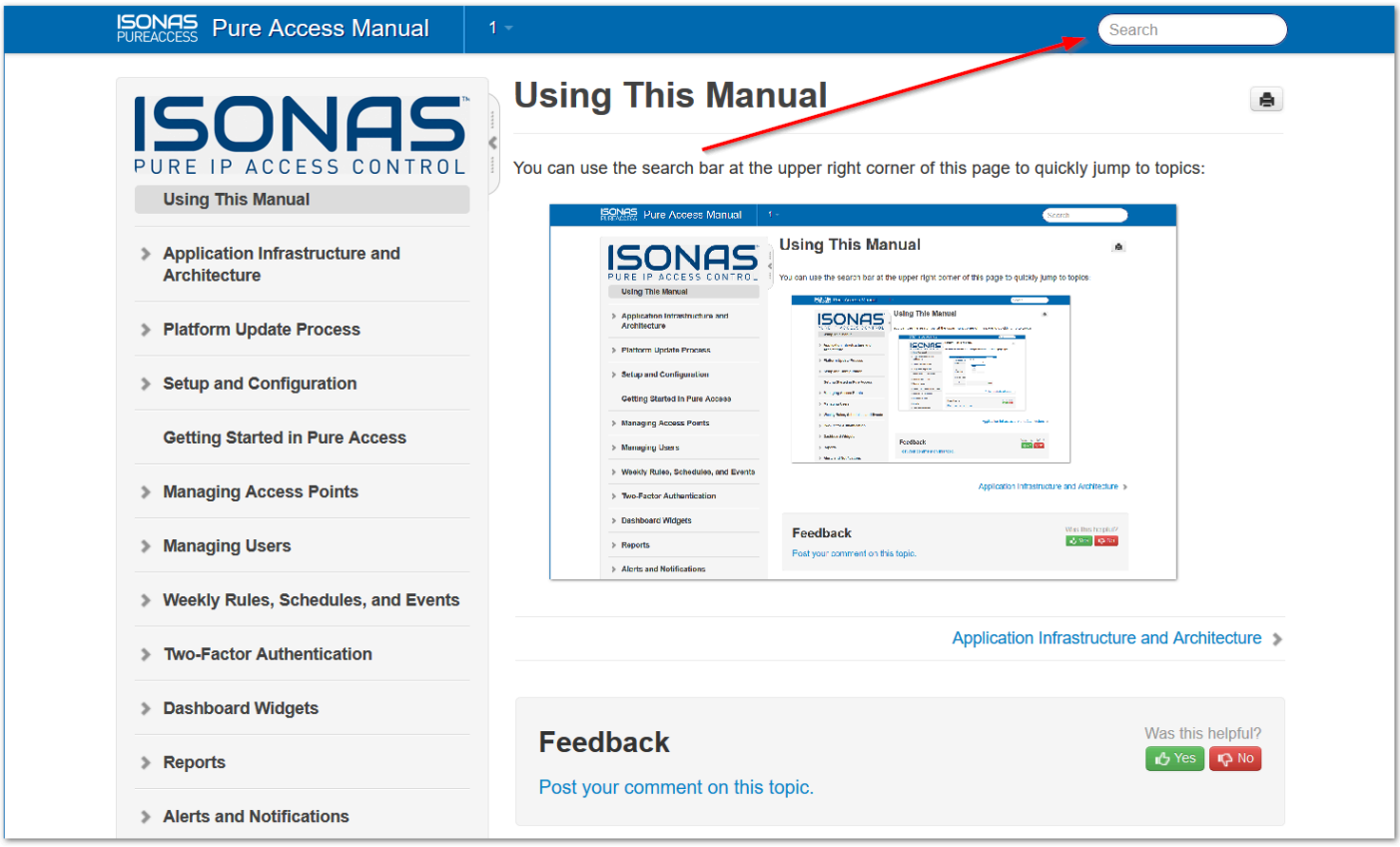
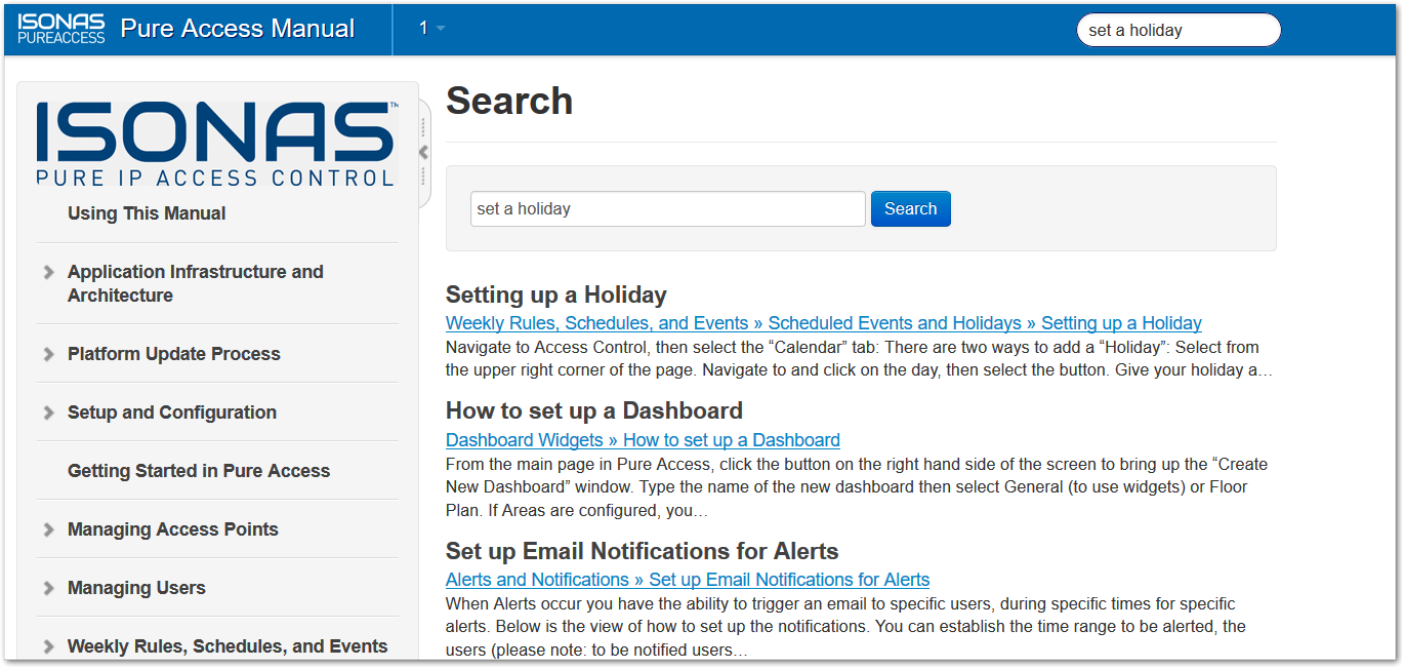
Table of Contents

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:



Last modified: 1 September 2023

Contact Support

Should you run into an issue, you can reach out to our technical support team at (877) 671-7011 Option #2 or by emailing isonas.tech.prod.support@allegion.com.

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.

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.

Sales and Order Status

Sales/System related questions: Reach our collective sales team at isonas.sales@allegion.com or call us directly at (877) 671-7011 Option #1 where any member of the team will be able to assist.

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

Last modified: 19 September 2024

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*.

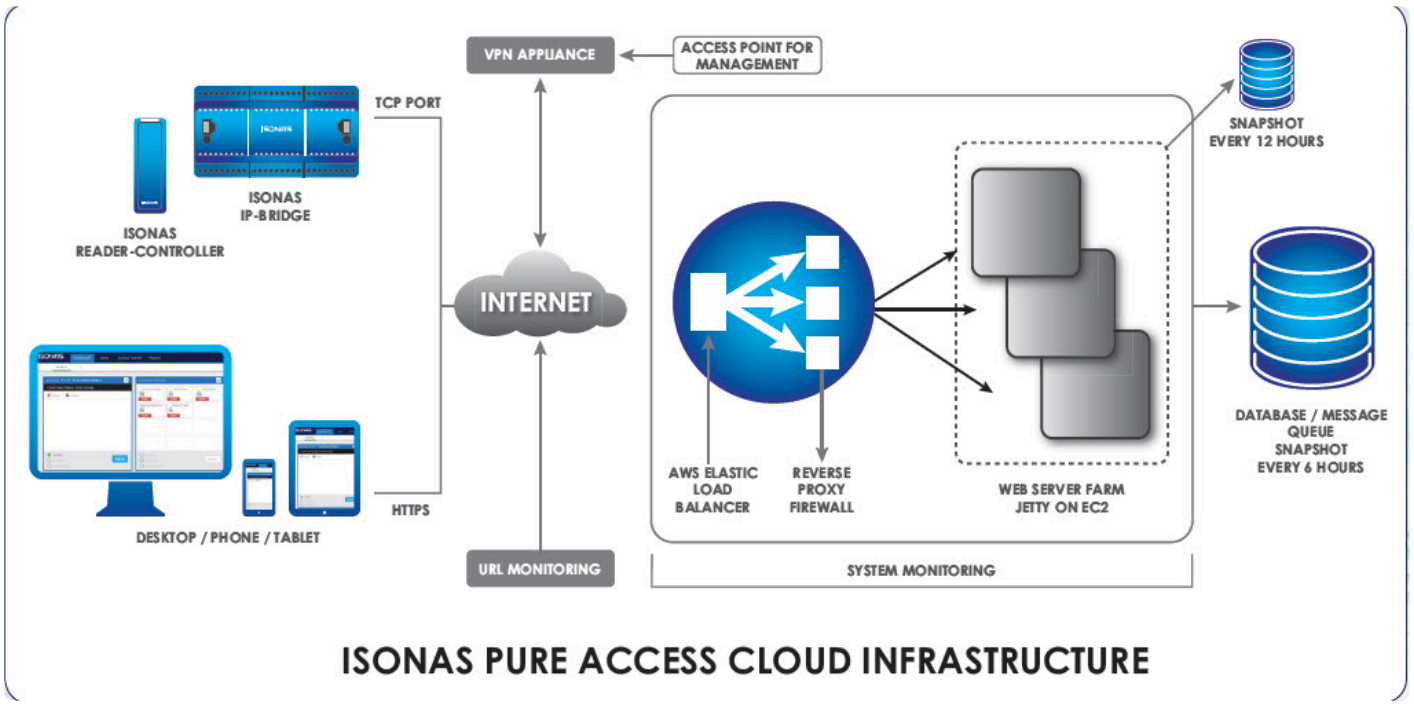
Pure Access Manager is housed in the same set up, but instead of being hosted by *AWS*, you are providing the server to host the platform within your internal network.

The following pages will display the infrastructure of each platform:

- Pure Access Cloud
- Pure Access Manager (on-premise)

Last modified: 26 February 2021

Pure Access Cloud Infrastructure



Last modified: 26 February 2021

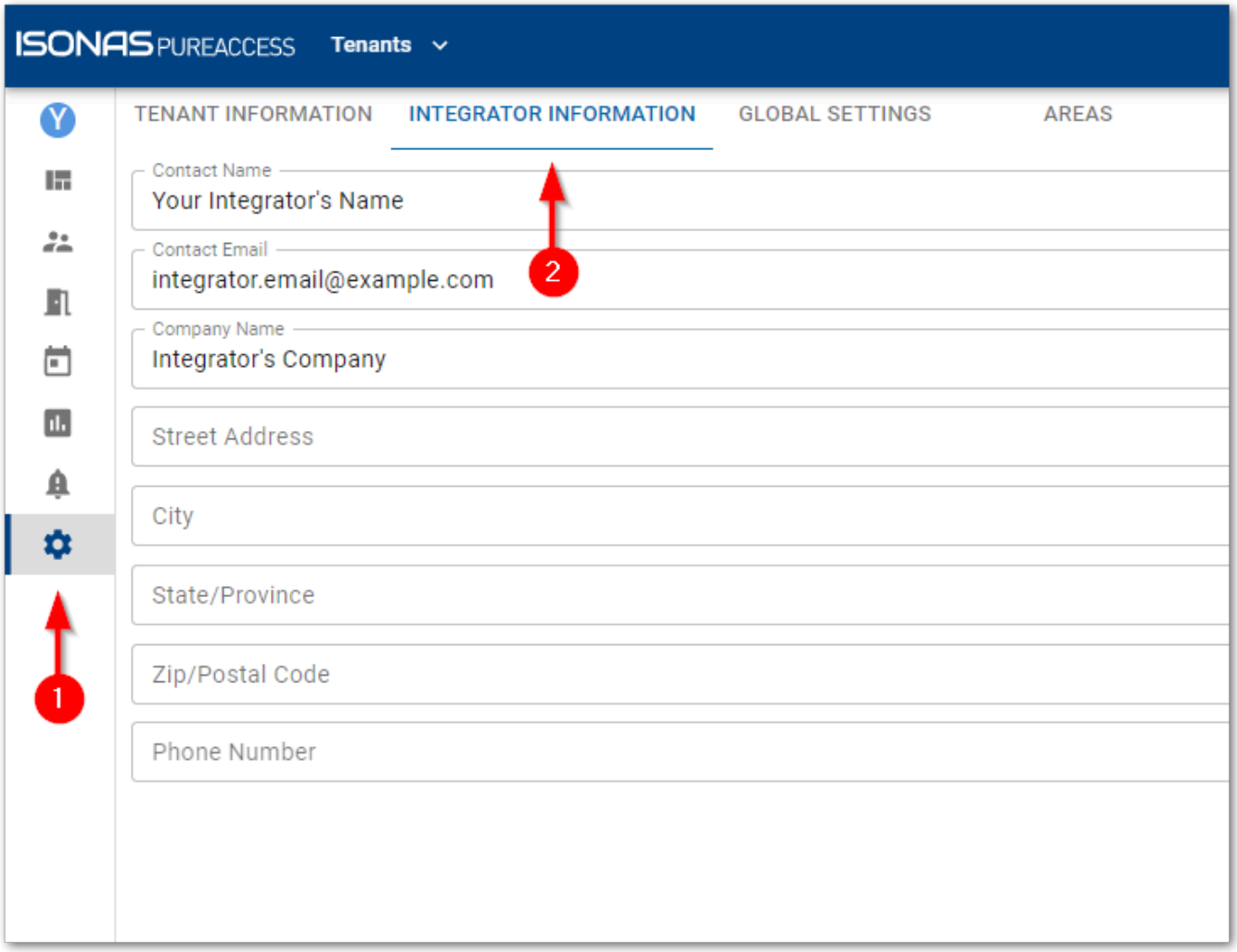
Pure Access Cloud License Renewal FAQ

How do I renew my license?

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

Access software.

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



How do I know when my license is due?

Email reminders are sent at 30, 15, 5, 3, and 1 day before the license is due for renewal. Who receives them depends on the license type:

License Type	Who Receives the Notification
Stand Alone Licenses (PAC-1-1, PAC-1-5, PAC-6-20)	All active Administrators will receive the notification emails at their established web-access email addresses.
RMR Licenses	Only the Administrator Email address listed in the Parent RMR Tenant

License Type	Who Receives the Notification
	Information settings receives the notification emails.

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

To view the license expiration date, navigate to the **Tenant Information** section within the tenant's settings. Here you can see the license type and other relevant information list listed for you.

How do I know what license I have?

This information is housed in the **Tenant Information** section within the tenant's settings. The license type will reflect the size and number of doors your license allows.

How do I update my contact information?

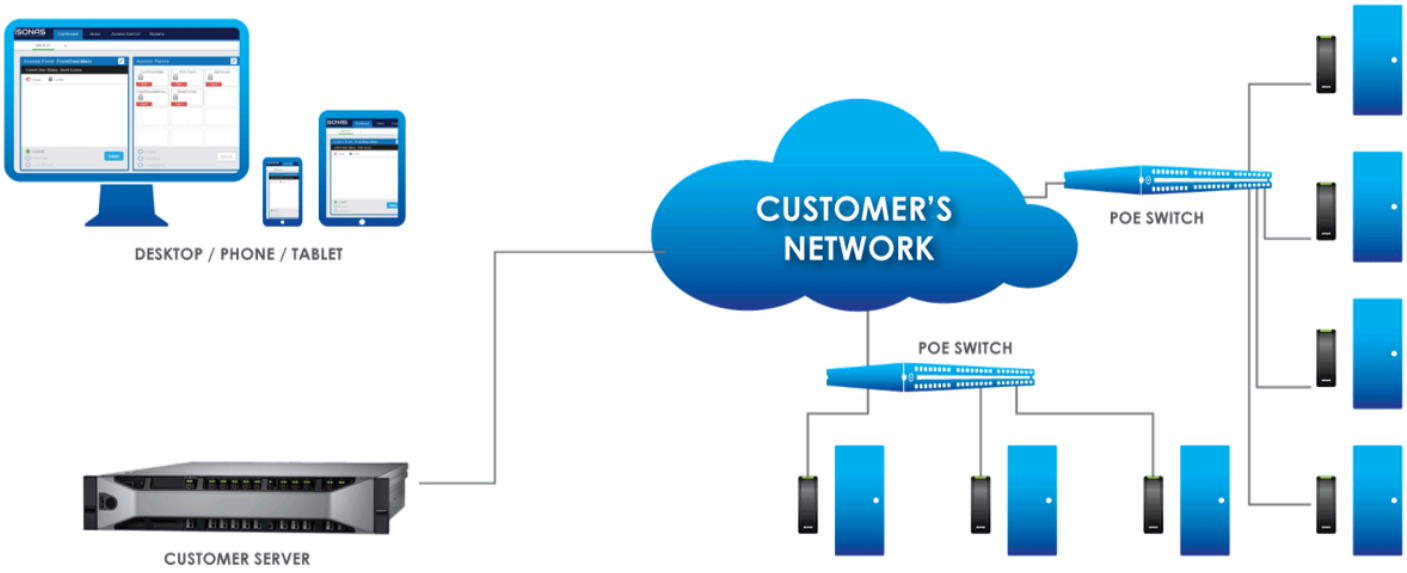
Select the settings button and you can update the integrator information at any time. You must have administrator access to update this information.

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

If the integrator information is not filled out, call 800-581-0083 and we can assist with connecting you to your installer.

Last modified: 1 July 2026

Pure Access Manager Infrastructure



Last modified: 26 February 2021

Pure Access Manager System Requirements

A dedicated machine running:

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

OR

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

Last modified: 26 February 2021

Platform Update Process

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

Last modified: 26 February 2021

Pure Access Cloud

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

Upgrades are typically released once per quarter.

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

(See next page for Pure Access Manager)

Last modified: 26 February 2021

Pure Access Manager

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

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

Last modified: 26 February 2021

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.

Last modified: 26 February 2021

Network Configuration and Troubleshooting

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

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

Resources

- IP Addressing
- Firewall Information
- Best Practices
- Troubleshooting connectivity issues
- Network Help Guide

Last modified: 13 October 2025

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

Last modified: 26 February 2021

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.

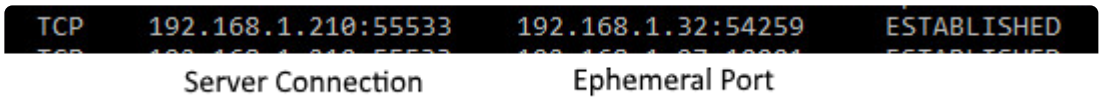


Figure 2 – IP-Bridge Example Connection

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

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

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

Figure 1 - RC-03 Example Connection

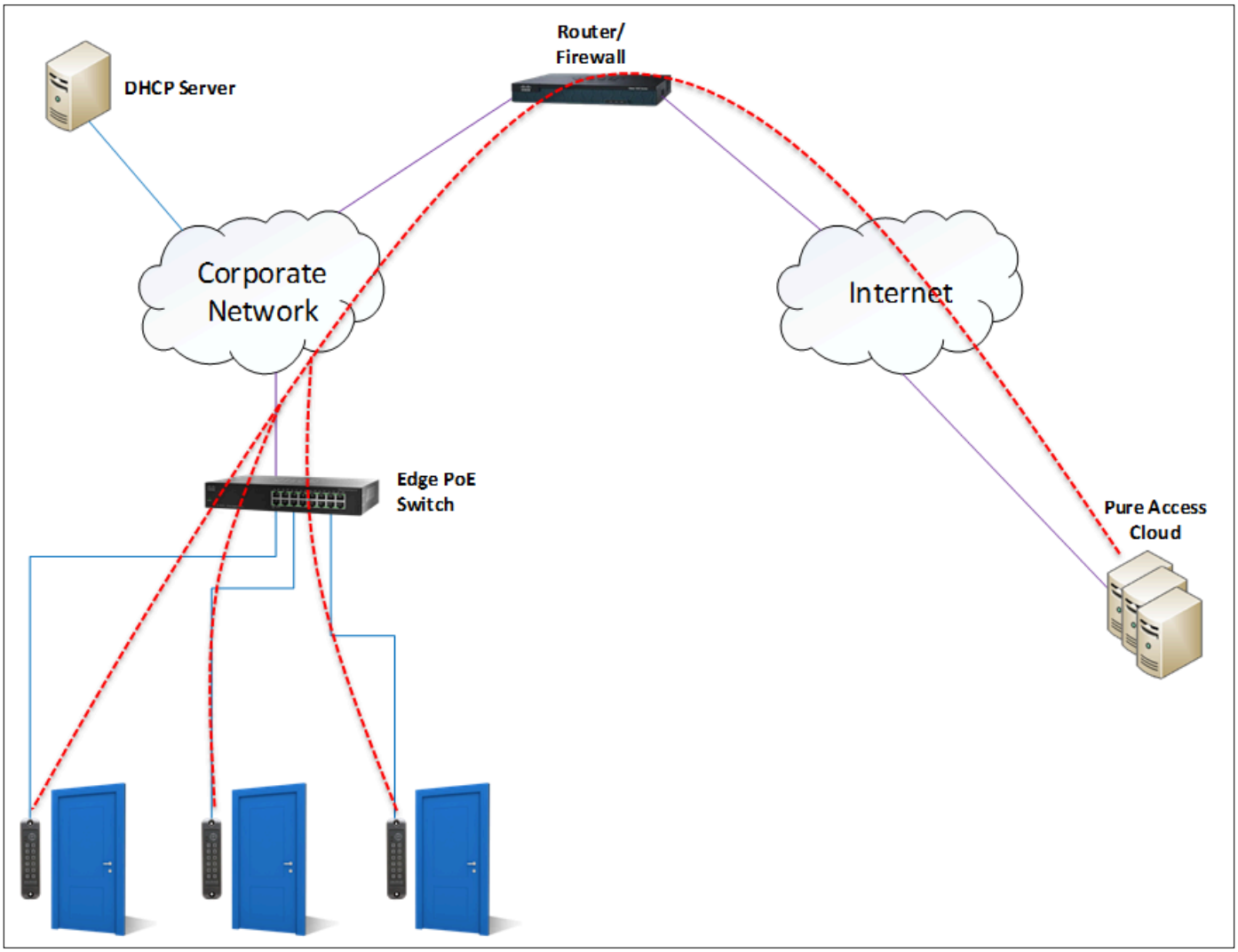


Figure 3 – Reader-controller Connections

ISONAS Devices (IP Bridge)

General

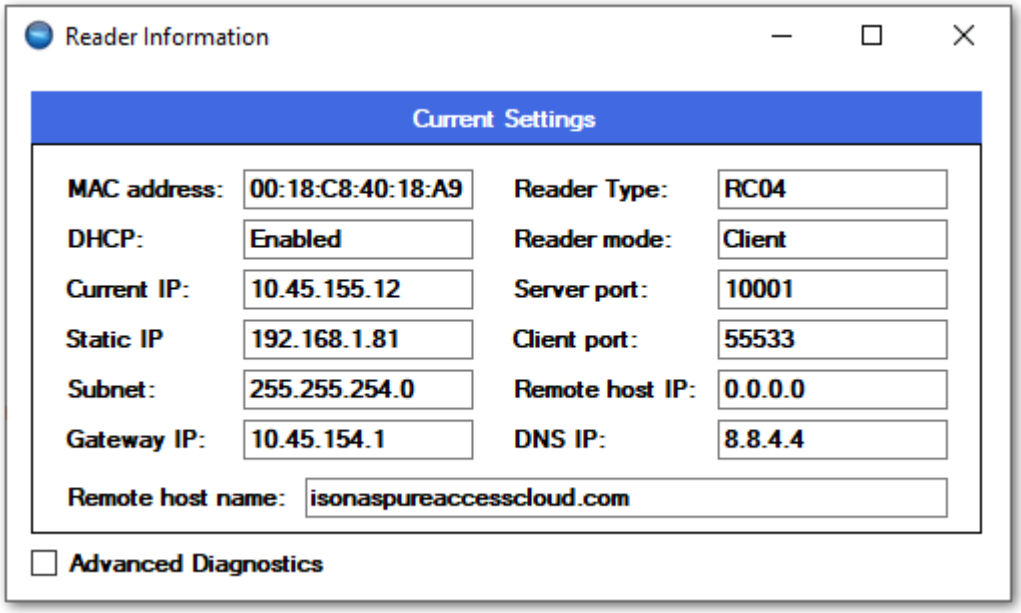
- Do you have **port 55533** open to the internet or at least open to **isonaspureaccesscloud.com**?
- How is your latency? If the latency to the **isonaspureaccesscloud.com** site is greater than 100ms, you may see minor issues. If greater than 200ms there could be larger communication problems.
    - 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 Zentra 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 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, which is advised, try to statically set a reader's IP to an available address on your network as a troubleshooting step. Setting the reader to a static IP will let us know if DHCP is preventing the connection.

- Try **bypassing the DNS**.
    - To do this, you will need to configure the reader(s) using the Cloud server's IP as the host address (click "*Specify Host IP Address*" in the configuration tool).
    - You can find the public IP address of our Cloud environment via command prompt by typing ***nslookup isonaspureaccesscloud.com*** then hitting enter.

    - If the device is able to connect this way, we know there is a DNS issue.
- 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.

Contact your network administrator for help configuring your network.

Schlage Devices

Schlage devices use both standard HTTP and HTTPS connections for communication. Encryption is provided through the TLS connection made over the HTTPS connection to the servers, as well as each credential is individually encrypted with a site specific scheme automatically generated by the system.

Schlage devices access the following sites for firmware and database updates, as well as reporting audits and alerts.
Schlage RC

- Engage WS: https://cloud-iot.isonas.com/engage/wss
- Engage CA: https://cloud-iot.isonas.com/engage/ca

Schlage NDE, LE (Wireless devices)

- cloud-iot.isonas.com

Last modified: 24 April 2026

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.
- Although the IEEE specification allows for cable length to be up to 328 feet (100 meters), we recommend that the cable length be a short as practical, not exceeding 100 feet, to minimize voltage drop between the switch and the device.
- Online devices cannot navigate DHCP credential-oriented landing pages. For example, a Hotel Wi-Fi that would require you to sign in using your room number and last name or a university that would require credentials and a EULA acceptance to be able to access the internet.

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**.

> There are two exceptions to this: (1) **RC-03 Classic** units should be set to 10Mb **half** duplex and (2) the **RC-04** running firmware version 78.04 (or later) supports 100Mb full 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: p(banner important). **Recommendation**: Create a group or VLAN for Schlage devices. Firewall rules will need to be created to allow traffic to the internet on ports 55533, 80, and 443 for both TCP and UDP. For any network admins looking to restrict access to only the destination IP addresses needed to communicate with our web APIs, the list of IPs can be found at https://www.cloudflare.com/ips/

Please note that this list of IP addresses is subject to change. We strongly recommend that automation be used to keep the firewall ACL up to date with the listed Cloudflare IP ranges.

Last modified: 5 June 2026

Additional Troubleshooting

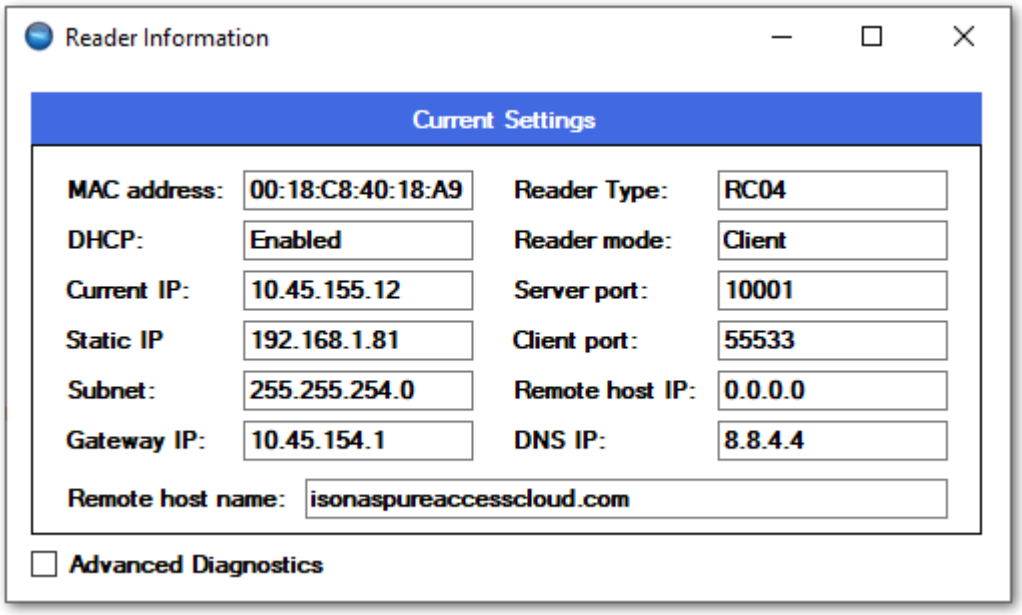
ISONAS DEVICES

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 as the host address (click "*Specify Host IP Address*" in the configuration tool).
    - You can find the public IP address of our Cloud environment via command prompt by typing ***nslookup 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.
- Pure Access Cloud runs on Cloudflare. If firewall exceptions need to be made, you can find a list of Cloudflare's IP address ranges here.
- Run a packet capture application such as Wireshark to determine where/when the data is dropping.

Physical Issues

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

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

SCHLAGE DEVICES

Schlage devices use both standard HTTP and HTTPS connections for communication. Encryption is provided through the TLS connection made over the HTTPS connection to the servers, as well as each credential is individually encrypted with a site specific scheme automatically generated by the system.

The following are used by the system admin inside the firewall when logged into Pure Access™ or the Zentra™ Web Application

- app.pureaccess.com

Schlage devices access the following sites for firmware and database updates, as well as reporting audits and alerts.
Schlage RC

- Engage WS: https://cloud-iot.isonas.com/engage/wss
- Engage CA: https://cloud-iot.isonas.com/engage/ca

Schlage NDE, LE, CTE (Wireless devices)

- cloud-iot.isonas.com

Contact your Access Control Software provider for their server address if your devices are managed by a PACS System

- If Whitelisting is used, the IP ranges listed here must be cleared in order to work properly with our devices o https://www.cloudflare.com/ips/

Last modified: 19 March 2026

Network Help Guide

IP-based security devices (such as ISONAS and Schlage reader-controllers, the IP-Bridge, and similar equipment) are IoT-style devices that require minimal network configuration to operate.

This document provides guidance to ensure they are installed and configured correctly.

Last modified: 10 December 2025

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 by 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)

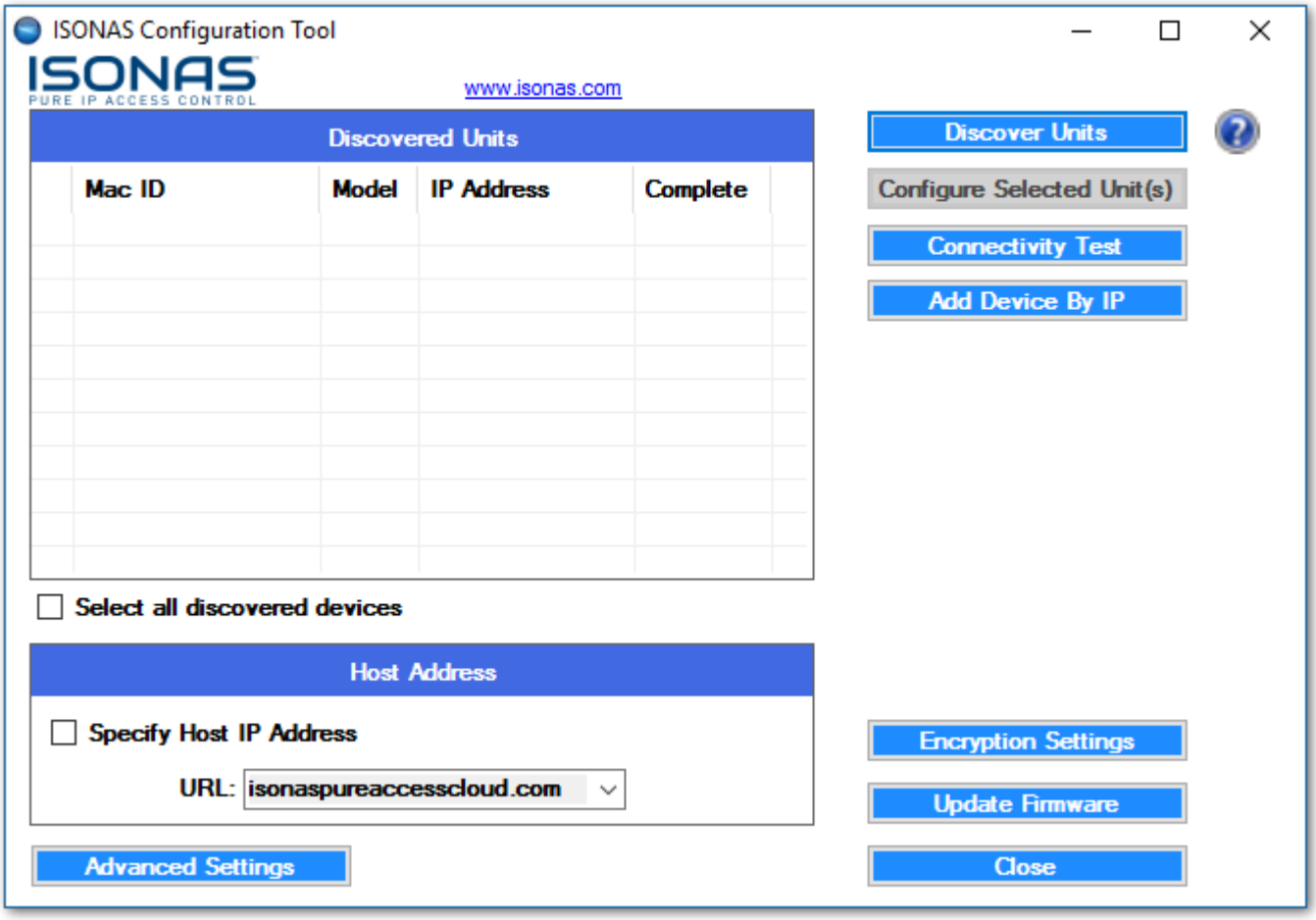
For information on how to install RC-03's and IP-Bridges (including LED status information and jumper configuration), please review these PDF documents:

1. RC-03 Installation
2. IP-Bridge Installation

Last modified: 15 January 2026

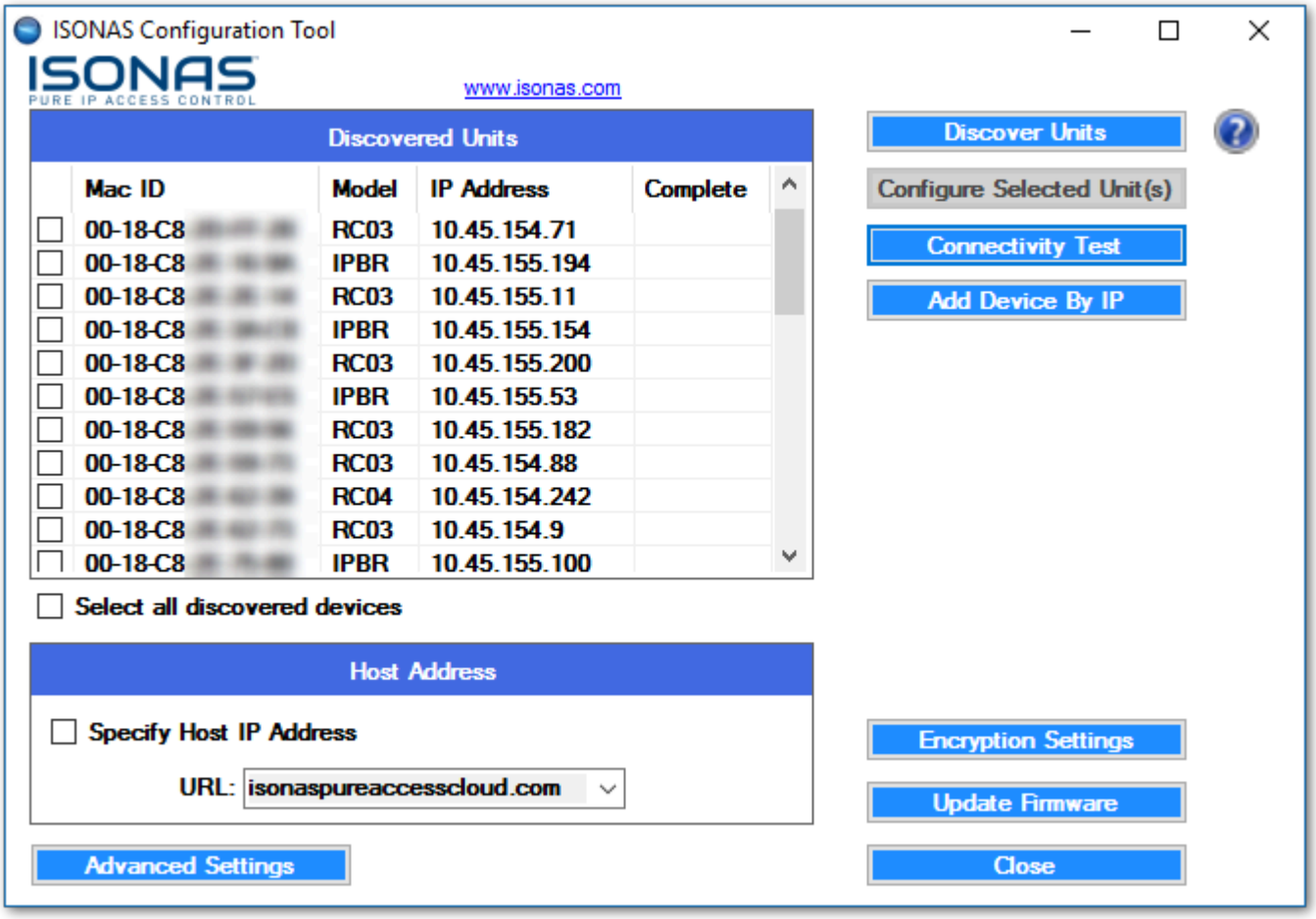
Using the Configuration Tool

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



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

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

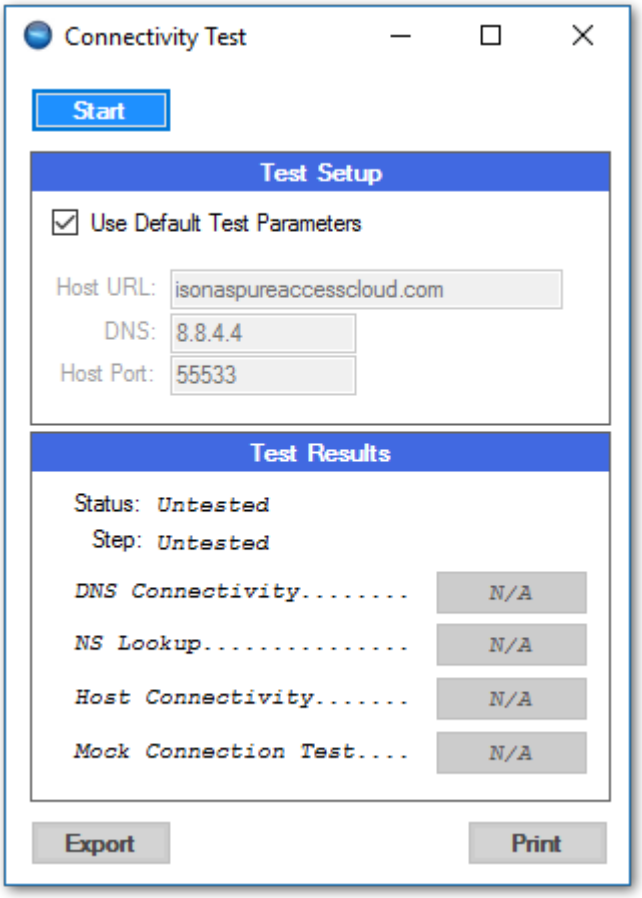


If you are not able to find the devices on the network, see the Discovering Units section.

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

- The Connectivity Test will determine if the network segment that the Configuration Tool is running on can make a connection to our server. This simulates a device connection by your PC and does not perform a connectivity test of devices discovered by the tool.

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



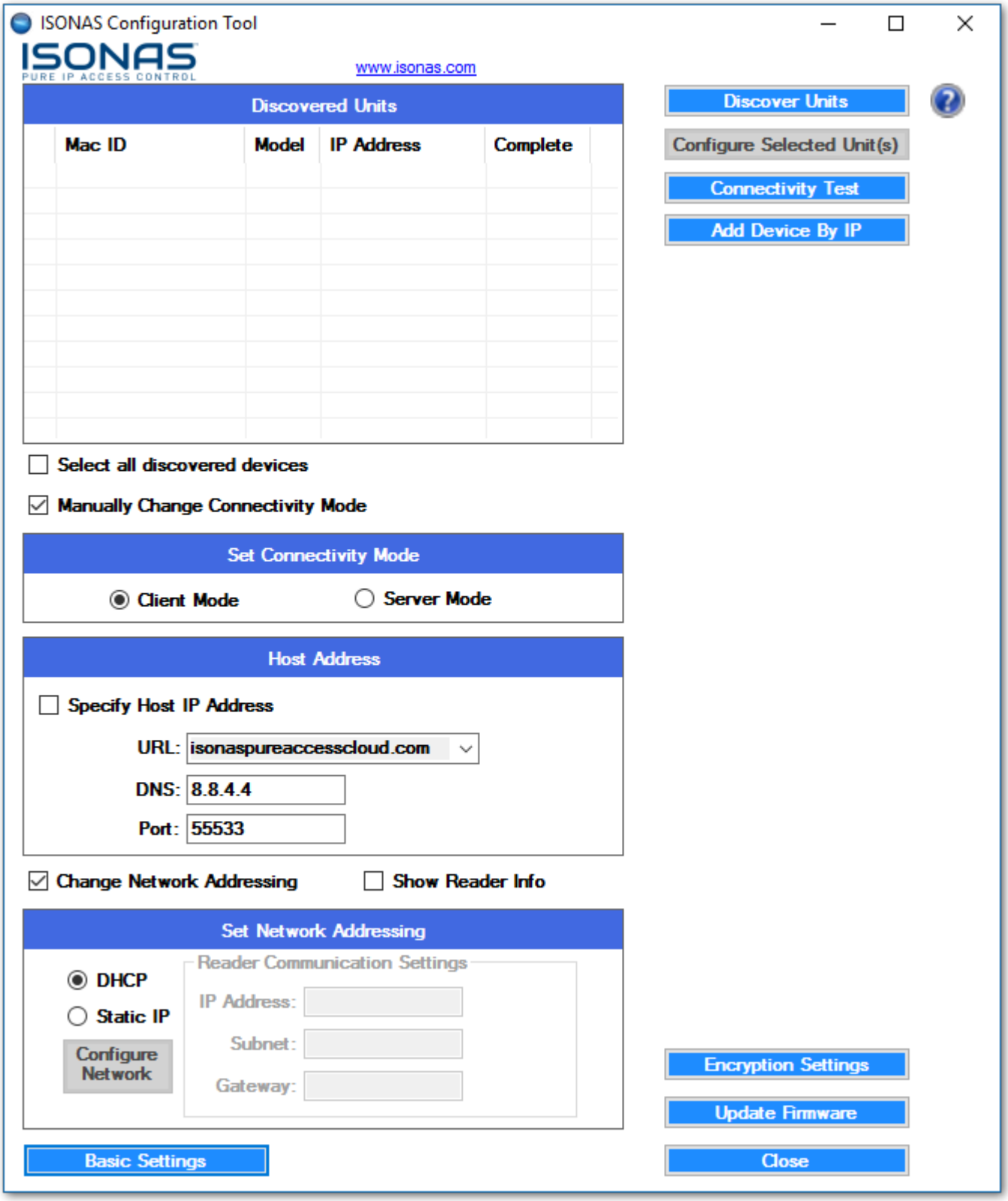
If the devices were discovered, proceed to Advanced Configuration to continue setting up the controllers.

Last modified: 10 April 2026

Advanced Configuration

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

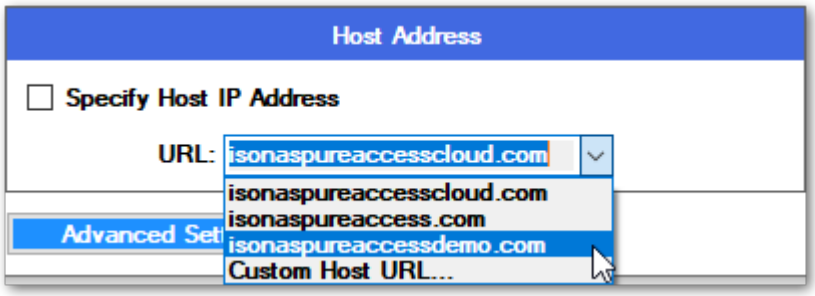
The options now available allow you to change where the device(s) will be attempting to connect as well as the ability to set the readers to either DHCP (preferred) or static IP addresses.



Establishing a connection to Pure Access:

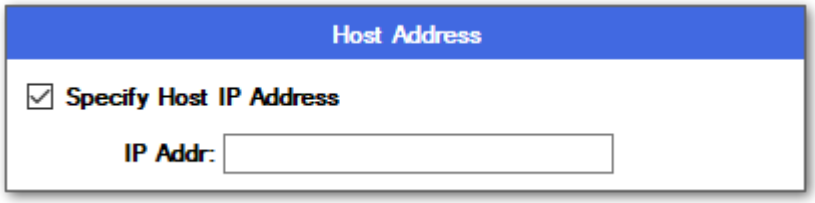
1. All devices must be set to **Client Mode** in order to initiate a connection with Pure Access. **Server Mode** is reserved for updating the firmware of the devices only.

