#">Auto-Unlock w/ Badge</a> rule has started.</td>
</tr>
<tr>
<td>Decline Badge</td>
<td>Presented credential has not been accepted (ensure the <a href="#">weekly rules</a> have been configured properly)</td>
</tr>
<tr>
<td>Not Found</td>
<td>Not Found</td>
</tr>
<tr>
<td><strong>Decline Outside Schedule</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Decline Tamper</strong></td>
<td>A credential is declined because there is a tamper alert.</td>
</tr>
<tr>
<td>Device Connect</td>
<td>The device has connected to the software.</td>
</tr>
<tr>
<td>Device Disconnect</td>
<td>The device has lost connection to the software.</td>
</tr>
<tr>
<td>Compile Send</td>
<td>New/Updated information has been sent to all access points.</td>
</tr>
<tr>
<td>Compile Complete</td>
<td>New/Updated information has been sent to all connected access points.</td>
</tr>
<tr>
<td>Compile Failed</td>
<td>Some or all information was not able to reach the reader.</td>
</tr>
<tr>
<td>Credential Sent to Reader</td>
<td>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.</td>
</tr>
<tr>
<td>Locked Down</td>
<td>A lockdown of access points has been activated.</td>
</tr>
<tr>
<td>Lockdown Ended</td>
<td>Reader has been set back to the current schedule and is no longer locked down.</td>
</tr>
<tr>
<td><strong>Decline Lockdown</strong></td>
<td>Credential has been declined because access point is currently locked down.</td>
</tr>
<tr>
<td>REX Admit</td>
<td>There was a REX event on the device, unlocking the door unless set to &quot;REX w/o Unlatch.&quot;</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AUX Admit</td>
<td>AUX admit occurred from an input button tied into the device.</td>
</tr>
<tr>
<td>Status Only</td>
<td>Command sent to reader unrelated to active process.</td>
</tr>
<tr>
<td>Reader Error</td>
<td>Hardware error (the Coldfire and Coprocessor firmware may be mismatched). Please contact support if this persists.</td>
</tr>
<tr>
<td>Internal Error</td>
<td>Hardware error. Please contact support if this persists.</td>
</tr>
<tr>
<td>Offline</td>
<td>The virtual device has been deactivated.</td>
</tr>
</tbody>
</table>

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.
8.1.4. Setting up an 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 anywhere on one of the three Custom Widget panels, then select “ACCESS POINT ADMIT” from the list. Click Next.

   ![Widget Selection](image)

2. Select an access point from the drop-down menu, then click Done.

3. To use this widget, simply press the “Admit” button and the access point will unlock for the duration of its latch interval (set to 3 seconds by default).
8.1.5. Setting up the Lockdown Access Points Widget

This widget is used to set your access points into lockdown. You can set it up to lock down all access points, a single access point, or a group of access points. A locked down reader will have a red LED which blinks every few seconds.

1. Click anywhere on one of the three Custom Widget panels, then select “LOCKDOWN ACCESS POINTS” from the list. Click "Next".

2. Select an access point or group from the drop-down menu, then click "Done".
3. To use this widget, simply press the “Lock Down” button and the access point(s) will go into lockdown mode.
4. To take the access point(s) out of lockdown, click on “Reset”.
You can also take access points out of lockdown by pushing the “Schedule” command from a Single or Multiple Access Point widget.

⚠️ Only a credential set with the master property can open a door in lockdown.
8.1.6. Setting up a User Profile Dashboard 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 anywhere on one of the three Custom Widget panels, then select “USER PROFILES” from the list. Click Next.

2. Select the access point or access point groups you would like to monitor:
9. Reports

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

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

Types of reports:

1. History
2. Users
3. Access Points
4. Schedules
5. Holidays
6. Attendance
7. Permissions
8. User Export
9. Scheduled Reports
9.1. History Report

A **history report** shows all event history on your tenant by access point, time, the type of event, credential (if applicable), and the name of the person (if applicable).