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



    c. If your tenant is on our legacy environment, this will need to be ***isonaspureaccess.com***. **[Note: This environment has been deprecated.]**

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



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

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

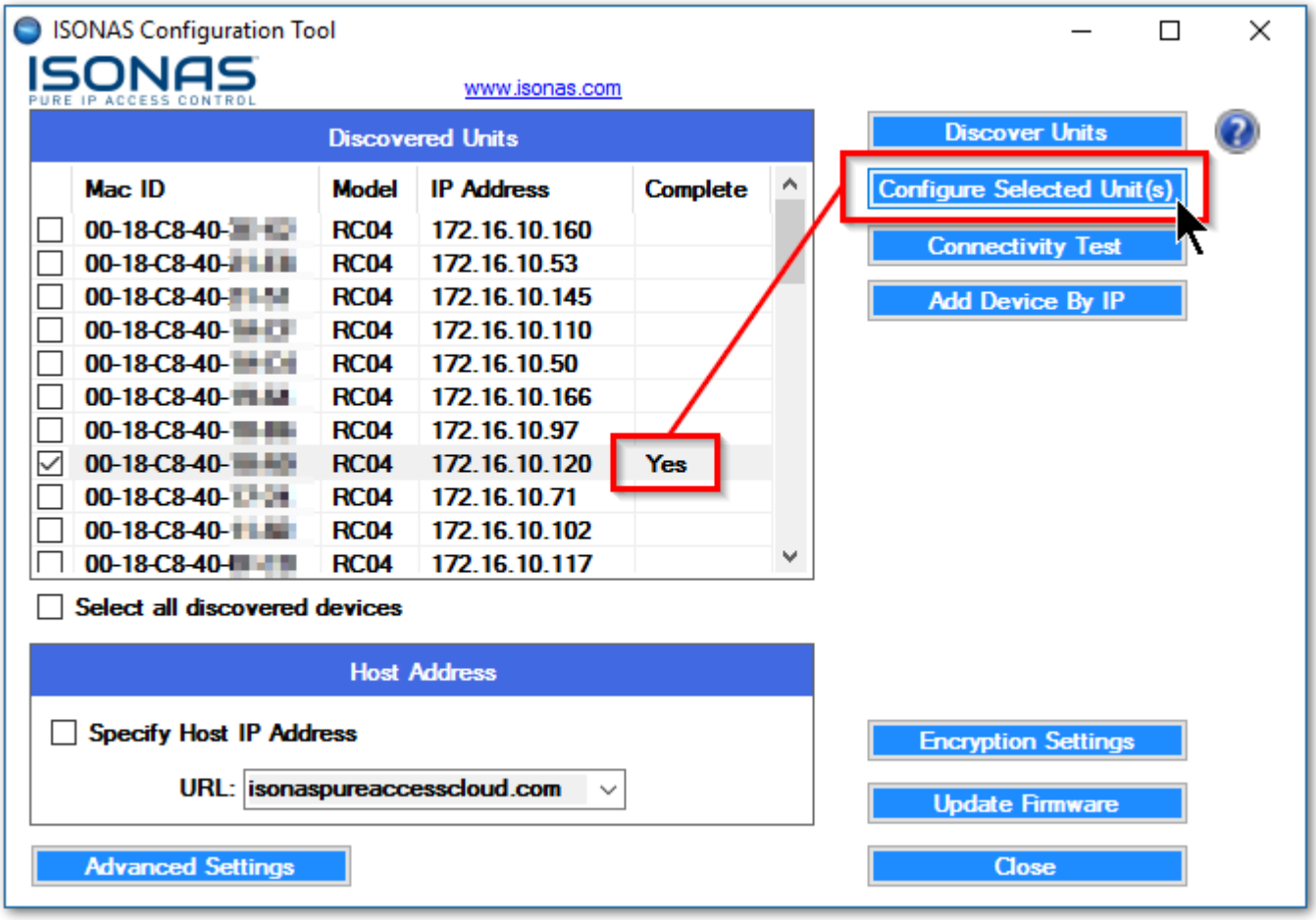


Figure 8 – Configure Selected Unit

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

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

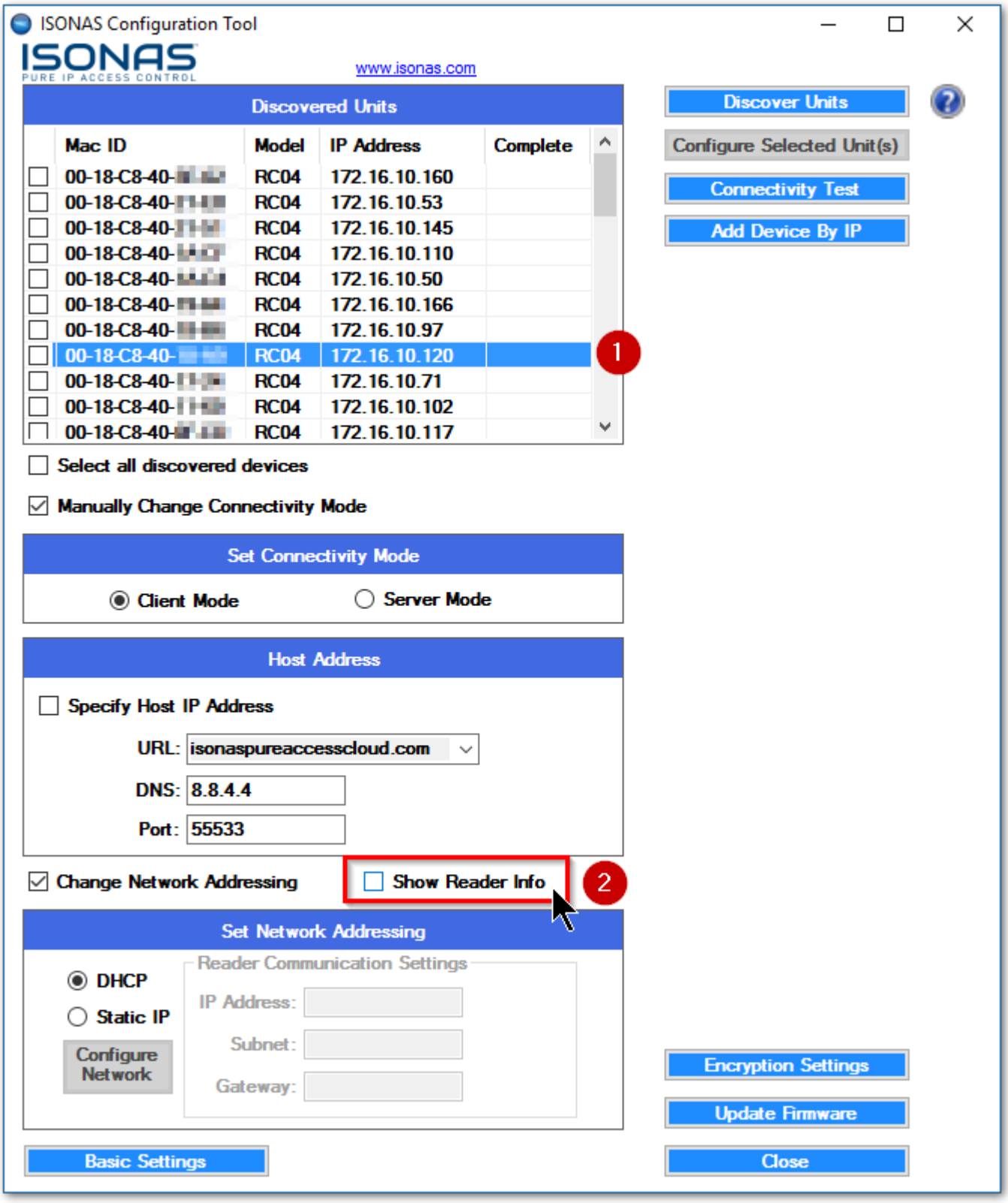
Last modified: 1 March 2023

Reviewing Network Config Settings

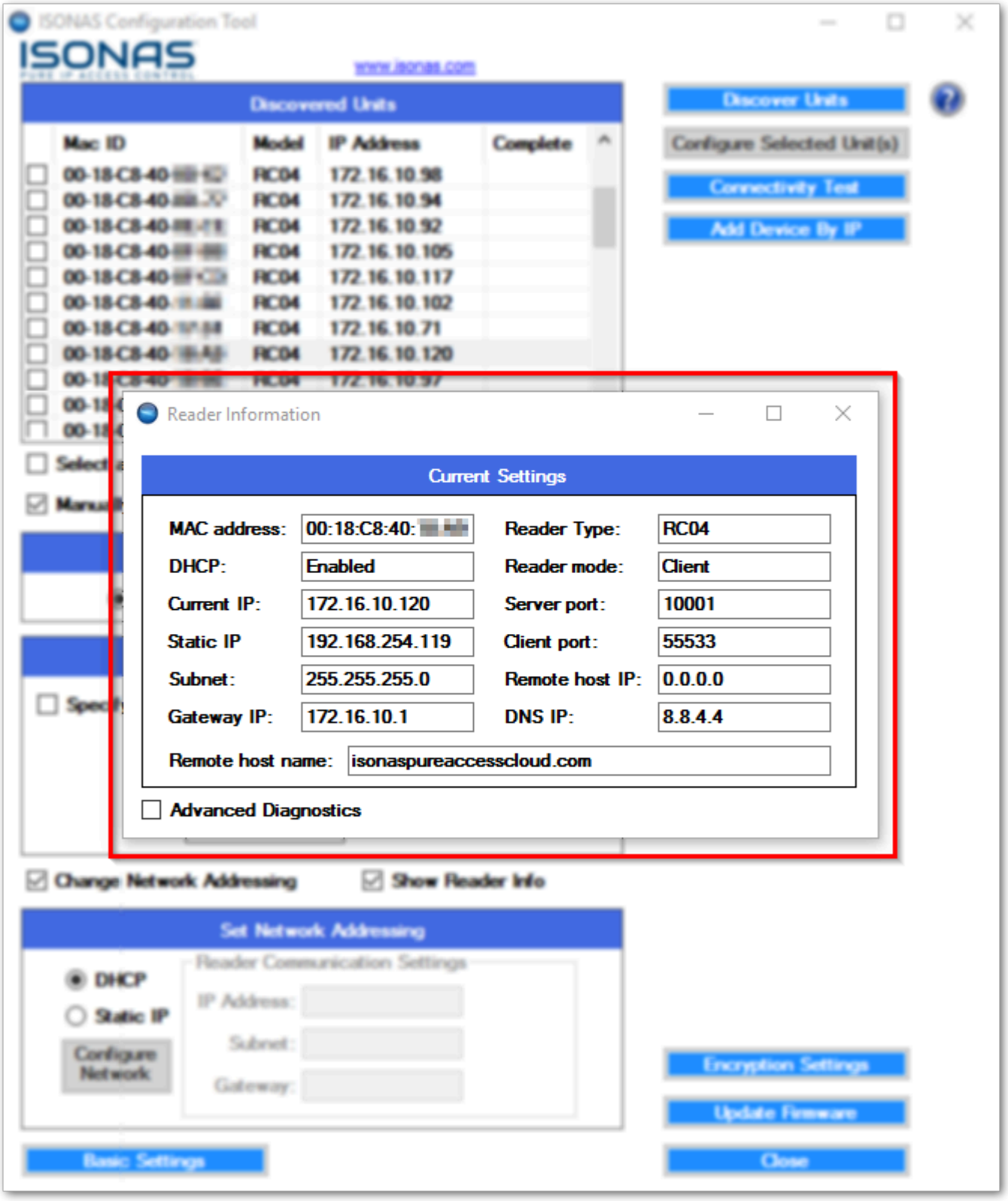
To see the current configuration of a device:

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

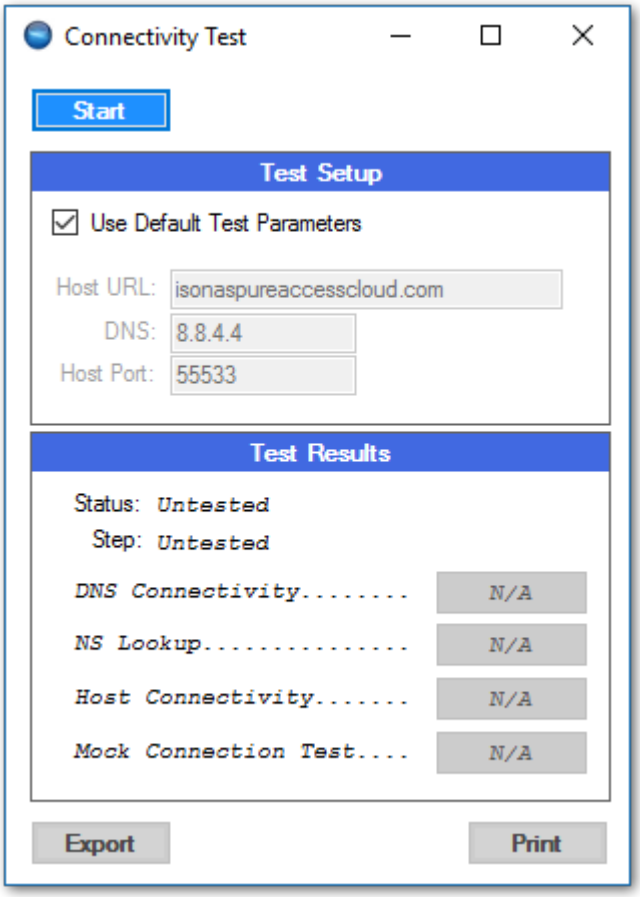
With the **Current Information** window open, you can simply highlight another device in the config tool to quickly display its settings. This is a handy way to compare the configuration settings of multiple units.

Last modified: 26 February 2021

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.

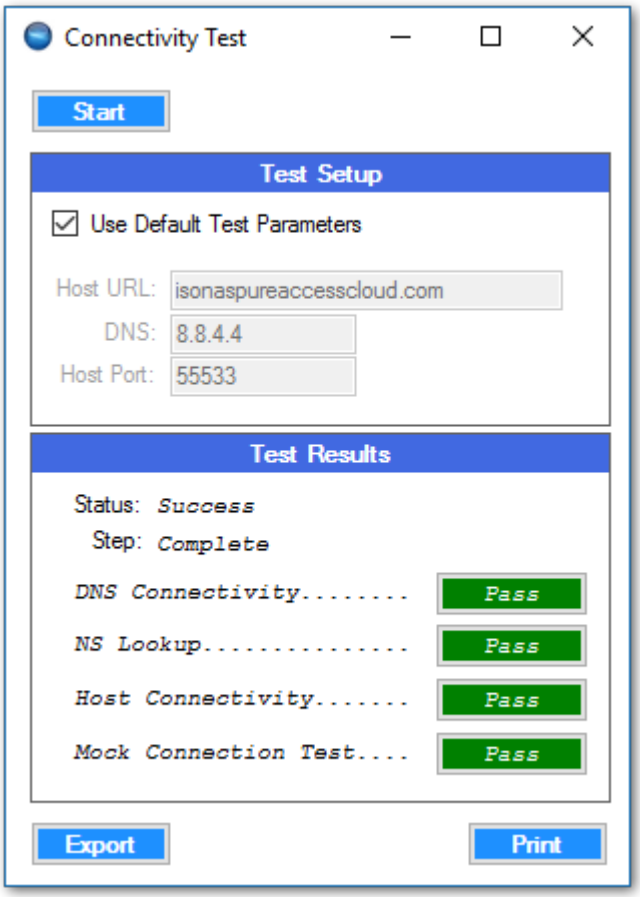
The Connectivity Test will determine if the network segment that the Configuration Tool is running on can make a connection to our server. This simulates a device connection by your PC and does not perform a connectivity test of devices discovered by the tool.



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.

Last modified: 10 April 2026

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.

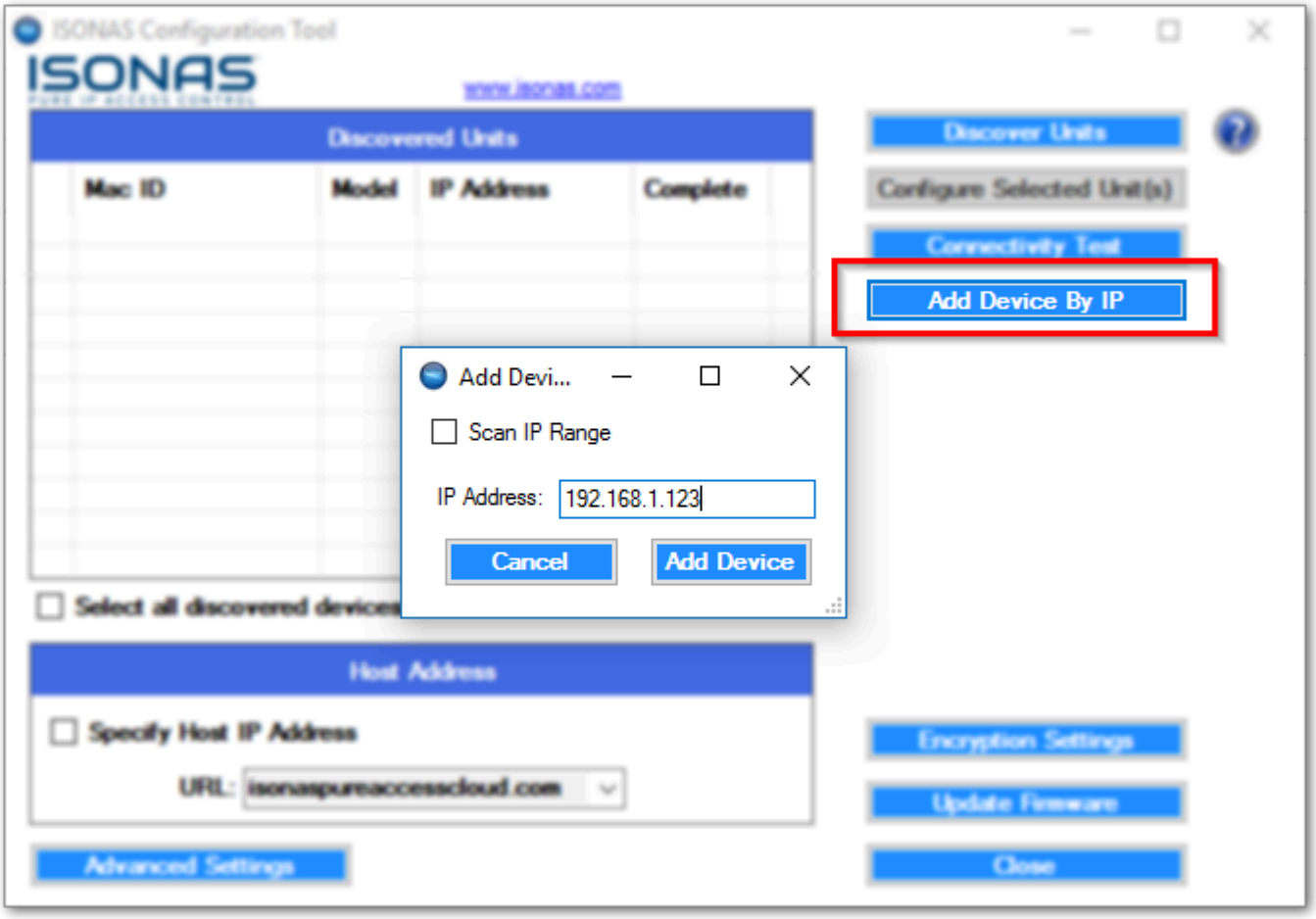
Fully booted RC-03

Fully booted IP Bridge

Last modified: 26 February 2021

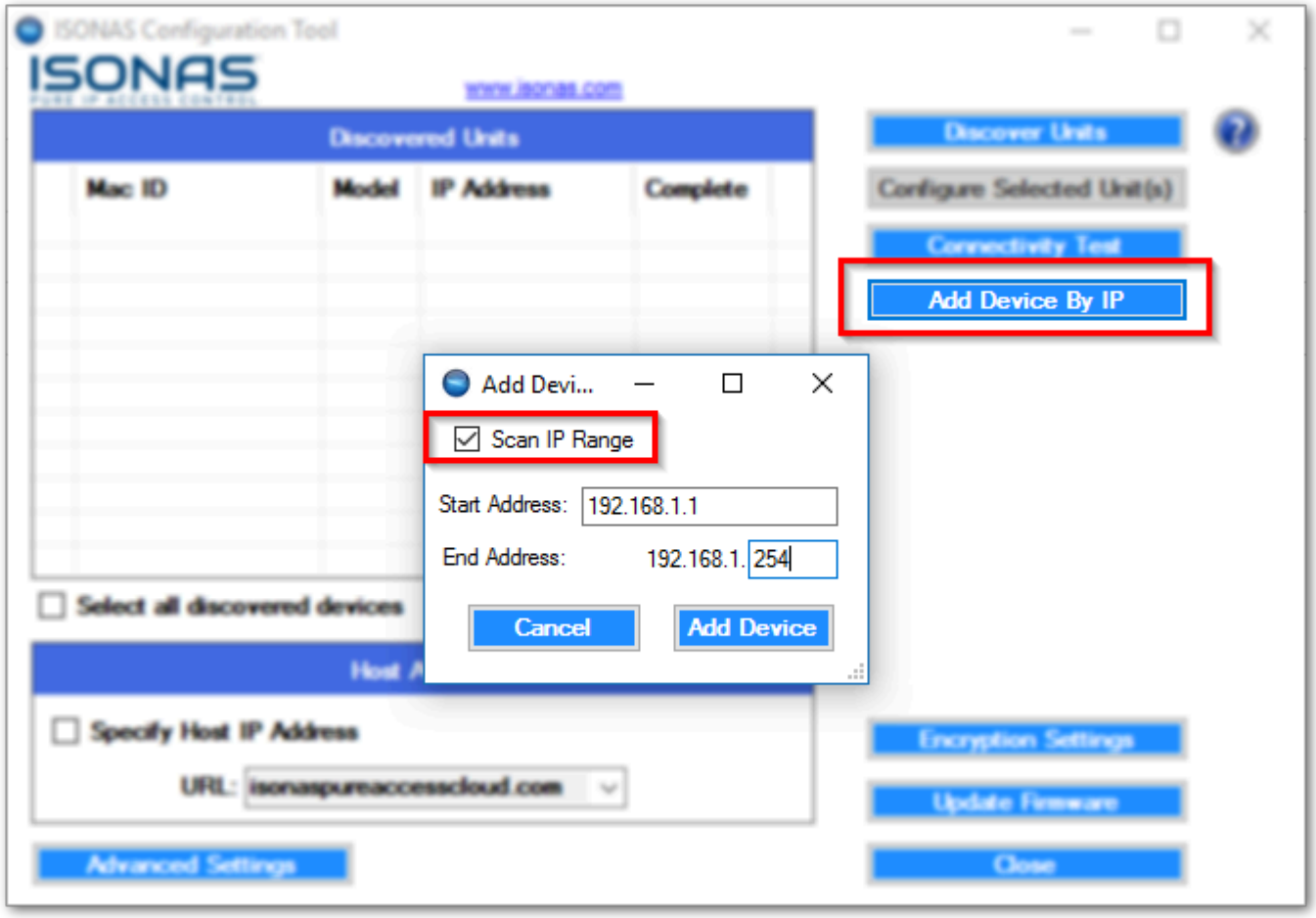
Find device by IP

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.

Last modified: 26 February 2021

Updating Firmware

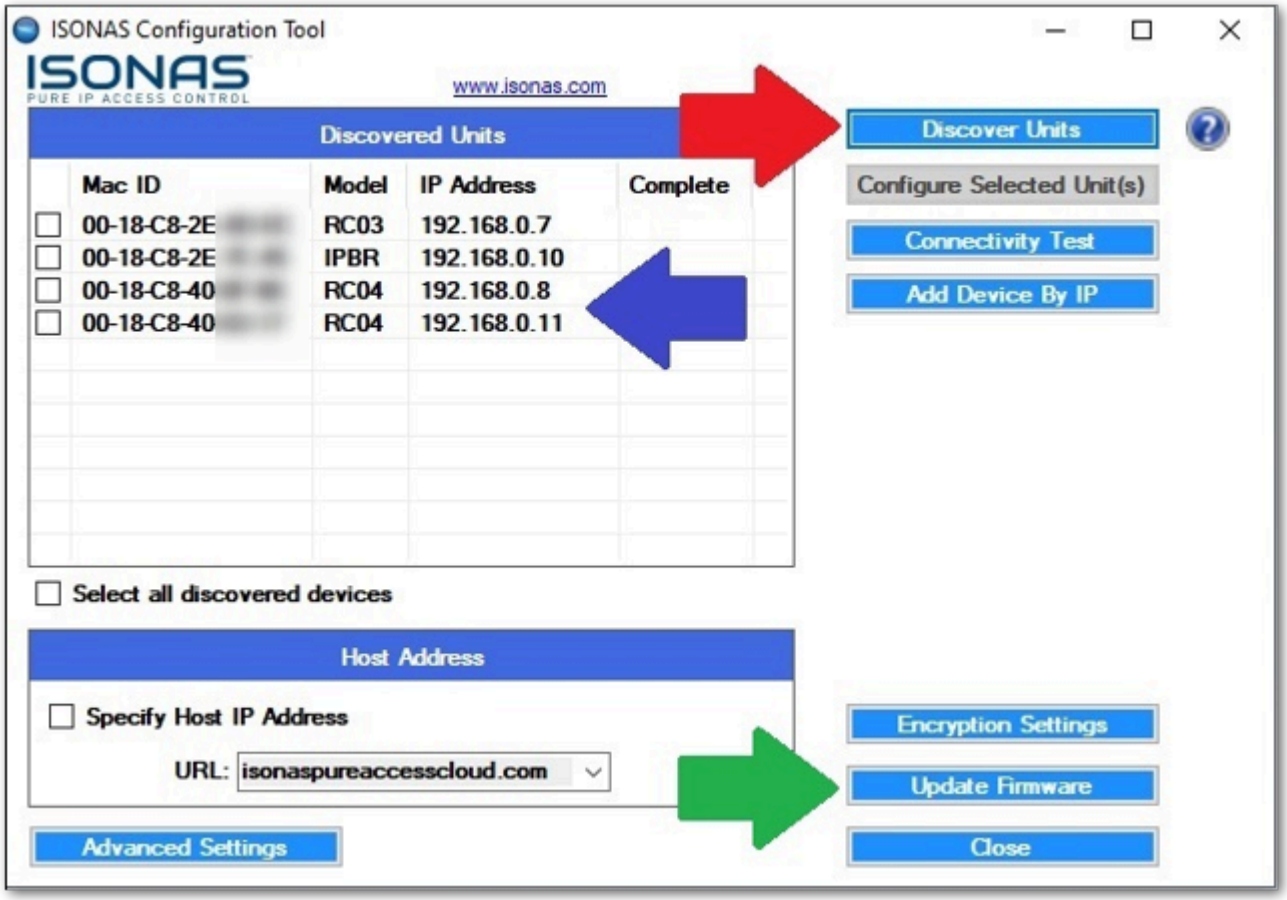
There are two necessary components for updating firmware on your ISONAS hardware:

1. The ISONAS hardware configuration tool
2. The latest firmware files for your device

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

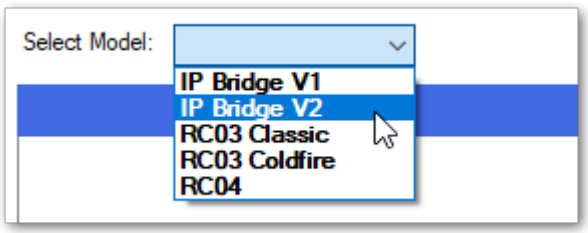
Instructions

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



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

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



   a. The device(s) should populate the "**Available Units**" field.

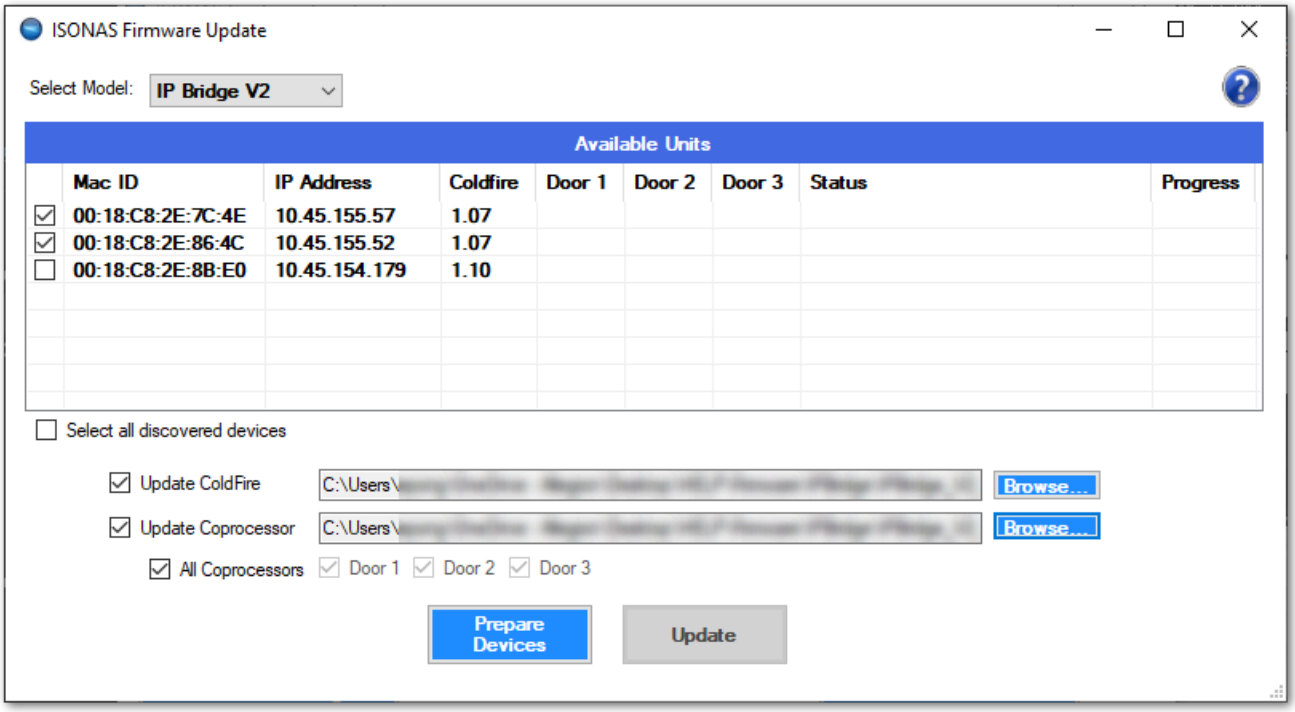
   b. Note that the ColdFire version displayed will confirm whether the Coprocessor needs to be

loaded.

i. With an IP-Bridge v2 on ColdFire version **1.07 or lower**, the Coprocessor will need to be updated to v1.03 (current as of ColdFire v1.19).

ii. With an IP-Bridge v2 on a ColdFire version **higher than 1.07**, the Coprocessor updates are not necessary.

5. Use the check-boxes to select the device(s) that need to be updated.
6. Click Browse... then navigate to the folder where the firmware files have been unzipped.
7. Select the firmware file (only the correct file type will appear) then click "**Open**".

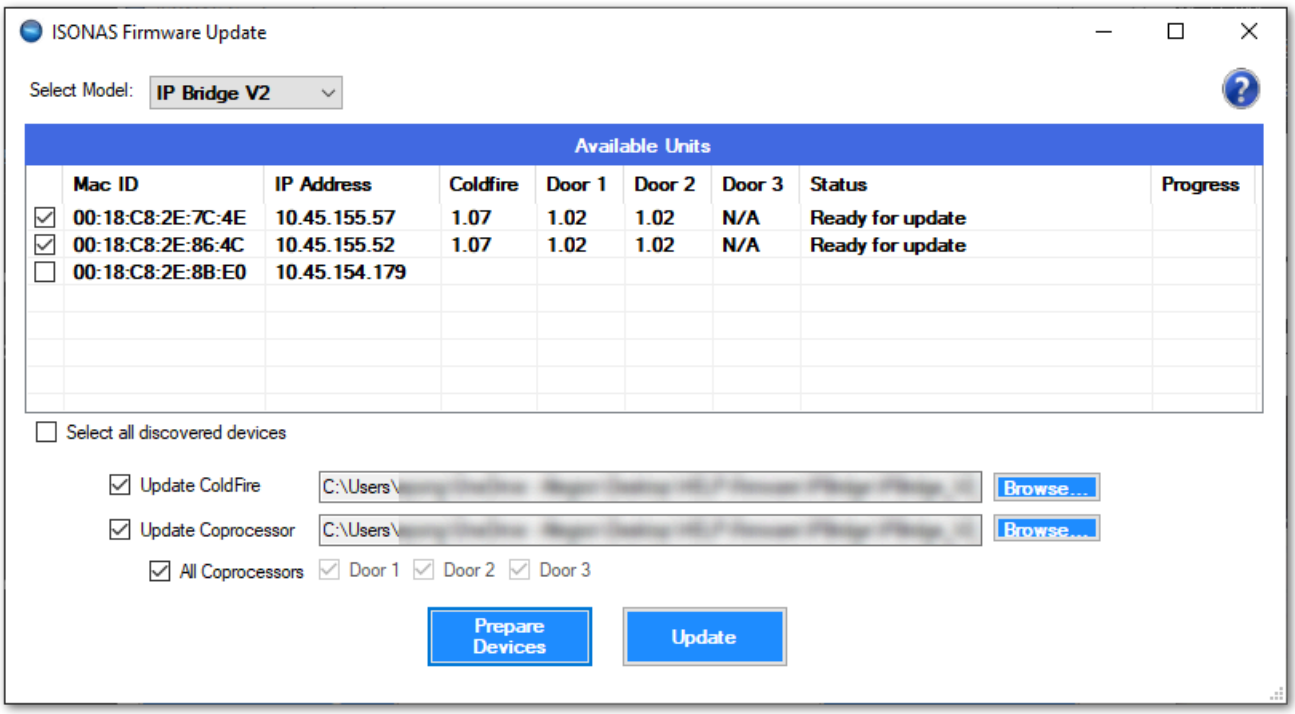


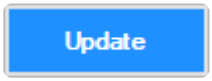
a. For RC-03's: Select **Update ColdFire** as well as **Update Coprocessor**. Both of these will need to be updated.

b. For RC-04's: Select **Update ColdFire**. See note below for more information.

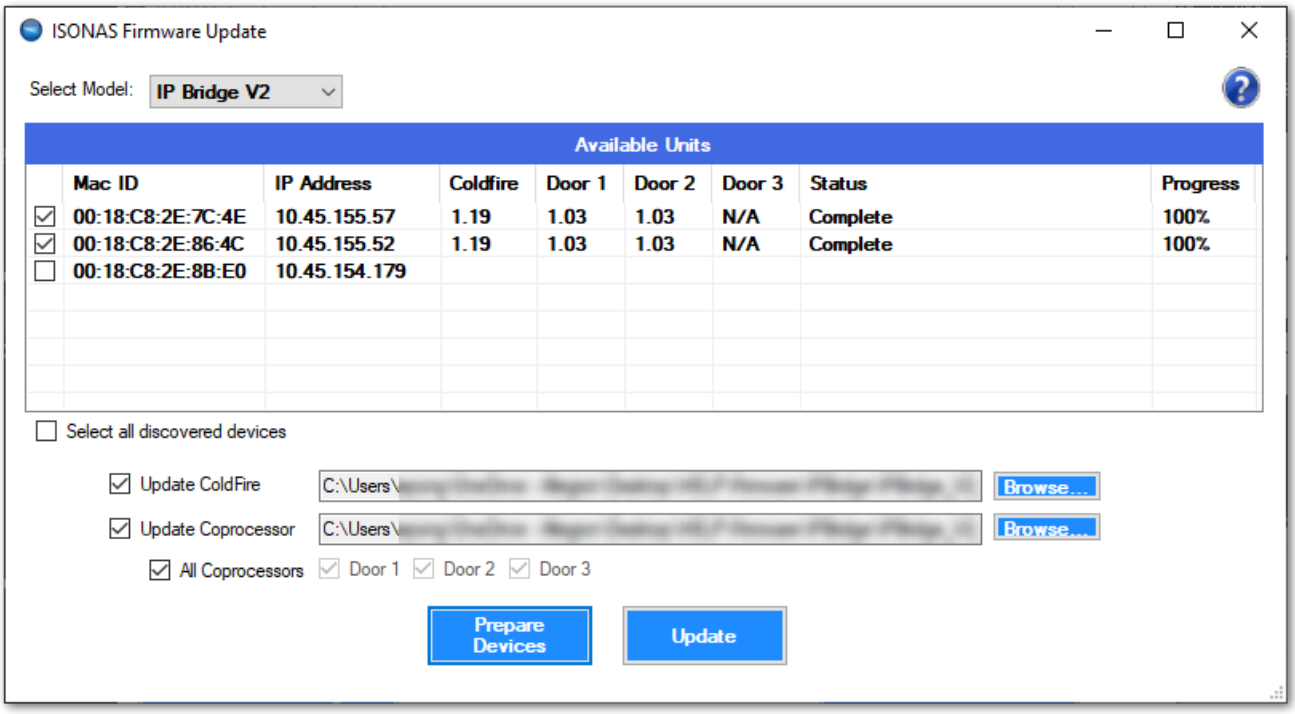
c. For IP-Bridges: **Only update the Coprocessor if it is out-of-date.** Please review this article as it contains important information regarding when to update the Coprocessor.

8. Once the firmware files have been selected, click 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 

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.



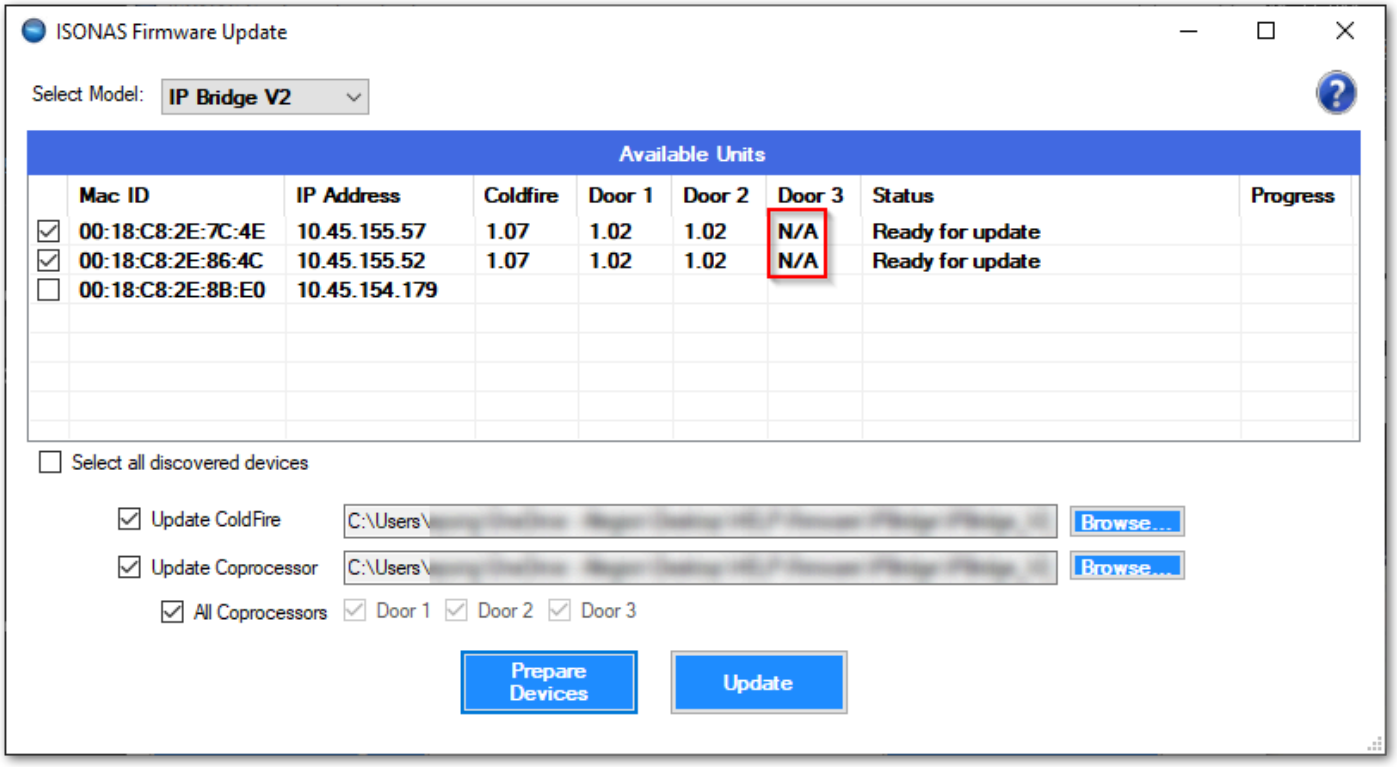
The RC-04's Coprocessor board and BLE (Bluetooth Low Energy) chip have not received updates in quite some time and are no longer included in this process.

Last modified: 27 June 2022

IP-Bridge Firmware Information

2-Door IP-Bridges

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



When to update the Coprocessor

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

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

Door displaying a question mark

If any ColdFire or Coprocessor errors on update, the device will display a "**?**". See troubleshooting steps

below for how to correct this.

Troubleshooting Firmware Update:

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

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

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

Last modified: 27 June 2022

Wiring and Hardware Installation

Please review these to find diagrams for basic configurations.

- ISONAS RC-04 Wiring Diagram Guide
- ISONAS IPBridge Wiring Diagram Guide

If you cannot find your particular setup using the above, please contact Isonas.Tech.Prod.Support@allegion.com.

Last modified: 10 February 2026

RC-04 Installation Guide

Here is an installation guide for the RC-04 in PDF format.

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

Last modified: 26 February 2021

IP-Bridge Installation Guide

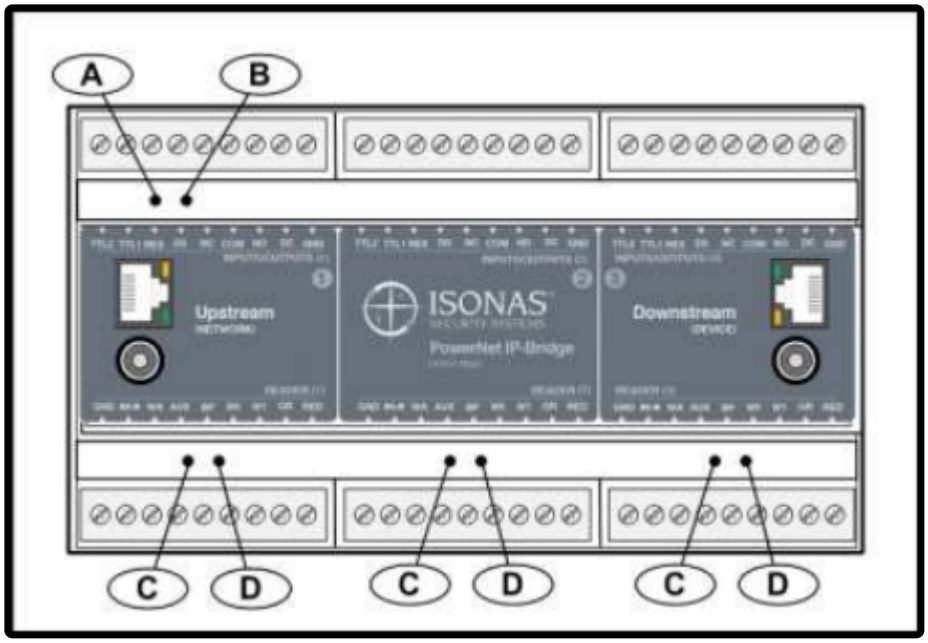
Here is an installation guide for the IP-Bridge in PDF format as well as the insert that comes in the box.

For information on how to add a bridge to Pure Access, please review the Managing Access Points section.

Last modified: 26 February 2021

IP-Bridge Status Light Indicators

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



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

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

IP-Bridge Status	LED "A" Color	LED "B" Color
IP-Bridge is not powered on	Off	Off
Power Turned On – Waiting in Boot Loader mode (~10 sec)	Red	Red
Performing All IP work, all mode, duration depends on settings	Amber	Red
IP Work completed (except long DNS lookups), ports/DNS	Red	Amber
Startup Complete – Errors reported	Green	Amber
Startup Complete – No issues reported	Green	Off
IP-Bridge is on and in a normal state	Green	Green
Dynamic IP lease expired on the network but the IP-Bridge did NOT release it's IP-Address. Note: Set the IP-Bridge to Static, and reserve an IP by MAC address in the router settings.	Green	Red
DNS look up did not find a host	Green	Red

Door Status	LED "C" Color	LED "D" Color
Normal Operation / Door is locked	Red	Off
Door is in the Lockdown state	Red	Red

Standard Credential Approval	Green	Off
Rex Admit	Green	Off
Unlock Command from the web app	Green	Green
Toggle Unlocked	Green	Green
Auto-unlock rule or event	Green	Green
Admit command from the web app (with latch interval)	Green	Green
Waiting in Startup or Performing Boot Load	Amber	Amber
Device is not responding – power cycle the device	Amber	Amber
Waiting to be activated or door process issue	Off	Amber
No Door (2-door Bridge)/Deactivated Door	Off	Off

Last modified: 16 March 2026

Guide for adding an IP Bridge

The attached document here is a step by step guide with screenshots to aid in adding an IP Bridge to your Pure Access system

Guide to commissioning an IP Bridge

Last modified: 22 October 2025

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.

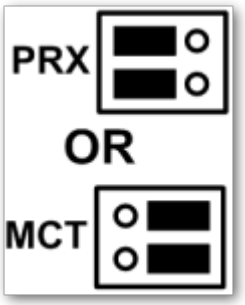
Last modified: 26 February 2021

RC-03 Jumper Configurations

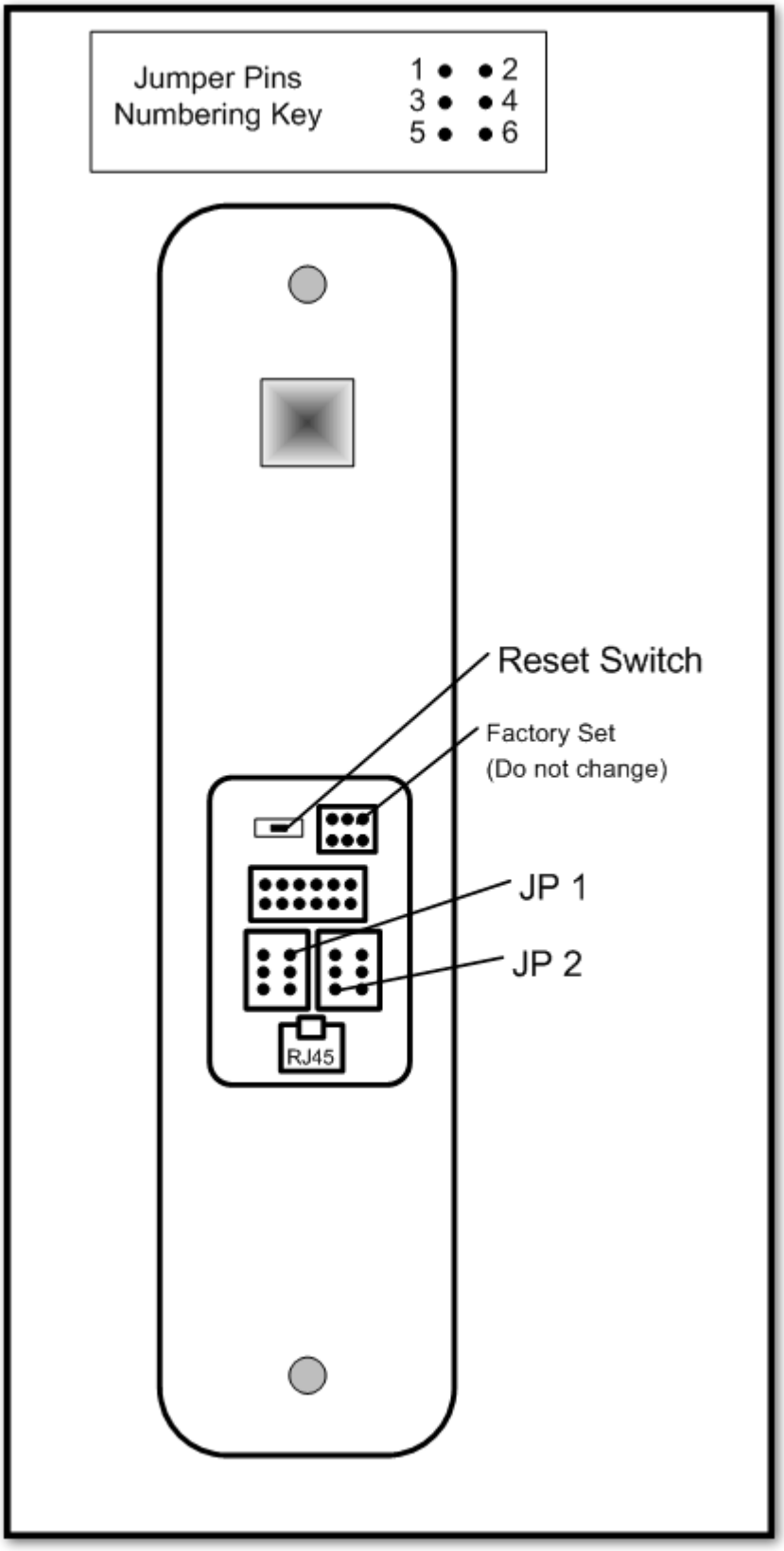
The RC-03 PowerNet reader-controller has a set of jumper pins that configure both its input power source and its lock control circuit. The device can be configured for power to be supplied to it through the 12 conductor pigtail (either 12VDC or 24VDC) or through the RJ45 connector (Power Over Ethernet).

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.

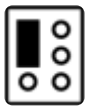
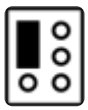
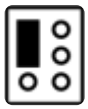
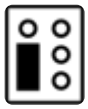


The below image shows the components on the back of the RC-03:



RC-03 Jumper Configurations:

Feature	JP 1 Jumpers	JP 2 Jumpers

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

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

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

Last modified: 26 February 2021

ASM Status Light Indicators

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

Power LED:

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

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

Communication Status LED:

Located on the side towards the lock wiring.

LED status meanings are described in the table below.

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

Last modified: 26 February 2021

Factory Resetting a Device

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

RC-03:

Small horizontal button above the RJ-45 input.

RC-04:

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

IP-Bridge:

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

Last modified: 26 February 2021

Wiegand Interface Module (WIM)

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

Function:

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

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

To enable this functionality:

1. Put the RC-03 in server mode.

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

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

Last modified: 26 February 2021

Getting Started in Pure Access

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

Last modified: 16 March 2021

Pure Access Cloud

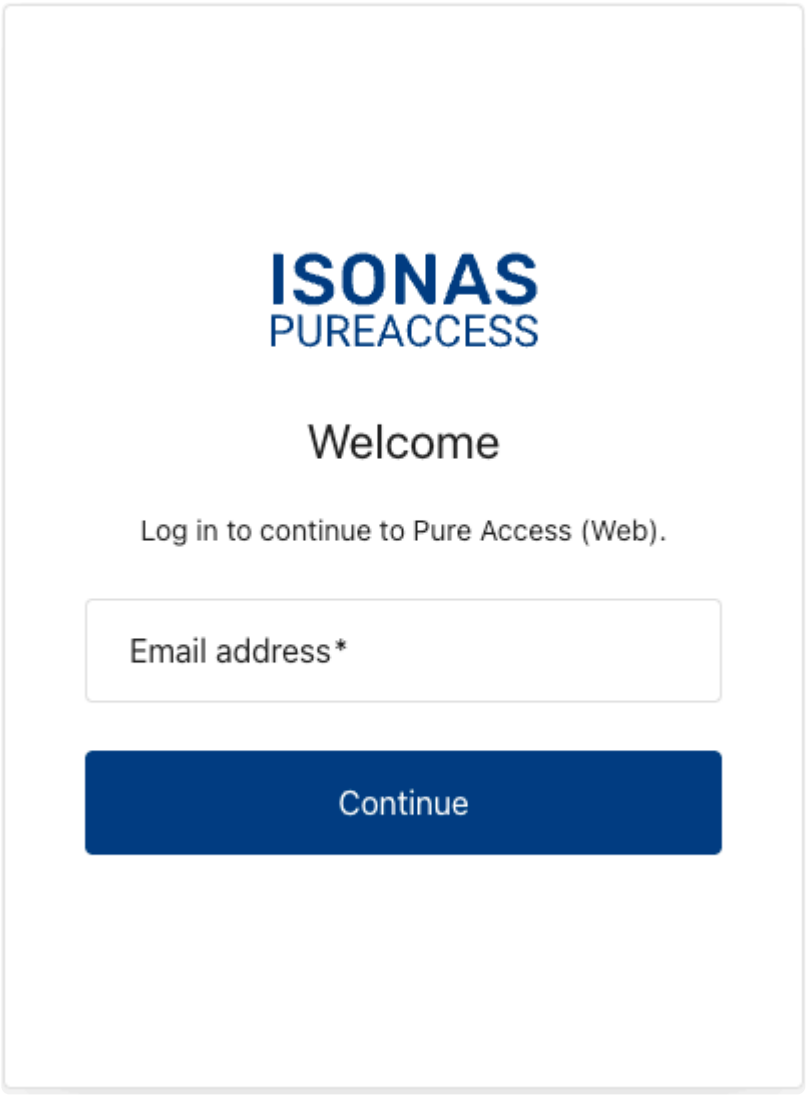
This section of the manual will cover these common topics:

- 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

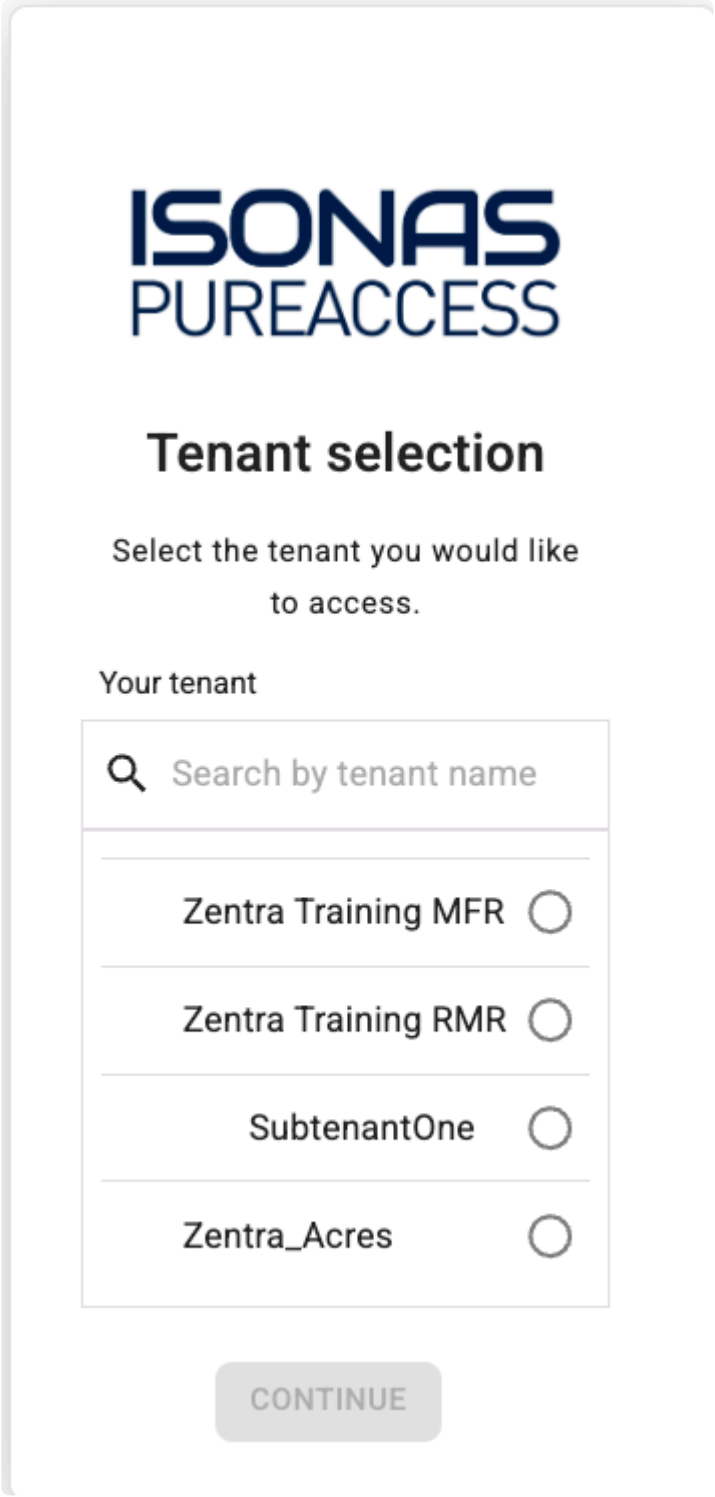
Last modified: 26 February 2021

Logging into a Pure Access Cloud tenant

From the login page located at **https://app.pureaccess.com/**, simply type in your username and password then click "**Log In**":



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



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

Forgot password? Locked out?

For security, we are not able to reset passwords upon request. You can reset your password by clicking on

the “**Forgot Password**” link from the login page. See next page for instructions.

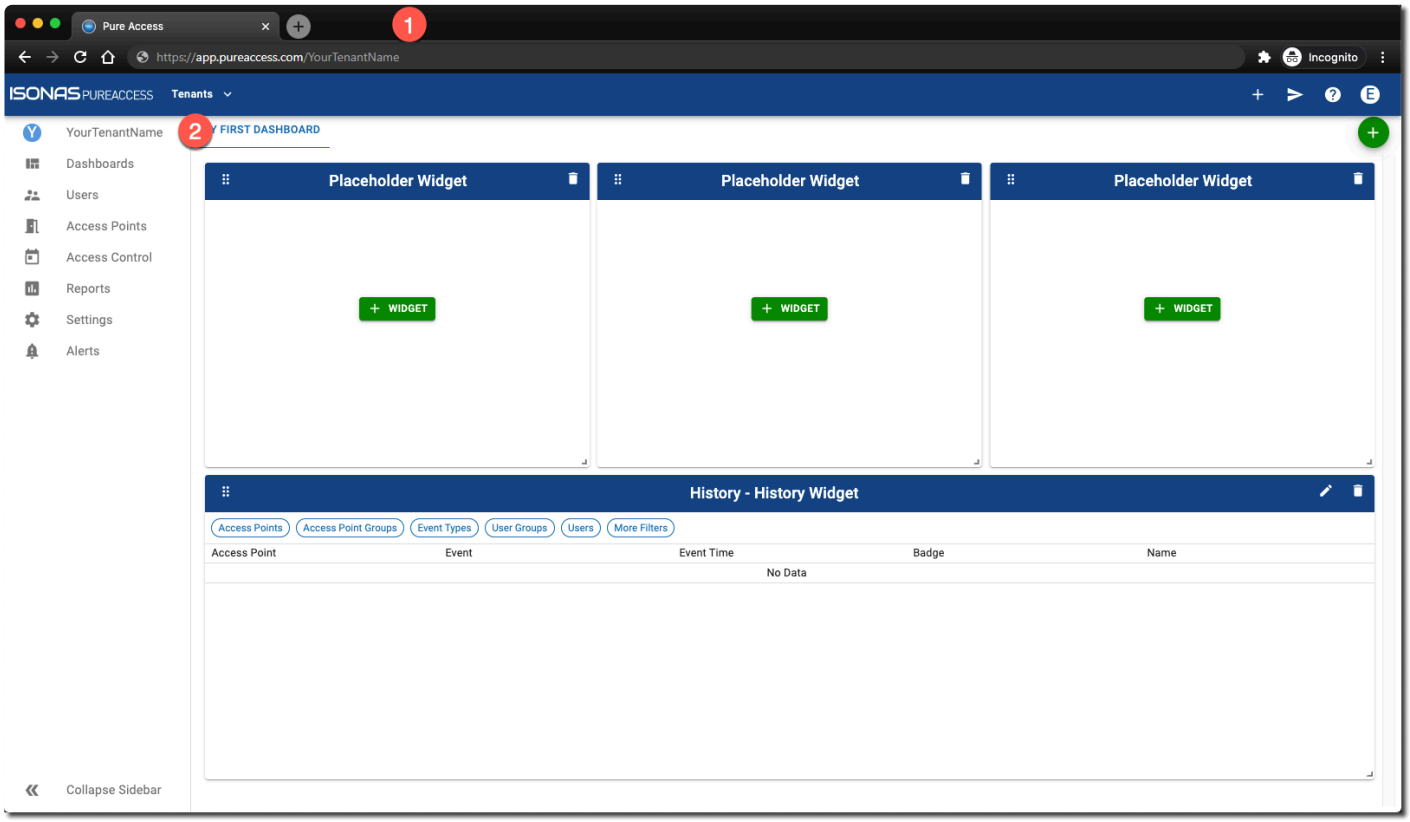
Last modified: 5 June 2026

Tenant Name

What’s my tenant name?

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

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

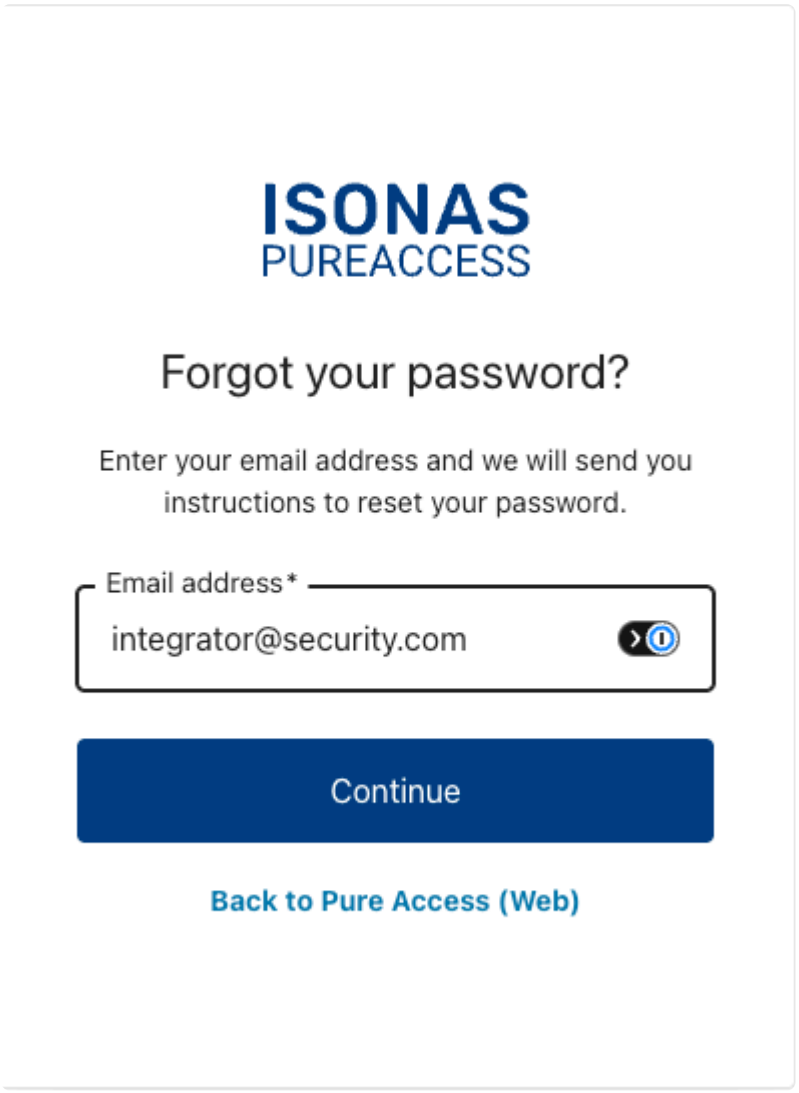


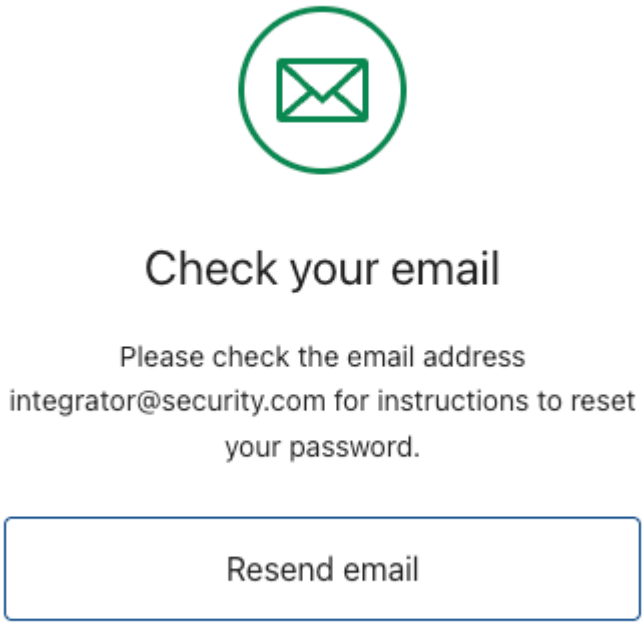
Last modified: 1 March 2023

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 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.


ISONAS
PUREACCESS
Forgot your password?
Enter your email address and we will send you instructions to reset your password.
Email address*
integrator@security.com
Continue
Back to Pure Access (Web)



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.

Last modified: 5 June 2026

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.

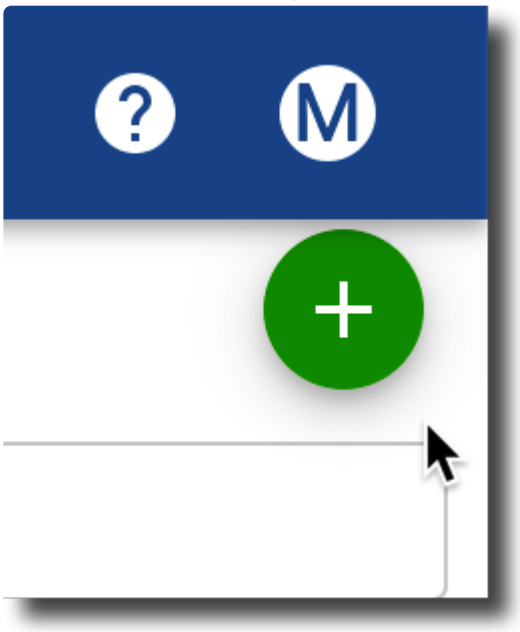
We advise against using a parent tenant for access control. Please create a new subtenant to be used for this purpose.

Last modified: 26 February 2021

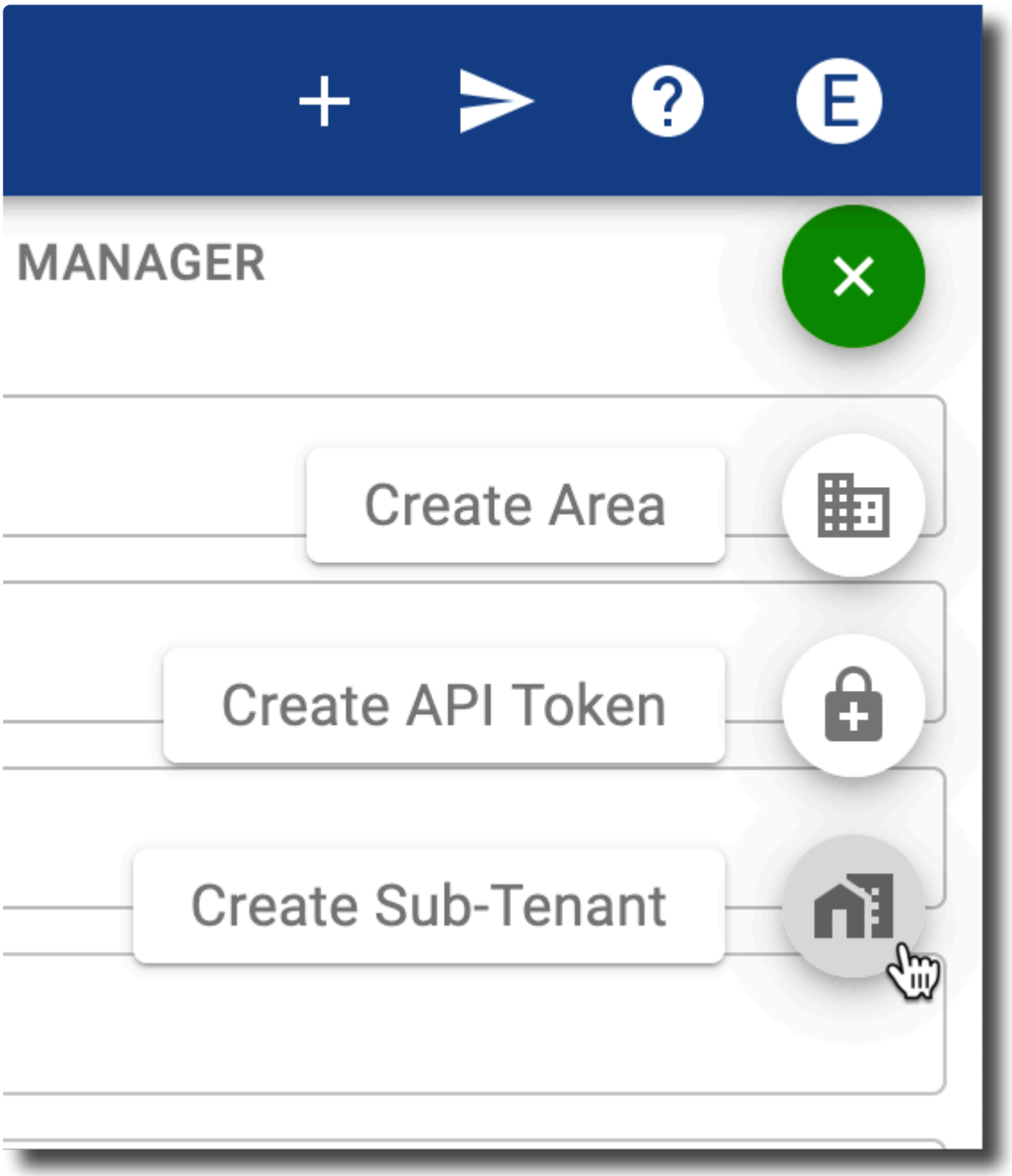
Creating Subtenants

1. Navigate to **Settings**.

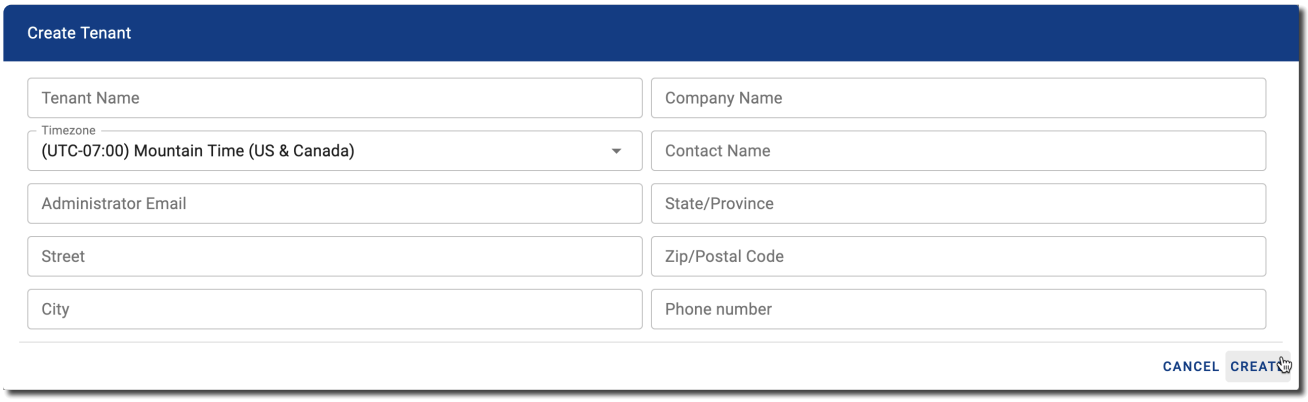
2. Hover over the plus sign to reveal the menu. You may need to scroll to the right to see this menu.



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



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



The 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.

Last modified: 26 February 2021

Pure Access Manager

> ! **Please note that Pure Access Manager is end-of-life and no longer supported as of December 2023.**

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.

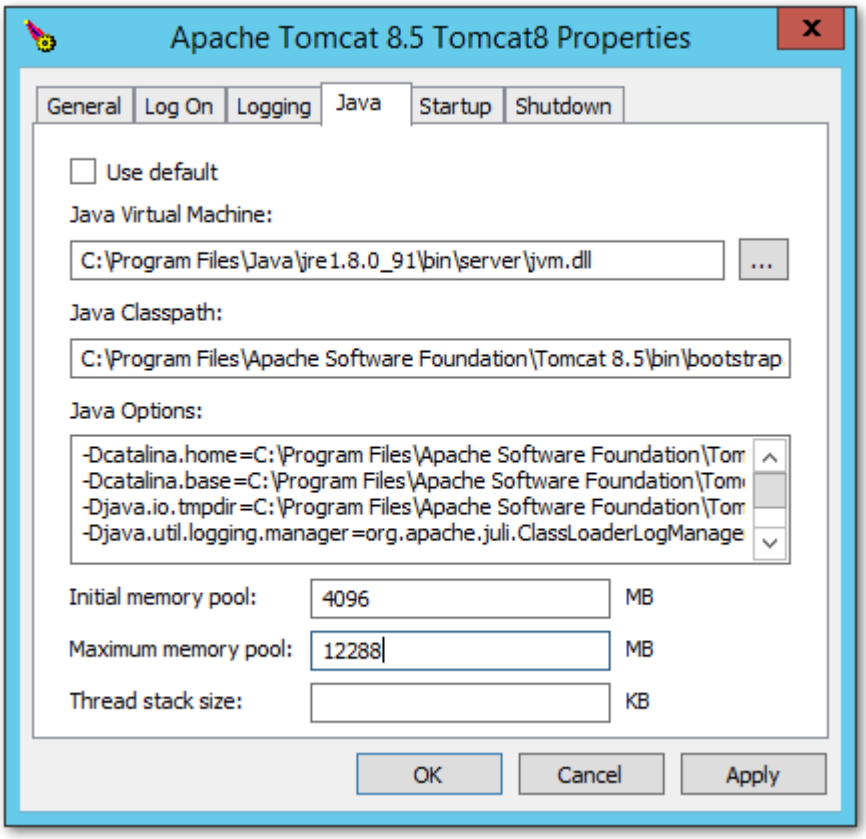
Last modified: 26 May 2026

Java Memory Allocation

> ! **Please note that Pure Access Manager is end-of-life and no longer supported as of December 2023.**

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



Last modified: 26 May 2026

SMTP Configuration (Pure Access Manager)

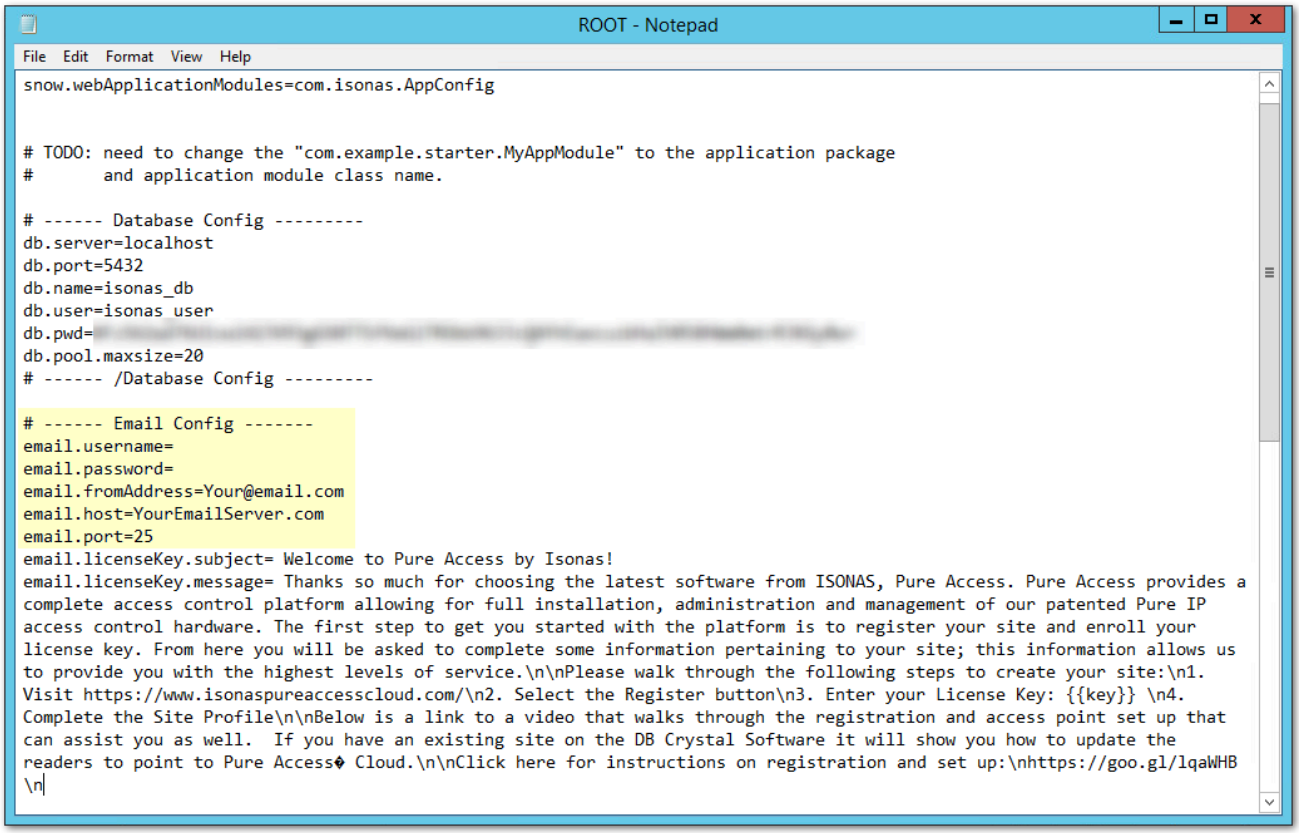
Please note that Pure Access Manager is end-of-life and no longer supported as of

December 2023.

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

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

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



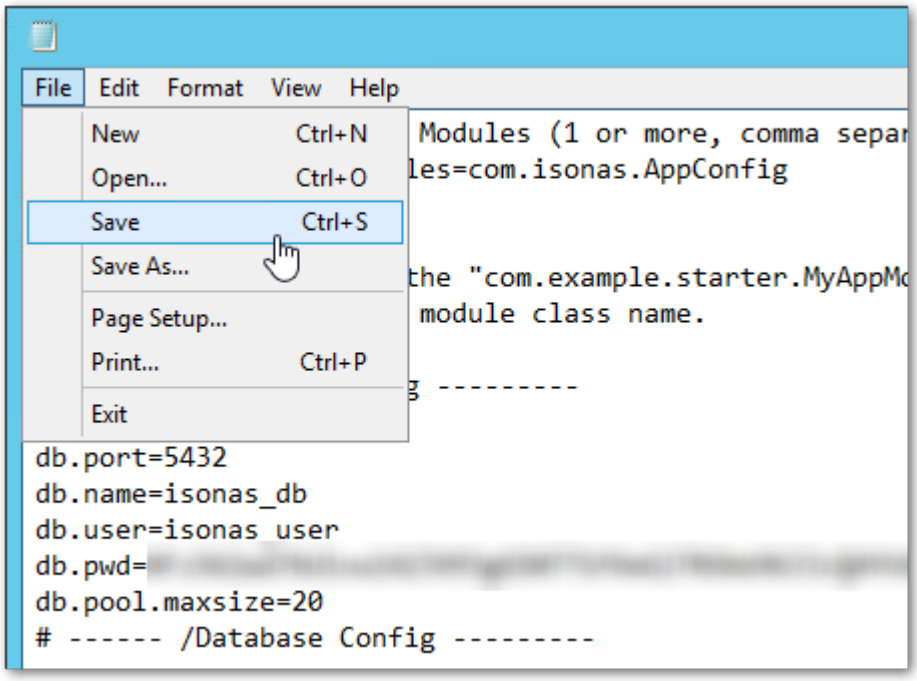
4. Additionally, you need to set the **email.file.base.path** value so that the hyperlinks within emails can direct users to the correct system. By default, this is set to *https://isonaspureaccesscloud.com*, but must be changed to the **PAM server's IP address or hostname**:

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

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

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

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



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

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

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

Example:

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

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

eula.path=/_docs/eula.html

server.urllist=http://localhost

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

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

Last modified: 26 May 2026

Configuring Pure Access Manager for SSL

> ! **Please note that Pure Access Manager is end-of-life and no longer supported as of December 2023.**

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.

Last modified: 26 May 2026

Backup and Restore Process (Pure Access Manager)

> **Please note that Pure Access Manager is end-of-life and no longer supported as of December 2023.**

Ensure that both Pure Access Manager instances are on the latest version before proceeding.

Back up 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.

Last modified: 26 May 2026

Migrating from One Tenant to Another

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

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

1. Moving users from one tenant to another

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

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

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

3. Moving access points

1. Before proceeding, please be aware that once an access point is deleted from a tenant you will **no longer be able to view reports** for that device.
    a. If you need to view historical events for auditing purposes, you will want to generate and download the reports now.
2. Deactivate and then delete an access point from the old tenant.
3. Add this access point to the new tenant.
    a. It is best practice to migrate access points one at a time.

   b. Once added to the new tenant, update access points and then verify that a credential is operational before proceeding.

4. Repeat steps 2 and 3 until all of the access points have been moved over.

Last modified: 17 March 2022

PAM to PAC Migration Guide

The attached document can be used as step by step guide to migrating your Pure Access Manager system to the Pure Access Cloud solution.

Pure Access Manager to Cloud Migration Path

Last modified: 22 October 2025

Integrations

1. Active Directory
2. Pure Access API
3. Entrust Datacard TruCredential

Last modified: 26 February 2021

PANRServ

PANRServ Installation and Setup

Last modified: 17 May 2022

Entrust Datacard TruCredential

Please review the following links for more information on the Entrust Datacard TruCredential

1. ISONAS + Entrust Datacard Brochure
2. ISONAS + Entrust Datacard Webinar Presentation
3. Entrust Datacard Trucredential Software Specifications
4. How to Integrate ISONAS Pure Access and Entrust Datacard TruCredential

Last modified: 20 February 2026

Milestone XProtect

> ! The Milestone integration is outdated and no longer functional. At this time, we are unable provide an estimated timeline for restoration.

Please review the following links for more information on the Milestone XProtect integration.

1. ISONAS Pure Access + Milestone XProtect installation instructions
2. Installation files:
    a. Pure Access Cloud
    b. Pure Access Manager

Last modified: 3 February 2026

Online Interface

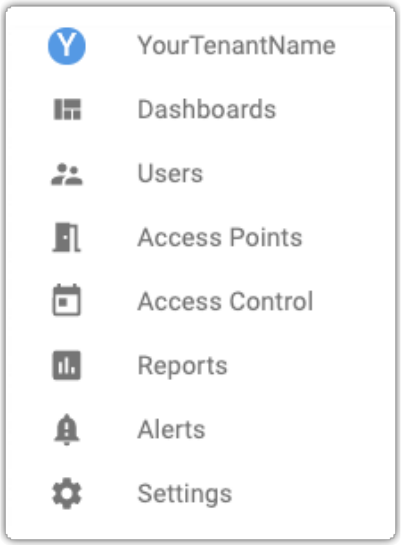
Navigation

Side Menu

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

Collapsed

Expanded

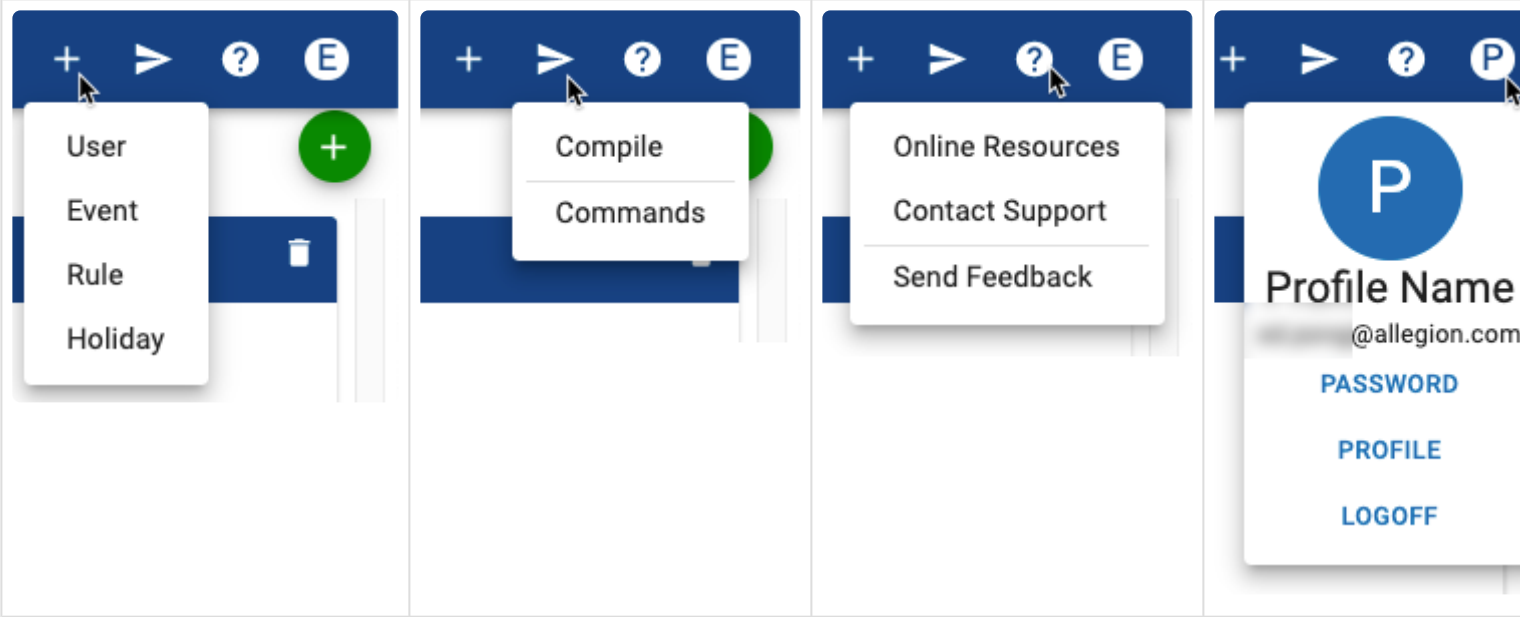


Context Menu

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

Quick Links

Quick Add	Commands	Help	Profile



Last modified: 1 March 2021

App Bar

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

App Bar on a Web Browser

App Bar on a Mobile Device

Default view:

Select  *to view actions:*

The actions that can be performed are:

Last modified: 16 April 2021

Tenant Select

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

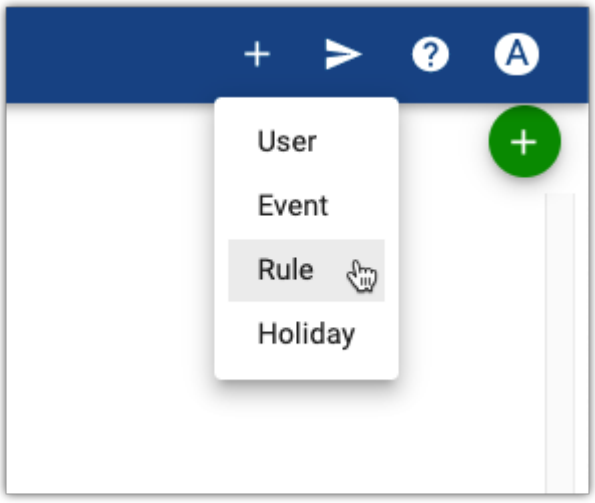
Simply click or tap 

then make a selection from the list to be redirected to that tenant.

Last modified: 16 April 2021

Quick Add

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



Last modified: 16 April 2021

Send Commands

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

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

Sending a Compile

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

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

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

Sending a compile requires that the web access user has one (or more) of the following permissions:

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

Sending Additional Commands

1. Click  from the App Bar

2. Select **Commands**
3. Select the access point(s) you would like to send a command to, then choose the action:
    - **Admit**: unlocks the access point or access point group for the latch interval set per device
    - **Lock Down**: locks down the access point or access point group. While in Lock Down mode, access is denied to all users except those whose credentials include the Pass-Through special property.
    - **Schedule**: places access point into a normal state (following the configured weekly rules)
    - **Unlocked**: unlocks the access point or access point group
    - **Lock**: overrides an Auto Unlock Weekly Rule or Event, returning the access point or access point group to a locked state (Schlage devices only)
    - **Clear Tamper**: clears a tamper alarm on an access point (Schlage devices only)

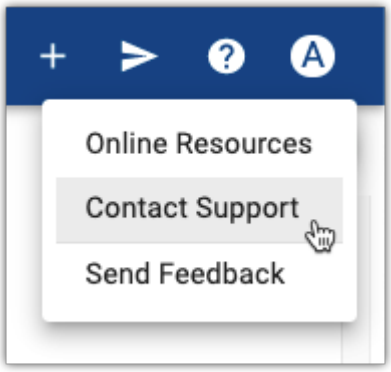
Sending command via the App Bar requires that the web access user has one (or more) of the following permissions:

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

Last modified: 27 March 2026

Help Button

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

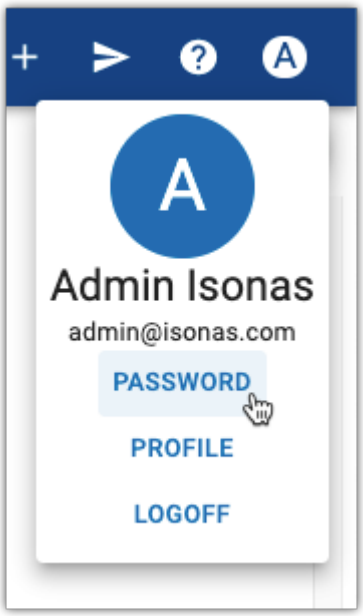


Last modified: 16 April 2021

User Profile

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

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



Last modified: 16 April 2021

Dashboards

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

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

Last modified: 26 February 2021

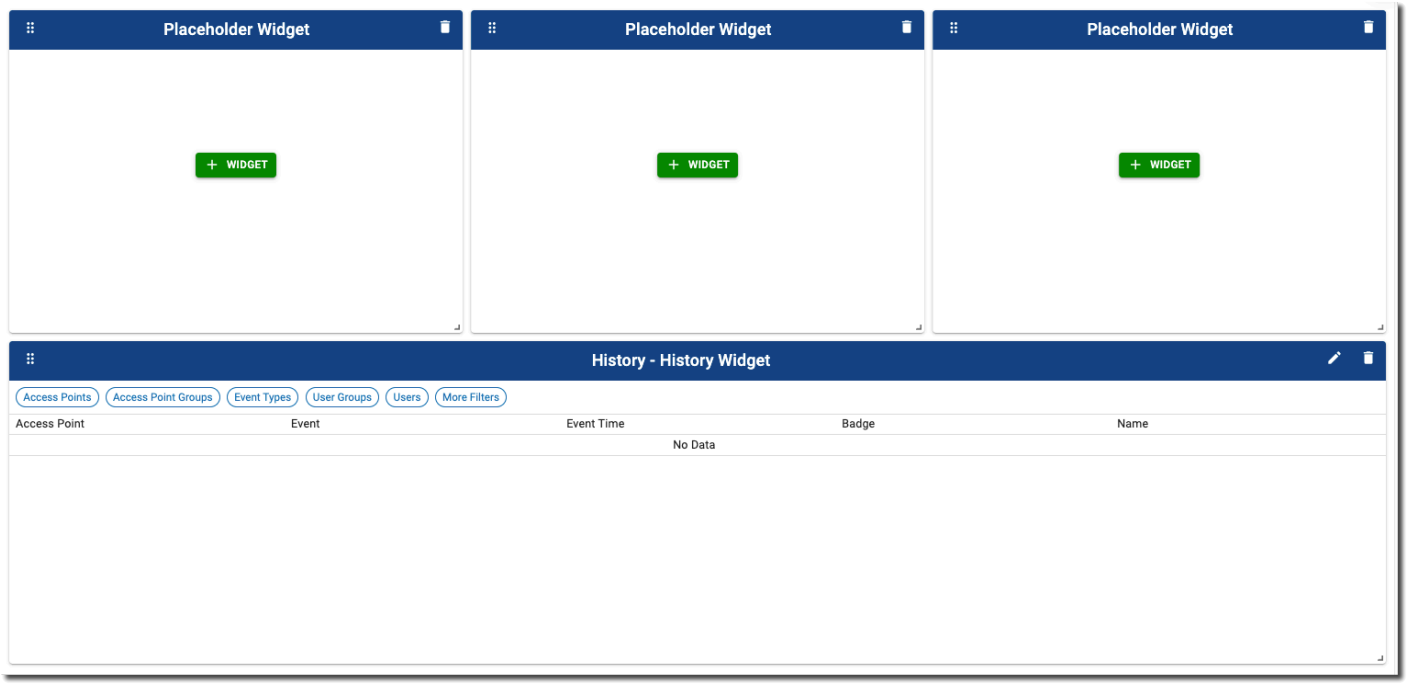
Create Dashboard

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

Last modified: 26 February 2021

Widgets

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



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

- **Single Access Points** allow you to track and monitor real time activity, status as well as take actions on a single door.

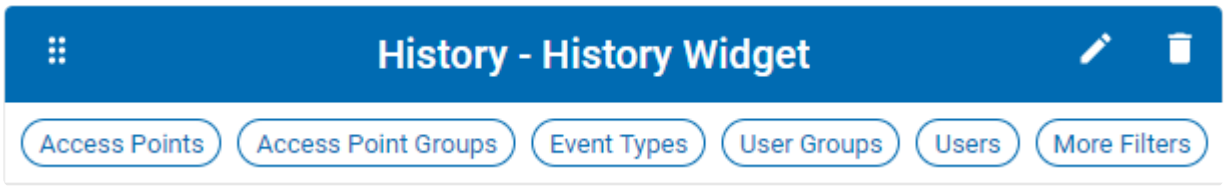
- **Multiple Access Points** allows you to track and monitor real time status and take actions on multiple doors (up to 12).
- **History** provides the ability to see real-time monitoring of access points but provides further abilities to filter to specific people, events or actions.
- **Access Point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

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

Last modified: 19 May 2023

History Widget

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



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

Adding an additional history widget:

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

See Standard History Events for icon and message definitions.

Last modified: 26 February 2021

Standard History Events

Icon	Event	Description	NDE Series	LE Series	Schlage RC	RC-04	IP Bridge
	Critical Battery	Battery critically low. Replace batteries immediately.	X	X			
	Low Battery	Battery low. Replace batteries soon.	X	X			
	Battery Level	System received a battery level update from device.	X	X			
	Compile Failed	Failed to update access point with updated access information.					
	2FA: Approve (1/2)	First credential (card or mobile) accepted in two-factor authentication	X	X	X	X	X
	2FA: Approve (2/2)	Second credential accepted, two-factor authentication successful	X	X	X	X	X
	2FA: Approve (Card/PIN)	Card and PIN combination accepted for access	X	X	X	X	X
	Commissioning Started	Started setting up a new access point	X	X	X	X	X
	Compile Complete	Access point successfully updated with updated access information.	X	X	X	X	X
	Credential Add Complete	New credential was successfully added to the system	X	X	X	X	X
	Credential Update Complete	User credential was successfully updated in the system	X	X	X	X	X

	Device audits reported: BLE	Wireless lock sent its activity logs via Bluetooth	X	X			
	Device settings reported: BLE	Wireless lock reported its configuration via Bluetooth	X	X			
	DeviceAlertsReportedWIFI	The wireless access point alert information via WiFi	X	X			
	DeviceAuditsReportedWIFI	The wireless access point has successfully sent all audit data during a Wi-Fi check in.	X	X			
	DeviceSettingsReportedWIFI	The wireless access point reported its configuration via a Wi-Fi check in.	X	X			
	HMAC ON	Enhanced security protocol was enabled on the access point	X	X	X	X	X
	Sync completed: BLE	Successfully completed Bluetooth sync with wireless lock	X	X			
	HMAC Off	Enhanced security protocol was disabled on the access point	X	X	X	X	X
	Tamper Alert Cleared	Previous tamper alert has been resolved			X		
	Compile Queued	An update was sent to an access point, but it was not online to receive it. Will be delivered when it comes back online	X	X	X		
	Device Settings Mismatch	Door controller settings don't match the expected configuration			X		
	Credential Delete Complete	Credential was successfully removed from the system	X	X	X	X	X
	Commissioning Error – A general error occurred	General error occurred during new access point setup	X	X	X	X	X

	Commissioning Error – Bad payload	Error during new access point setup – invalid data	X	X	X	X	X
	Commissioning Error – Bad request sent to Engage	Error during new access point setup – invalid request	X	X	X	X	X
	Commissioning Error – Engage Service Unavailable	Error during new access point setup – service unavailable	X	X	X	X	X
	Reporting sync status failed: BLE	Failed to report Bluetooth synchronization status	X	X			
	Sync failed: BLE	Bluetooth synchronization with wireless lock failed	X	X			
	Sync start failed: BLE	Failed to start Bluetooth sync with wireless lock	X	X			
	Device Limit Exceeded	Device was not added to the system because the license is at it’s device limit.	X	X	X	X	X
	2FA: Decline – Process Error (1/2)	System error occurred during two-factor authentication	X	X	X	X	X
	2FA: Decline – Process Error (2/2)	System error occurred processing second credential	X	X	X	X	X
	2FA: Decline – Process Error (Card/PIN)	System error occurred during Card+PIN authentication	X	X	X	X	X
	Scheduled Event	A scheduled event occurred at the access point	X	X	X	X	X
	Admit	A person was granted a single entry through the door			X		
	State Override: Admit	Administrator manually granted one-time access			X		
	2FA: Decline – Timeout ½	Two-factor authentication timed out waiting for second credential	X	X	X	X	X
	2FA: Decline – Timeout (2/2)	Two-factor authentication timed out during second	X	X	X	X	X

		credential					
	2FA: Decline – Timeout (Card/PIN)	Timed out waiting for PIN after card presented	X	X	X	X	X
	End All Scheduled And Override Modes	All scheduled events were canceled and door returned to normal	X	X			
	Locked	Door was locked, requiring valid credentials for access			X		
	Scheduled Auto Unlock End	Scheduled unlock period has ended, door returned to locked	X	X	X		
	Scheduled Badge Unlock End	Scheduled badge-unlock period has ended	X	X	X		
	Scheduled Badge Unlock Start	Door entered badge-unlock mode according to schedule	X	X	X		
	Scheduled Lock End	Scheduled lock period has ended	X	X	X		
	Scheduled Lock Start	Door automatically locked according to the schedule	X	X	X		
	Scheduled Lockdown End	Scheduled lockdown period has ended	X	X	X		
	Auto Unlock End	Automatic unlock period ended, door returned to locked	X	X			
	Lockdown To Locked	Door changed from lockdown mode to normal locked mode			X		
	Secured	Door returned to normal secured state requiring credentials			X		
	State Override: Locked	Administrator manually locked the door, overriding schedule			X		
	2FA: Decline – Lockdown (2/2)	Second factor rejected because access point is in lockdown mode	X	X	X	X	X

	Lockdown	Door was put in emergency lockdown mode, preventing all access			X		
	Locked To Lockdown	Door changed from locked mode to emergency lockdown			X		
	Scheduled Lockdown Start	Door entered scheduled lockdown mode according to schedule	X	X			
	State Override: Lockdown	Door was manually placed in lockdown mode by administrator			X		
	Unlock To Lockdown	Door changed from unlocked mode to emergency lockdown			X		
	2FA: Decline – No Credential (2/2)	Second credential not found in system during two-factor authentication	X	X	X	X	X
	2FA: Decline – No Schedule (2/2)	Second credential used outside authorized schedule	X	X	X	X	X
	Scheduled Auto Unlock Start	Door automatically unlocked according to schedule	X	X			
	Unlocked	Door was unlocked, allowing free access without credentials			X		
	Auto Unlock Start	Door entered automatic unlock mode	X	X			
	Auto Unlock Start – First Person In	First authorized user arrived and triggered office mode unlock	X	X			
	Lockdown To Unlocked	Door changed from lockdown mode to unlocked mode			X		
	Passage	Door was put in passage mode (unlocked state for free access)			X		
	Passage – Master	A master credential put the			X		

		door in passage (unlocked) mode					
	State Override: Unlocked	Administrator manually unlocked the door, overriding schedule			X		
	Sync started: BLE	Started syncing data with wireless lock via Bluetooth	X	X			
	Door Opened	Door was physically opened			X		
	Door Closed	Door was physically closed			X		
	Door Position Sensor Tamper	Someone attempted to tamper with the door position sensor			X		
	Forced Door Alert	Door was forced open without a valid credential			X		
	Forced Door Alert	Door was forced open without proper credentials	X	X			
	Tamper Alert	Someone attempted to tamper with the door hardware			X		
	Tamper Alert	Someone attempted to tamper with the wireless lock	X	X			
	Device Disconnect	Door controller disconnected from the access control system			X		
	Device Connect	Door controller connected to the access control system			X		
	2FA: Decline – Bad PIN (1/2)	Incorrect PIN entered during two-factor authentication	X	X	X	X	X
	2FA: Decline – Bad PIN (2/2)	Incorrect PIN entered for two factor authentication	X	X	X	X	X
	2FA: Decline – Bad PIN (Card/PIN)	Incorrect PIN entered after card was presented	X	X	X	X	X
	Credential Add Failed	Failed to add new credential to the system	X	X	X	X	X
	Credential Delete Failed	Failed to remove credential	X	X	X	X	X

		from the system					
	Credential Update Failed	Failed to update user credential in the system	X	X	X	X	X
➢	Compile Send	System sent updated access data to access point controller	X	X	X	X	X

✻ 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.