1. To run a history report, navigate to the **Reports** tab and then select the **History** tab from the top navigation.

2. On the right hand side of the page, you can set filters to narrow down what information is displayed in the report. If you are looking for a specific event or person, simply select the down arrow to expand the field and then select/deselect the relevant users, access points, events, etc.
3. You can set parameters on the **From** and **To** filters allowing you to narrow down the date and time of the events contained within the report.
4. Once you have the filtering the way you’d like, select the Run Report button on the top right to generate the requested information.

5. All reports can be exported as a PDF or a CSV file. Simply select Save as PDF or Save as CSV to download your report.

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

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

1. To run a users report, navigate to the Reports tab and then select the Users tab from the top navigation.

2. On the right hand side of the page, you can set filters to narrow down what information is displayed in the report. If you’d like to view a specific person, group, or area; simply select the down arrow to expand the field and then select/deselect the relevant information.
3. Once you have the filtering the way you’d like, select the Run Report button on the top right to generate the requested information.

4. All reports can be exported as a PDF or a CSV file. Simply select Save as PDF or Save as CSV to download your report.

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

Example of a Users report:
Users Report

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

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

<table>
<thead>
<tr>
<th>User Group</th>
<th>User Name</th>
<th>Email Login ID</th>
<th>Badge ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>R. Marty</td>
<td>N/A</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>R. Marty</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>OfficeDept.</td>
<td>Bemberg, Dennis</td>
<td>N/A</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Fletcher, Bill</td>
<td>N/A</td>
<td>50</td>
</tr>
<tr>
<td>PartsDept.</td>
<td>Arans, Kendra</td>
<td>N/A</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Brooks, Brandon</td>
<td>N/A</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Kuch, Mark</td>
<td>N/A</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Reinsch, Katie</td>
<td>N/A</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>S., Dennis</td>
<td>N/A</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Taylor, Frank</td>
<td>N/A</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Tietz, Rodney</td>
<td>N/A</td>
<td>76</td>
</tr>
<tr>
<td>SalesDept.</td>
<td>Gohsman, Julie</td>
<td>N/A</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>RTO, Ryan</td>
<td>N/A</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>RTO, Ryan</td>
<td>N/A</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>Baker, Dallas</td>
<td>N/A</td>
<td>46</td>
</tr>
</tbody>
</table>
9.3. Access Points Report

The **access points report** is very similar to the users report. It provides a list of all **active access points**, their **MAC address**, **test status**, and any **description** that has been entered.

1. To run an access points report, navigate to the **Reports** tab and then select the **Access Points** tab from the top navigation.

2. On the right hand side of the page, you can set filters to narrow down what information is displayed in the report. If you’d like to view a specific access point, group, or area; simply select the down arrow to expand the field and then select/deselect the relevant information.
3. Once you have the filtering the way you’d like, select the Run Report button on the top right to generate the requested information.

4. All reports can be exported as a PDF or a CSV file. Simply select Save as PDF or Save as CSV to download your report.

Example of an Access Points report:
To view which access points are assigned to specific access point groups, you will want to utilize the **Access Point Groups** filter from the options on the right.

This report will show the **group name**, the **access points assigned to that group**, the **MAC address**, and **test status**.
Access Point Groups report
9.4. Schedules Report

The schedules report allows you to see the schedules in your system and their type, the days, start and end times, and if they are valid.

Schedules report can be filtered by type, specific schedules, or area.

Definition of schedule 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.
9.5. Holidays Report

The holiday’s report provides an overview of all currently scheduled holidays in the system. You can use the start and end date filter to show you all past, current or future holidays to ensure you have all appropriate holidays in place.
9.6. Attendance Report

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

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

The permissions report shows a collective view of all rules; who can go where and when they can go there.