✻ Note: Immediate history is only applicable for online devices.

✻ Note: Actions, such as the admit and lock, are only applicable for online devices.

Last modified: 18 June 2026

Single Access Point Widget

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

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

✻ See Standard History Events for icon and message definitions.

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

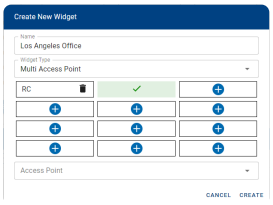
- Admit
- Lock Down
- Unlocked
- Lock (Engage devices only)

Last modified: 8 March 2021

Multiple Access Point Widget

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

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



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

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

- Admit
- Lock Down
- Lock
- Unlocked
- Clear Tamper

Last modified: 26 February 2021

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

Last modified: 26 February 2021

Lock Down Access Points Widget

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

> ! Only a credential set with the master property can open a door in lockdown.

1. Click + WIDGET on one of the three **Placeholder Widget** panels.

- Alternately, hover over  and then choose **Create Widget**.

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

Last modified: 26 February 2021

User Profile Widget

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

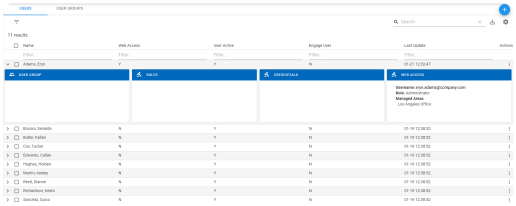
1. Click + WIDGET on one of the three **Placeholder Widget** panels.
    - Alternately, hover over  and then choose **Create Widget**.
2. Enter a name for the widget, and then choose **User Profiles** from the drop-down menu.
3. Choose one or more Access Points or Access Point Groups from the drop-down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

Last modified: 26 February 2021

Users

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

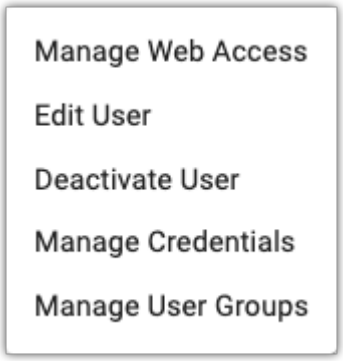
2. All active users in your system will be displayed



- After selecting one or more check boxes next to user(s), the following buttons will appear at the top:
  - ADD TO GROUP : Select a group from the drop-down and then click SAVE
  - ACTIVATE : The user(s) will be activated
  - DEACTIVATE : The user(s) will be deactivated

- Select > to the left of a user's name to display the following additional details: **User Group**, **Rules**, **Credentials**, and **Web Access** (if applicable)

- Select ⋮ to show the menu for **Manage Web Access**, **Edit User**, **Deactivate/Activate User**, **Manage Credentials**, and **Manage User Groups**

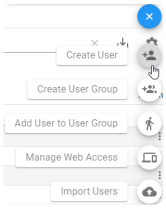


Last modified: 13 April 2021

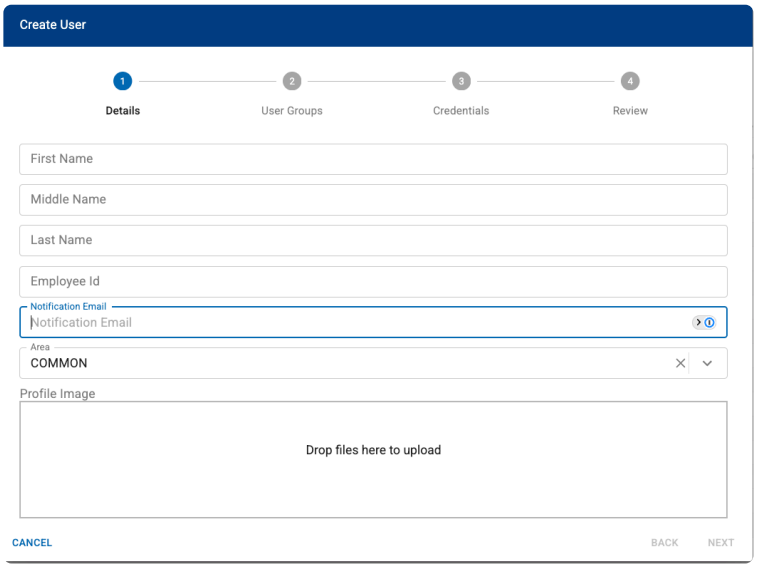
Create User

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

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



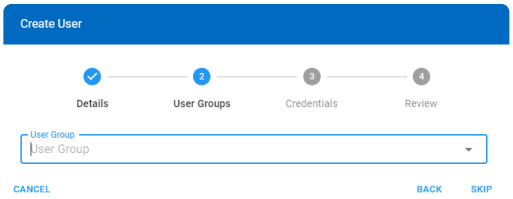
3. Fill in the users information.



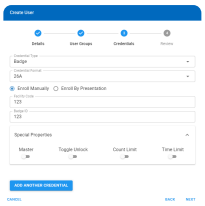
   - The Notification Email field allows users who do not have web access to receive email notifications for Alerts, Scheduled Reports, and Custom Rules. Once an email address is entered in this field, it will appear in the recipient drop-down menus for those features. Email addresses associated with web access accounts are included in those drop-down menus by default.
     - If a web access user also has a Notification Email address entered in their profile, notifications will be sent to the Notification Email address rather than their web access email address.
   - Select an area from the drop-down list.

4. To add a profile photo, drag a file to the **Profile Image** area. Then, click NEXT.
    - To replace an existing image, drag a new image file into the Profile Image area. The new image will overwrite the current one. Images cannot be deleted once added to a profile — they can only be replaced.

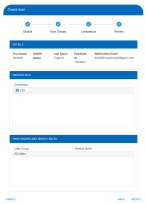
5. Choose the user group from the drop-down list, and then click NEXT. Click SKIP to skip this step for now.



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



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



Last modified: 27 March 2026

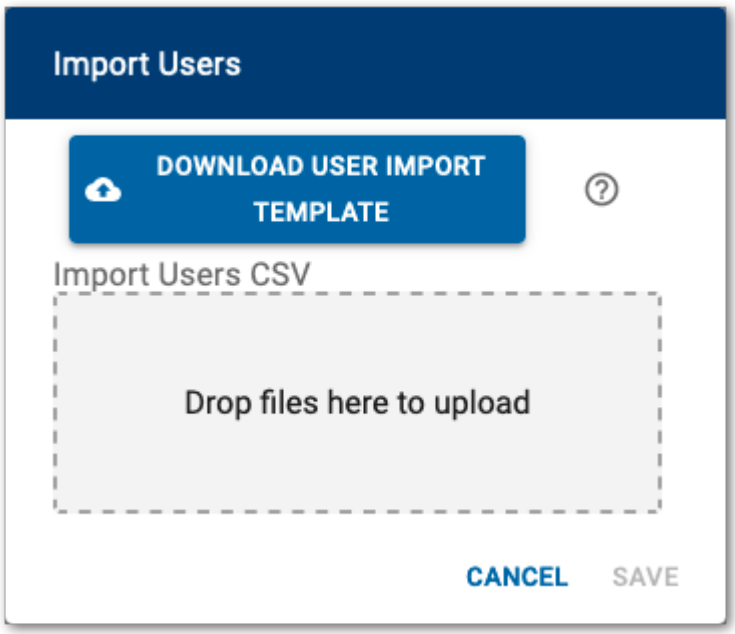
Importing Users

Summary

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

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

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



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

Environments

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

- My tenant is in Pure Access Cloud and only contains legacy devices.
- My tenant is in Pure Access Cloud and it is linked with Engage.
- My tenant is in Pure Access Manager.

Last modified: 28 April 2022

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

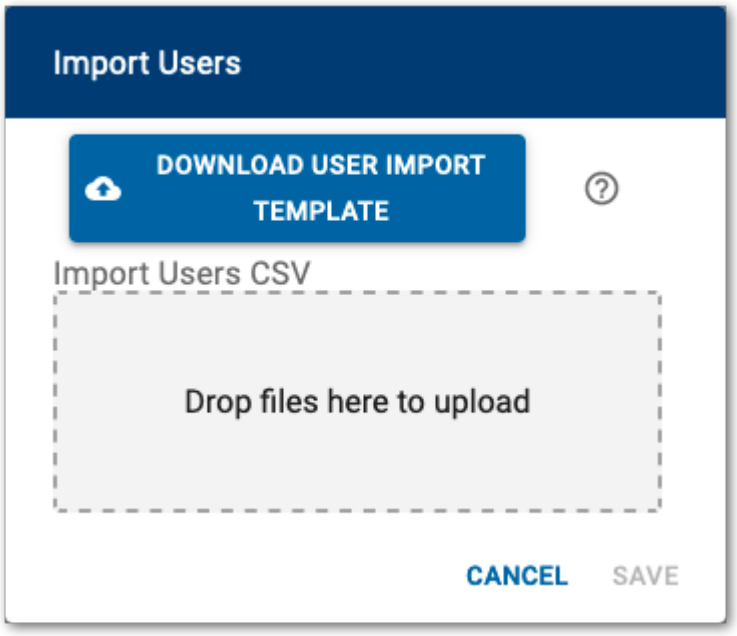
Before continuing, please note that the **formatting** of the template file, including proper **capitalization**, is very important.

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

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

> Note that row 1 (containing the column headers) *must remain as is* for the import to be successful. Pure Access is looking for specific data so these fields must remain **exactly** as they are found in the template.

1. From the **Users** page, hover over the + quick dial then select **Import Users** and click "**DOWNLOAD USER IMPORT TEMPLATE**".
    - Open the template CSV file and input the user(s) information. The only required fields for importing someone (*without* a credential) are **LastName** and **FirstName**.



    - In a tenant that is not linked with Engage, the **BadgeId** column should contain either the hot-stamped number printed on the user's badge, a keypad code, or a mobile/bluetooth Device ID number.
        - Note: In order to import multiple credentials for the same person, the user must be added to more than one row of the CSV (one row for each credential being added).
    - **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).
2. To add users to user groups, populate the **UserGroups** column using the following formatting and notes:
    a. Ensure that the user group(s) **already exist** in Pure Access. The user import ***does not*** create new groups.

   b. Ensure that the capitalization and punctuation of the group(s) are identical.

   c. To add someone to multiple groups, you will need to separate the names of the groups with a semi-colon (;) *without* spaces in-between.

      i. For example, to add someone to the *All Users* and *Managers* groups, the cell would contain: All Users;Managers

3. If areas are *not* being used in this tenant, the **AreaName** cell should be left empty.

4. If areas are being used in this tenant, please review the following formatting and notes:

   a. Ensure that the area(s) **already exist** in Pure Access. The user import ***does not*** create new areas. If an **AreaName** cell is populated with an area that does not exist in Pure Access, **the import will fail**.

   b. Populate the **AreaName** column.

   c. Ensure that the capitalization and punctuation match the area(s) in Pure Access identically. To confirm exact spelling, please refer to the "Areas" tab on the Settings page.

5. The columns titled **CountLimitFlag**, **RemainingUses**, and **ExpirationDate** are optional, but please note that these column headers **must remain in the CSV** for the import to function.

   - If you do not wish to include a credential expiration date or usage limit, skip ahead to step 5.

   a. If you wish to set an **ExpirationDate** on one or more credentials, you can do so using the date format: yyyyMMdd

      - **Example**: April 1st, 2022 would be *20220401*

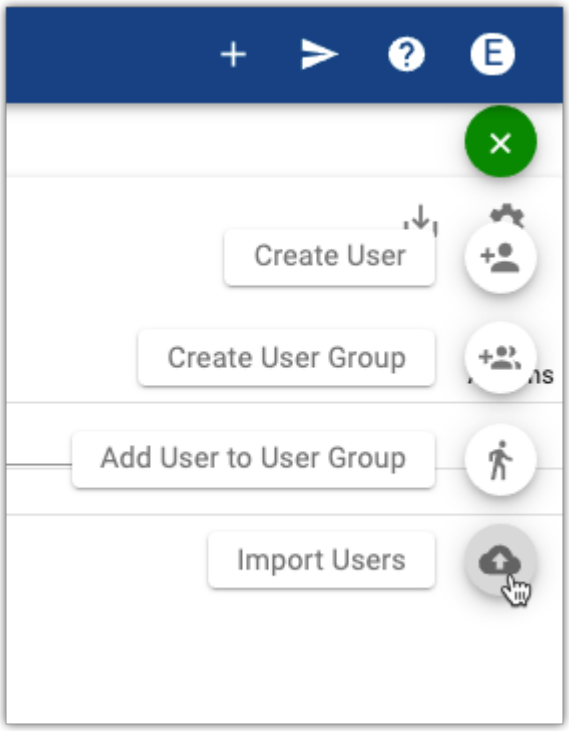
   b. If you wish to set a usage limit on a credential:

      i. **CountLimitFlag** must contain a lowercase "**t**" (for "true").

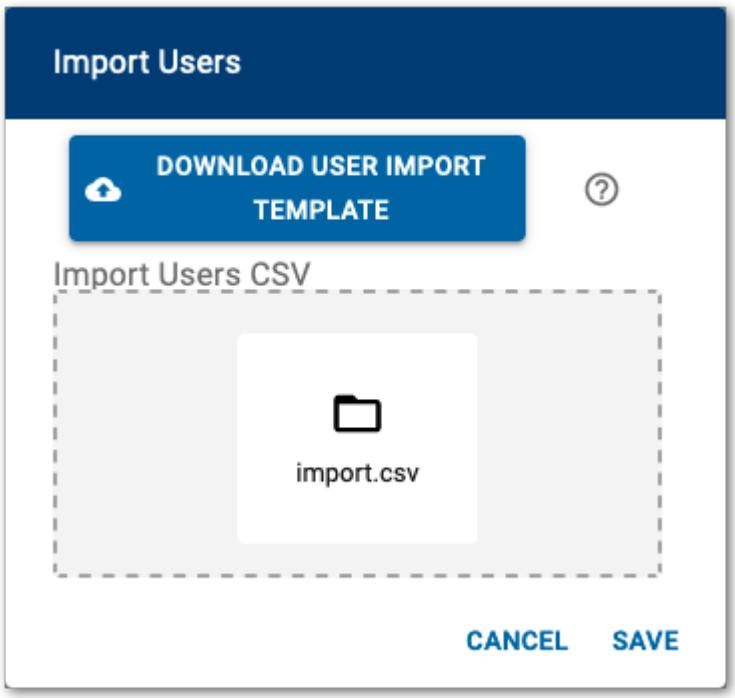
      ii. **RemainingUses** will be the number of times the credential can be presented before it is deactivated.

6. Before finalizing the import CSV, please note that tenants linked with Engage require additional information for credential formats that are not proprietary to Isonas. Details can be found on the next page.

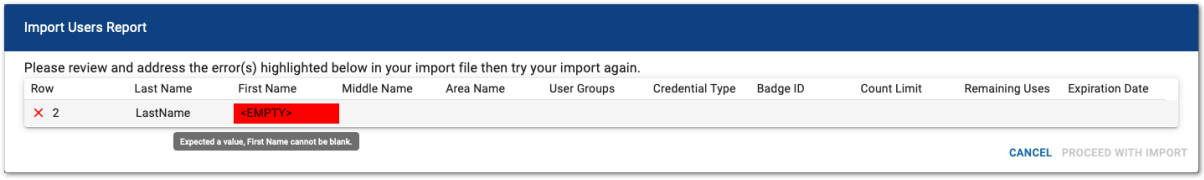
7. If it had been closed, once again select the **Import Users** button from the **Users** page.



8. Drag the **.csv** file into the upload area then click SAVE

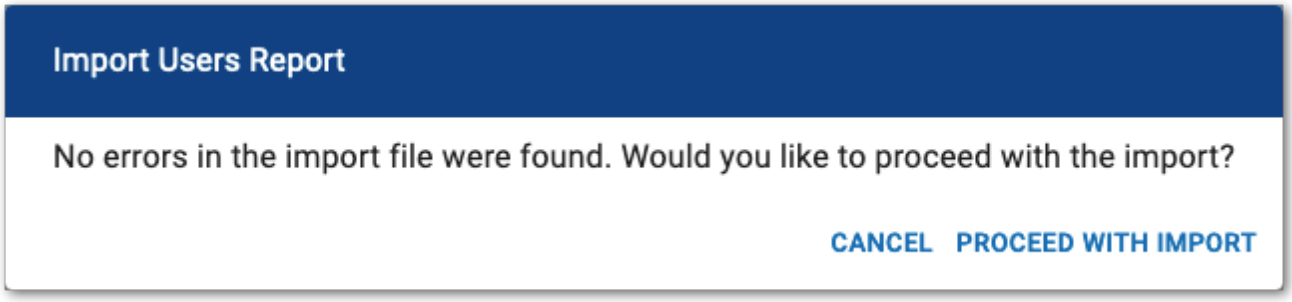


   a. If any errors are found, a table will be displayed noting the issues. If you hover over the red cell with your mouse, you will be able to see helpful tips on the exact error discovered.



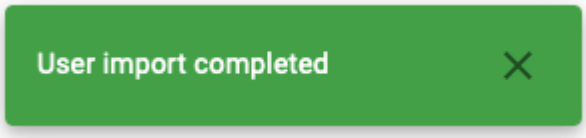
b. Use this feedback to update the CSV file, then try importing again.

9. If no errors are found, click PROCEED WITH IMPORT



a. Note that depending on the size of the import, it could take anywhere from a few seconds to a few minutes to complete.

b. You can continue to use the application while the import is being processed in the background. A notification will let you know that the import has completed.



Last modified: 23 April 2026

Importing Users into Pure Access Cloud (Engage linked tenant)

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

In the user import template CSV, the additional parameters are:

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

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

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

Card Format Name	CredentialType	CardFormat	Hotstamp	BadgeId	FacilityCode	IssueLevel
26A (26 bit)	1	2	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
28G	1	27	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
28H	1	28		*[REQUIRED]*		
32K	1	36	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	*Between 32 and 63*
32X	1	30		*[REQUIRED]*		
33D	1	25	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
34N	1	33	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
34S	1	41	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
35C	1	13	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
35X	1	42	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
36B	1	38	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
36C	1	39	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
36L	1	34	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
36M	1	37	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
36X	1	40	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
37B	1	35	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
37H	1	21		*[REQUIRED]*		
37P	1	32	**DO NOT**	*[REQUIRED]*	*[REQUIRED]*	

			USE			
37X	1	19	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
40X	1	31	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	
48X	1	26	**DO NOT USE**	*[REQUIRED]*	*[REQUIRED]*	*Between 0 and 63*
ISONAS Prox	1	43		*[REQUIRED]*		
ISONAS HID	1	22	*[REQUIRED]*			
EV2	1	29		*[REQUIRED]*		
Keypad	2			*[REQUIRED]*		
Isonas Mobile	3			*[REQUIRED]*		
Schlage Mobile	4		**DO NOT USE**	*[REQUIRED]*	110000	20

Last modified: 2 April 2026

Importing Users into Pure Access Manager

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

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

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

Instructions

1. Download this CSV template
    a. Note that row 1 (containing the column headers) *must remain as is* for the import to be successful
2. Open the template CSV file and input the users' information
    - The required fields are: **LastName**, **FirstName**, **BadgeID**, and **CredentialType**
    a. The **BadgeId** column should contain either the hot-stamped number printed on the user's badge, a keypad code, or a mobile/bluetooth Device ID number.

- If you intend on adding a user profile *without* a credential, you *must* have a “0” in this column or the *import will fail*.
- To import multiple credentials for a single user, they will need more than one row in the CSV (one row for each credential being added)

b. **CredentialType** will need to be either a “**1**” (if the credential is a *badge*), “**2**” (if it’s a *keypad*), or “**3**” (for *mobile/bluetooth* credentials)

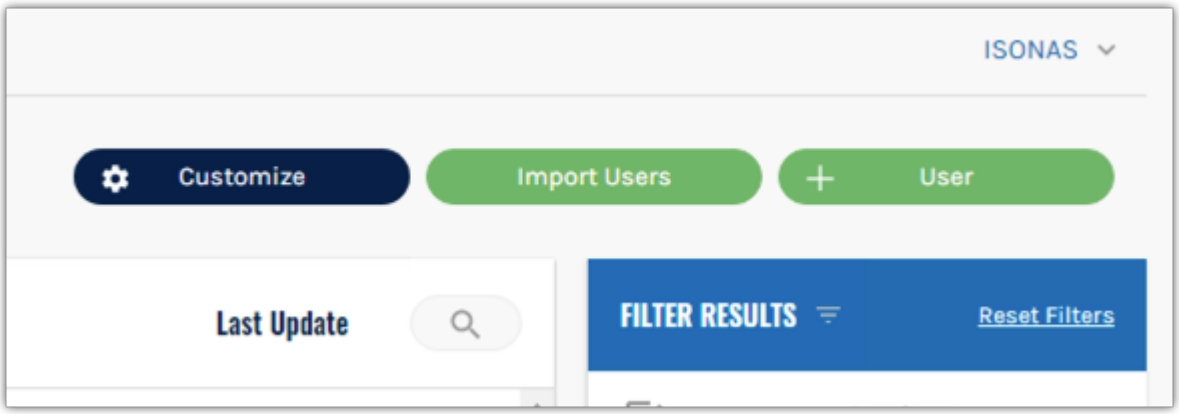
c. If areas are *not* being used in this tenant, the **AreaName** cell should be left empty.

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. If an **AreaName** cell is populated with an area that does not exist in Pure Access, the user will be placed into *COMMON*.
   ii. Populate the **AreaName** column
   iii. Ensure that the capitalization and punctuation match the area(s) in Pure Access

e. The columns titled **CountLimitFlag**, **RemainingUses**, and **ExpirationDate** do not require data for the import to be successful. These columns must remain in the CSV for the import to function, however.
   i. If you wish to set an **ExpirationDate** on one or more credentials, you can do so using the date format: *yyyyMMdd*
      - **Example**: April 1st, 2022 would be *20220401*
   ii. If you wish to set a count limit on one or more credentials, **CountLimitFlag** will need to be true (the cell will need to contain a “**t**”) and the **RemainingUses** cell will be the number of times the credential can be presented beforeit is deactivated

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

g. Click the **Import Users** button from the **Users** page



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

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

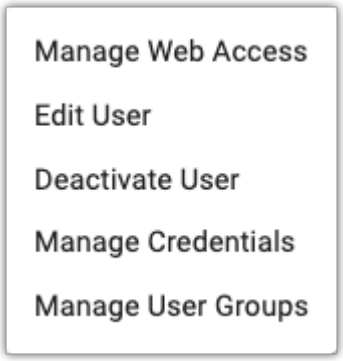
For Pure Access Manager 2.12.2 and lower, **CountLimitFlag** will be **CountLimit** (as provided in the template). The ability to add users to groups via user import was added into Pure Access in version 3.1 and is not available in any version of PAM.

Last modified: 23 April 2026

Edit User

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

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



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

To replace an existing image, drag a new image file into the Profile Image area. The new image will overwrite the current one. Images cannot be deleted once added to a profile — they can only be replaced.

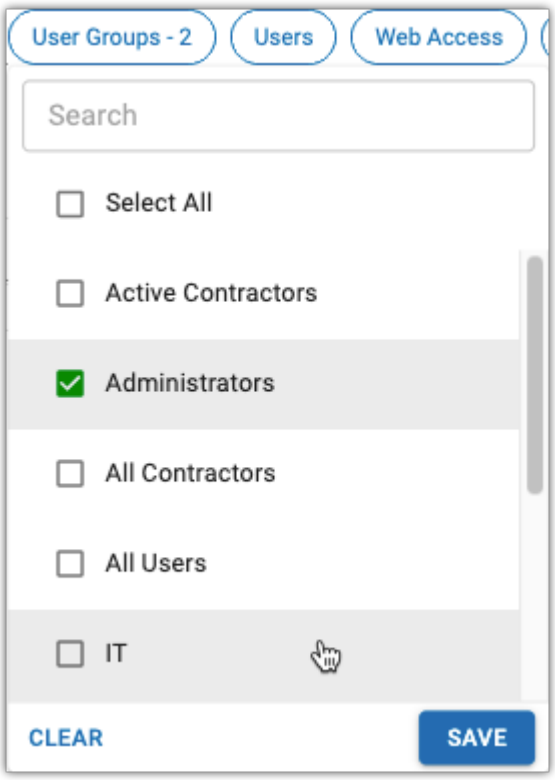
Last modified: 13 March 2026

User Search and Filters

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

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

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



- Alternatively, click CLEAR to remove all filters for the selected category

Last modified: 13 April 2021

User Groups

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

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

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

a. Click > next to a user group to display the rules applied to that group.

b. Click ✎ to change which users are included in the group.
   - When a user is added to a group, they are granted all access associated with that group.

c. Click 🗑 to delete the group.
   - When a group is deleted, all users associated with that group will lose all the access that was associated with that group.

Last modified: 29 January 2021

Create User Group

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

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

Last modified: 1 March 2021

Manage User Groups

User groups should only consist of people who should all have the same access rights. Organizing users into groups allows you to manage many users with a single group vs. managing many individual users separately.
There are several ways to change which user groups a user is included in:

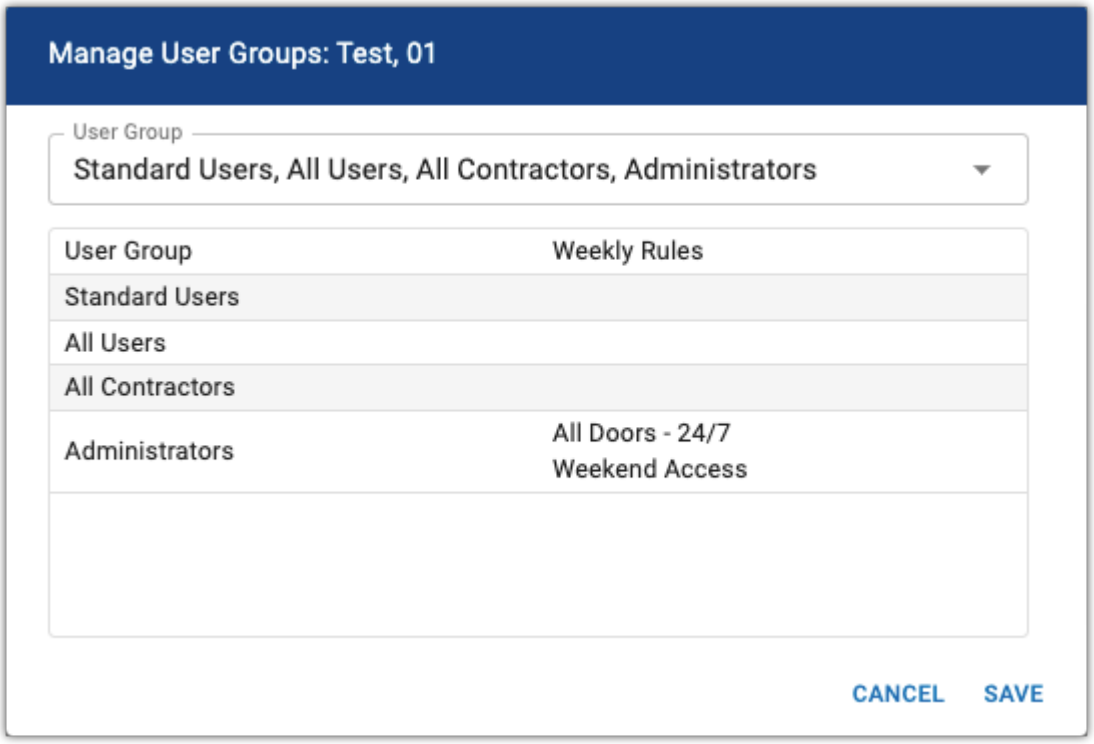
Add a user(s) to a group from the Users page

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

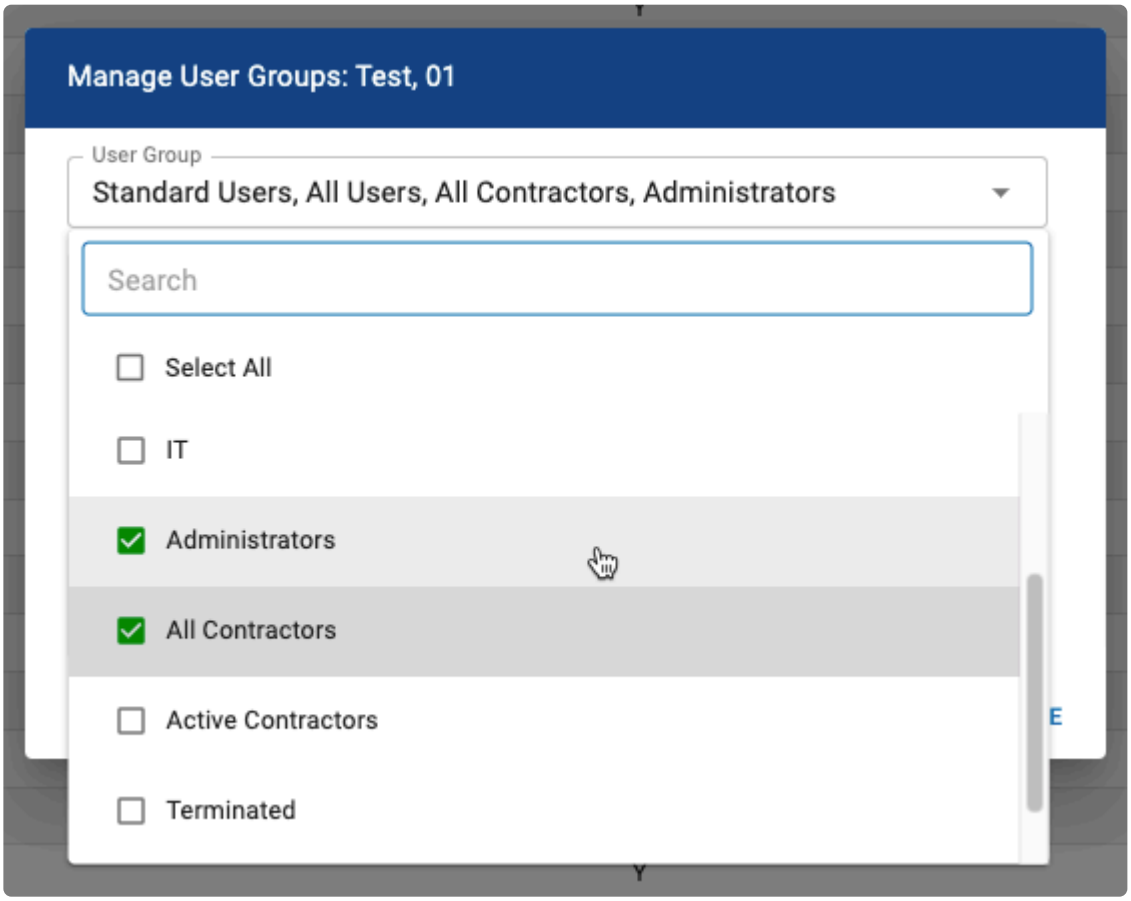
2. Navigate to the **Users** tab.

3. Select ⋮ next to the user you want to edit and choose **Manage User Groups**.

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



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



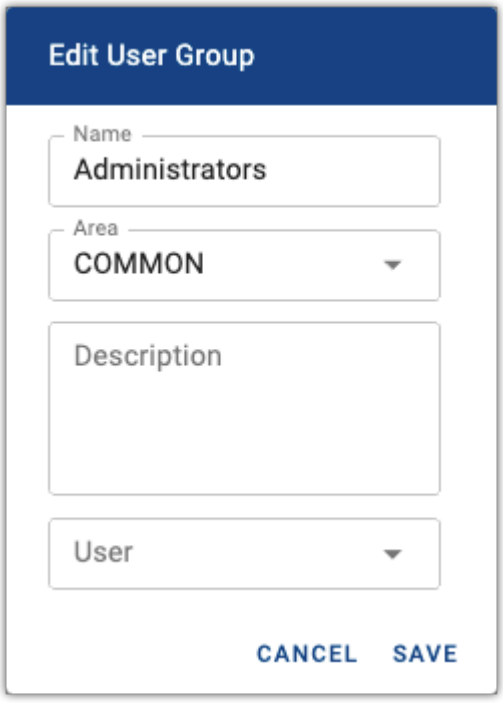
6. Click SAVE

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

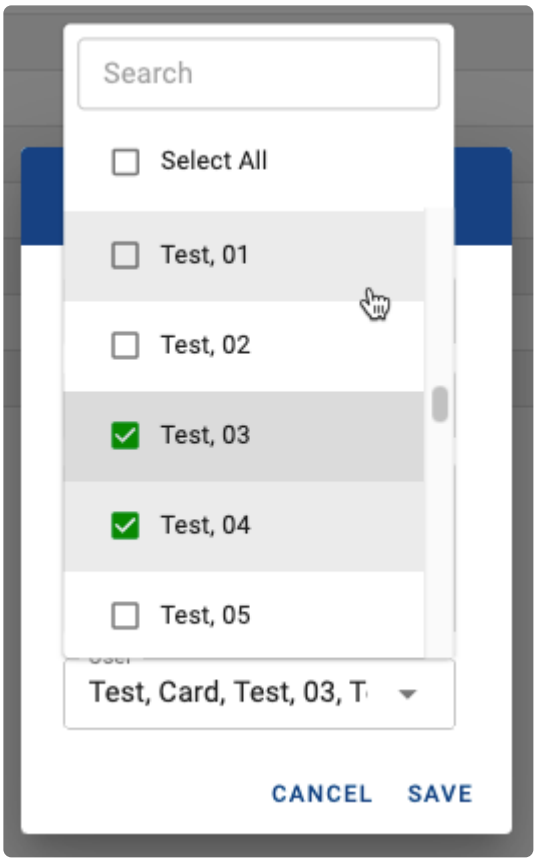
1. Click the **Users** tab on the left side navigation:

2. Navigate to the **User Groups** tab.

3. Select the pencil icon ( ) under **Actions** to open the **Edit** dialog.



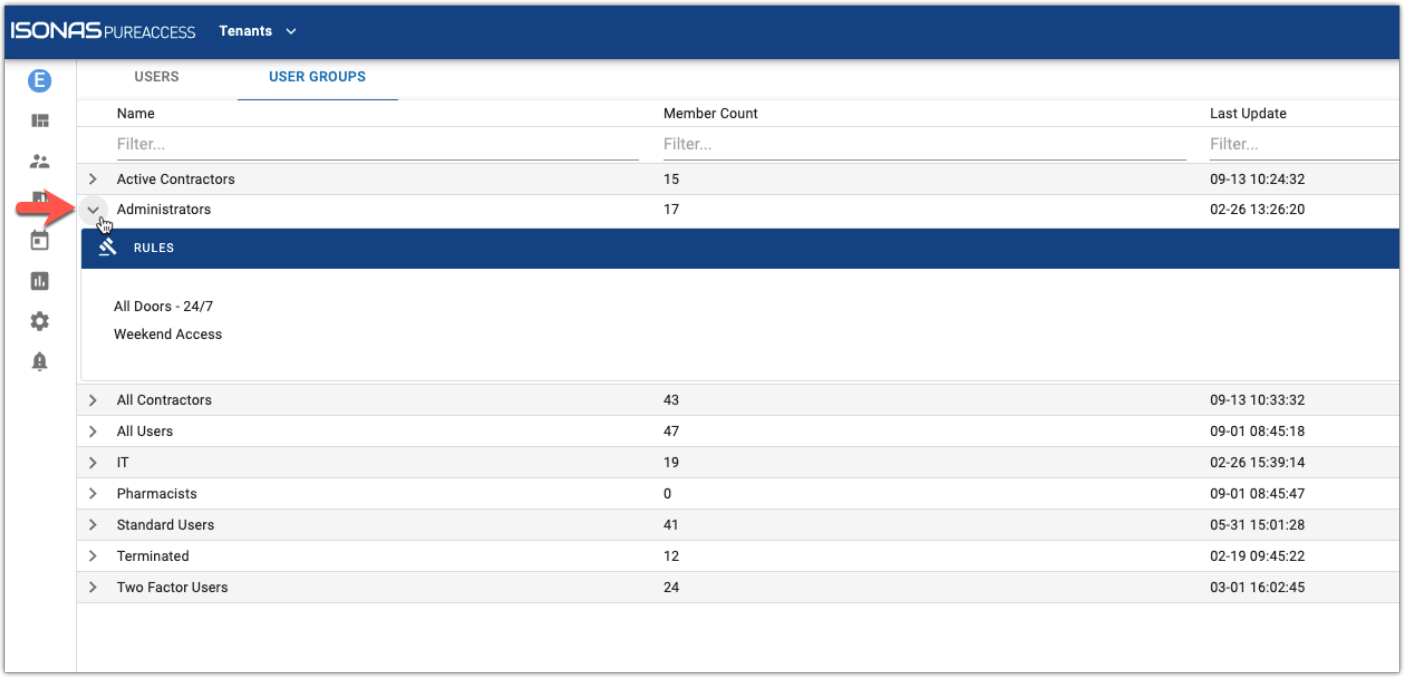
4. Select/Deselect user(s) from the drop-down list.



5. Click SAVE

Viewing user group details

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



Last modified: 1 March 2021

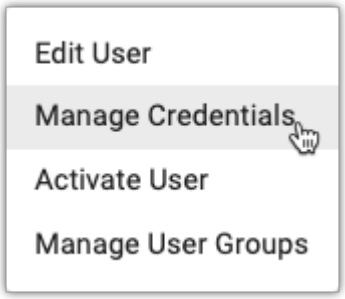
Manage Credentials

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

Navigating to the *Manage Credentials* dialog:

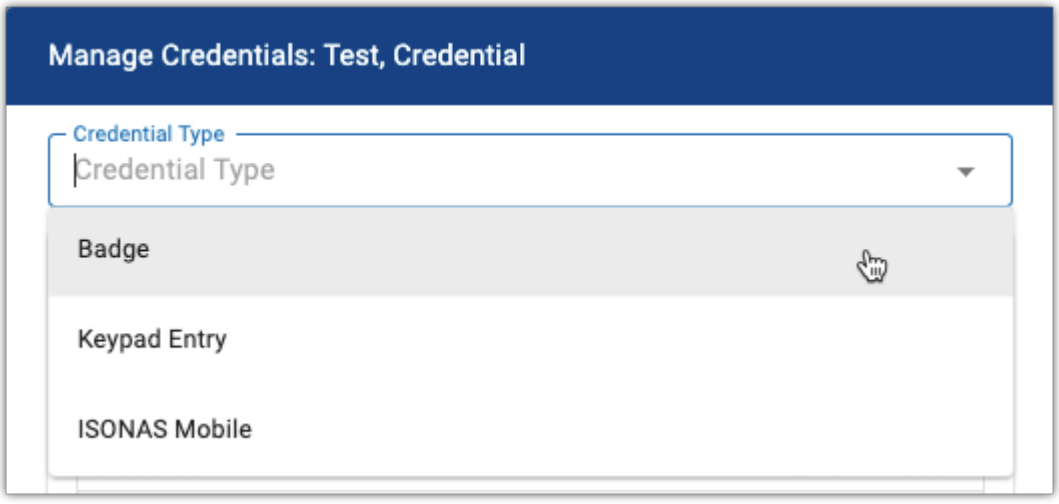
1. Click the **Users** tab from the left side navigation:

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



Adding a credential (overview):

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

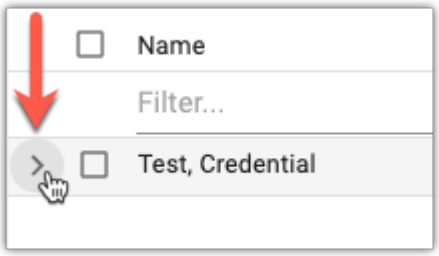


2. For a badge or mobile credential, choose one of the following methods:
   a. *Enroll Manually*
   b. *Enroll By Presentation*
3. For a keypad credential, choose one of the following methods::
   a. *Enroll Manually*
   b. *Generate Random PIN*
4. Input credential value (required) and add special properties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

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

Modifying a credential:

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



b. Under the "**Credentials**" section, select the credential that needs to be modified

3. Make the desired changes

4. Click SAVE

Credential Types						
Type	**Format**	**Facility Code**	**Issue Level**	**Hot Stamp**	**Badge ID**	**Special Properties**
Badge	26A, 37X, 33D, 48X, 28G, 40X, 37P, 34N, 36L, 37B, 36M, 36B	X			X	Master, Toggle Unlock, Count Limit, Time Limit
	37H				X	
	ISONAS Prox (HID Compatible)	X		X		
	28H, Isonas EV2, 32X				X	
	32K	X	X		X	
Keypad Entry	PIN	n/a				
ISONAS Mobile	Device ID					
Schlage Mobile	Mobile Phone Number					

Last modified: 3 May 2021

Badge

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

In a tenant not linked with Engage:

Enrolling Manually

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

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

If the bitmask is set correctly:

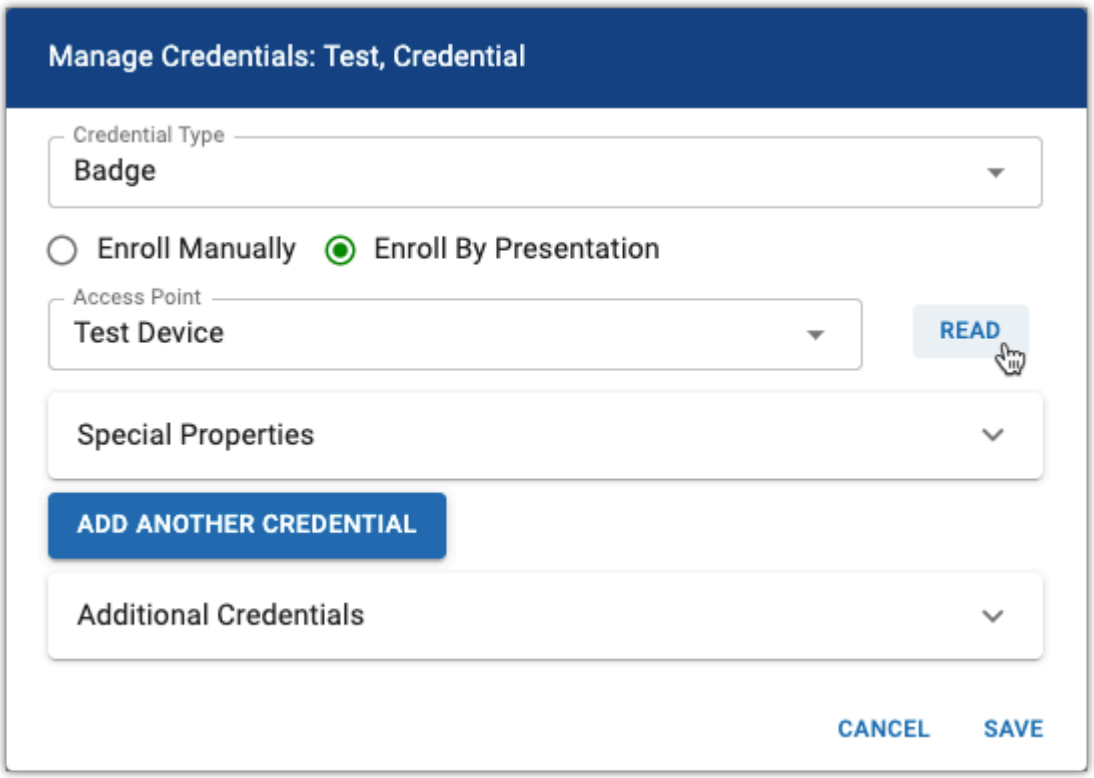
1. Navigate to the Manage Credentials dialog for a user
2. Select "**Badge**" from the **Credential Type** dropdown
3. Select "**Enroll Manually**"
4. Input the hot stamped number from the card/fob into the **Badge ID** field (required)
    - Add special properties (optional)
5. Click SAVE

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

Enrolling By Presentation

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

presented then click READ



- Add special properties (optional)

6. Click SAVE

The declined credential will clear after 15 minutes. *

In a tenant linked with Engage:

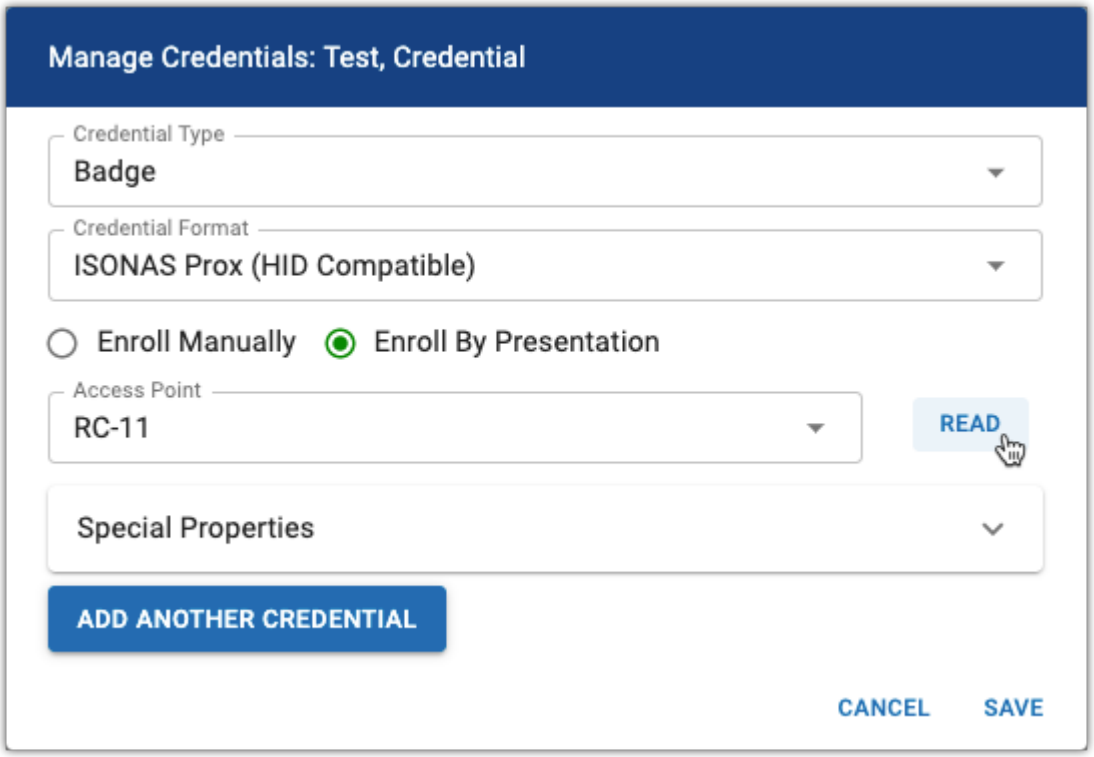
Enrolling Manually

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

6. Click SAVE

Enrolling By Presentation

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



    - Add special properties (optional)
7. Click SAVE

Last modified: 3 May 2021

Keypad Entry

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

you may generate a randomized PIN.