Field Descriptions:

1. **Name**: this represents the name of the user group or user if you have individual rules assigned
2. **Access Point**: this is the list of doors that are included in the rule
3. **Rule Type**: is the type of action that takes place during this rule
   a. **Grant Access**: Anyone added to the User Group will have access to the group of Access Points during the schedule assigned. The door will remain locked until a badge is presented at which point it will unlock for the duration of the latch interval.

* If you have set up all rules by user group, then this report will only populate when you select the user group option. If you set up individual rules by user, then those rules will be reported by selecting users in the filter.
b. **Grant Access – Two-Factor**: Same as above, but access is only granted if the globally configured two-factor process is successfully completed. See the two-factor section of the manual for more details.

c. **Auto-Un lock**: Any access points or group of access points will unlock and relock using the schedule provided. Users are not associated with this rule type because no badge is required to change the door state.

d. **Auto-Un lock w/Badge**: Any access points or group of access points will unlock once someone in the user group has presented their badge and will relock following the assigned schedule.

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

When filtering by access point(s), **Rule Type** will be replaced with the **Rules** with which the doors are currently following:

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

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

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

In addition to on demand reports, you also have the ability to schedule reports to be sent by email on the days and times configured.

You can schedule the following types of reports:

- History
- Users and User Groups
- Access Points and Access Point Groups
- User Attendance and Group Attendance
- User Permissions and Group Permissions

To set up a scheduled report:

1. Navigate to Scheduled Reports by either:
   a. Clicking on Go to Scheduled Reports from the lower right corner of the Reports page:
   b. Alternatively, you can click on Settings then the Scheduled Reports tab:
2. To create a new report, select the + Report button, enter the name of the report, then click Save.

3. From here you will choose the Report Type, apply the appropriate filters, set who should receive the report via email, and set the day(s) of the week and time.
   a. First, select the Report Type from the drop-down:
b. Depending on the report you select, the appropriate filters will appear. Select the filters you want on the report. For example, if you chose the *History* report you can filter by user, access points, event types, or badge ID.
c. Select the people you would like the report to be emailed to. All users will be listed, however, only those with Alert Notification Email Address or web access configured can receive the reports.
d. Set the time, time zone, and day(s) you’d like the report sent:
i. **Report Time** is set on a 24-hour clock and can be narrowed down to the minute

ii. **Time Zone** pertains to which time zone you’d like the report time to follow (by default it will be the time zone your tenant is currently set to). If you’d like the report to be sent on a different time zone, simply select it from the drop-down.

4. Click [Save Changes] from the upper right. To edit a report simply select it from the list on the left:
In section 3d above, the report will send every Friday at 8:00pm Mountain. This will contain all information since the last time the report had run (the previous Friday at 8:00pm). If this report was set to run every day, however, it would consist of information from the previous 24 hours.
10. Alerts and Notifications

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 or the bell icon (🔔) from the upper right.

A red dot will appear to notify you that there is an unacknowledged alert.
10.1. Alert Types and Setup Procedure

Pure Access supports the following alerts:

1. Unauthorized Open
2. Extended Open
3. Tamper
4. AUX Alarm
5. REX Alarm
6. Credential Rejected/Expired/Over Limit
10.1.1. 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. Within Pure Access, select the Access Control tab.
3. Select the Access Points tab.
4. Select the access point you wish to modify, ensure the “Enable” box is checked, then complete the Door Sense test.
5. Follow the prompts:

Door Sense

Enabling this feature will cause the test to start when you click 'Ready'. This may cause the door to unlock regardless of the current schedule.

Cancel  Ready

Open the door...
10.1.2. 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. Within Pure Access, select the **Access Control** tab.
3. Select the **Access Points** tab.
4. Choose the access point you wish to modify.
5. Scroll down to the **Door Sense** setting and ensure it is enabled, then complete the door sense test.
a. Follow the prompts:

Door Sense

Enabling this feature will cause the test to start when you click 'Ready'. This may cause the door to unlock regardless of the current schedule.

Open the door...
c. Click

6. Click

7. Now set the “Extended Open Threshold” which can be found in the Alerts tab under Settings.
10.1.3. 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 readers tamper sensor.

Enabling the Tamper Sensor

1. Within Pure Access, select the Access Control tab.

2. Select the Access Points tab.
3. Choose the access point you wish to modify.
4. Scroll down to the Tamper setting and select “Enabled” from the drop-down menu.

5. Click Save Changes.
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.
10.1.4. 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. Within Pure Access, select the **Access Control** tab.

2. Select the **Access Points** tab.

3. Choose the access point you wish to modify.

4. Scroll down to the **AUX/REX** setting and ensure it is set appropriately from the drop-down menu:

5. Click **Save Changes**
10.1.5. 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.
11. Custom Rules

Custom Rules provide the ability to set *IF, THEN* actions in the Pure Access 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.
11.1. Creating a Custom Rule

1. Select the **Access Control** tab in the main navigation and then select the **Custom Rules** tab:

   ![Custom Rules Tab]

2. Click the add button on the right hand side.

3. Give this rule a name and hit the save button.

   ![Add Custom Rule]

**Setting the IF condition(s):**

1. First you will need to choose the first IF condition by clicking on the gear icon (⚙).
2. From the drop-down menu, choose from the list of available **IF functions**:
3. Click the green check mark button (✓) to finalize the selection.

4. Click on the gear (⚙️) next to your selection to edit or the gear below this to add an additional condition:

5. Add conditions to meet your preference on what, specifically, will trigger the response:
Setting the DO condition:

1. Select the gear icon, then choose what will happen once the IF condition is triggered:

2. Specify the access point(s), user(s), etc. that will be affected, then hit or 

A Master Condition Cannot be deleted

Lock down a specified door/group of doors

Present an alert notification

Unlock a specified door/group of doors

Reset a specified door/group of doors to a no...

Deactivate a card for a particular person
Here is the custom rule we just created:
If an AUX input is triggered at the Server Room access point, all access points in the IT Rooms group will be put into lockdown.

You can cancel your selection by choosing the grey x (×). If you choose to delete a condition, you must delete the sub conditions first before deleting the master conditions.

Translation:

If an AUX input is triggered at the Server Room access point, all access points in the IT Rooms group will be put into lockdown.

Please be aware that all custom rules are host dependent features and are NOT stored or triggered on readers locally. In other words, if the reader is not communicating with the Pure Access server(s), it will not function.
11.2. Changing a Custom Rule

1. You have the ability to change a custom rule at any time. Simply select the gear icon (⚙️) next to the portion of the rule you need to change and make the new selection.

2. Make your change, then choose the green check mark (✔️) to save it.

3. If you want to delete a custom rule completely, select the gear icon next to the name of the rule at the top of the screen, then select the red trash can (🗑️).
12. Two-Factor Authentication

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

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

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

1. Card/PIN
2. Two User
3. Two-User – Card/PIN

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

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

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

NOTE: This PIN is separate from the keypad credential used for single authentication.
12.2. Two User

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

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

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

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

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

To configure two-factor authentication you must:

1. Globally enable two-factor authentication on the settings page
2. Set up two-factor credentials (for any Card/PIN configuration)
3. Set up a two-factor rule
12.4.1. General Settings Page

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

1. Navigate to the General Settings page by clicking the Settings button on the left navigation bar.
2. Directly under the “Global Settings” heading, you will see a “Two-Factor Settings” heading.
3. In the first drop-down, you can choose from the three two-factor modes or globally disable two-factor.

When first enabling two-factor authentication, Pure Access will check all of the connected readers/devices to make sure they are on a supported firmware version. If none of the connected devices are on a supported firmware version, you’ll be prompted to update your firmware.

Pure Access will also notify you if some of your devices require a firmware update before enabling two-factor authentication.