Enrolling Manually

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

Generating a Random PIN

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

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

Last modified: 12 April 2021

ISONAS Mobile

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

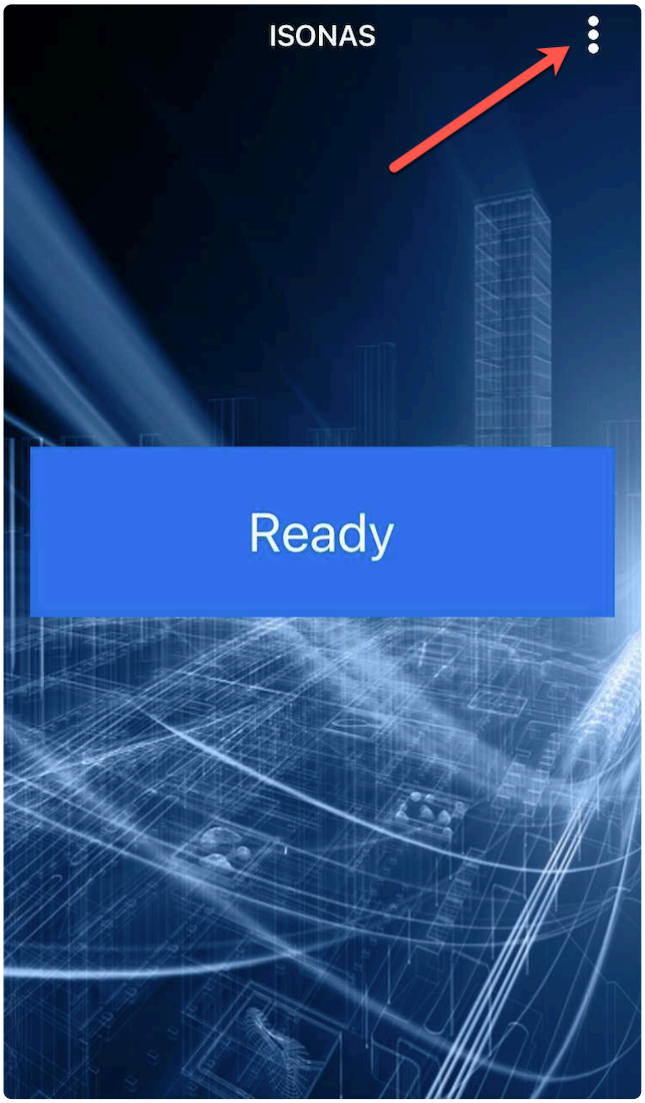
Prerequisite

In order to use the ISONAS Mobile Bluetooth credential, you must first install the Pure Mobile app from the

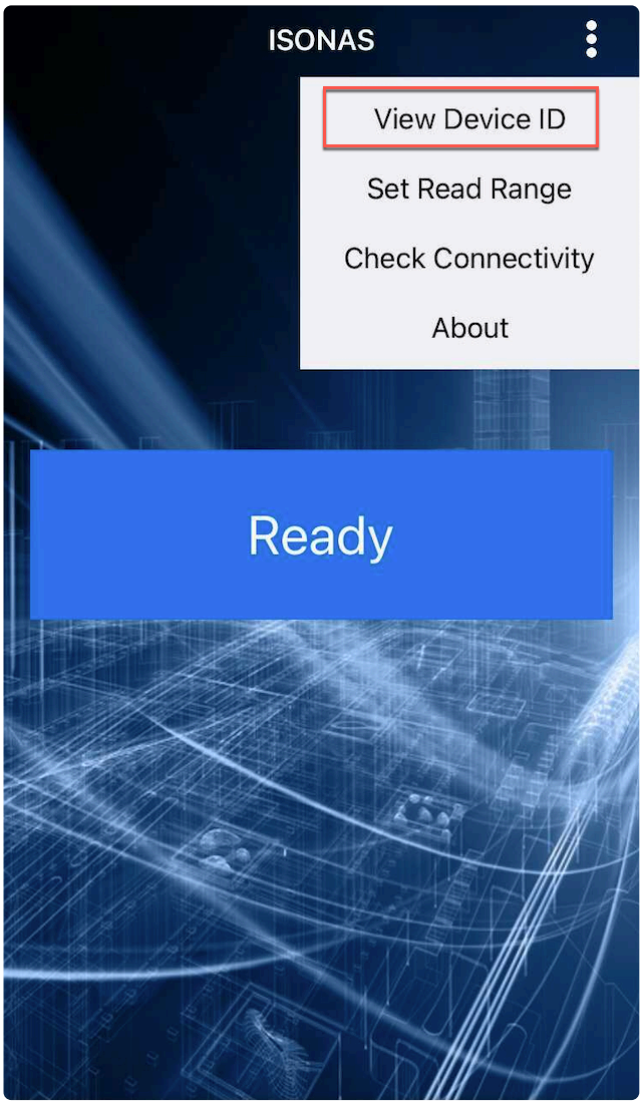
iOS App Store or Google Play Store.

Enrolling Manually

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



    b. Click “**View Device ID**”



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

5. Click SAVE

Enrolling by Presentation

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

presented then click READ

- Add special properties (optional)

6. Click SAVE

> ! Please note that the **Device ID** (credential value) is randomly generated using the application's UUID which is assigned on install. If the **ISONAS Pure Mobile** application is uninstalled then reinstalled, the **Device ID** will be renewed and the credential will need to be re-enrolled for the user; there is no way to recover an old credential/Device ID after reinstallation.

Last modified: 18 October 2024

Using the Mobile Credential to Unlock a Door

ISONAS Pure Mobile App

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

Schlage Mobile App

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

Last modified: 26 February 2021

Schlage Mobile

Prerequisite

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

Enrolling by Text

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

Enrolling By Presentation

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

> ! If the user changes phones or the app is uninstalled and reinstalled, the credential will no longer exist in the mobile app and cannot be restored. To recover access, deactivate the existing Schlage Mobile credential from the user's profile and enroll a new credential by Text.

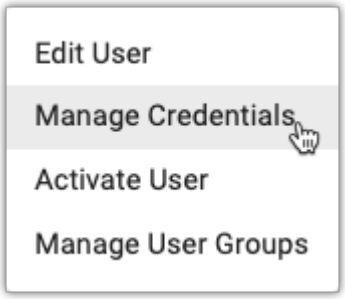
Note that Schlage Mobile Access credentials are only compatible with Schlage locks and Schlage reader controllers. These *will not* function with legacy ISONAS hardware. In order to enable this functionality, your tenant must first be linked with Engage.

Last modified: 5 June 2026

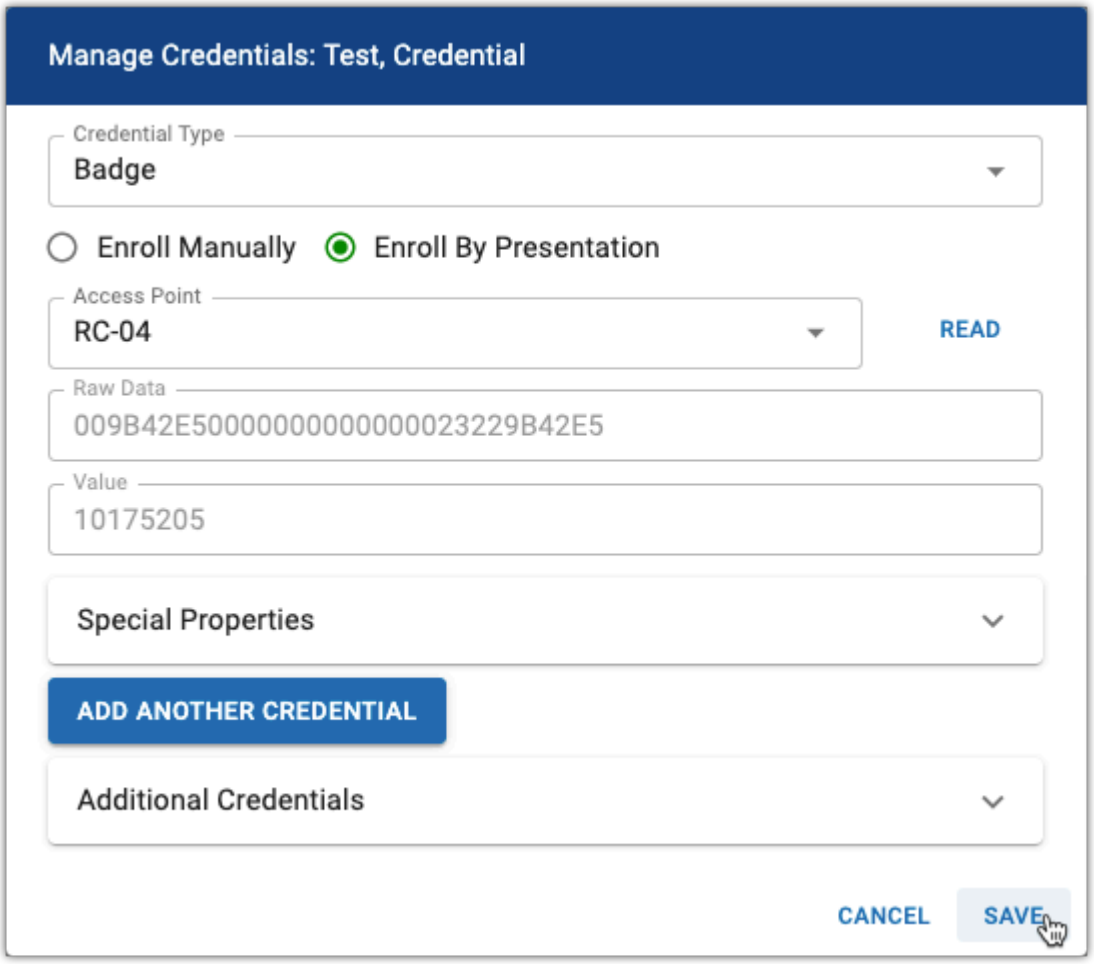
Enrolling by Presentation

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

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



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



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

The declined credential will clear after 15 minutes.*

Last modified: 3 May 2021

Special Credential Properties

Special Property	Description	"Schlage Device Types"		RC-03, RC-04, IPB
		Schlage RC	NDE, LE	
"Pass Through – aka Master":	This features programs the credential to act like a 'Pass Through' credential. Specifically, it will either bypass a locked down access point, bypass a two-factor rule or provide 24/7 "Always" access to doors where user currently has Grant Access permissions. • Schlage devices cannot be combined with Toggle Unlock	X	X	X
Toggle Unlock	When a badge is presented it will unlock devices based on the selection below. Choose All Access points, an Access Point Group, or a single Access Point. • Schlage devices cannot be combined with Pass Through on the RC, and the NDE & LE cannot be combined with Pass Through & Toggle Unlock	X	X	X
Count Limit	Limits how many times a credential may be presented before being deactivated.	X		X
Time Limit	Limits the time during which a credential will be active. • The NDE, LE, XE360, CTE and Schlage RC only support credential activation and expiration time resolution down to the hour while the IP-Bridge/MTB and the Control support activation and expiration time down to the minute. This currently will cause the IP Bridge to expire at a different time than the NDE, LE, and Schlage RC. • For example, if someone set a credential expiration time to 5:16pm, access would actually expire at 5:00pm for NDE, LE, and RC, while access would expire at 5:16pm on an IP-Bridge.	X	X	X
Force Check In	Causes the device to check in with Zentra when the credential is presented. Note: A sync or Wi-Fi check		X	X

	must occur at the device after a credential is programmed with this feature before it will work.			
“ADA Relock Delay”	Used to bypass the latch interval (default is 3 seconds) of the door to provide more time for the resident to move through the door.	X		

Last modified: 26 May 2026

Pass Through Credential

This special programming feature is currently misnamed as “Master” but is functionally a **Pass-Through** credential property.

This property enables the credential to bypass specific lock states, but the functionality will vary depending on the device:

Schlage Devices (NDE, LE, RC)

- A credential with this property will unlock a door for which it has access even when the door is in a locked down state

ISONAS Devices (IP-Bridge, RC-04, RC-03)

- A credential with this property will unlock a door for which it has access even when the door is in a locked down state
- A credential with this property grants 24/7 access to any door where the user currently has Grant Access permissions
- A credential with this property will bypass a configured 2FA weekly rule

> ! Note that the pass-through/master credential property ***does not*** provide grant access permission to all doors in a site. 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.

> ✻ **Pass Through** was known as **Master** credential previously.

Last modified: 16 March 2026

Toggle Credential

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

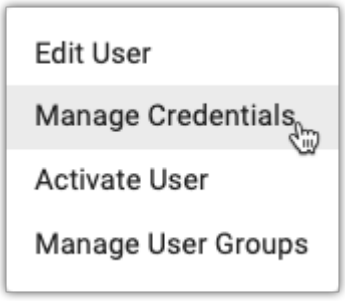
It *cannot*, however, be used to override an **Auto-Unlock** nor **Auto-Unlock w/ Badge** rule. Toggle lock can *only* reset a toggle unlock.

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

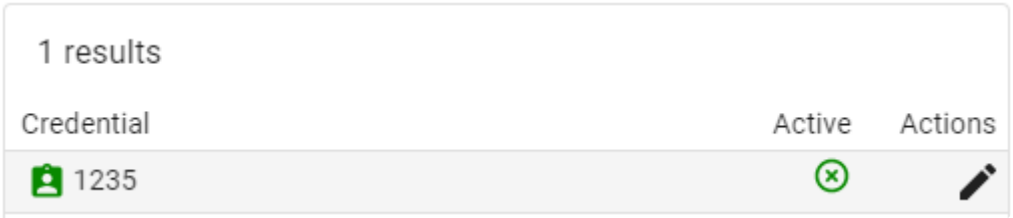
Adding Toggle Credential Special Property

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

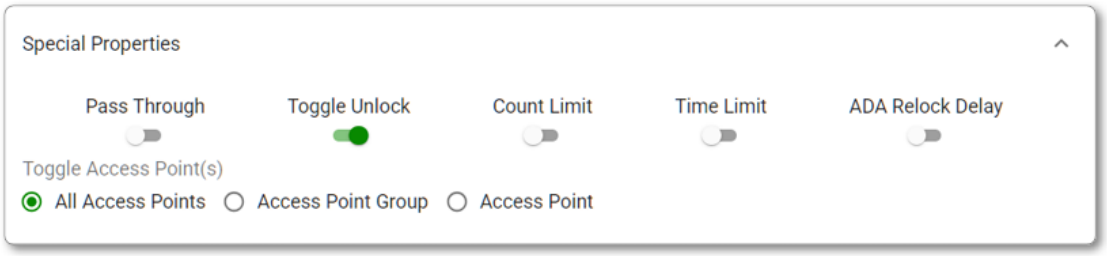
2. Click ⋮ next to the user for which you want to add a toggle credential
3. Select **Manage Credentials**



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



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



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

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 credential to toggle an entire group of access points with a single presentation.

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

Re-Lock Time

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

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

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

5. Click SAVE and then enter your password to confirm

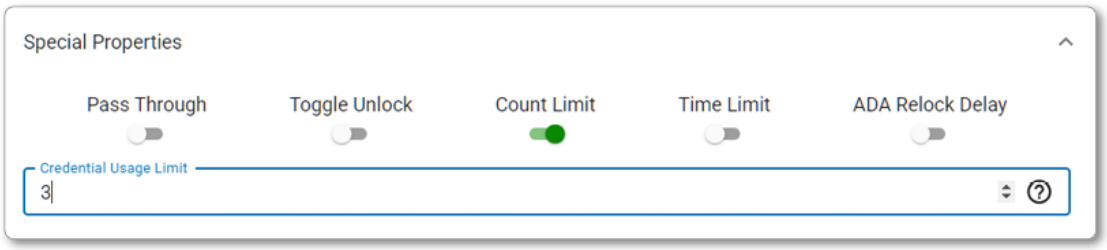
> ! The Schlage RC *does not* support the re-lock feature at this time.

Last modified: 25 September 2025

Count Limit

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

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



Last modified: 25 September 2025

Time Limit

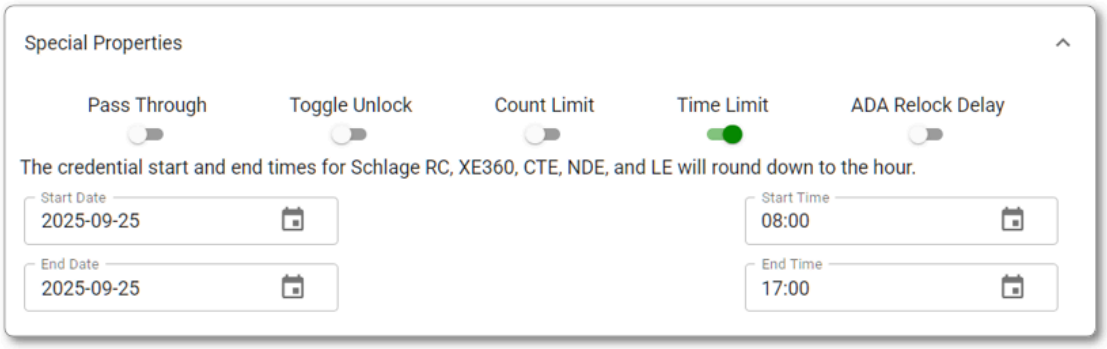
Time Limit is used to limit the time during which a credential will be active.

1. Select the **Time Limit** slider.

2. Choose the **Start Date**, **Start Time**, **End Date**, and **End Time**.
3. Click SAVE.

The NDE, LE and Schlage RC only support credential activation and expiration time resolution down to the hour while the IP-Bridge/MTB and the RC-04 support activation and expiration time down to the minute. This currently will cause ISONAS Devices to expire at a different time than the NDE, LE and Schlage RC.

For example. If someone set an credential expiration time to 5:16pm, access would actually expire at 5:00pm for NDE, LE and RC, while access would expire at 5:16pm on the IP-Bridge.



Last modified: 16 October 2025

Force Check-In

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

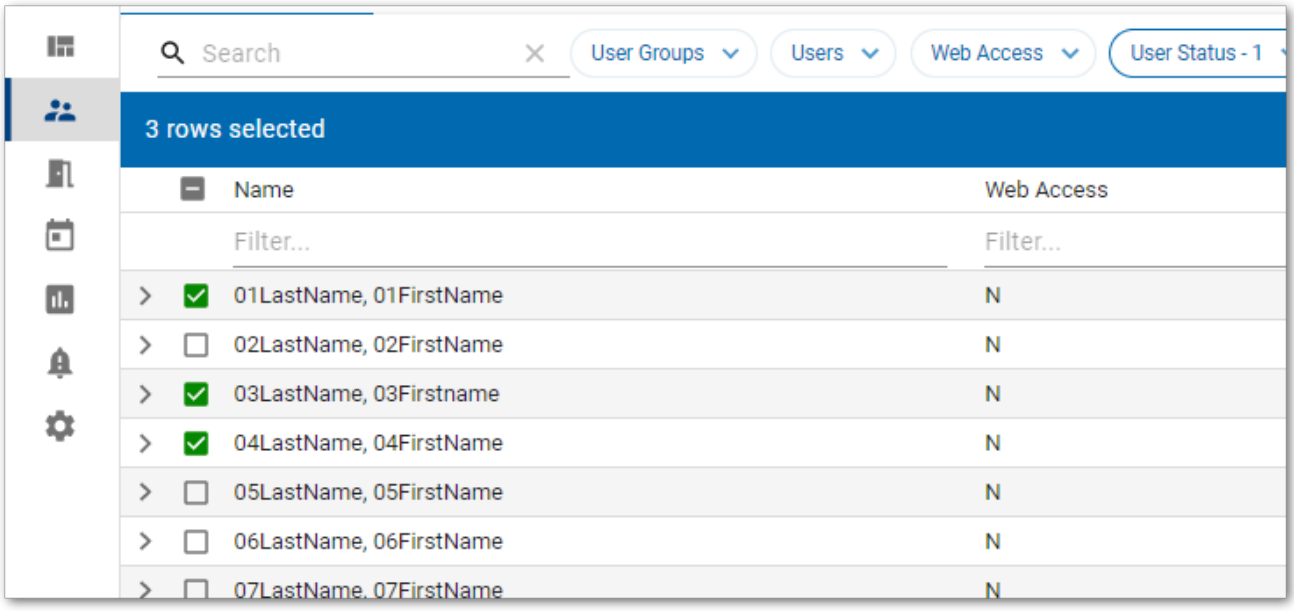
Last modified: 17 June 2022

Migrate Credentials (Legacy to ENGAGE)

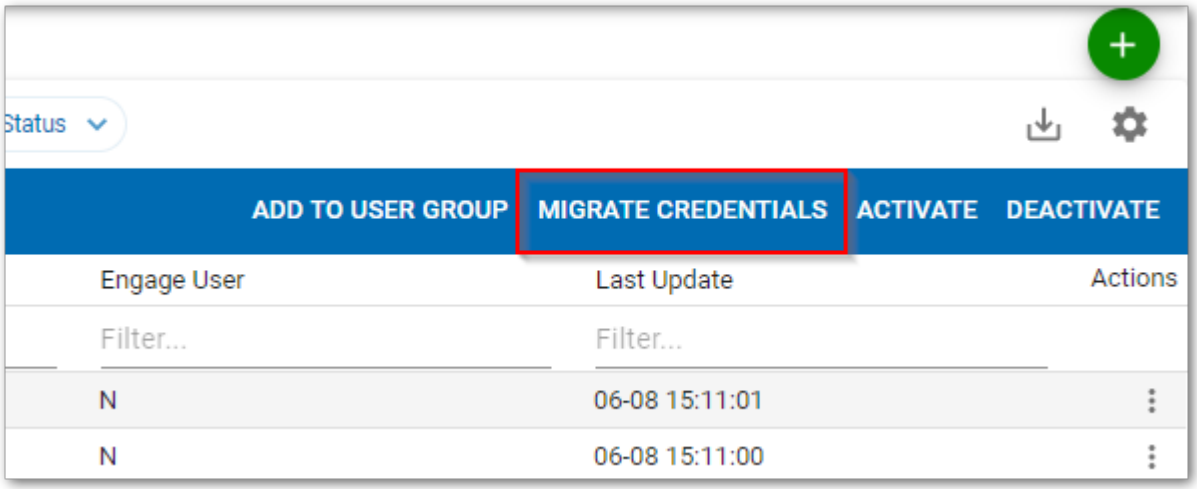
After linking an existing tenant (with active credentials) to ENGAGE, each credential will need to be migrated before it will function at an ENGAGE device (Schlage RC, LE, NDE, etc.).

Process:

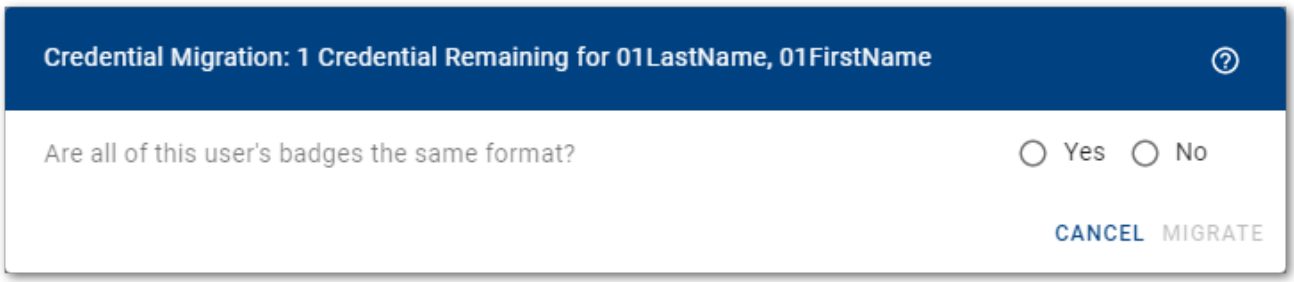
1. Navigate to the **Users** page
2. Select from 1 to a maximum of 10 users with legacy credentials at a time



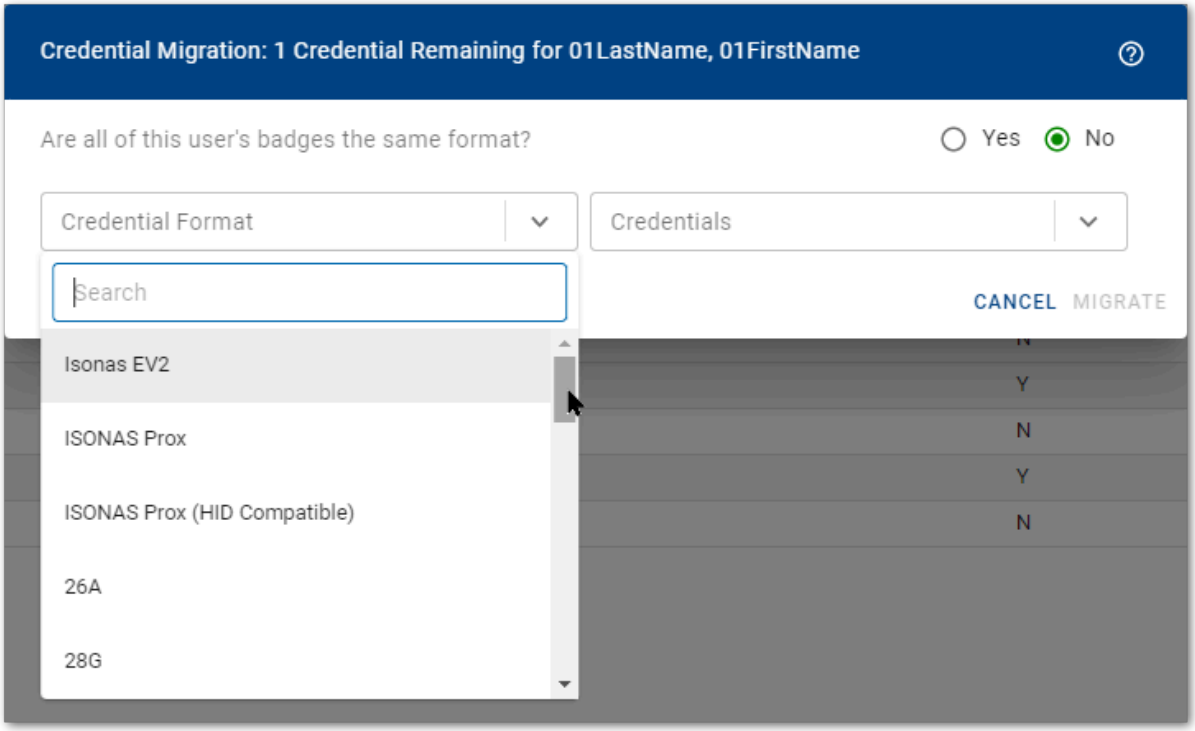
3. Click the **MIGRATE CREDENTIALS** button



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



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

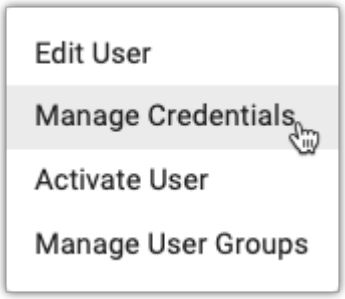


Last modified: 24 April 2026

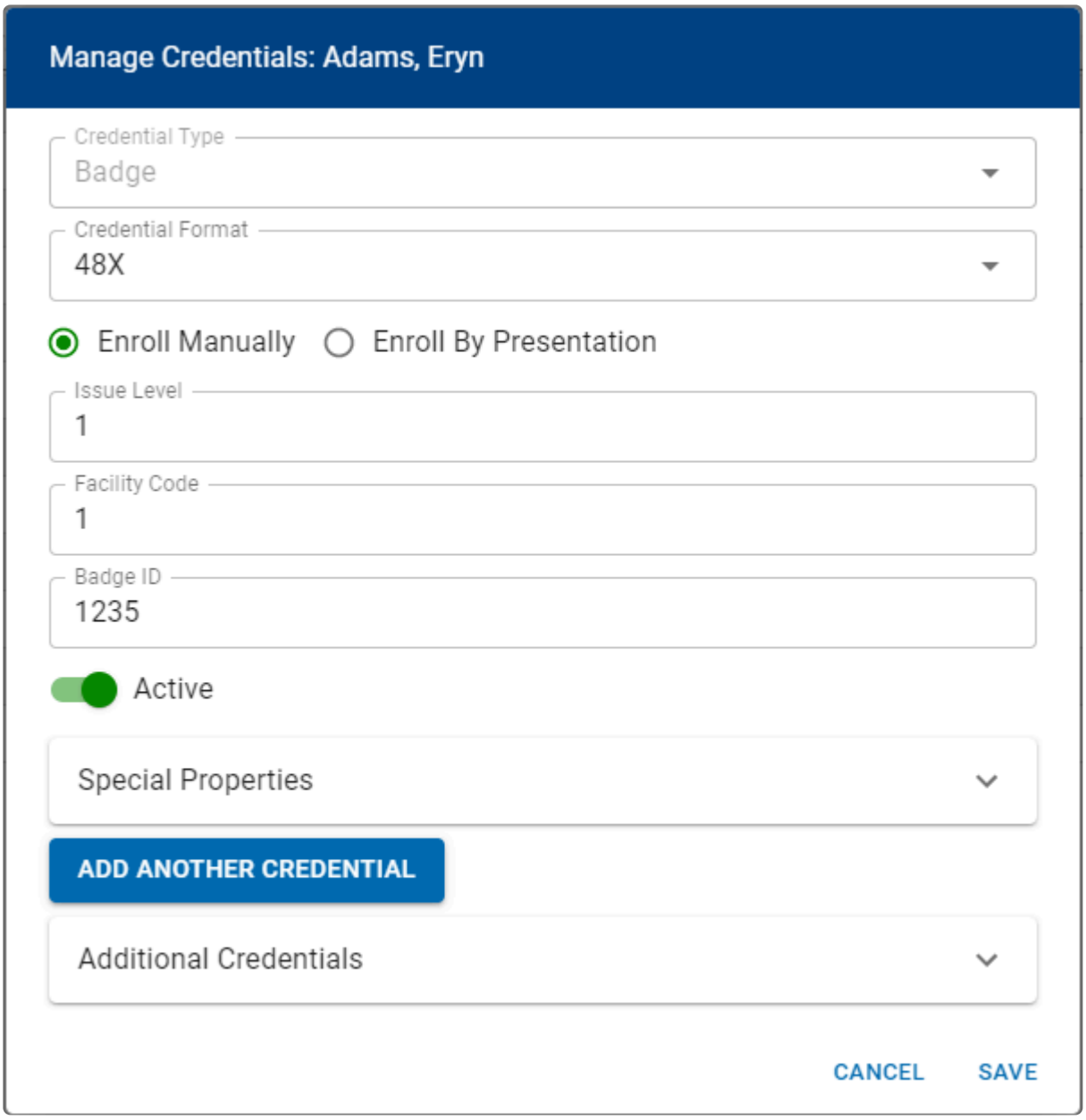
Deactivating Credentials

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

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



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



4. Click SAVE

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

Last modified: 26 February 2021

Manage Web Access

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

If either of these criteria are not met but your user profile *should* be able to log in, an **Integrator** or an

Administrator of the tenant will need to ensure your user role is properly set and will need to send an invitation for web access to a valid email address (if this has not been done or if the invitation has expired).

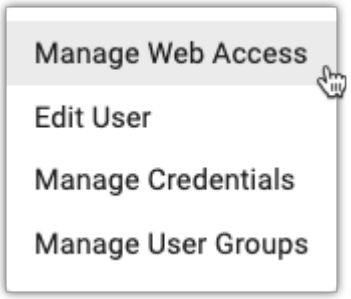
Last modified: 4 April 2023

Setting up Web Access for a User

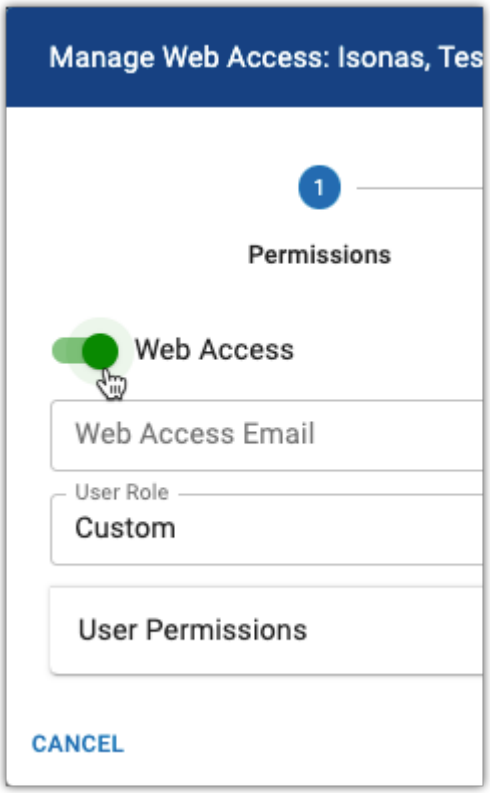
Web access rights allow a user to log into and manage a tenant.

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

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



3. **Permissions:**
    a. Select the **Web Access** slider



   b. Enter the email address of the user

   c. Choose one of the four preset roles from the **User Role** drop-down menu or select **Custom** to choose their permissions individually

      i. To view/edit the specific permissions granted, click on **User Permissions**

4. Click NEXT

5. **Area Access:**

   a. From the drop-down menus under the **Access** column, select the appropriate permissions for each area

6. Click SEND INVITE

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

> ! New users should note that ISONAS does not have the ability to re-send invitations that have expired. Users who have let their invitation expire will need to navigate to the login page, enter their email address and then select **Forgot Password?** to create a password and access the tenant.

Last modified: 27 March 2026

User Roles

What do the pre-defined roles provide access to?

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

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

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

- API Tokens
- Reports
- Scheduled Reports
- Engage (feature coming soon)

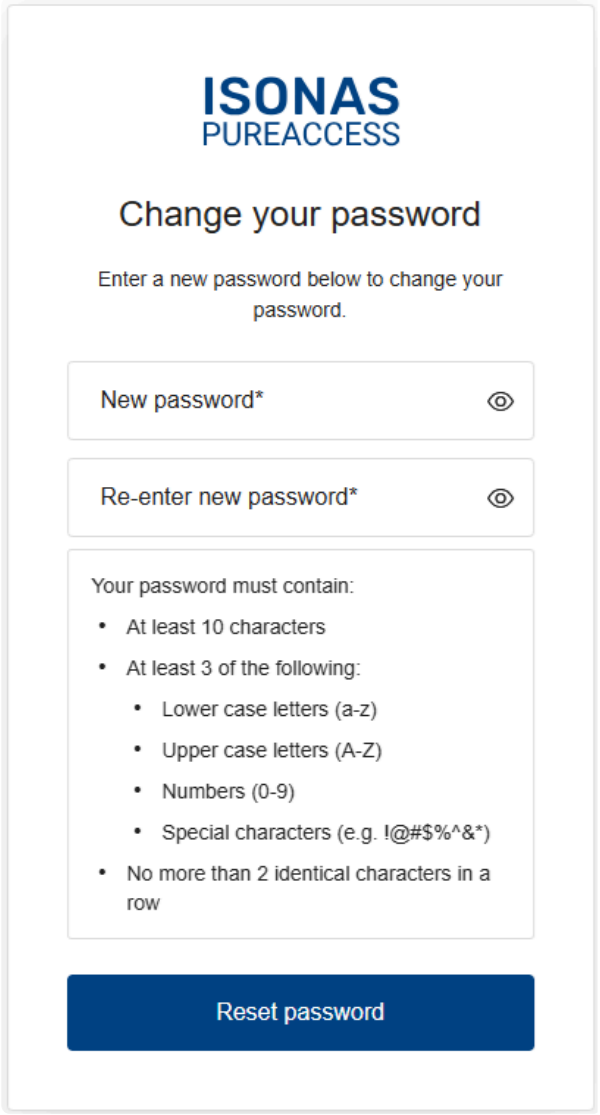
> Additional information on the **Custom** user role: only web access users with modify privileges for a specific permission can grant another person view/modify access to that permission. For example, if a web access user who does not have modify access to Dashboards attempts to grant another person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

Last modified: 13 April 2021

Accepting the Web Access Invitation

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

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



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

Invitation not working?

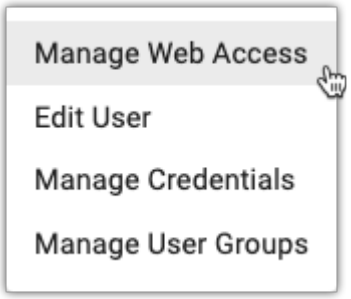
If you accept the web access invitation and it there is no space for you to enter your information, you are likely using Internet Explorer or another unsupported browser. Please retry using **Chrome** or **Firefox** instead.

Last modified: 19 February 2025

Removing Web Access Privileges

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

2. Select ⋮ next to the user from which you want to remove web access and click **Manage Web Access**



3. Select the slider next to **Web Access** so that it is no longer green

1. Click NEXT
2. Click SAVE

Alternative

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

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

Last modified: 13 April 2021

Deactivate User

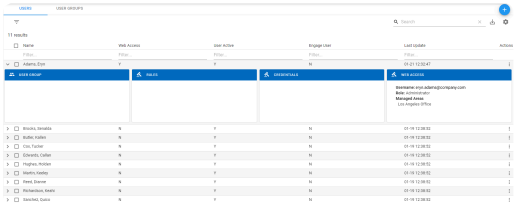
If you have a person from whom you need to remove all access rights, you can simply deactivate their user profile. This will automatically disable all credentials assigned to this user.

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

Deactivating multiple users:

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

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

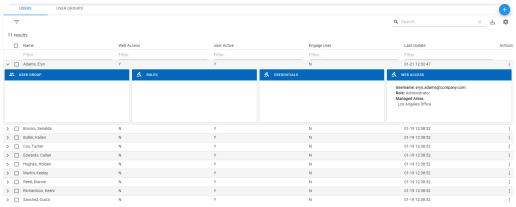


3. Click on **Deactivate**:

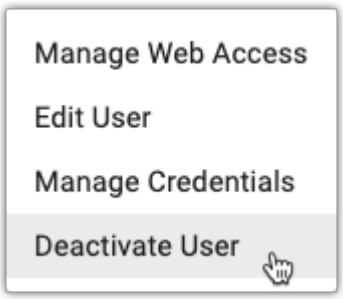
Deactivating one user:

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

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



3. Click on **Deactivate User**:



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

Last modified: 1 March 2021

Viewing Deactivated Users

See User Search and Filters

Last modified: 7 December 2023

Activating a User Profile

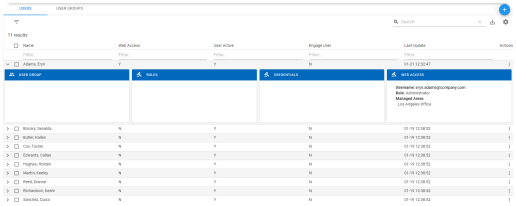
If a User was previously deactivated, you can easily reactivate the profile.

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

Activating multiple users:

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

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



3. Click on 

.

Activating one user:

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

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

Last modified: 26 February 2021

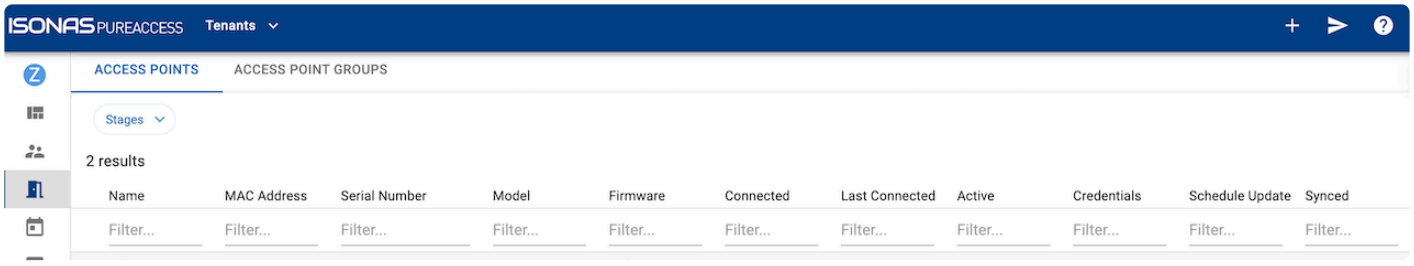
Access Points

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.

Last modified: 26 February 2021

Access Point Main Page

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



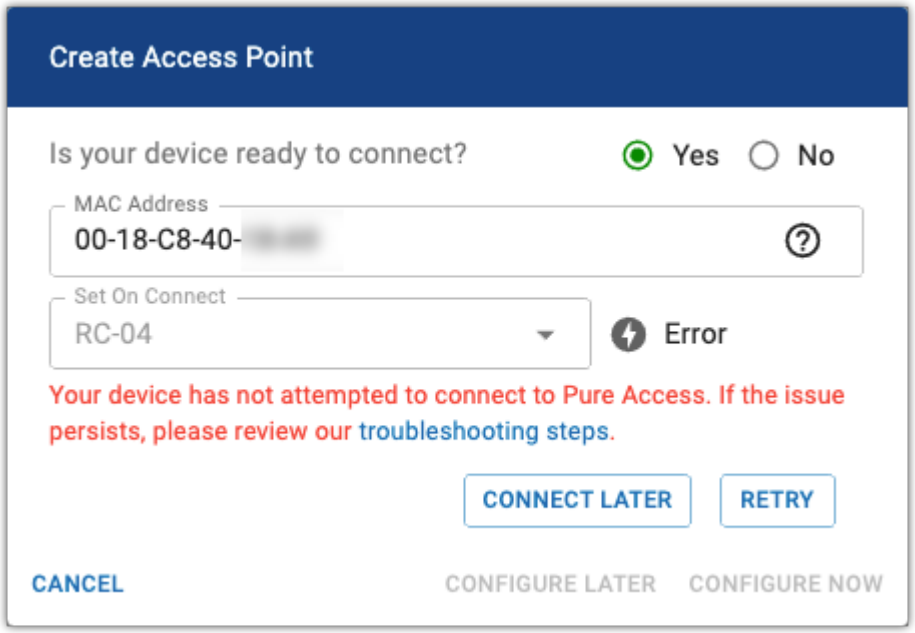
Name	Name of the Device
MAC Address	MAC Address of the Device (online devices only)
Serial Number	Serial Number of the device
Model	Model of the Device
Firmware	Latest Out-of-date
Connected	Connection Status of the Device (online devices only)
Last Connected	Last time the device communicated with Zentra. See history for which activity occurred at that time. • For online devices, this date may reflect a connectivity check rather than a specific activity and a corresponding history event would not exist for this timestamp.
Active	Active/Not Active
Credentials	% of possible Credentials associated with the device

Schedule Update	If an update is scheduled or not
Synced	Not used
Actions	Edit Access Point Edit Device Settings Activate/Deactivate Device

Last modified: 19 June 2026

Adding a Reader Controller (legacy device)

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



    b. For a device that is either not plugged in or not currently discoverable on the network:
        i. Select “No” to the question “Is your device ready to connect?”
        ii. Input the MAC address of the reader controller (located on the back and side of the device)

iii. Choose the device type from the drop-down list (this may auto-populate with the correct type)

c. Input a name for the access point Ensure it meets our requirements.
   - 1-20 characters (Engage allows up to 25)
   - Letters, numbers, and symbols (#, -, and spaces) only
   - Cannot start or end with spaces
   - No special characters beyond those listed

d. Input a description (optional)

e. Select the relevant access point group(s) from the list (optional)

f. Choose the Area to which this access point belongs (if applicable)

g. Select either "**Configure Later**" or "**Configure Now**"

Troubleshooting

I get an error after selecting "Yes — is my device ready to connect?"

This error occurs when you do not have Manage access to the COMMON area. Select "No" instead — an Area field will appear allowing you to assign the device to an area you have Manage access to.

I selected "No" but no Area field is appearing.

The Area field only appears when you have access to at least two areas — Manage access to the area you want to commission into, plus at least VIEW or Manage access to one additional area. Contact your administrator to verify your area permissions.

The Area field appears but commissioning still fails.

You have likely selected an area where you only have VIEW access. Only areas where you have Manage access can be used for commissioning. Select a different area from the dropdown, or contact your administrator to update your permissions.

I selected "Configure Later" and got an error.

Manage access to the target area is required regardless of whether you select Configure Now or Configure Later. Ensure you have Manage access to the area before proceeding.

Last modified: 5 June 2026

Adding a Schlage device using ENGAGE

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

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

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

1. Select the site where you want to add a new ENGAGE device from the list
2. Tap the "+" button from the upper right corner of the app
3. Select the type of device you would like to add to Pure Access
    - **Note**: *Only the Schlage RC, NDE, and LE devices are currently supported in Pure Access*
4. Follow the device specific instructions to continue (NDE/LE locks will require you to physically turn and release the interior handle)
5. All devices that are powered on and not currently commissioned to an ENGAGE site will appear in the list
    a. Select the device you'd like to commission and tap continue
    b. You can find the serial number on the sticker under the battery cover of the device
6. For NDE/LE – select "**Use Default Settings**"
7. The ENGAGE app will now attempt to establish a Bluetooth connection to the lock
    a. If successful, the LED on the device will start to blink
    b. Tap "**Continue**" after confirming the correct device's LED is blinking
8. Enter a name for the device
    - Ensure device names meet Pure Access requirements:
        - 1-20 characters (Engage allows up to 25)
        - Letters, numbers, and symbols (#, -, and spaces) only
        - Cannot start or end with spaces
        - No special characters beyond those listed
9. If your Wi-Fi network is not yet saved in ENGAGE, select "**Add a New Network**" and enter your Wi-Fi settings
    - **Note**: *Leave your host configuration unchanged*

10. Tap “**Finish**” to complete the process of adding the Schlage device

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

> ! **Schlage devices are automatically added to the COMMON area upon commissioning.** Unlike Isonas devices, the ENGAGE app does not allow you to select an area during this process. To see the device in Pure Access after commissioning, your account must have at minimum **VIEW** access to the COMMON area. **MANAGE** access to the COMMON area is required to configure the device.

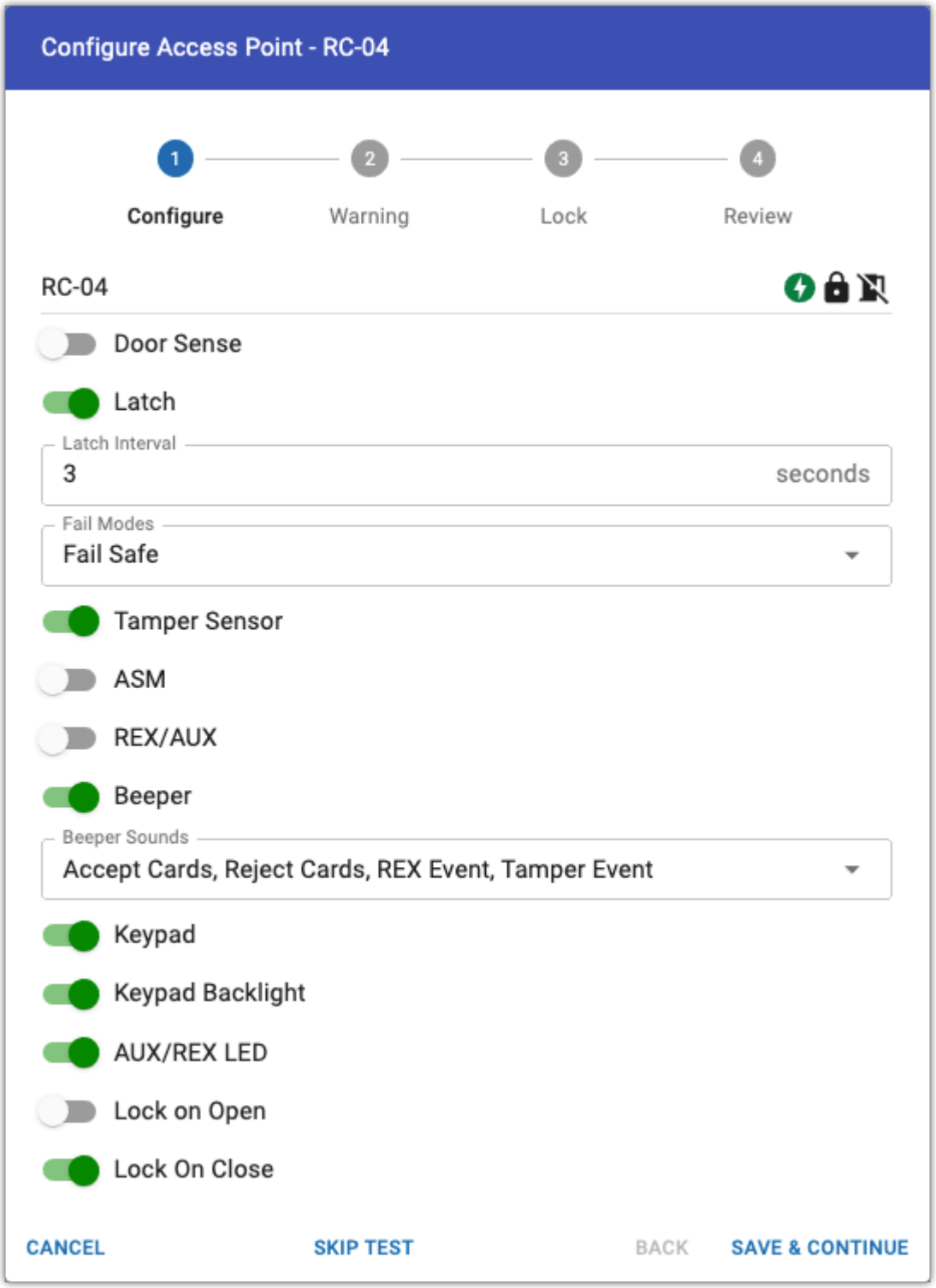
Last modified: 24 April 2026

Configuring an Access Point

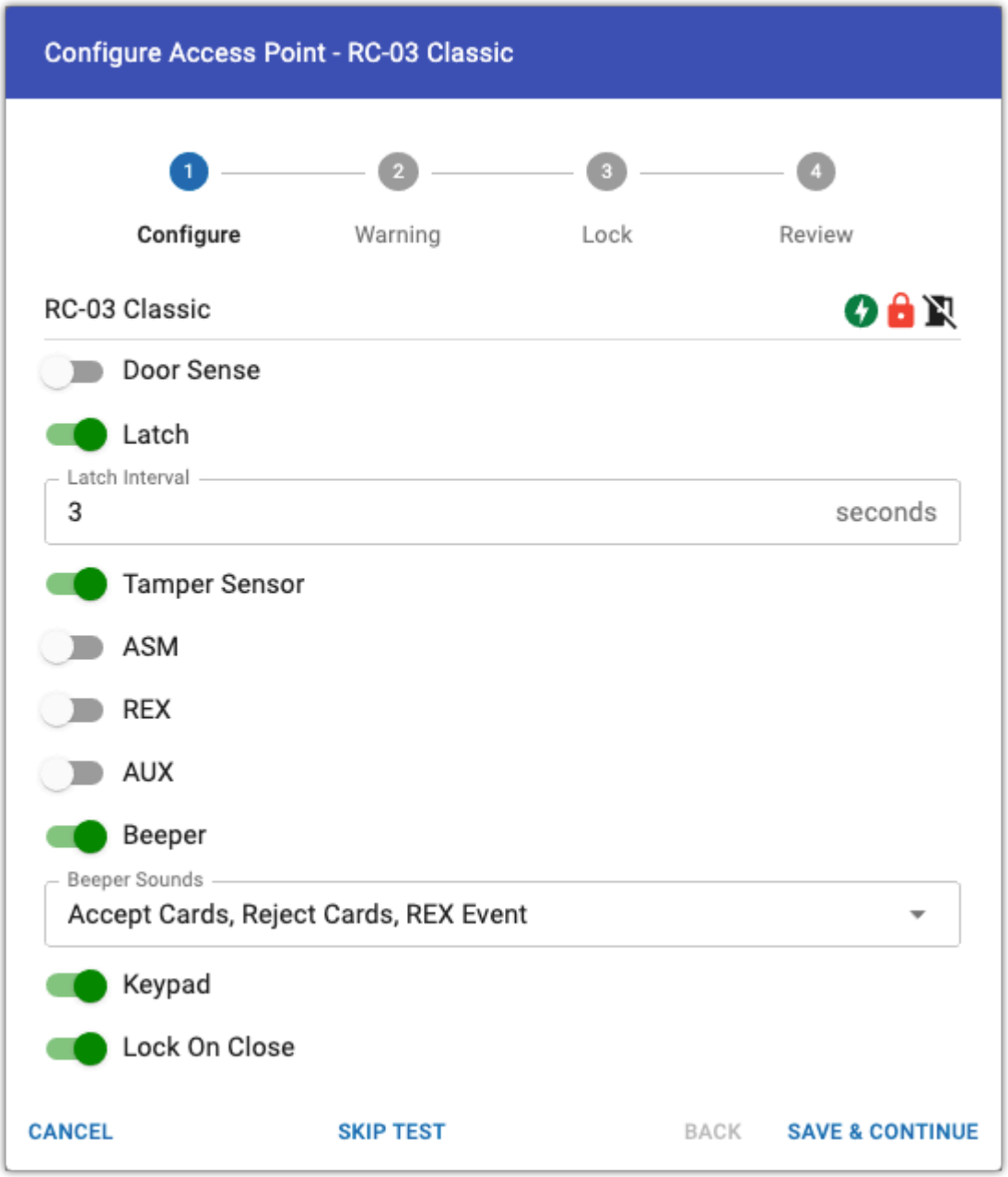
Configure Now

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

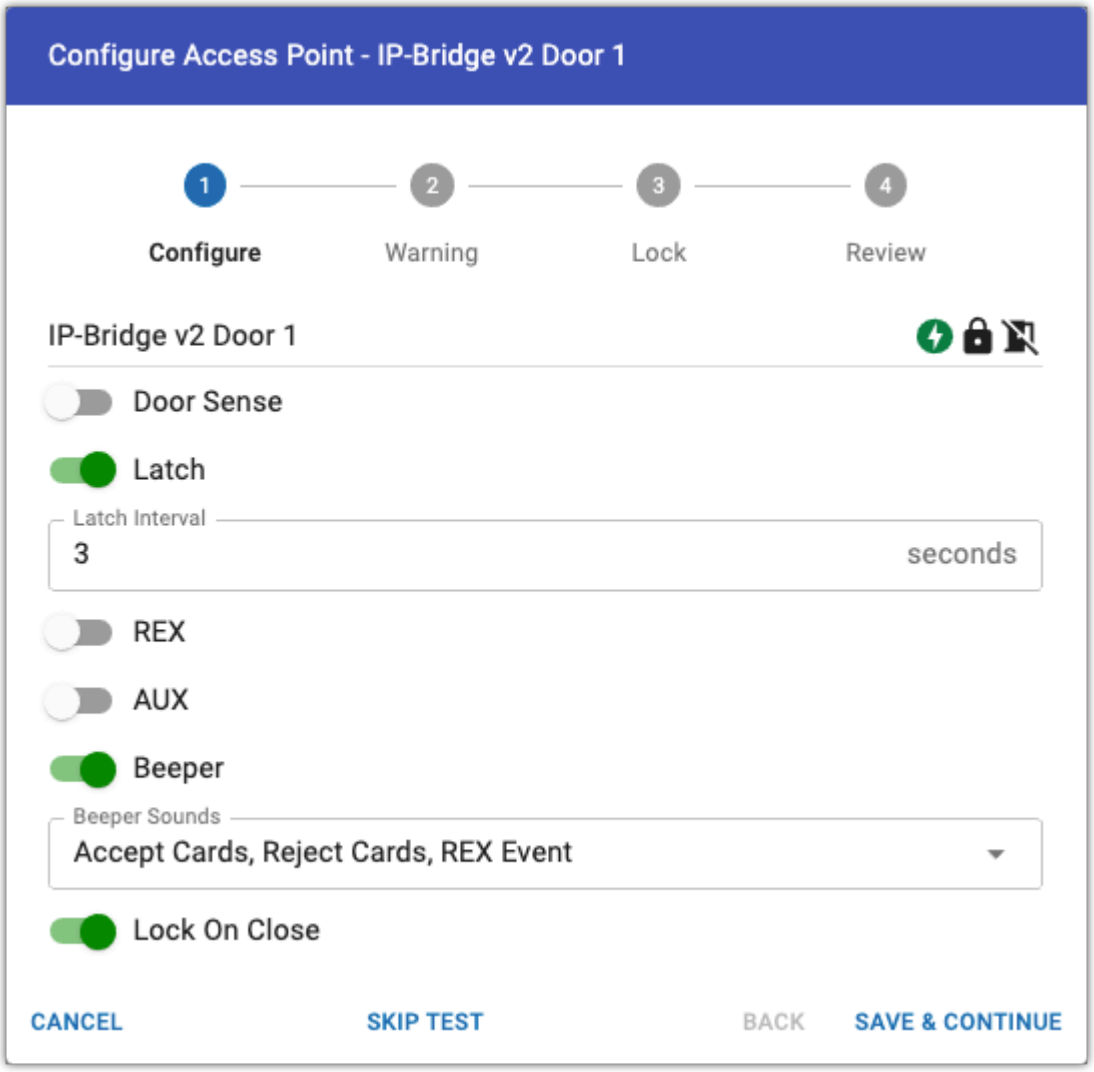
- **RC-04**


Configure Access Point - RC-04
1
2
3
4
Configure
Warning
Lock
Review
RC-04
Door Sense
Latch
Latch Interval
3
seconds
Fail Modes
Fail Safe
Tamper Sensor
ASM
REX/AUX
Beeper
Beeper Sounds
Accept Cards, Reject Cards, REX Event, Tamper Event
Keypad
Keypad Backlight
AUX/REX LED
Lock on Open
Lock On Close
CANCEL
SKIP TEST
BACK
SAVE & CONTINUE

- **RC-03**


Configure Access Point - RC-03 Classic
1
2
3
4
Configure
Warning
Lock
Review
RC-03 Classic
Door Sense
Latch
Latch Interval
3
seconds
Tamper Sensor
ASM
REX
AUX
Beeper
Beeper Sounds
Accept Cards, Reject Cards, REX Event
Keypad
Lock On Close
CANCEL
SKIP TEST
BACK
SAVE & CONTINUE

- **IP-Bridge**



Configure Later

To modify the configuration settings on a device:

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

Last modified: 26 April 2021

Configuring the Advanced Security Module (ASM)

1. Navigate to the **Access Points** page
2. Select ⋮ next to the Access Point for which you need to configure the ASM, then choose **Edit Device Settings**
3. Toggle the **ASM** slider to the on position
    a. **Note**: *When using an ASM, the **Fail Mode** must be set to "Fail Secure"*
4. Select SAVE & CONTINUE to proceed
5. Select the desired lock state (once testing is complete) then click either READY or NEXT
    - *It should be noted that once the latch test is completed, the access point will remain in the state that was selected; either Lock or Unlocked. This can result in openings being unintentionally left unsecured.*
6. Follow the prompts to configure the ASM
    a. First, factory reset the ASM by using a pin to hold the reset button down until the status light flashes green 3 times.
    b. Once the ASM has been reset, click CONTINUE
    c. An admit will be sent as a test:
        i. The reader's LED should turn green for the duration of the latch interval
        ii. The ASM's status light should turn green for the duration of the latch interval
        iii. The physical lock should unlatch for the duration of the latch interval
    d. If the admit test did not successfully unlatch the lock, click NO then follow the prompts to repeat the configuration process
7. Proceed through the tests (or click SKIP TEST), then select SAVE when finished
8. Once you have successfully paired the ASM module with the Reader Controller, send a Schedule command to the corresponding access point to set it back to Schedule.

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

process must be repeated (you may need to factory reset the ASM).

Last modified: 10 April 2026

Configuration Settings

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

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

- **Lock On Open**: enable this slider to lock the door when the door is opened (requires a door position sensor)
- **Check-In Settings** (Schlage devices communicating via WiFi Only): Use this to configure the check-in frequency*. You can use a daily schedule and have the device check in anywhere from every 1 hour to every 24 hours. You can use a weekly schedule and only have the device check in at specific times on specific days of the week.

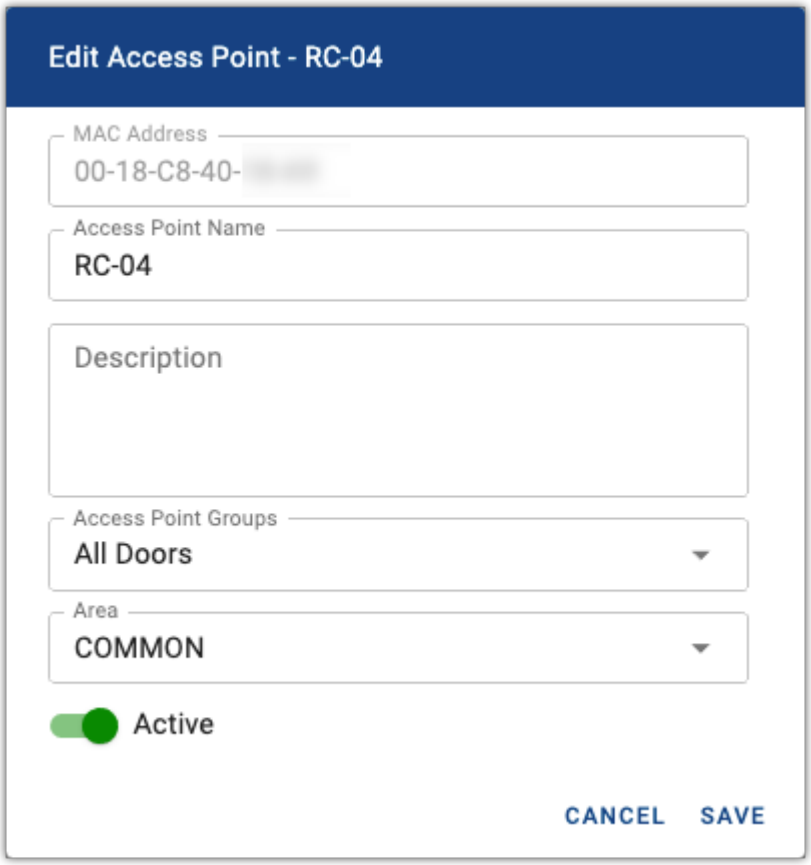
Check-In Frequency refers to how often a Schlage device will wake up and communicate with Pure Access via it's WiFi connection. When a device check-in occurs it will receive updated device settings and access control configuration from Pure Access as well as report its activity history.

Last modified: 22 June 2022

Edit Access Point

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

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



3. Here, you can see:
    - **MAC Address**
    - **Name** Ensure it meets our requirements.
        - 1-20 characters
        - Letters, numbers, and symbols (#, -, and spaces) only
        - Cannot start or end with spaces
        - No special characters beyond those listed
    - **Description**: a helpful description of the Access Point
    - **Serial Number**: this is the serial number of the physical device (Engage devices only)
    - **Access Point Groups**: you can change which Access Point Group(s) this device is associated with
    - **Area**: you can change which Area this device is associated with
4. Click SAVE to save your changes

Last modified: 18 March 2026

Deactivate Access Point

What Happens When a Device Is Deactivated

Deactivating a device does not disable credential access or suspend access rules. The device continues to operate using its onboard database. Deactivation severs the server connection only — the device cannot receive updates or sync until it is reactivated.

Behavior by Device Type

Device Type	Credential Access	Receives Server Updates	BLE / Wi-Fi Sync
Online	Physical, BLE credentials continue to work	No	N/A
Offline/Wireless (LE, LEB, NDE, NDEB)	Physical, BLEcredentials continue to work	No	Not possible while deactivated

Deactivation is a required step before deletion. To permanently remove a device, deactivate it first, then proceed to delete it.

Method 1

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

Method 2

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

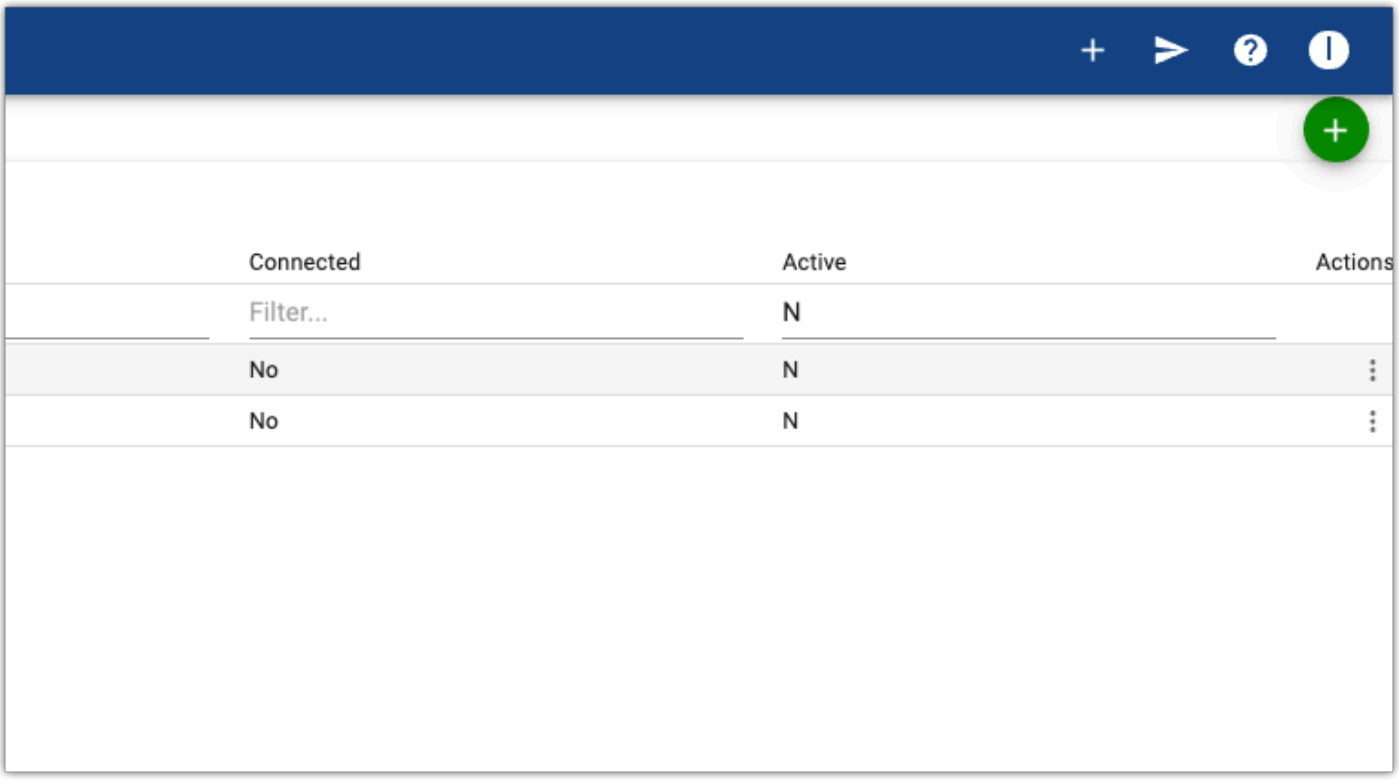
✻ Deactivating an access point will not suspend access permissions at it; grant access and auto unlock rules will continue to operate at the device according to the last compile it

processed. When an online device is deactivated it will lose connection from the server and will not be able to reconnect until it is reactivated.

Last modified: 22 June 2026

Viewing Deactivated Access Points

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



Last modified: 23 April 2021

Replacing an Access Point with Another Device

In order for a device to be replaced with another device, it will first need to be deactivated.

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

4. The **MAC Address** field can now be modified; input the MAC address of the device that will be replacing the old one. *This step is only applicable for Isonas devices (RC-03, RC-04, IP Bridge)*
5. Click SAVE

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

The following rules apply when replacing an access point by MAC address:

- RC-03 access points can only be replaced by an RC-03 device.
- IP Bridge access points can only be replaced by an IP Bridge door slot. The replacement device may have the same or a different MAC address.
- RC-04 devices can replace both RC-03 and RC-04 access points.

Last modified: 27 March 2026

Deleting an Access Point

In order for a device to be deleted from the system, it will first need to be deactivated.

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

Instructions

1. Navigate to the **Access Points** screen
2. If deleting a Schlage Device (RC, NDE, LE), click the speed dial the top right corner, and select '**Sync ENGAGE Devices**'. Select **CONFIRM**. NOTE: This step is not required when deleting an Isonas devices(RC-03, RC-04, IP Bridge)
3. From the deactivated access point you wish to delete, select the ⋮ to view more actions
4. Select **Delete Access Point**

Last modified: 5 November 2025

Access Point Groups

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

the same schedules). You can create a new Access Point Group before adding any Access Points and new Access Points can be added to or removed from the group at any time.

Last modified: 23 April 2021

Create Access Point Group

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

Last modified: 23 April 2021

Add Access Point to Access Point Group

Method 1

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

Method 2

1. Navigate to the **Access Points** page
2. From the access point you wish to add to a group, select the to view more actions
3. Select **Edit Access Point**

4. Select an access point group or multiple access point groups from the drop-down list
5. Click SAVE

Last modified: 23 April 2021

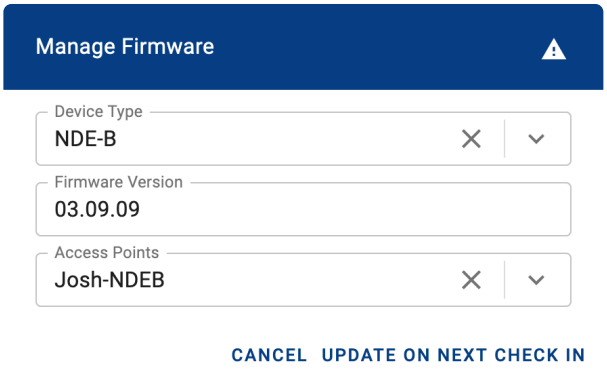
Update Firmware for Schlage Devices

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

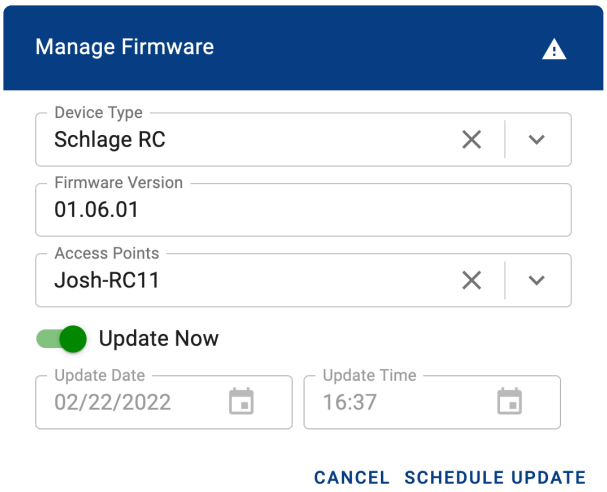
> This menu selection will only be available when a firmware update is necessary.

> NDE/LE will enter a Fail Safe mode when accepting a firmware update

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



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



Last modified: 23 October 2025

Schlage Devices and Time Changes

Isonas legacy real-time devices (Isonas RC-04 & IP Bridge) will update their time automatically as long as they are connected to the server at time of the update. If not, they need to be reconnected and a compile pushed from the web app.

As of March 2026, All Schlage devices (Control, NDE, LE, XE360, CTE, Schlage RC) automatically receive Daylight Saving Time (DST) configuration and updates. The device audits and access schedules update automatically when DST occurs – based on their designated time zone.

> If your offline or wireless devices have not been synced or been updated since before March 2026, your audits and access schedules may be operating on incorrect hours.

To confirm which devices have received the DST update, use the **Sync Report** in Zentra. Filter the report by date to identify any devices that have not synced since the DST change occurred. Devices that have not yet synced will update the next time a sync is performed.

For offline locks that have not yet synced, perform a Device Sync using the Engage Mobile App to apply the update immediately.

Last modified: 10 April 2026

What happens when you reach your license device limit

If you try to add more devices to your tenant thant your current license will allow, the software will not allow you to add the device until the license is updated or a device is deactivated.

Adding Schlage devices from the web app

When adding an RC through the Engage mobile app AND the license is at its limit

- Device will still exist in the Engage app, but will not be added to PAC.
- History event will be created showing that Device Limit Exceeded.
- The RC will attempt to connect 1x every 5 minutes moving forward, generating the Device Limit Exceeded history events every 2 days, until one of the following occurs:

1. The license type is updated to be larger. If this occurs, the device will automatically be added to the site upon its next attempt.
2. A device is removed/deactivated. If this occurs, the device will automatically be added to the site upon its next attempt.
3. It is deleted in the Engage MAPP. If this occurs, it will stop attempting to check in/connect.
4. No toasts or pop ups will be generated in the WAPP during this time.

Adding a wireless lock through the Engage mobile app (Update from Server)

When adding a wireless lock through the Engage mobile app AND the license is at its limit, upon hitting Update from Server from the MAPP, the following will occur:

- Device will still exist in the Engage MAPP, but will not be added to PAC.
- History event will be created showing that Device Limit Exceeded.
- If the user hits Update from Server multiple times, the audit will only be generated once upon the initial attempt.
- Once the license type is updated to be larger, or a device is removed/deactivated, the lock will automatically be added to PAC the next time Update from Server or Sync with Engage is initiated.
- No toasts or pop ups will be generated in the WAPP during this time.

Adding a wireless lock through the web app (Sync with Engage)

When adding a wireless lock through the Engage mobile app AND the license is at its limit, upon hitting Sync with Engage button in the Web App, the following will occur: * Device will still exist in the Engage MAPP, but will not be added to PAC.

- History event will be created showing that Device Limit Exceeded.
- If the user hits Sync with Engage multiple times, the audit will only be generated once upon the initial attempt.
- Snackbar/Toast will appear in the WAPP stating: *You have reached the maximum number of access*

points allowed for your license size. Please contact your integrator/installer to upgrade your license.

- Once the license type is updated to be larger, or a device is removed/deactivated, the lock will automatically be added to the PAC the next time Sync with Engage is pressed.

Adding legacy ISONAS devices from the web app

When adding a legacy ISONAS device via Connect Now:

- Snackbar/Toast will appear in the WAPP stating: _You have reached the maximum number of access points allowed for your license size. Please contact your integrator/installer to upgrade your license. _

When adding a legacy ISONAS device via Connect later:

- Snackbar/Toast will appear in the WAPP stating: *You have reached the maximum number of access points allowed for your license size. Please contact your integrator/installer to upgrade your license.*
- History event will be created showing that Device Limit Exceeded.

Last modified: 23 January 2026

Access Control

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

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

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

Last modified: 20 April 2021

Weekly Rules

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

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

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

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

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

In order to visualize your weekly rules better, you may want to map them out using columns:

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

Example

Rule Name	Who? *[users/user groups]*	Where? *[access points/access point groups]*	When? *[scheduled days and times]*
24/7 Admin Access	Upper Management	All Doors	24/7
IT Closet & Server Access	IT Managers	Server Room + IT Closet	M-F 5AM to 9PM

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

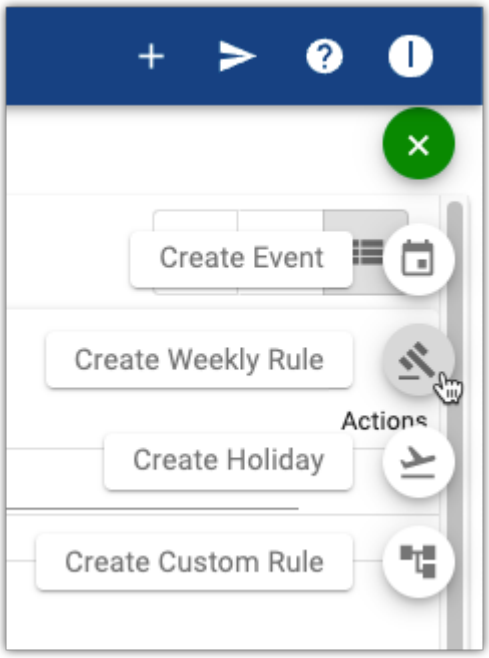
> We *highly recommend* utilizing groups (for both users and access points) when configuring any weekly rule. Assigning individual people or doors to rules adds unnecessary complexities that can put a strain on the system when compiling this data to the devices.

Last modified: 26 May 2023

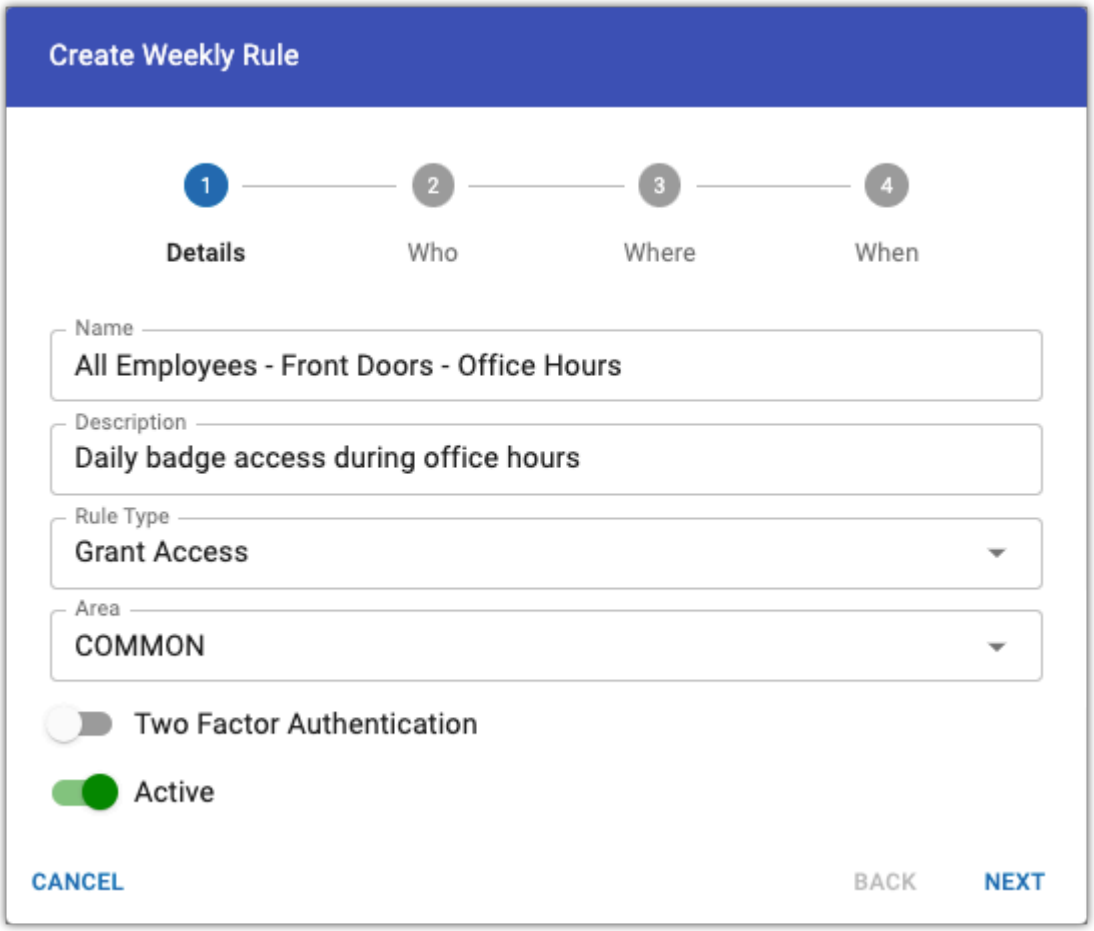
Create Weekly Rule

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

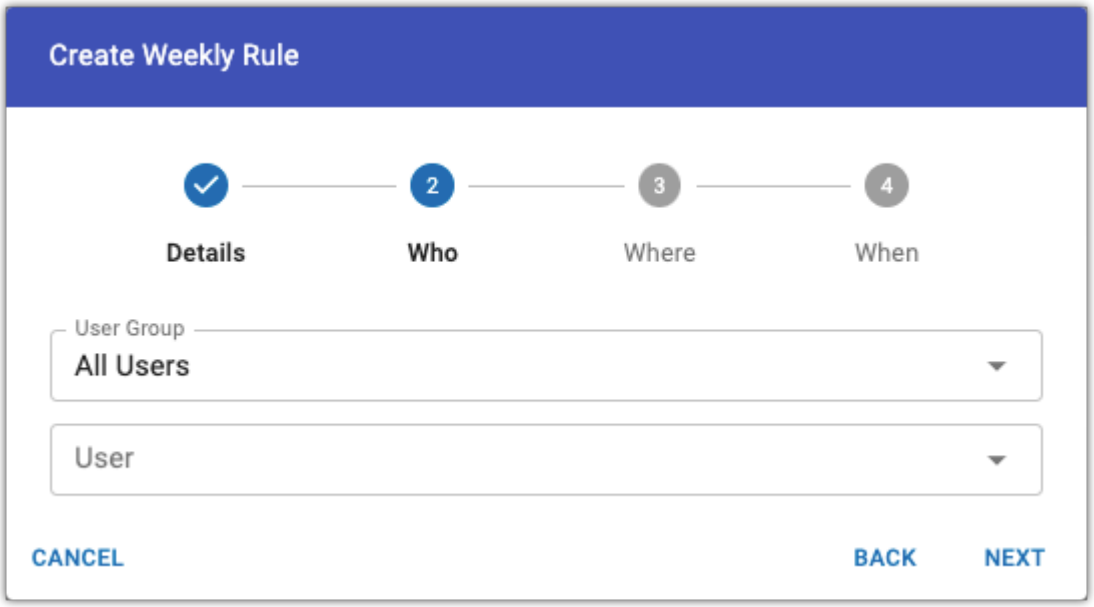
2. Hover over  and then choose **Create Weekly Rule**



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

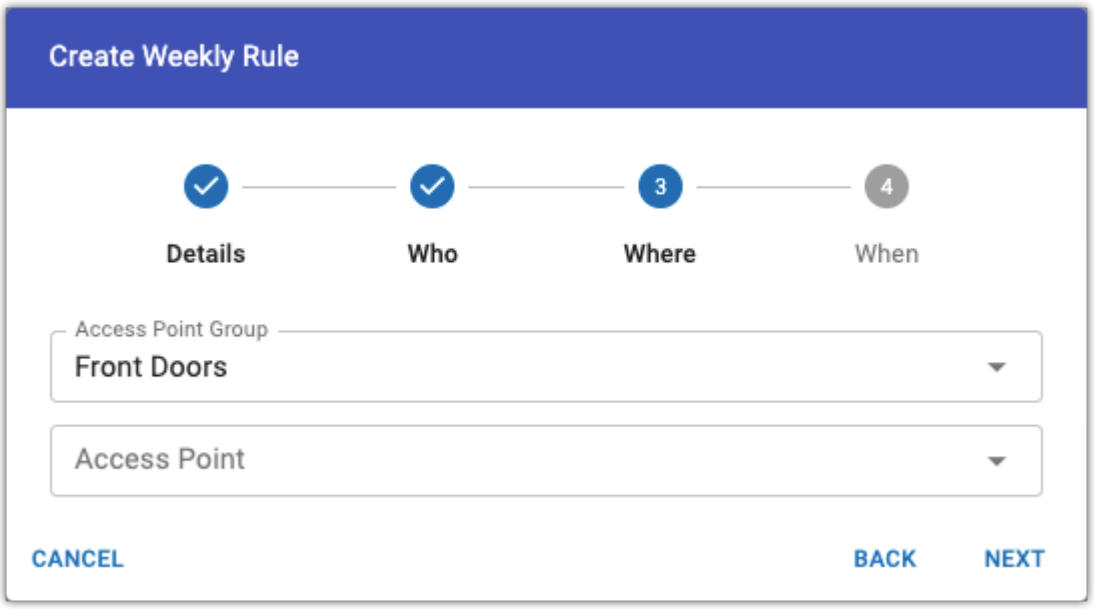


4. Choose the User Group or Users who should be included, then click NEXT



- You can use either User Groups, Users, or both (we recommend using User Groups for ease of management)

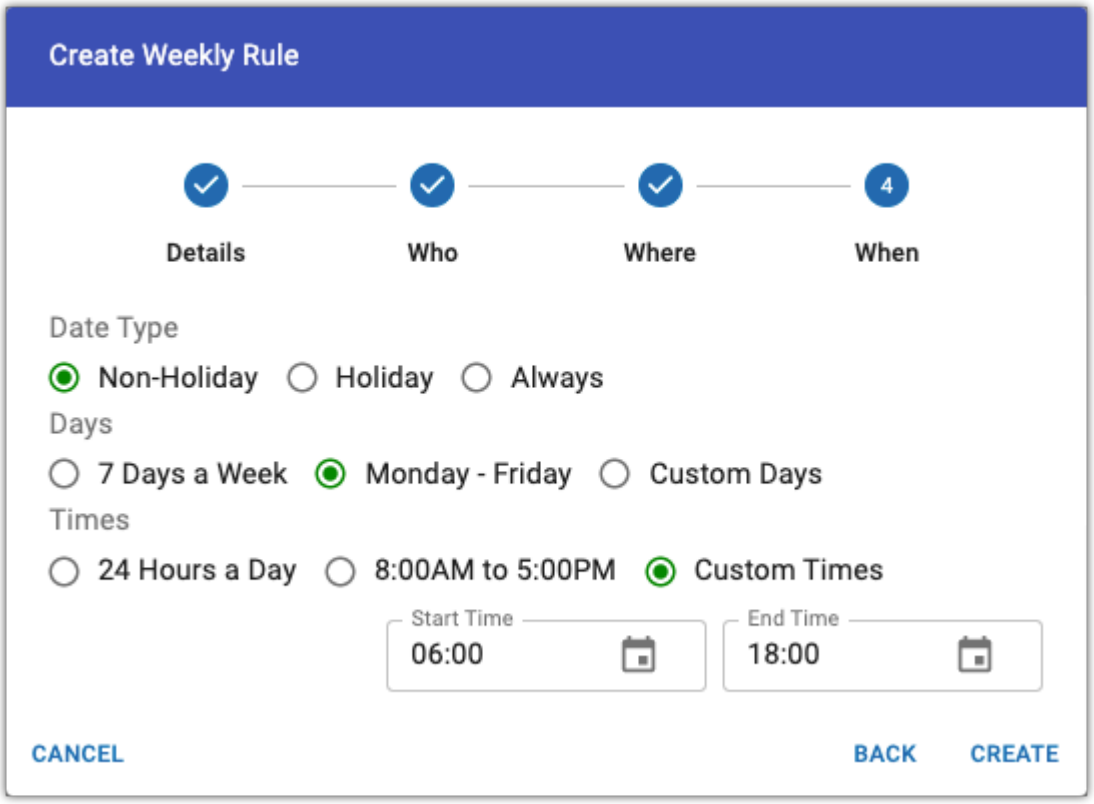
5. Choose the **Access Point Group** or **Access Point** that should be included, then click NEXT



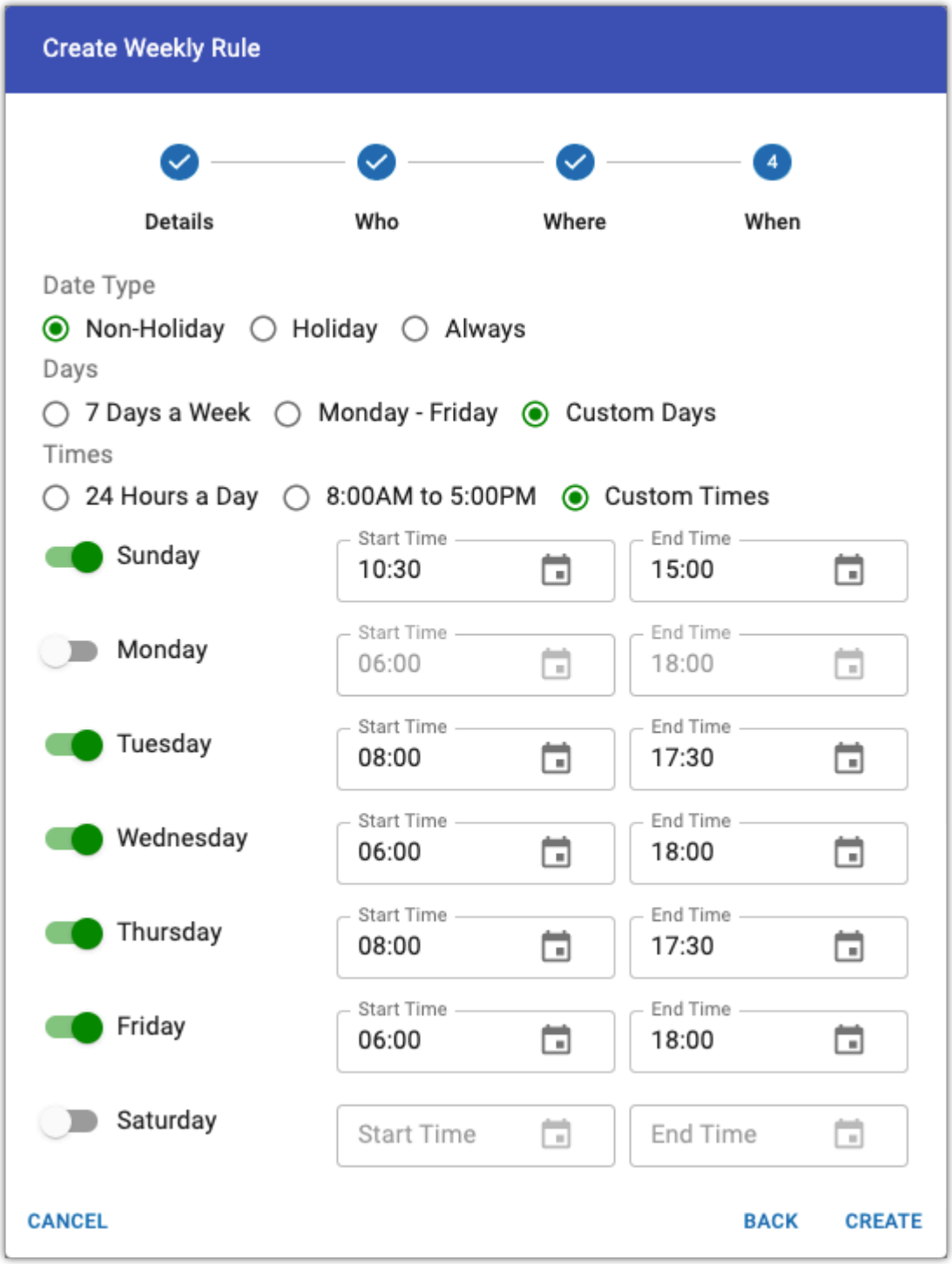
- You can use either Access Point Groups, Access Points, or both (we recommend using Access Point Groups for ease of management)

6. Choose the **Date Type** for the rule
Note: This option is not available for Engage linked sites.
   - *Non-Holiday*: the rule will be active only on non-holiday days
   - *Holiday*: the rule will be active only on days designated as Holidays
   - *Always*: the rule will be active on all days

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



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



Once the rule is created the devices need to be updated in order for those changes to go into effect

Connection Type	Devices	How to Update
Online	RC-03, RC-04, IP Bridge, Schlage RC	Send a compile from the web portal — the “compile” must complete at each device

WiFi	NDE/B, LE/B	Sync at the next scheduled WiFi sync.

Last modified: 27 April 2026

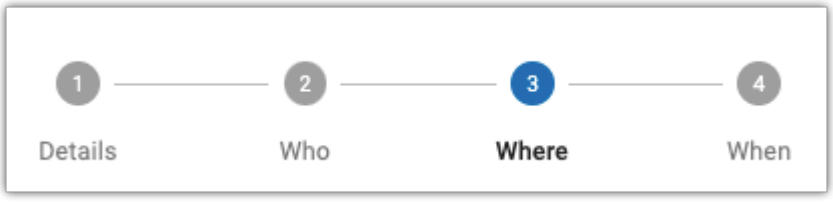
Edit Weekly Rule

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

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

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

3. Edit the rule as necessary
   - Click NEXT to move to the next screen
   - You can skip to any of the pages by clicking either **Details**, **Who**, **Where**, or **When**



4. Click SAVE when you are finished

Once the rule is edited. the devices need to be updated in order for those changes to go into effect

Connection Type	Devices	How to Update

Online	RC-03, RC-04, IP Bridge, Schlage RC	Send a compile from the web portal — the “compile” must complete at each device
WiFi	NDE/B, LE/B	Sync at the next scheduled WiFi sync.

Last modified: 27 April 2026

Deactivate Weekly Rule

List View

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

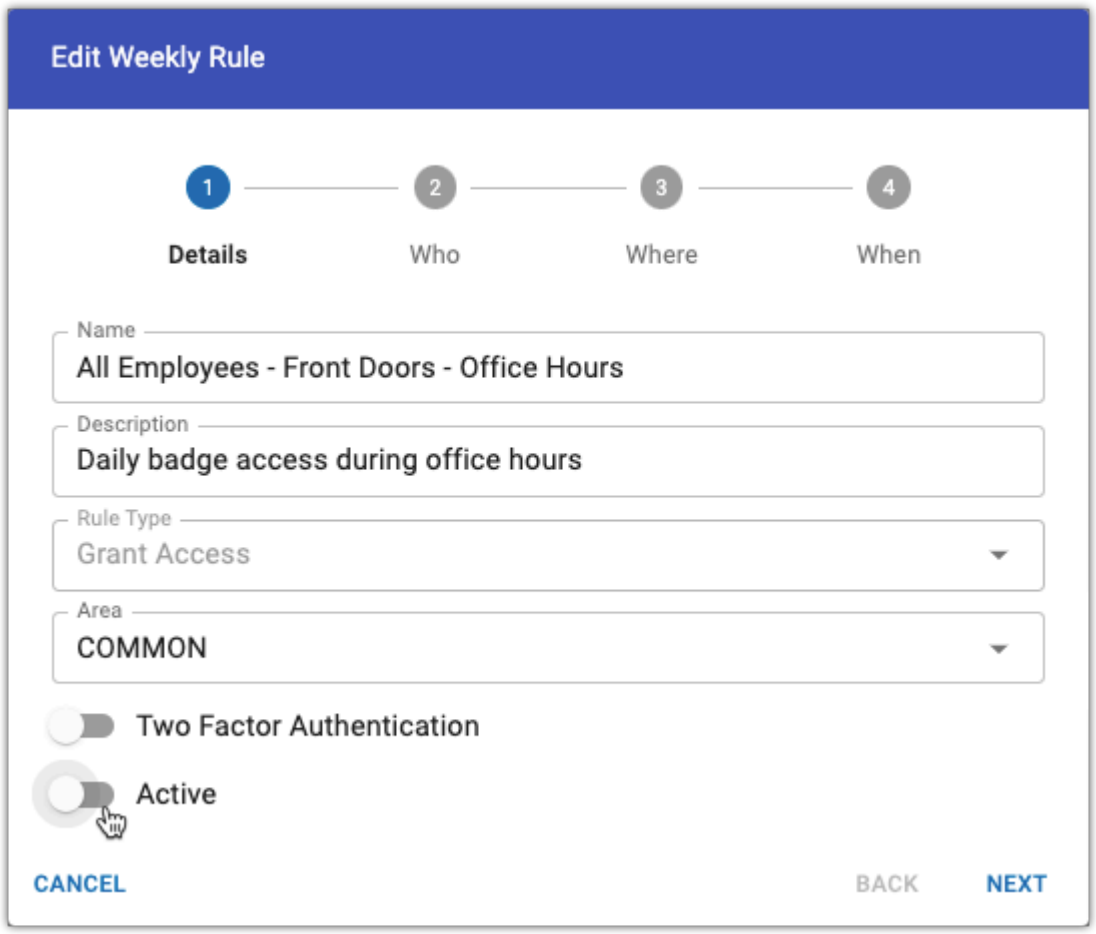
2. Click to enter list view
3. In-line with the rule you wish to deactivate, click to open the action options
4. Select **Deactivate**

Weekly View

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

2. From the **weekly view** ( ), locate the rule you wish to deactivate
3. Click on the rule to bring up the information pop-out, then click

4. Select **Details**



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

Once the rule is edited. the devices need to be updated in order for those changes to go into effect

Connection Type	Devices	How to Update
Online	RC-03, RC-04, IP Bridge, Schlage RC	Send a compile from the web portal — the “compile” must complete at each device
WiFi	NDE/B, LE/B	Sync at the next scheduled WiFi sync.

Last modified: 27 April 2026

Events

In addition to your normal weekly schedules, you may wish to set up events. **Events** are used to override weekly rules. An event can be set for a minimum of one minute up to an entire day.