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

Two Factor is available in firmware versions:

- RC-04 – Coldfire v75.06 / WL v1.8 / BLE v1.6
- RC-03 Rev M/N – Coldfire v63.01 / PIC v33.03
You can also configure a two-factor timeout interval between 5 and 30 seconds. This interval is the amount of time allowed to complete each individual step of the two-factor entry process. After successfully performing a step in the entry process, the timeout interval counter is reset.
12.4.2. 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.
12.4.3. 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.
12.5. 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:

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Short Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-Factor – Credential 1 of 2 Accepted</td>
<td>Approve (1)</td>
<td>The first credential in a two-user or two-user card and PIN process has been accepted</td>
</tr>
<tr>
<td>Two-Factor – Credential 1 Rejected – Timeout</td>
<td>Denied – Timeout (1)</td>
<td>The first credential in a two-user or two-user card and PIN process has been denied due to reaching the configurable timeout interval.</td>
</tr>
<tr>
<td>Two-Factor – Credential 1 Rejected – Process Error</td>
<td>Denied – Process Error (1)</td>
<td>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.)</td>
</tr>
<tr>
<td>Two-Factor – Credential 1 Bad PIN</td>
<td>Denied – Bad PIN (1)</td>
<td>The first credential in a two-user or two-user card and PIN process has been denied due to an invalid two-factor PIN.</td>
</tr>
<tr>
<td>Two-Factor – Credential 2 of 2 Accepted</td>
<td>Approve (2)</td>
<td>The second credential in a two-user or two-user card and PIN process has been accepted. Access granted.</td>
</tr>
<tr>
<td>Event Description</td>
<td>Result Description</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Two-Factor – Credential 2 Rejected – No Credential Found</td>
<td>Denied – No Credential (2)</td>
<td>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.</td>
</tr>
<tr>
<td>Two-Factor – Credential 2 Rejected – No Authorized Schedule</td>
<td>Denied – No Schedule (2)</td>
<td>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.</td>
</tr>
<tr>
<td>Two-Factor – Credential 2 Rejected – Device in Lockdown</td>
<td>Denied – Lockdown (2)</td>
<td>The second credential in a two-user or two-user card and PIN process has been denied due to access point being in lockdown.</td>
</tr>
<tr>
<td>Two-Factor – Credential 2 Rejected – Two-Factor Timeout</td>
<td>Denied – Timeout (2)</td>
<td>The second credential in a two-user or two-user card and PIN process has been denied due to reaching the configurable timeout interval.</td>
</tr>
<tr>
<td>Two-Factor – Credential 2 Rejected – Two-Factor Process Error</td>
<td>Denied – Process Error (2)</td>
<td>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.)</td>
</tr>
<tr>
<td>Two-Factor – Credential 2 Rejected – Bad PIN</td>
<td>Denied – Bad PIN (2)</td>
<td>The second credential in a two-user or two-user card and PIN process has been denied due to an invalid two-factor PIN.</td>
</tr>
<tr>
<td>Two Factor – Accepted (Card/PIN)</td>
<td>Approve (Card/PIN)</td>
<td>Valid credential and PIN presentation. Access granted.</td>
</tr>
<tr>
<td>Two Factor – Timeout in PIN Entry (Card/PIN)</td>
<td>Denied – Timeout (Card/PIN)</td>
<td>Denied due to reaching the configurable timeout interval during the card and PIN procedure.</td>
</tr>
<tr>
<td>Two-Factor – Process Error (Card/PIN)</td>
<td>Denied – Process Error (Card/PIN)</td>
<td>Denied due to a process error during the card and PIN procedure.</td>
</tr>
<tr>
<td>Two-Factor – Bad PIN (Card/PIN)</td>
<td>Denied – Bad PIN (Card/PIN)</td>
<td>Denied due to an incorrect PIN during the card and PIN procedure.</td>
</tr>
</tbody>
</table>
13. Still Need Help?

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

Should you run into an issue, you can reach out to our support team at (800)581-0083 option 2 or by emailing support@isonas.com. Alternatively, you can schedule a call on our appointment booking site.

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.