Event Types

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

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

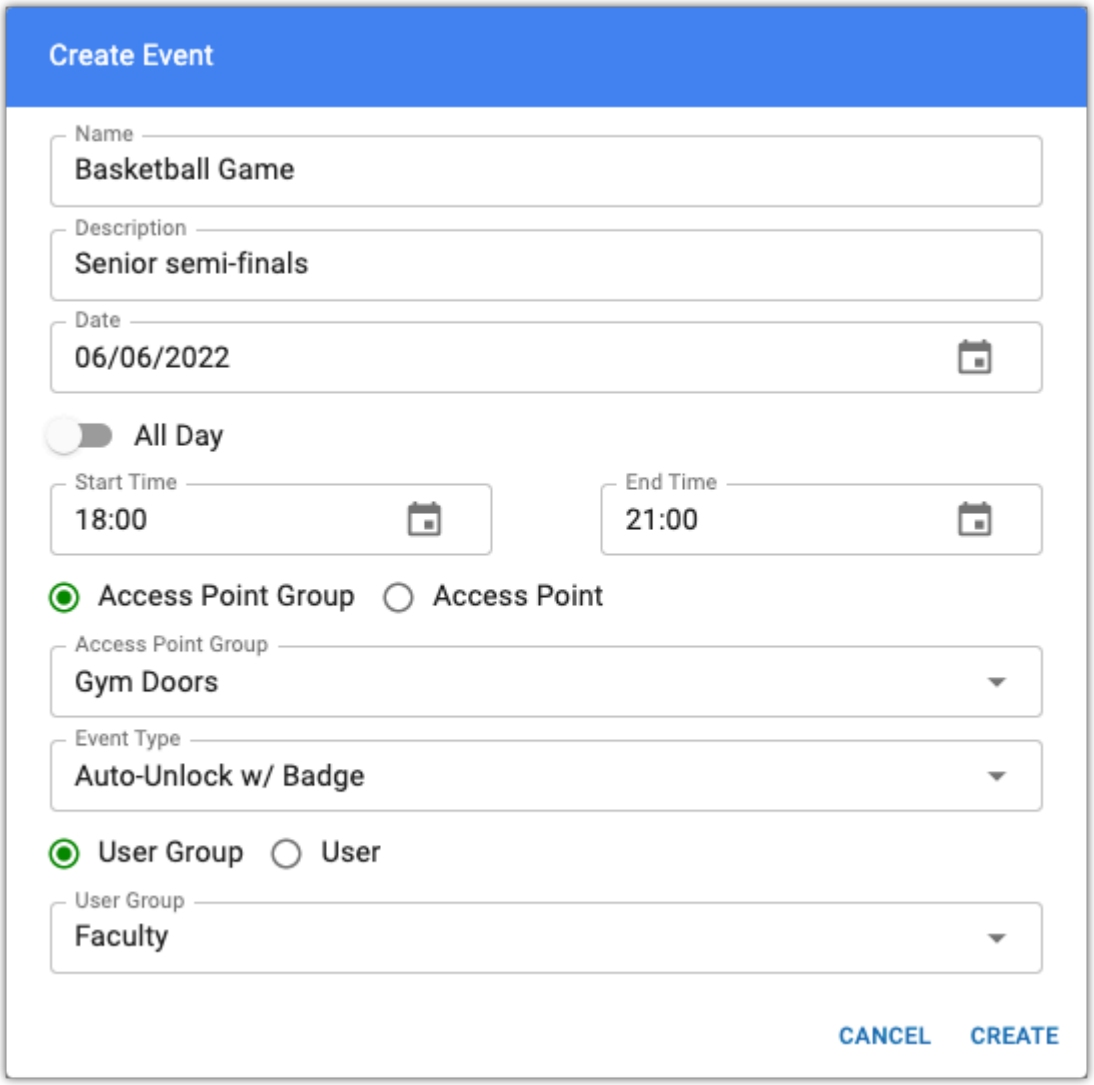
Please note that the "**Auto-Unlock w/ Badge**" event type is not supported by Engage devices.

Last modified: 3 May 2021

Create Event

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

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



- **Name**: name of the event
- **Description**: a description of the event (optional)
- **Area**: choose an area (if applicable)
- **Date**: the day the Event should be active
- **Start Time/End Time** or **All Day** toggle: the start and end times for the event or toggle the event to last all day
- **Access Point Group** or **Access Point** radio buttons: choose one of the radio buttons, as appropriate
- **Access Point Group** or **Access Point** drop-down: choose the appropriate access point(s) or group(s)
- **Event Type**: choose the appropriate Event Type

4. Click CREATE

Last modified: 27 April 2021

Edit Event

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

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

Last modified: 20 February 2026

Custom Rules

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

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

Example:

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

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

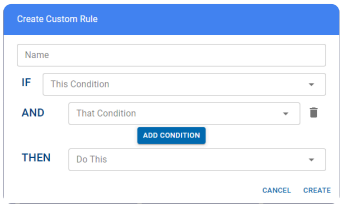
> **Custom Rule** functionality requires an active connection to the Pure Access software. If an ISONAS device is offline or disconnected, custom rules associated with this device will not be triggered.

Last modified: 26 February 2021

Create Custom Rule

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

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



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

3. Click 

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

Last modified: 26 February 2021

Custom Rule Conditions

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

IF

- An alert is present at an access point
- There is an unauthorized open alert

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

AND

- At a particular door/group of doors
    - Access Point Group
    - Access Point
- To a particular person/group of people
    - User Group
    - User
- During These times
    - Days of the week
    - Start Time
    - End Time
- Not during these times
    - Days of the week
    - Start Time
    - End Time
- When a door is in lock down
- When a door is in X status
    - Door Status

THEN

- Send an email to a specified person
    - Email Users

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

Last modified: 26 February 2021

Holidays

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

✻ If an access point is following a weekly rule that is configured to run “Always”, the door will follow this rule on days set as a **Holiday** in the tenant.

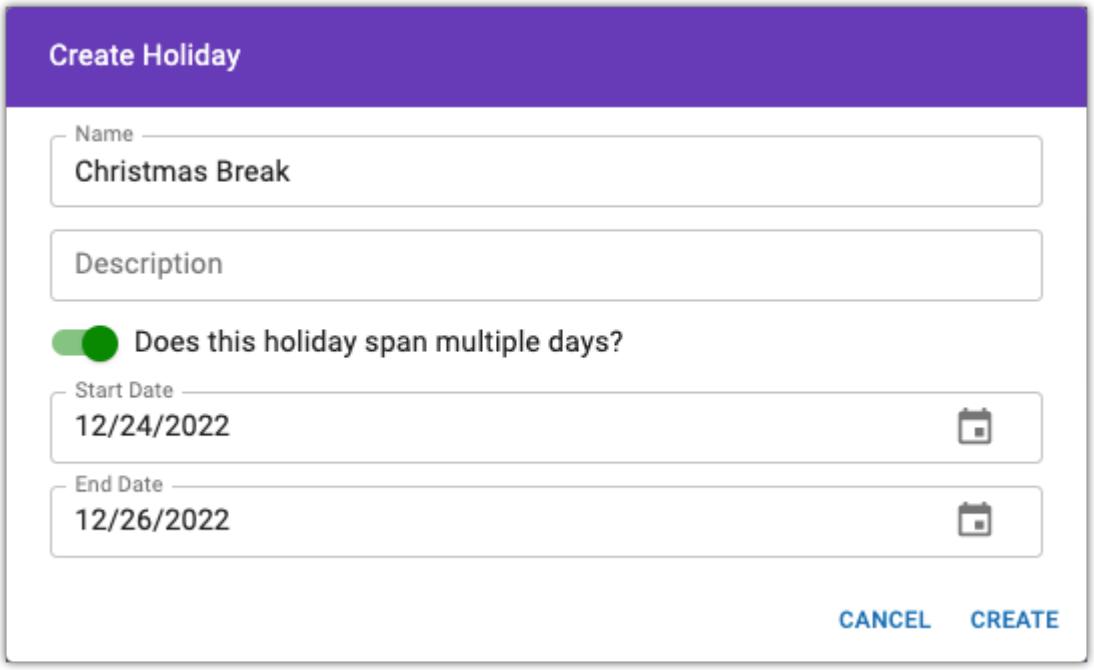
! Holidays are not supported by **Engage** devices and cannot be used within Engage-enabled tenants at this time.

Last modified: 3 May 2021

Create Holiday

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

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



   - **Name**: name of the holiday
   - **Description**: a description of the holiday (optional)
   - Toggle the slider for **Does this holiday span multiple days?** if the holiday lasts more than one day
   - Choose the day(s) for the holiday from the calendar(s)
4. Click CREATE

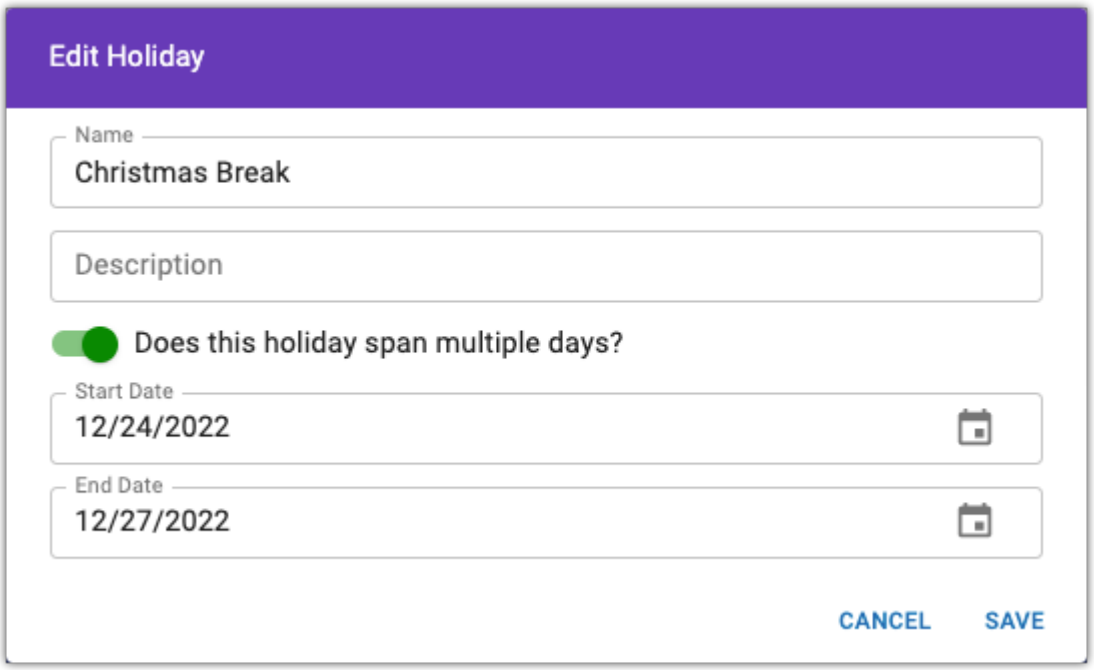
> ! Holidays are not supported by **Engage** devices and cannot be used within Engage-enabled tenants at this time.

Last modified: 3 May 2021

Edit Holiday

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

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



4. Click 

when finished

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

Last modified: 20 February 2026

Schedule Date Types

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

Last modified: 19 February 2021

Reports

There are a variety of reports that can be utilized within Pure Access. Depending on the report being run, they can be sorted by start date and end date, filtered by users, access points, event types, badge information, and/or areas.
All reports can be exported as a .PDF or .CSV for further analysis. In addition, each column can be sorted alphabetically (ascending/descending) by selecting the headers.

1. Navigate to the **Reports** page

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

5. To download this information, click 

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

Types of reports:

- Access Point Groups Report
- Access Point Permissions Report
- Access Points Report
- History Report
- Holidays Report
- User Attendance Report
- User Export Report
- User Group Attendance Report
- User Group Permissions Report
- User Groups Report
- User Permissions Report

- Users Report

Last modified: 19 April 2021

Access Point Groups Report

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

This report contains the following information:

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

This report can be filtered by:

- *Access Point Groups*
- *Areas*

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

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

Last modified: 19 April 2021

Access Point Permissions Report

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

This report contains the following information:

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

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

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

Last modified: 19 April 2021

Access Points Report

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

This report contains the following information:

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

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

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

Last modified: 19 April 2021

History Report

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

This report contains the following information:

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

This report can be filtered by:

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

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

! Activity history data is removed after two years. Historical logs older than two years will be inaccessible.

Last modified: 1 August 2024

Holidays Report

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

This report contains the following information:

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

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

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

Last modified: 19 April 2021

User Attendance Report

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

This report contains the following information:

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

This report can be filtered by:

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

Example

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

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

Last modified: 19 April 2021

User Export Report

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

This report contains the following information:

- *First Name*
- *Last Name*
- *When the user was created (date and time)*
- *Email address (notification email)*

- *Area*
- *Employee ID*
- *User defined fields*

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

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

Pure Access Manager

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

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

Last modified: 19 April 2021

User Group Attendance Report

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

This report contains the following information:

- *User group name*
- *Name of user*
- *Time in*

- *Time out*
- *Total (amount of time)*

This report can be filtered by:

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

> ! Please note that deactivated users will also appear in this report.

Example

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

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

Last modified: 28 October 2024

User Group Permissions Report

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

This report contains the following information:

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

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

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

Last modified: 19 April 2021

User Groups Report

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

This report contains the following information:

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

This report can be filtered by:

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

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

Last modified: 19 April 2021

User Permissions Report

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

This report contains the following information:

- *Name of user*
- *Access point name(s)*
- *Rule name and type*

- *Day(s) rule is active*
- *Start time of the rule*
- *End time of the rule*

This report can be filtered by users.

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

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

Last modified: 19 April 2021

Users Report

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

This report contains the following information:

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

This report can be filtered by:

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

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

Last modified: 19 April 2021

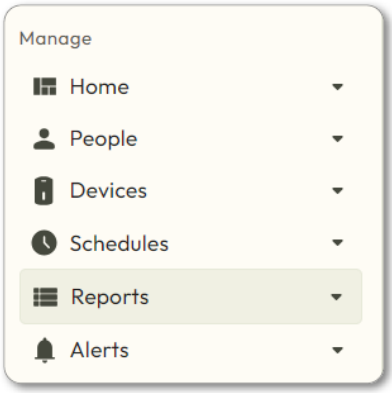
Sync Report

The Sync Report allows property staff and integrators to identify which devices on a property have or have not been successfully synced since a specified date and time. This report is useful in a variety of situations, including:

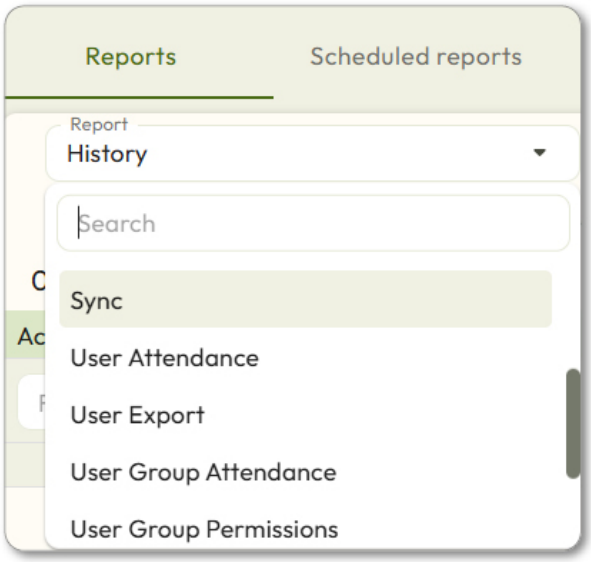
- Tracking sync progress after a lost master credential when syncing has been interrupted.
- Monitoring Wi-Fi devices to confirm they are checking in on schedule.
- Verifying that all devices have been synced following a migration from Engage to Zentra.

Running the Sync Report

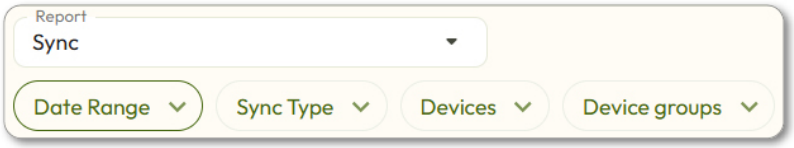
1. Navigate to the **Reports** page.



2. Choose **Sync Report** from the Report drop-down menu.



3. Set your desired filters from the drop-down boxes (see “Filters” below).



4. Click the **Run Report** button.
5. To download the report, click the download icon and select either **Download as CSV** or **Download as PDF**.

Filters

The Sync Report can be filtered by the following:

- **Start Date & Time** — Select the date and time to use as the starting point for the report. The report will evaluate syncs relative to this point.
- **Sync Type** — Filter results by sync method:
  - **Not Synced** — Lists devices that have HAVE NOT been successfully synced via BLE or Wi-Fi since the selected date and time.
  - **Wi-Fi** — Lists devices that HAVE been successfully checked in via Wi-Fi since the selected date and time.
  - **BLE** — Lists devices that HAVE been successfully synced via BLE since the selected date and time.
- **Devices** — Filter by one or more individual devices.
- **Device Group** — Filter by one or more device groups.
- **Area** — Filter by area, consistent with other reports in Zentra.

Report Results

The report displays a list of devices matching your selected filters and report logic. If a device was synced multiple times since the selected start time, the most recent successful sync time will be displayed.

- **Device Name**
- **Device Type**
- **Last Sync Time** (most recent sync since the selected start date/time, if applicable)
- **Sync Type** (Wi-Fi or BLE)
- **Area**

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

Scheduling the Sync Report

The Sync Report CANNOT currently be configured as a Scheduled Report, allowing it to be delivered automatically by email on a recurring basis. This will be addressed and fixed in an upcoming release.

Last modified: 11 March 2026

Settings

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

- Tenant Information
- Integrator Information
- Global Settings
- Areas
- Credential
- Active Directory
- User Defined Fields
- API

Last modified: 26 February 2021

Tenant Information

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

- License Type
- License Key
- License Expiration Date

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

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

- Notes

Last modified: 22 February 2021

Integrator Information

The **Integrator** is the person or entity who set up and maintains your Pure Access system. Their information should be kept up-to-date.

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

If the **Integrator Information** is not completed, contact support for help.

Last modified: 27 March 2026

Global Settings

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

Changing settings on this page will affect site operation. Make sure you understand these settings before making changes.

Default PIN Length

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

Re-lock Time

This setting controls the default time of day that ISONAS devices will re-lock if they were left unlocked by a toggle credential. Devices unlocked by a command, event, weekly rule, or custom rule will not be relocked by this setting. Schlage devices will not be re-locked by this feature.

- Note: when a re-lock does occurs, no corresponding history event is generated.

Timezone

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

Access Point Encryption

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

Two-Factor Authentication

Last modified: 24 April 2026

Two-Factor Authentication

Two-Factor Authentication adds an additional layer of security for important points in your access control system. Two factor is compatible with the following hardware devices: Schlage RC, 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.

Last modified: 18 December 2023

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.

Last modified: 26 February 2021

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.

Last modified: 26 February 2021

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.

Last modified: 26 February 2021

Configuration Process

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

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

Last modified: 3 May 2021

Enable Two-Factor Authentication

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

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

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

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

Two Factor is available for the following firmware versions:

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

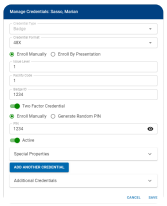
Before globally disabling two-factor, you'll need to ensure that all two-factor rules are removed from Pure Access.

Last modified: 3 May 2021

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.

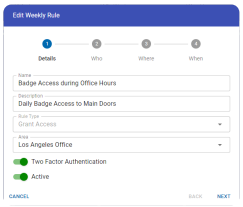
To enhance the security of the two-factor system, you will be unable to reveal the configured PIN once it has been saved.

Last modified: 26 February 2021

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.

Last modified: 26 February 2021

Two-Factor History Events

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

Two-factor history events:

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

Credential 2 Rejected – Device in Lockdown	*Lockdown (2)*	has been denied due to access point being in lockdown.
Two-Factor – Credential 2 Rejected – Two-Factor Timeout	*Denied – Timeout (2)*	The second credential in a two-user or two-user card and PIN process has been denied due to reaching the configurable timeout interval.
Two-Factor – Credential 2 Rejected – Two-Factor Process Error	*Denied – Process Error (2)*	The second credential in a two-user or two-user card and PIN process has been denied due to a process error (ie presenting a badge when the reader is expecting a PIN or presenting the same badge twice.)
Two-Factor – Credential 2 Rejected – Bad PIN	*Denied – Bad PIN (2)*	The second credential in a two-user or two-user card and PIN process has been denied due to an invalid two-factor PIN.
Two Factor – Accepted (Card/PIN)	*Approve (Card/PIN)*	Valid credential and PIN presentation. Access granted.
Two-Factor – Timeout in PIN Entry (Card/PIN)	*Denied – Timeout (Card/PIN)*	Denied due to reaching the configurable timeout interval during the card and PIN procedure.
Two-Factor – Process Error (Card/PIN)	*Denied – Process Error (Card/PIN)*	Denied due to a process error during the card and PIN procedure.
Two-Factor – Bad PIN (Card/PIN)	*Denied – Bad PIN (Card/PIN)*	Denied due to an incorrect PIN during the card and PIN procedure.

Last modified: 26 February 2021

Areas

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

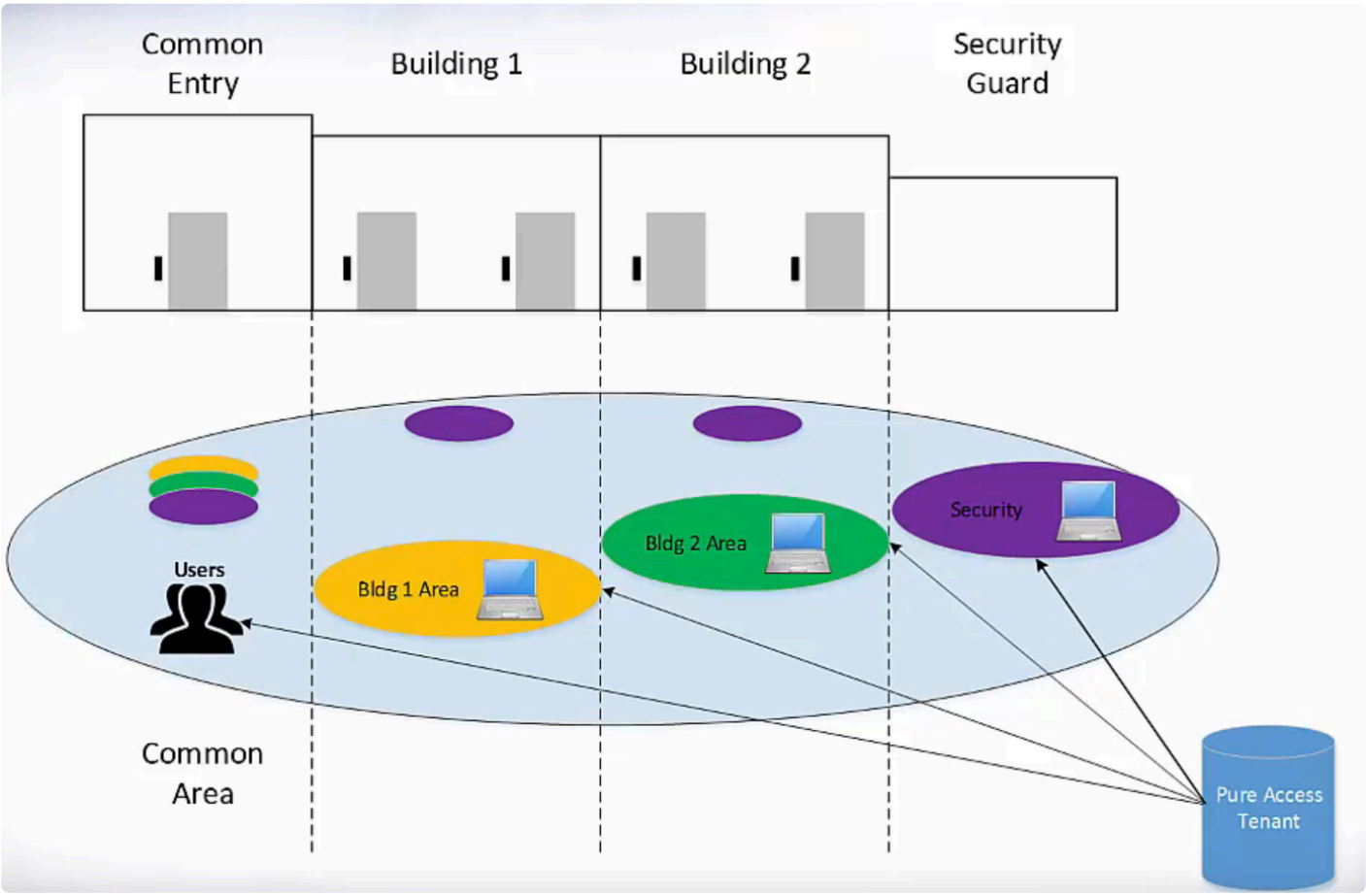
- Areas *are not* used for designating access control; configuring them is optional.
- Areas should only be used if administrative segmentation is needed to protect the security of the system.
- Areas should be planned before the system is fully configured since every object in a Pure Access tenant must be assigned to an area (by default, everything will be assigned to a “**COMMON**” area).

Last modified: 22 November 2024

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 more than one building, especially if those buildings are in different time zones.

Last modified: 22 November 2024

Areas — Roles, Permissions, and Setup Rules

What Areas Do (and Do Not) Control

Areas are **administrative containers** only. They determine which administrators can see and manage which objects in the software. They have no effect on which doors a badge holder or mobile credential user can access — that is controlled by user groups and schedules.

How Areas Affect Each Role

Role	Area Access	Notes
Integrator	Full access to all areas — automatic	No assignment needed. An Integrator always sees every area and can commission devices, create users, and make changes anywhere on the site.
Administrator	Only areas explicitly assigned	Must have Manage access on an area to create or modify any object in that area, including commissioning locks.
Human Resources	No area management	Can view and modify users but cannot view or change area settings.
Operator	No area management	Read-only access to users, events, dashboards, alerts, and reports only.
Resident / Resident with NFC	No web access	Areas are not relevant to this role.

Custom roles and areas

- A Custom role user's area access depends on which permissions are enabled for that role.
  - If the Areas permission is enabled with Modify, the user must still be explicitly assigned to each area, the same as an Administrator.
  - If the Areas permission is not enabled, the user has no area management access.
- A Custom role user can also only grant area access to others up to the level they themselves hold — they cannot assign access to an area they do not have, or at a level higher than their own.

Area Access Levels

When assigning a web access user to an area, three access levels are available. The area access level works **together** with the user's web access permissions — it does not replace them. What a user can actually do is the intersection of both settings.

Level	What It Means
None	The user has no access to objects assigned to that area, regardless of their web access permissions.
View	The user can view objects assigned to that area, in accordance with their web access permissions.
Manage	The user can view and modify objects assigned to that area, in accordance with their web access permissions.

> ! To commission a lock to an area, the web access user must have **Manage** access to that area. View access is not sufficient — the user will not be able to add or configure devices.

> ! A web access user who logs in and sees nothing has likely not been assigned any area access. Every web access user must be assigned at least View access to COMMON — or they will see a blank site after logging in.

The COMMON Area

Every site starts with a single area called **COMMON**. By default, every object in the site — devices, users, user groups, schedules, rules, dashboards, and events — is automatically assigned to COMMON.

- If a site uses only the COMMON area, no area assignment decisions are needed.
- If additional areas are added, every new object must be explicitly assigned to one of the existing areas upon creation.

Most sites only need the COMMON area. Adding additional areas is optional and should only be done when different administrators need to be restricted to managing separate parts of the system. Speak with your integrator before implementing multiple areas.

Last modified: 5 June 2026

How to Configure Areas

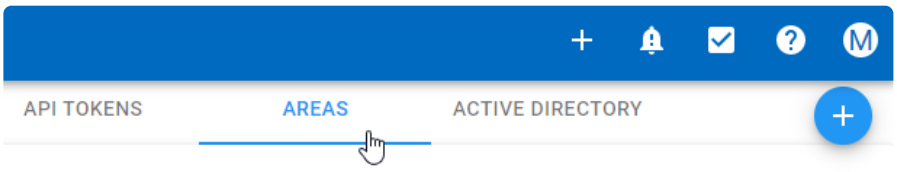
By default, every Pure Access tenant is automatically configured with a single area named “**COMMON**”. In this default state, every object in the tenant (groups, access points, users, schedules, etc.) is automatically added to the COMMON area.

Once another area is added to the system, anything created in the system will need to be explicitly designated to one of the existing areas upon creation/modification.

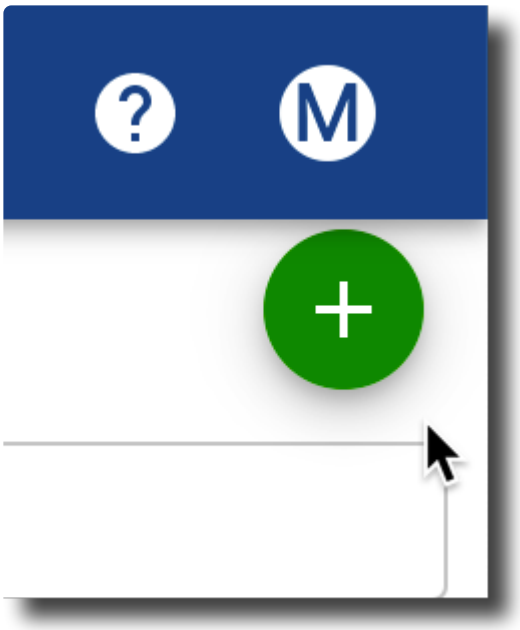
Creating an Area

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

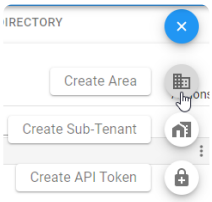
2. Select the **Areas** tab.



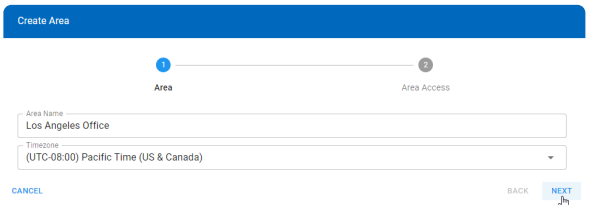
3. Hover over the plus sign to reveal the menu. You may need to scroll to the right to see this menu.



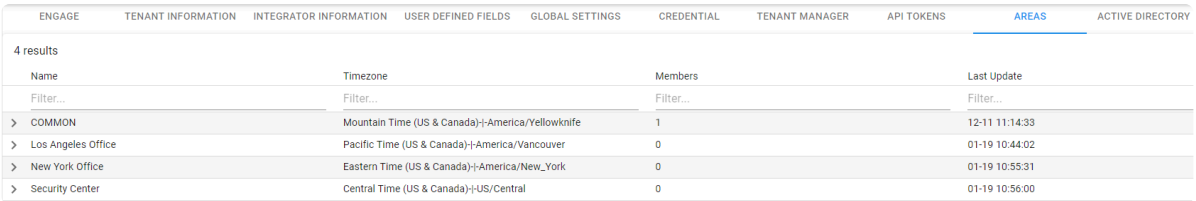
4. Click **Create Area**.



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



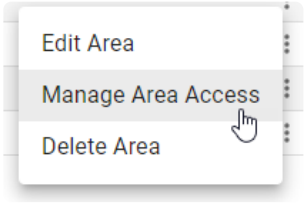
For the below example, we've created three new areas in addition to COMMON – *Los Angeles Office*, *New York Office*, and *Security Center*.



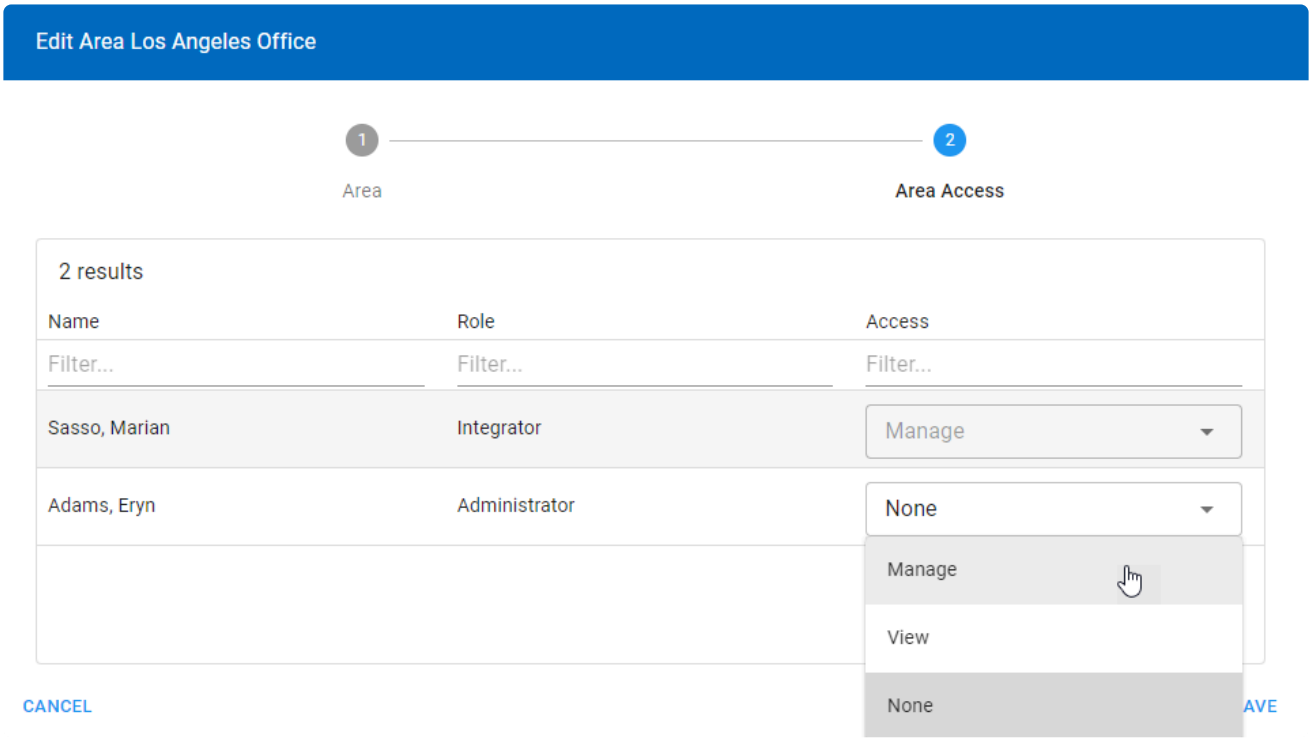
Assign Administrators to an Area

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

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



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



> Users must have web access granted before they can be assigned as an administrator. See Setting Up Web Access for a User.

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

Last modified: 22 November 2024

Assigning Dashboards to an Area

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

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

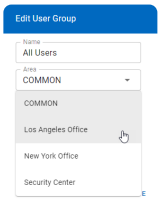
Last modified: 1 March 2021

Assigning Groups to an Area

User Group

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

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

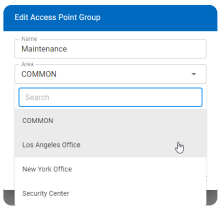


4. Then click SAVE.

Access Point Group

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

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



4. Then click SAVE.

Last modified: 1 March 2021

Assigning Access Points to an Area

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

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

Last modified: 26 February 2021

Assigning Users to an Area

1. Edit a User.

2. Choose the appropriate Area from the **Area** drop-down menu.
3. Click SAVE

Last modified: 26 February 2021

Assigning Weekly Rules to an Area

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

Last modified: 26 February 2021

Assigning Events to an Area

1. Edit an Event.
2. Choose the appropriate Area from the **Area** drop-down menu.
3. Click SAVE

Last modified: 26 February 2021

Step by Step Guide to using Areas

The attached document can be a useful guide when using Areas to allow management of distinct Access Points (doors) and Users (people) and assigning login rights to Users.

Areas in Pure Access

Last modified: 11 December 2025

Managing Area Administrators

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

1. Enable Web Access
2. Grant Area access to the User:

a. Click from the left-side menu.

b. Click **Areas** from the top navigation.

c. Click next to the Area to which you want to add the Administrator.

d. Select the level of **Access** you want to grant from the drop-down box next to the User name.

- **Manage**: make changes in the system
- **View**: view settings in the system
- **None**: no access

e. Click SAVE.

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

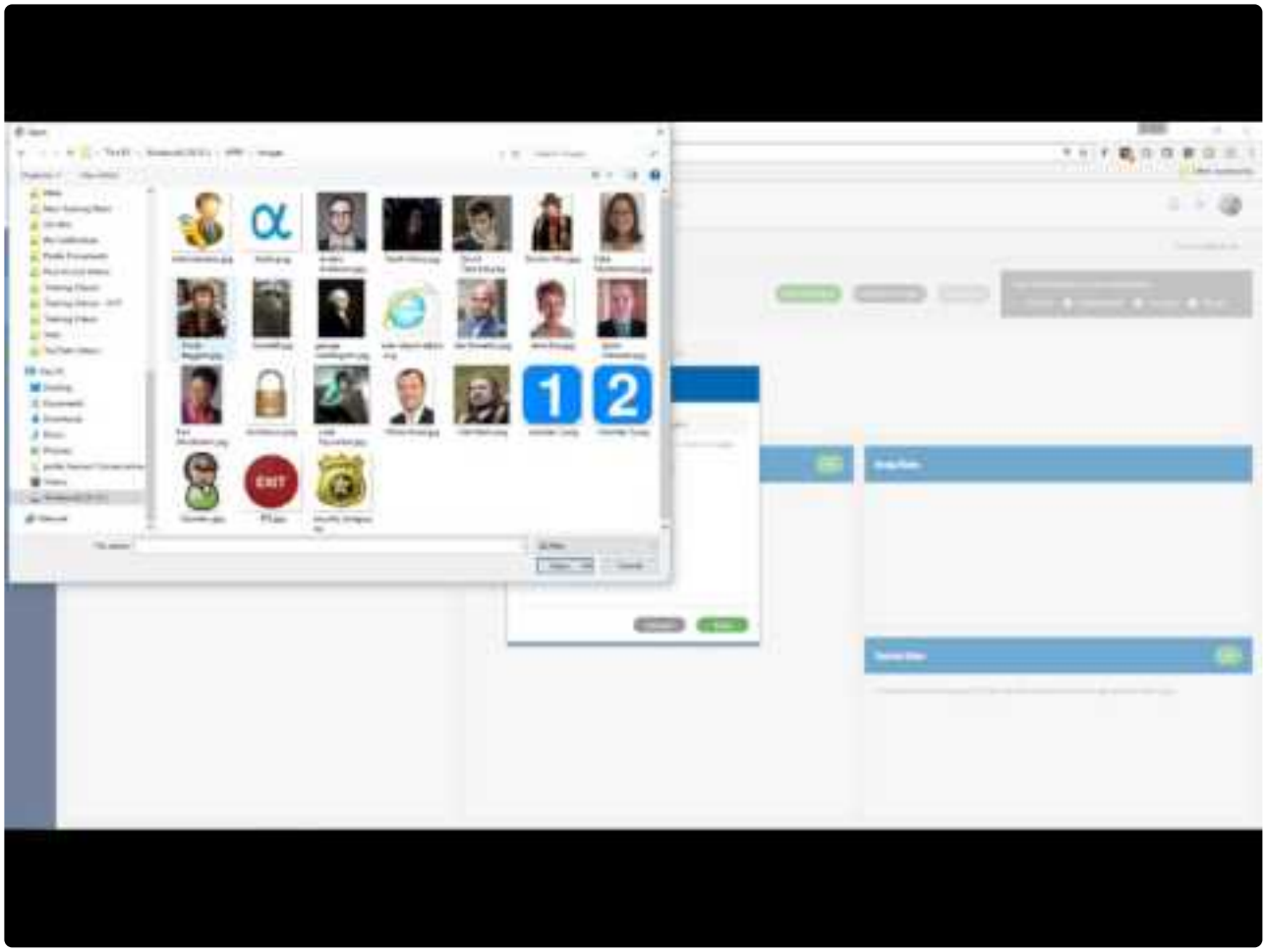
Last modified: 1 March 2021

Credential

This section is used to control Bitmasking of the credentials in your system.

Last modified: 25 February 2021

Bitmasking



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

Resources

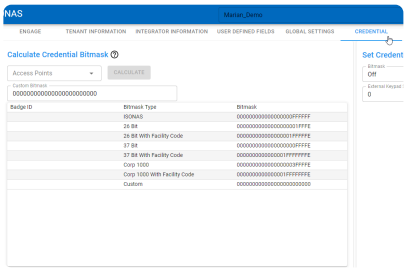
- Verifying the currently set bitmask.
- Discover and set a bitmask.
- Pushing bitmask settings to all readers.
- Pushing bitmask settings to all readers in PAM 2.12.2 or below.
- Setting an external keypad site code.
    - Configuring site code on an R-1 reader.
- Creating a custom bitmask.

Last modified: 26 February 2021

Verifying the Currently Set Bitmask

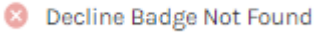
1. Navigate to the **Settings** tab:

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



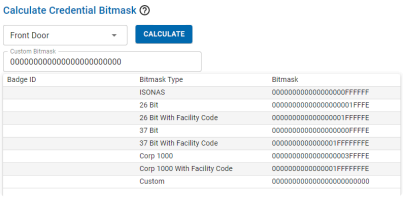
Last modified: 26 February 2021

Identifying Credential Data

1. Present an unenrolled badge/fob to a reader. You should see a 

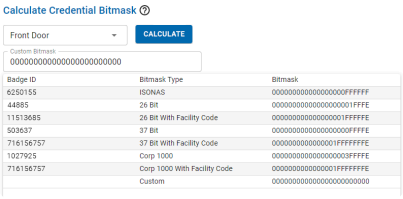
event in the history.
2. Navigate to the **Settings** tab:

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



5. Click 

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



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

- Enroll by presentation
- Calculate and use a custom bitmask

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

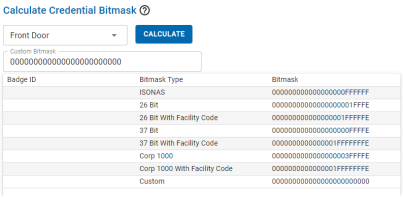
Last modified: 26 February 2021

Discover the Appropriate Bitmask

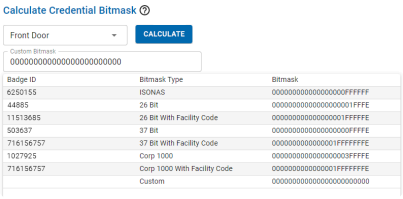
Verifying the correct bitmask for your credential:

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 CALCULATE.



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.

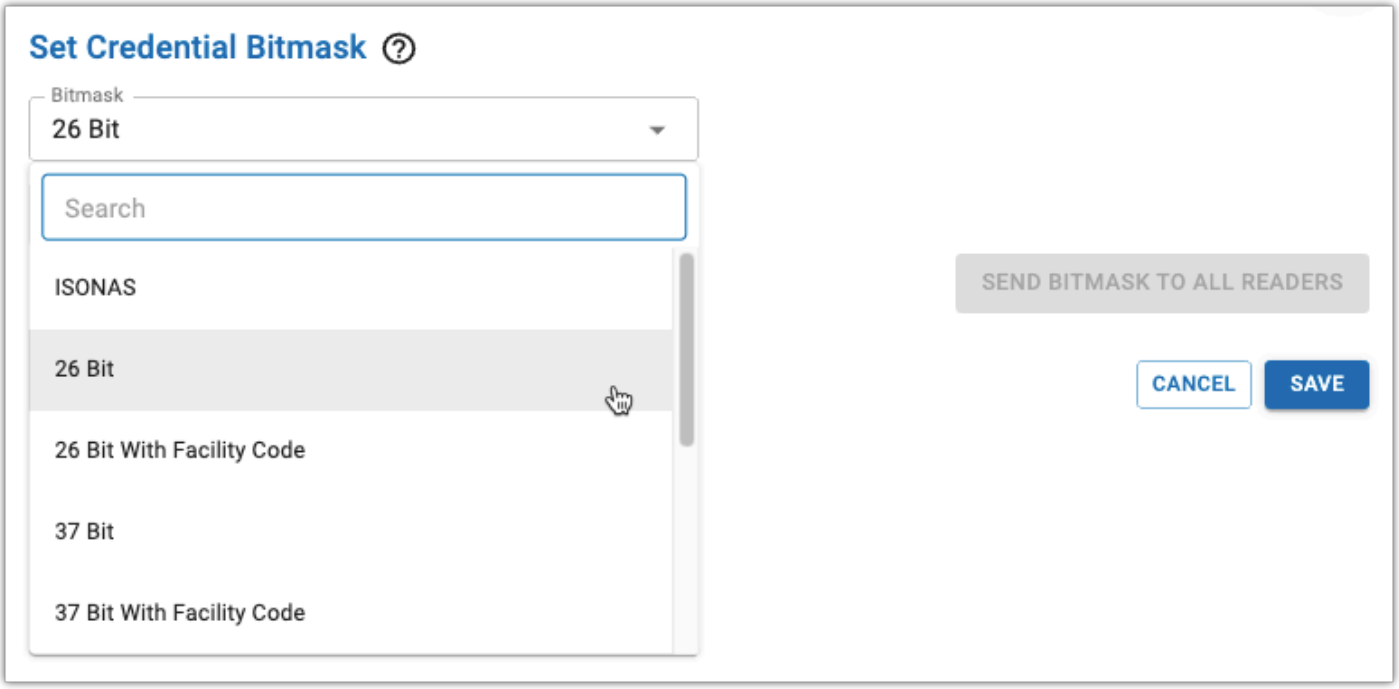


If there is **no matching badge ID** in step 4, you will either need to calculate a custom bitmask in order to manually enroll these credentials or you are using a high frequency credential and will need to enroll them by presentation.

Last modified: 26 February 2021

Setting a Bitmask

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



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

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

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

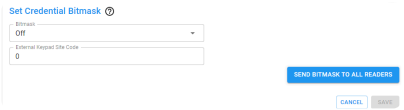
Last modified: 1 March 2021

Pushing the Current Bitmask Setting to All Readers

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

2. Click the **Credential** tab.

3. Click the  button.

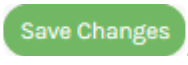


> The selected bitmask will be pushed out to all **connected** devices on the tenant. Note that this feature was added in Pure Access 3.1.0 and is not currently available in Pure Access Manager. Instructions for pushing bitmask settings in PAM can be found here.

Last modified: 26 February 2021

Pushing Bitmask Setting to All Readers (PAM)

1. Navigate to the **Settings** tab.
2. Click the **Credential** tab under **General Settings**.
3. Select any other mask (so that the  button appears), then return to the desired/original bitmask.

4. Click  .

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

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

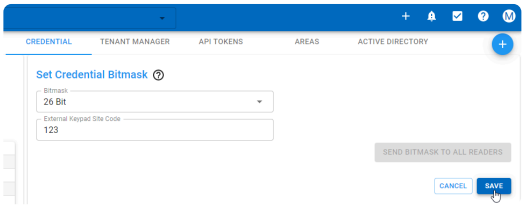
Last modified: 1 March 2021

Setting an External Keypad Site Code

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

2. Click the **Credential** tab.

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



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

Last modified: 1 March 2021

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 8 9 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.

Last modified: 26 February 2021

Custom Bitmasking

Overview:

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

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

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

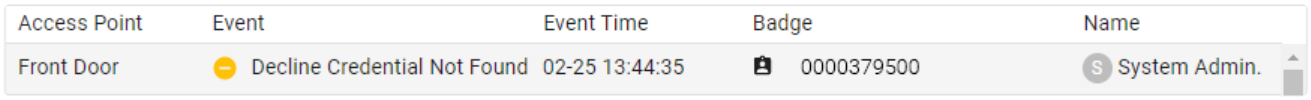
Prerequisites:

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

Gathering Data:

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

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



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

2. Gather the "**Raw Data**" value of the credential:

   a. Navigate to **Users** and then click ⋮ > **Manage Credentials** next to a User.

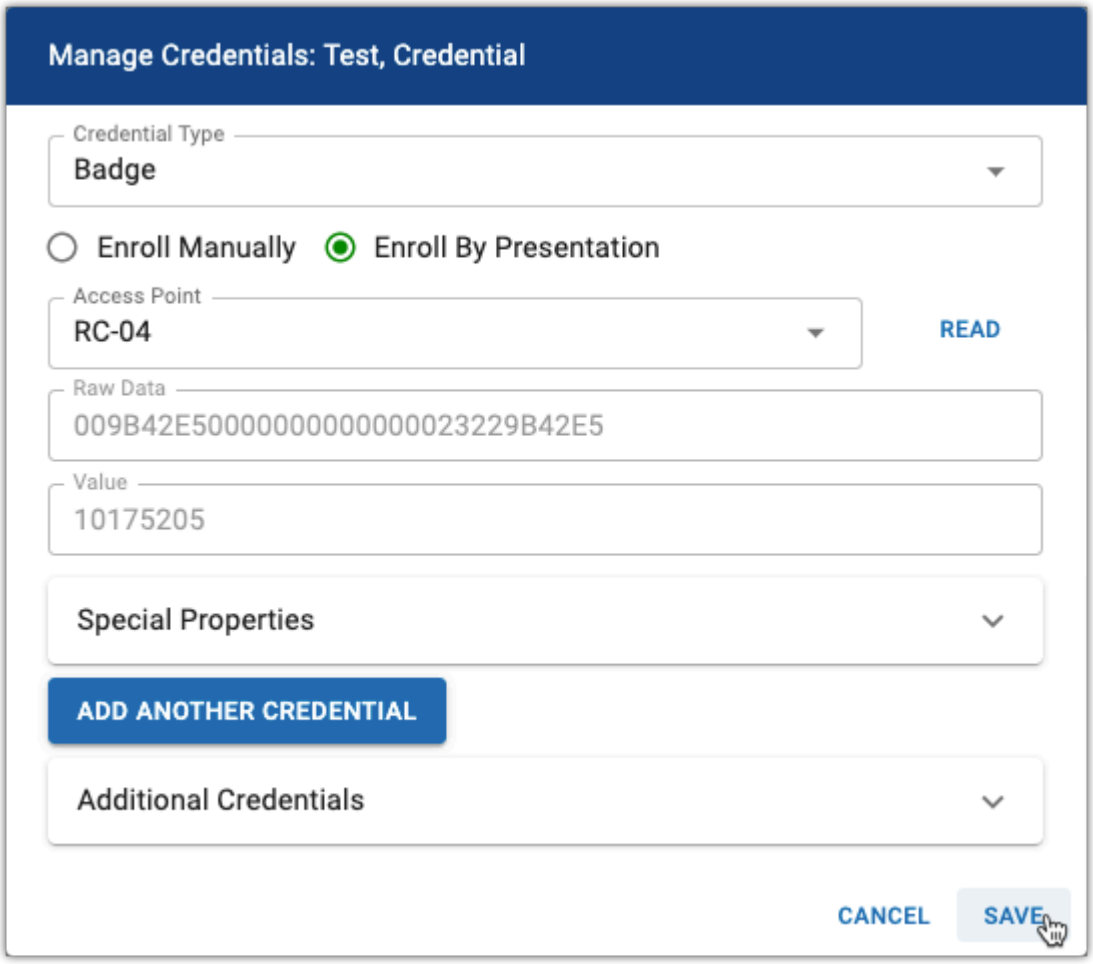
   b. Choose **Badge** from the **Credential Type** drop-down box.

   c. Choose the **Credential Format** (bit format) from the drop-down box.

   d. Click the **Enroll by Presentation** radio button.

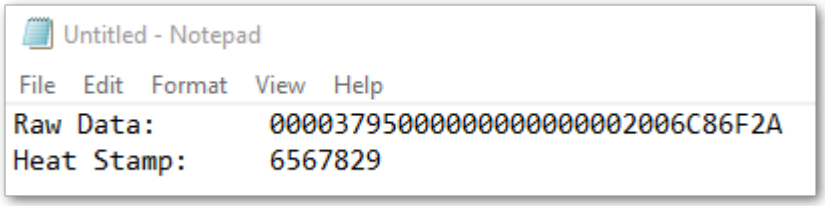
   e. Choose the **Access Point** to which you just presented the credential from the drop-down box.

   f. Click "**Read**":

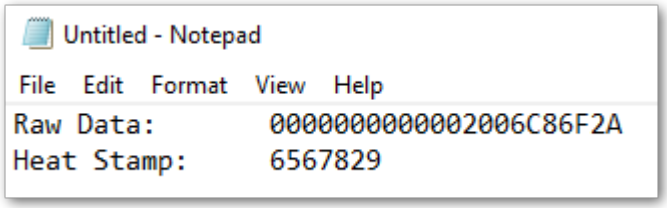


g. Copy the entire "**Raw Data"** value into a Notepad document.

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



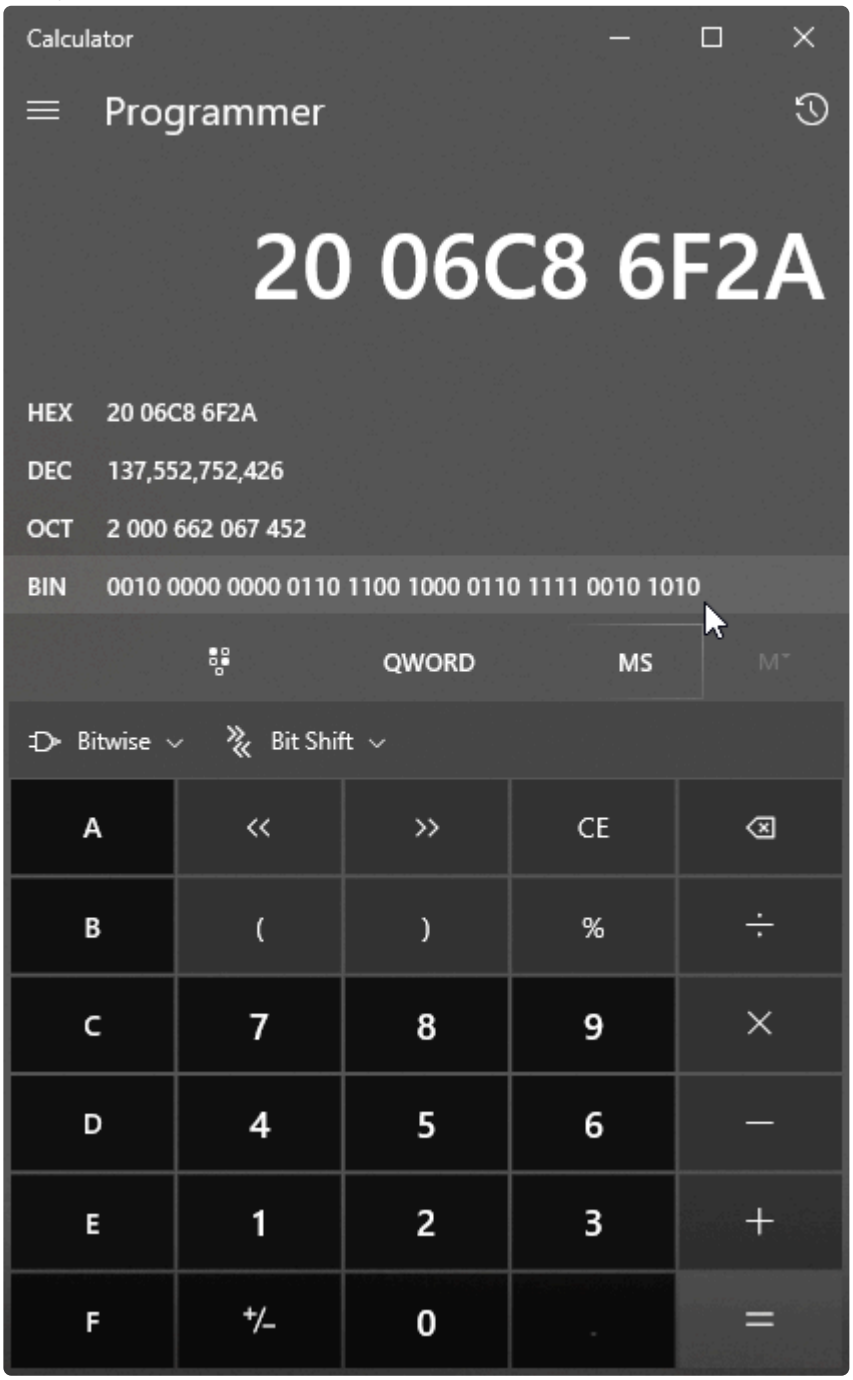
4. If we compare this raw data value with the badge number from the decline event in the history (see step one above), we can see that *0000379500* matches between the two. Delete this portion of the raw data from the document:



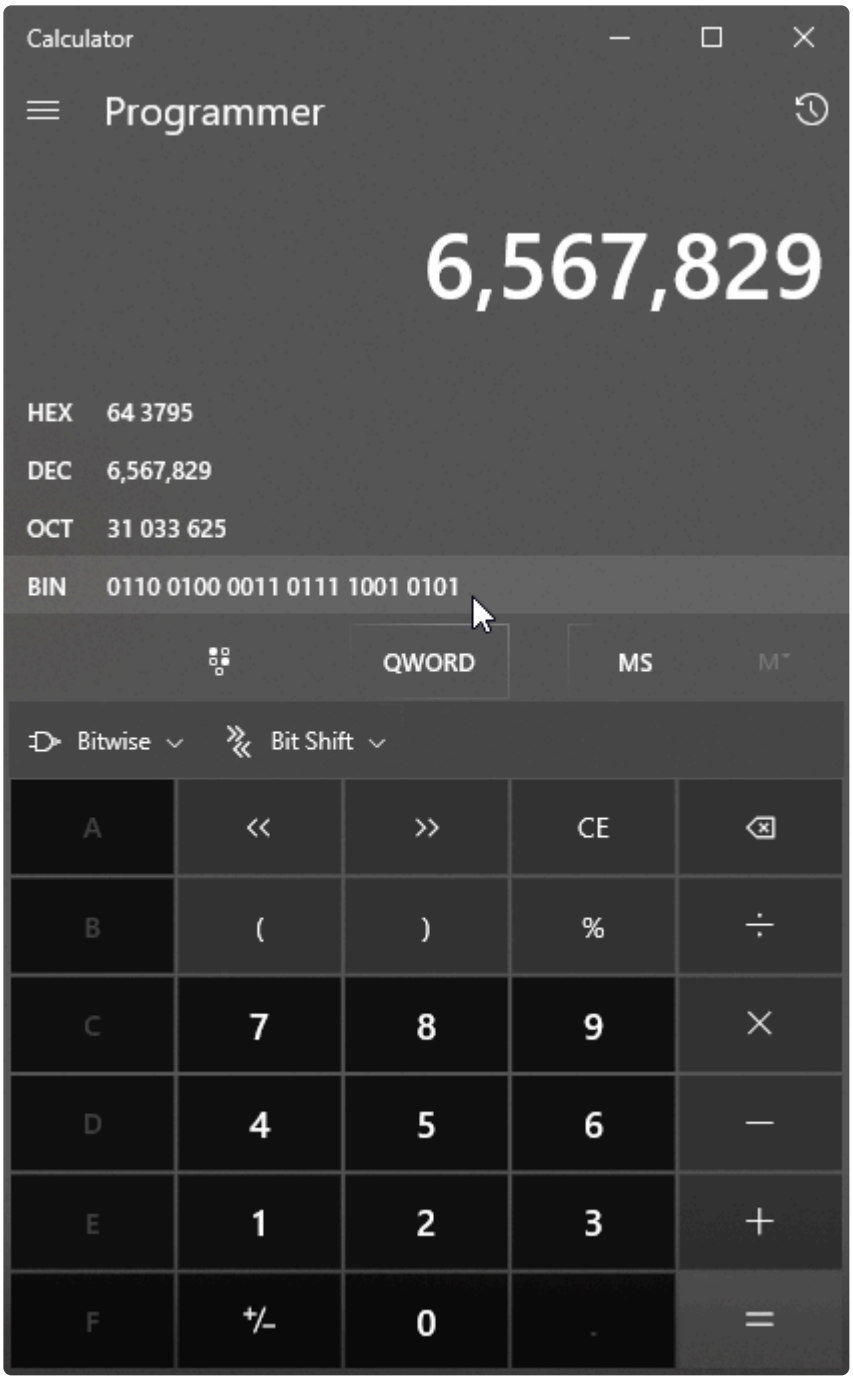
Converting data to binary:

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

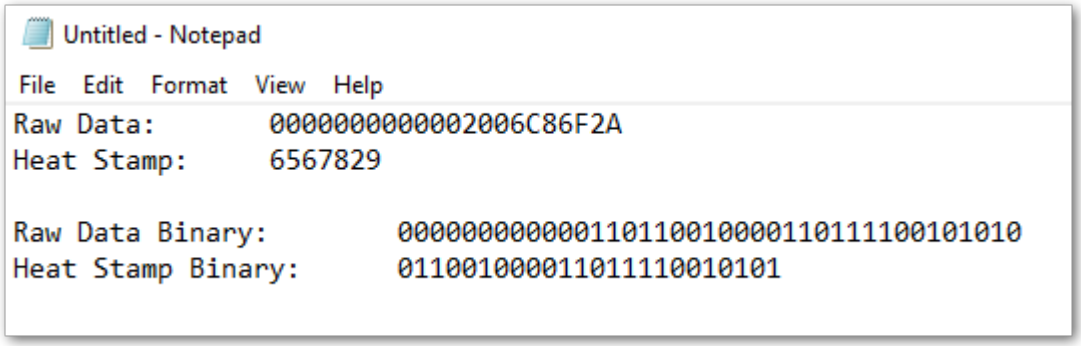
1. Copy the raw data value from Notepad and paste it into the calculator, then click “**BIN**” (binary).



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



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



Comparing the raw data with the badge ID:

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

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

```
Raw Data Binary:        00000000000011011001000011011110010101 0
Heat Stamp Binary:                    01100100001101111001010 1
```

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:        00000000000011011001000011011110010101 0
Heat Stamp Binary:                    01100100001101111001010 1
Wanted Bits:            00000000000000111111111111111111111110
```

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.

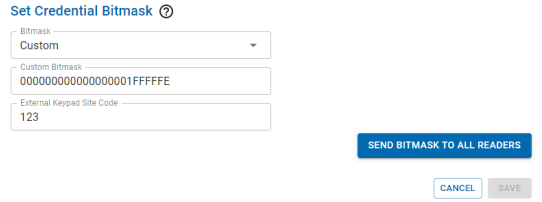
```
Wanted Bits:    11111111111111111111111110  =  1FFFFFE

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):

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

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



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.

Last modified: 26 February 2021

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.

Last modified: 26 February 2021

User Defined Fields

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

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

To add these fields to user profiles:

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

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

Last modified: 1 March 2021

Active Directory

Larger* Pure Access Cloud licenses and Pure Access Manager allow for Active Directory integration to

manage users and credentials via the AD Connect software.

Functionality includes:

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

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

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

** 51-100 license and above*

Last modified: 16 May 2022

AD Connect Limitations and Requirements

ENGAGE Device Limitations

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

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

Structures that will *NOT* work:

- The AD Connect Tool will not traverse trusts between domains.

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

Requirements:

- Active Directory running on Windows Server 2008 R2 or later.
    - Only on-premises Active Directory is supported. Cloud-based Active Directory (including Azure AD) is NOT supported.
- AD Connect communicates with Active Directory over LDAP only. LDAPS is not supported.
- 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.

> We recommend disabling users in Active Directory, rather than deleting. Disabled users will be deactivated in Pure Access upon next AD sync. Deleted AD users will lose their link to Pure Access, and as such, remain active until manually deactivated in Pure Access.

Service Account:

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

- You may attempt a less privileged account to see if this can read your directory. If authentication fails, elevate the account to Domain Admin. You may reduce privileges and retest to find the appropriate level for your directory.
- The service account name should only contain alphabetic characters.
    - Good username: isonasadconnect
    - Bad username: isonas-ad-connect, ison@sadconnect

- The username as entered will entirely depend on the AD configuration.
    - AD username Possibilities
        - isonasadconnect
        - isonasadconnect@domain.com
        - domain\isonasadconnect
    - You may need to modify based on your directory.
- There is not official support for authentication with a .local domain.

Directory Structure and Groups:

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

AD Connect Software:

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

Resources:

- General Best Practices for AD
- Key Principles on OU design

Last modified: 10 July 2026

Installation and Configuration

1. In Pure Access, create a new API token and uncheck “Read Only.”

- This is done from the **Settings** > **API Tokens** page.

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

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

Last modified: 4 August 2025

Configuring AD Sync Settings in Pure Access

1. Log into your Pure Access tenant.
2. Create User Groups which will be populated with user profiles from AD.
3. Navigate to **Settings** > **Active Directory**
4. Set sync times under **General Configuration**.

5. Map AD fields to Pure Access fields under User Field Mapping (you may need to refresh the fields for them to appear).
6. Map AD groups to Pure Access user groups under User Group Field Mapping (you may need to refresh the groups for them to appear).
7. Once everything is set up properly, click **FULL SYNC**.
    - Please note that this may take some time to complete if this is the first time syncing. If there doesn't appear to be activity after 10 minutes, refresh the page and try to sync again.
    - If the above did not work, restart the **Isonas AD Connect** Windows service and try again.

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

FAQ

1. **Changing Group Names in Active Directory**
    a. **Q** – *If the group names are updated in Active Directory, will the sync pick up these name changes, and will mapping the new names be needed in Pure Access Cloud?*
    b. **A** – The AD Group names are synced and stored to Pure Access Cloud (PAC) based upon their GUID, which is a unique non-changing identifier in Active Directory. If the AD Group name is updated in Active Directory, this name change will automatically update within PAC. Remapping will not be required as the names will flow and update directly without extra intervention.
2. **Changing Users' Names in Active Directory**
    a. **Q** – *If user names are updated in Active Directory, will the sync pick up these name changes, and will mapping the new names be needed in Pure Access Cloud?*
    b. **A** – The AD user names are synced and stored to Pure Access Cloud (PAC) based upon their GUID, which is a unique non-changing identifier in Active Directory. If a user's name is updated in Active Directory, this name change will automatically update within PAC. Remapping will not be required as the names will flow and update directly without extra intervention.

Last modified: 9 July 2024

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.

API V2 Introduction

Last modified: 20 February 2026

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.

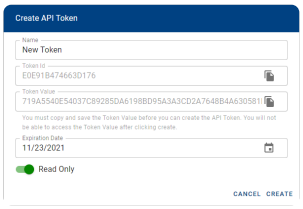
Last modified: 26 February 2021

API Tokens

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

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

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



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

Last modified: 26 February 2021

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 the information provided (e.g., a required parameter was omitted), and codes in the **5xx** range indicate a server error.

Throttling

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

Resources

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

https://app.swaggerhub.com/apis/isonaspureaccess/api-v2
API V2 Intro

Last modified: 20 February 2026

ENGAGE

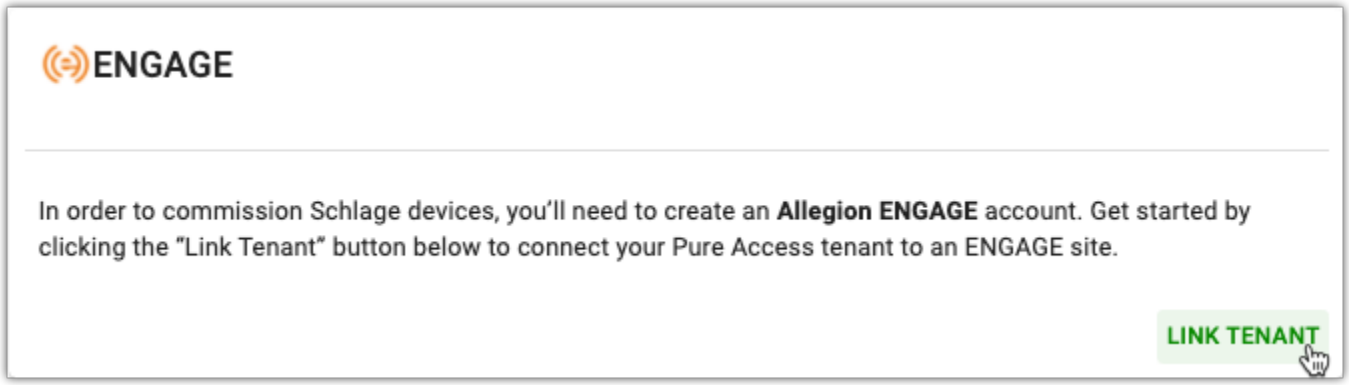
The Allegion ENGAGE™ ecosystem is a mobile application that delivers simple and convenient commissioning services for Schlage devices. In order to use Schlage devices (such as NDEB, LEB, and the Schlage RC), you'll need to link your Pure Access tenant to ENGAGE.

Last modified: 3 May 2021

Linking to ENGAGE

Overview

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



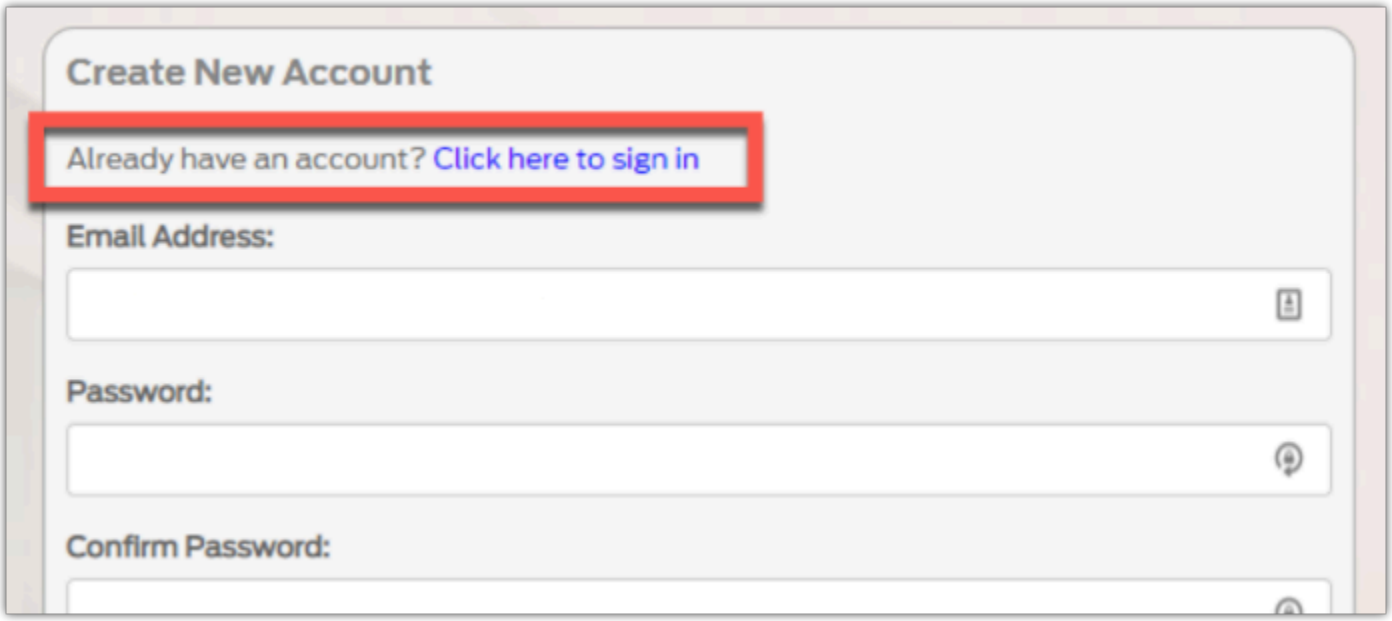
> ! Linking to ENGAGE will permanently change the way your tenant functions to ensure the most consistent experience possible across all device types.

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

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

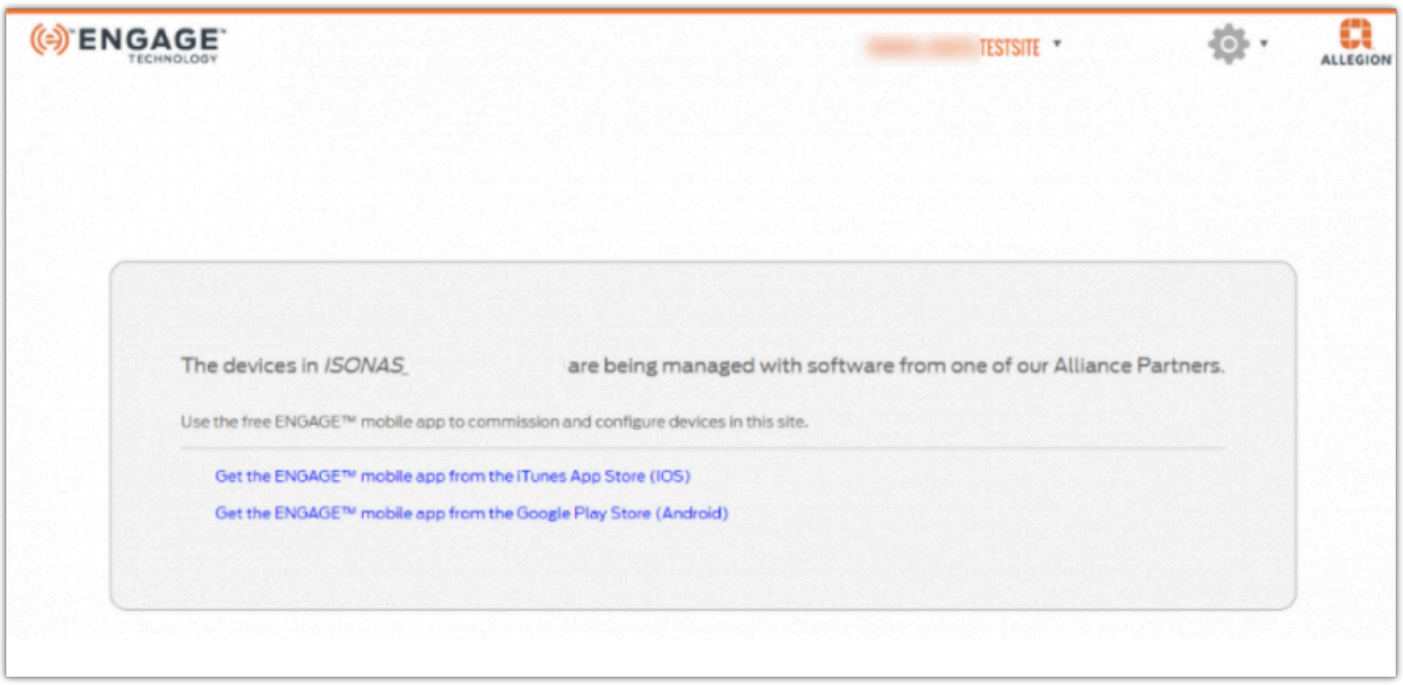
Instructions

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



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

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



Last modified: 4 May 2021

Inviting Users to ENGAGE

Preconditions:

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

> ! Please note that a web access user's role and permissions determine what that user can access within the Pure Access web application **only**. These user role permissions *do not* determine user privileges for the Engage Mobile application, meaning **users invited to Engage will have the ability to commission Schlage devices and pair with locks to push updates, gather audits, and initiate diagnostic tests**.

Inviting Pure Access Users to ENGAGE

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

Last modified: 26 May 2026

Wireless Device Check-In

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

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

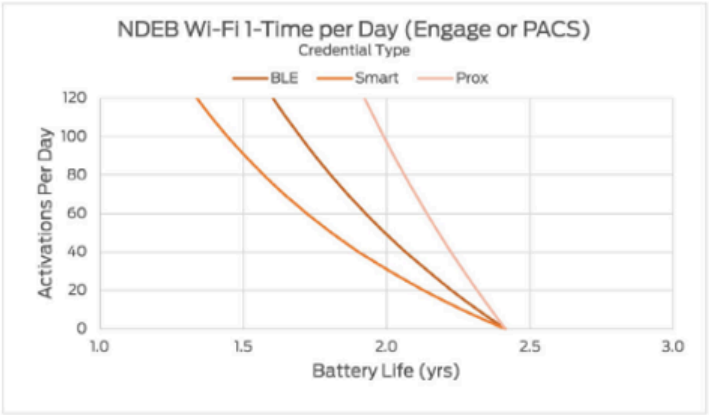
1. How frequently credentials are presented to the device
2. How frequently the device wakes up to establish a WiFi connection to transmit data back to the host software

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

Wi-Fi using ENGAGE or PACS system

Activations per day

Credential type	Light (5)	Medium (30)	Heavy (75)
BLE mobile	2.4 years	2.1 years	1.8 years
Smart	2.3 years	2.0 years	1.6 years
Proximity	2.4 years	2.3 years	2.1 years



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

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

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

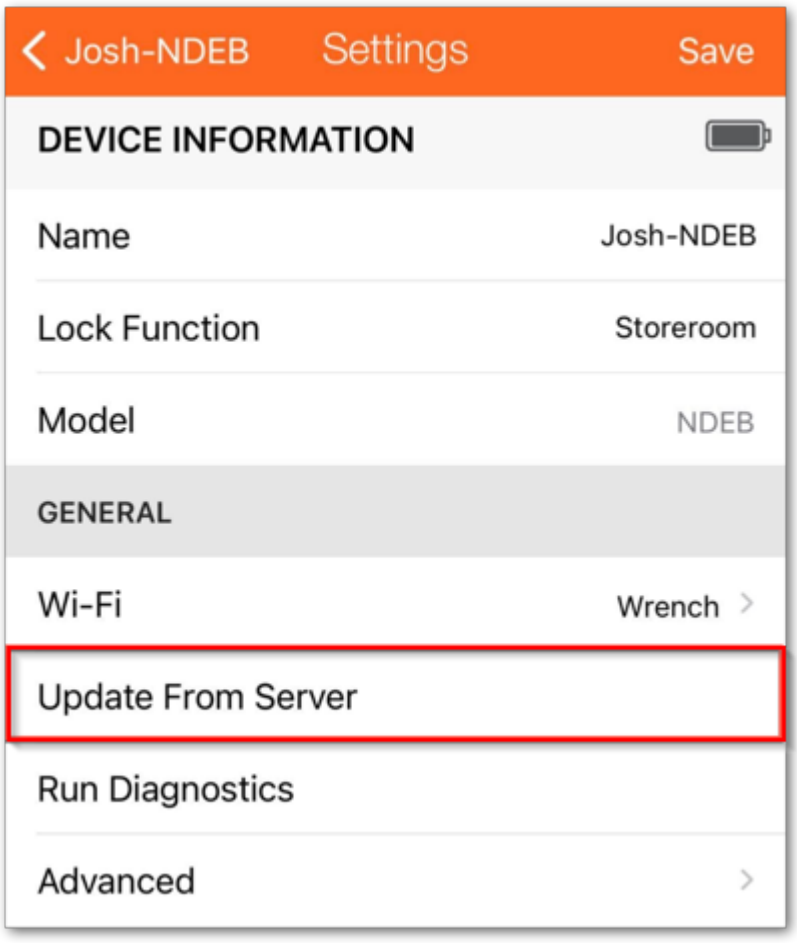
Due to the limited check-in frequency configured to preserve battery life, there may be times that you need to update a device immediately, outside of the normally scheduled recurring check-ins. This process is referred to as a Force Check-In.

Last modified: 22 June 2022

Force Wireless Device Check-In

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

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



2. Present a credential with the Force Check-In special property at the device.

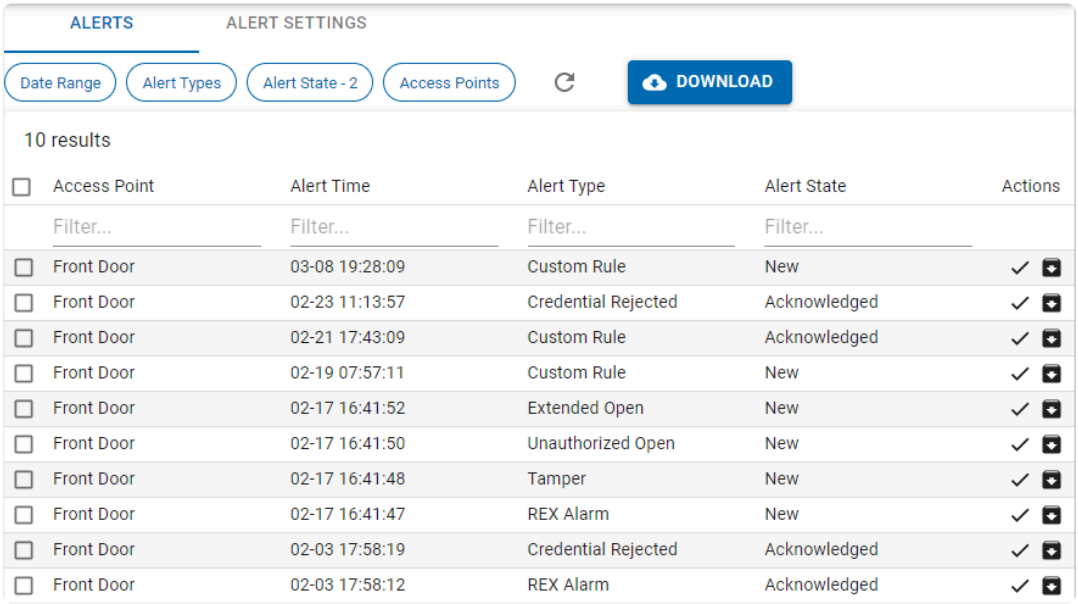
> Force Check-In is a credential special property that can be enabled on any credential type available in Pure Access. In order for this credential special property to work, the device must first update with Pure Access to add the credential to its database. This can either be accomplished by waiting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

Last modified: 22 June 2022

Alerts

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

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



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

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

Last modified: 9 March 2021

Alert Types and Setup Procedure

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

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

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

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

Alert Types

- Unauthorized Open
- Extended Open
- Tamper
- AUX/REX Alarm
- Credential Rejected, Expired, or Over Limit

Last modified: 26 February 2021

Unauthorized Open

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

Causes

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

Physical Requirements

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

Setting Up

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

Last modified: 7 December 2023

Extended Open

Extended Open is an alert that is intended to notify the user that a door was left open for an extended period of time.

Causes

This alert will trigger when a door is open past its latch interval plus the extended open threshold. If a door is forced open thus bypassing the latch interval, the alert will trigger after the extended open threshold alone.

Physical Requirements

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

Setting Up

1. Install and enable the door position sensor.
2. Enable **Door Sense** on the Access Point for which you want to receive alerts.
    - See Configuring an Access Point.
3. Navigate to the **Alerts** page, then to the **Alert Settings** tab.

Last modified: 2 July 2025

Tamper

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

Setting the Tamper Sensitivity

1. Set the **Tamper Sensitivity** to the desired level on the Access Point for which you want to receive alerts.
    - See **Configuring an Access Point**.

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.

Last modified: 7 December 2023

AUX/REX Alarm

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

Physical Requirements

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

Setting Up

1. Install and enable the AUX or REX switch on the device.

2. Enable **REX** and or **AUX**, and set the action on the Access Point for which you want to receive alerts.
    - See Configuring an Access Point.

Last modified: 7 December 2023

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.

Last modified: 26 February 2021

Alert Settings

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

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

4. Click SAVE.

Last modified: 5 March 2021

DPS Generated Alerts and Audits

The door position sensor (DPS) indicates whether a door is open or closed. Using DPS allows certain events at the door to be tracked and trigger alerts and audits.

DPS is supported by the following locks:

- Legacy (RC-04, IPBridge)
- Engage locks (NDE, LE, RC)

When DPS is enabled, you can also use Door Prop Delay (seconds) to trigger an audit and an alert (if configured) when the door is held open for longer than the Door Prop Delay setting.

For certain Schlage devices (NDE, LE, RC) when DPS in enabled, an audit will always be generated when the door is opened past the specified amount of time (default = 20 seconds).

This audit can be turned off using Configuration Settings for the Schlage RC, but not for other devices.

These audits are now generated for the wireless and offline devices and when sync's occur, the audits will appear in the history, but will not generate an alert.

Event	Device Status	Action	RC-04	Schlage RC	NDE, LE
Extended Open: Door is held open longer than the door prop delay threshold	Device is ONLINE when the event occurs	Alert	Extended Open	Extended Open	N/A
		Audit	N/A	Door Propped	Door Propped
	Device is OFFLINE when the event occurs	Alert	N/A	Extended Open	N/A
		Audit	N/A	Door Propped	Door Propped
Unauthorized Open: Door status changes from closed to open without a valid credential	Device is ONLINE when the event occurs	Alert	Unauthorized Open	Unauthorized Open	Unauthorized Open
		Audit	N/A	Forced Door	Forced Door
	Device is	Alert	N/A	Unauthorized	N/A

	OFFLINE when the event occurs			Open	
		Audit	N/A	Forced Door	Forced Door

Last modified: 13 March 2026

Troubleshooting and Frequently Asked Questions

Who receives license expiration emails?

Scenario	Who receives the email
Standalone tenant	Only users with the Administrator role and web access enabled. Regular web-access users and API user accounts do not receive it.
RMR license type	Not sent to user accounts. Sent instead to the contact email addresses stored on the tenant record: integratorContactEmail and contactEmail.
Reminder timing	Emails are sent 30, 15, 5, 3, and 1 day before the license expires.

Last modified: 30 June 2026

Release Notes & Current Firmware

September 23, 2025

Features & Enhancements

- Updated the descriptions for credential Special Properties programming to be clearer and more descriptive.

Bug Fixes

- Fixed a bug that prevented an Alert notification from appearing in the web app until you navigated to the Alerts tab.
- Fixed a bug that didn’t display users email address when being deactivated and reactivated in a certain flow.
- Fixed a bug that prevents filters from being saved and applied on the Reports page.

September 2, 2025

Features & Enhancements

- Credential Special Properties update: the ‘master’ feature is now called ‘Pass Through’ in order to better describe the functionality. Audits will now be titled Passage – Pass Through instead of Passage – Master
- Updated text to better communicate end and start time limitations per each lock type
- Support for reader tamper audit and alert on NDE, LE(B) ; introduced support for interior push button audit and alert on NDE and LE(B)
- New default Schlage RC firmware 1.12.0

Bug Fixes

- Fixed a bug that allowed a new auto-unlock rule to be created for control locks or an access point group containing only control locks, which is not supported on those devices. These locks will no longer appear in that drop down when trying to create that rule. An access point group that contains mixed devices will appear in the drop down and can be saved.
- Fixed a UI issue that showed an inactive menu option when the screen was minimized
- Fixed a UI where a user had to scroll the page to use the action buttons.
- Fixed a bug that caused filtering of events on the to be displayed incorrectly

- Fixed a bug that prevented a badge from being enrolled by presentation if the device and user were in different time zones.
- Fixed a bug where the value of the badge ID displayed for a custom bitmask in the bitmask calculator was inaccurately displayed.
- Fixed a bug where unsupported database elements were being sent to control locks, which was causing JSON parse errors
- Fixed a bug where a no-tour endpoint would query database for all users if there were no commands to generate

Last modified: 23 September 2025

Current Firmware Versions

Devices	Current Firmware
NDE	2.21.01
NDEB	3.19.03
LE	1.17.01
LEB	3.19.03
Schlage RC	1.15.01
IP Bridge	pic 1.05 cf – 1.19
RC-04	78.05 (1.2.0)

*The firmware for the RC-04 & IP Bridge do not currently appear as needing to update in the software UI. However, it can be updated as needed from the Allegion library.

Last modified: 15 July 2026

Release Notes

Last modified: 23 September 2025

Most Recent Release

July 15 2026

Firmware Updates:

- RC – 1.15.01

Bug Fixes

- Fixed an issue where sending a schedule command to an RC access point could leave the displayed lock status incorrect until the next access event occurred. The access point status now accurately reflects the lock state after any schedule command is sent. A new “State Override: Clear” audit entry will also appear in device history whenever a schedule command is applied

Last modified: 15 July 2026

Previous Releases

July 6, 2026

- Fixed an issue where security alerts (such as tamper or extended-open events) could be silently lost without notification if the associated access point was deleted while the alert was still being processed. Alerts are now reliably created and delivered even in this scenario.

June 22, 2026

- Fixed a bug during commissioning that ensures IP-Bridge REX values are now to set to DISABLED instead of NULL. Previously, if the setting was not modified in the software, it would still unlock when REX was triggered, even if the REX setting was showing disabled in the Software. This does not change existing customer configurations, only will fix the commissioning for new devices.

June 2, 2026

Bug Fixes

- Selected Rows Clear When Switching Tenants — Selected rows in list views were persisting after navigating to a different tenant. Row selections are now cleared when switching between tenants.

- Offline Device Command Prevention (Web) – Fixed an issue where commands (lockdown, unlock, admit, etc.) could be sent to offline devices and would incorrectly appear as successful in activity history. Commands to offline devices are now blocked buttons are disabled with an “Device is offline, commands cannot be sent” tooltip, and no activity history entries are generated. When sending a command to a group where some devices are offline, online devices still receive the command and a warning is shown

Firmware Updates:

- NDEB – 3.19.01

- LEB – 3.19.01
- LE – 1.17.01

March 30, 2026

- Fixed an issue on the Reports page where the User filter dropdown did not include all users in the account, making it impossible to run accurate user-filtered reports without workarounds.

March 11, 2026

Daylight Saving Time Auto-Update for Engage Locks

- Updated Engage locks (NDE, LE, Schlage RC) so that they will now receive Daylight Saving Time (DST) configuration and updates. The devices will now update automatically when DST occurs – based on their designated time zone – preventing scheduled access events to trigger one hour off and audit log timestamps to be inaccurate. Upon the locks next update (via BLE Sync or Wi-Fi checkin), time changes will be applied automatically to the devices moving forward.
- * With this change, the existing DST toggle in the Areas section has been hidden as that is no longer relevant.

In order for this update to be applied to the wireless devices, they must have be synced via BLE or complete a Wi-Fi check in. The Sync report is a useful tool to help customers know what devices have not checked or been synced since a specific date.

February 25, 2026

Features & Enhancements

- Created a new Sync Report that allows property managers and integrators to track which devices have or have not been sync'd or had a Wi-Fi check in within a specific date and time. NOT available as a Scheduled Report.
- Numerous performance improvements

February 11, 2026

- Fixed an issue where users could see activity in the dashboard History widget for areas they don't have permission to access. Activity is now properly restricted to only show events from areas the user is authorized to view.
- Fixed a critical issue where deleting a wallet-based (NFC) credential could cause approval audit logs

to be missing from history reports, for any events since the last Sync. Audit records now properly capture and retain all access events, including user approvals.

February 3, 2026

- Fixed an bug where door and lock status icons in dashboard widgets were not updating without refreshing the page when credentials were presented

January 27, 2026

Features & Enhancements

- Updating call to action when a user access living.zentra.co from a mobile web browser with a full cover prompt to download the mobile to gain their access and is dismissible.

Bug Fixes

- Fixed device filtering issue where the Connected column only accepted the letter ‘y’ as input; the filter now properly supports typing ‘Yes’, ‘No’, and partial text matches for easier device searches.
- Resolved login issue where users with specific access privileges encountered errors when attempting to accept the End User License Agreement (EULA), preventing them from accessing the web application. Users can now successfully accept the EULA and login regardless of their assigned permissions.
- Fixed a bug where no error was presented to the user if trying to log in with a deleted user account. Users will now see the message“No access for this web access user and requested tenant“
- The Alerts page now displays a message when alert results exceed 50 items, informing users of the total count and suggesting filters to refine results.
- Table selections are now properly cleared after performing actions like deleting access control rules or deactivating users, preventing confusion from stale selections.
- Numerous performance improvements

November 20, 2025

- Fixed a performance issue related to the /api/v2/users API. With this fix, the API should be responding in an appropriate amount of time

December 1, 2025

- Fixed an issue where history reports returned all event types when more than 4 event types were

selected in the filter.

November 18, 2025

Features & Enhancements

- Updated Schlage RC default firmware to 1.13.0
- Pure Access: In the Holidays section, updated text to be more clear that Holidays are applied to all access points

Bug Fixes

- Fixed an issue where alert times on a downloaded Alert Report was displayed incorrectly.

Previous behavior	New behavior
Downloaded Alerts reports (CSV/PDF) used the alert's update time (utime), so Alert Time could change when an alert was acknowledged/ cleared and could appear in an unexpected timezone. This was inconsistent with the Alerts UI.	Reports now use the alert's creation time (ctime) as Alert Time; acknowledging/clearing an alert no longer changes it.
	Reports show times in the user's/ browser time zone (not the tenant time zone)

October 22, 2025

Features & Enhancements

- In the case where a credential is declined at a Schlage RC, we can now correlate that event to a user in our system if the information from the decline matches data for a credential we have in our system for an active credential.

Bug Fixes

- Fixed the Areas filter on the Users report to display correctly on initial and update properly when switching between tenants.
- Performance improvements in credential creation and dropdown selection problems for web access users with extensive Area permissions in large tenants, improving overall usability.
- Fixed a bug that allowed user to think they scheduled a firmware update when it was not actually saved.
- Fixed an issue where our API allowed keypad credentials to be made that were not allowed. Existing

ones will continue to work, but new ones will not be allowed.

- Optimized the Dashboard to significantly reduce redundant API calls for access point status, improving load times and overall performance.
- Improved access point status updates by removing locking conflicts to reduce event loss and log noise, ensuring more reliable and timely status reporting.

September 25, 2025

Bug Fixes

- Fixed a bug where scheduled events could remain active on RC-04's after they were removed from access point groups

September 23, 2025

Features & Enhancements

- Updated the descriptions for credential Special Properties programming to be clearer and more descriptive.

Bug Fixes

- Fixed a bug that prevented an Alert notification from appearing in the web app until you navigated to the Alerts tab.
- Fixed a bug that didn't display users email address when being deactivated and reactivated in a certain flow.
- Fixed a bug that prevents filters from being saved and applied on the Reports page.

September 2, 2025

Features & Enhancements

- Credential Special Properties update: the 'master' feature is now called 'Pass Through' in order to better describe the functionality. Audits will now be titled Passage – Pass Through instead of Passage – Master
- Updated text to better communicate end and start time limitations per each lock type
- Support for reader tamper audit and alert on NDE, LE(B), ; introduced support for interior push button audit and alert on NDE and LE(B)

- New default Schlage RC firmware 1.12.0

Bug Fixes

- Fixed a UI issue that showed an inactive menu option when the screen was minimized
- Fixed a UI where a user had to scroll the page to use the action buttons.
- Fixed a bug that caused filtering of events on the to be displayed incorrectly
- Fixed a bug that prevented a badge from being enrolled by presentation if the device and user were in different time zones.
- Fixed a bug where the value of the badge ID displayed for a custom bitmask in the bitmask calculator was inaccurately displayed.
- Fixed a bug where unsupported database elements were being sent to control locks, which was causing JSON parse errors

Last modified: 6 July 2026

Browser Support

Tested and supported web browsers include: Google Chrome, Mozilla Firefox, & Microsoft Edge, Apple Safari.

Untested and unsupported web browsers include: Internet Explorer, Netscape, and Opera

Last modified: 20 February 2026

Glossary

Last modified: 26 February 2021

Admit

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

Last modified: 16 February 2021

ASM

ASM: Advanced Security Module

Last modified: 16 February 2021

AUX

AUX: Auxilliary Input

Last modified: 15 February 2021

Compile

Compile is the action of updating access points.

Last modified: 15 February 2021

Door

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

Last modified: 15 February 2021

Fail Safe

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

Last modified: 18 February 2021

Fail Secure

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

Last modified: 18 February 2021

First Person In

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

Last modified: 18 February 2021

Lock Down

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

Last modified: 13 March 2026

REX

REX: Request for Exit

Last modified: 15 February 2021

Secured

Secured is another word for locked.

Last modified: 10 December 2025

Lock Functions

Lock Functions define how a lock controls access from the outside while allowing egress from the inside. Not all Lock Functions are supported on every device type.

- **Apartment**: The door does not relock automatically, preventing the user from being locked out of their residence. The interior pushbutton or deadbolt allows the resident to lock the door from the inside.
- **Office**: Uses the interior pushbutton or deadbolt to allow users to lock the door from the inside. Can be overridden by a valid credential.
- **Privacy**: Uses the interior pushbutton or deadbolt to allow the user to lock the door from the inside. While in Privacy Mode, valid credentials are denied access.
- **Storeroom**: The lock remains secured until a valid credential is presented. The inside lever will always open the door.

Each device model is different and may support a limited set of lock functions. Refer to each device setting individually.

Last modified: 16 June 2026

Appendix A: Linking ENGAGE Site to Pure Access

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

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

ISONAS + Schlage Device Environment – Customer Pre-'ENGAGE' Questionnaire

Commissioning Hardware

All Schlage devices: RC, NDEB, and LEB will be commissioned to an ENGAGE site that is created in the Pure Access Cloud account.
All legacy RC-04 and IP Bridges will be commissioned direct to Pure Access Cloud via the ISONAS configuration tool.

Programmers

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

Credential Migration

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

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

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

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

Physical Credential Parity

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

The RC-04 only supports three message formats:

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

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

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

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

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

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

Mobile ID Credential Parity

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

Holidays

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

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

Active Directory

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

RC Differences

- The RC-04 has an 8-wire pigtail and the Schlage RC has a 12- wire pigtail. The adapter cable is still in development and not released. Q4 2024 is the anticipated timeframe.

- The Schlage RC added a separate AUX input, two AUX outputs, and RS 485 connection but Pure Access Cloud software at present build does not support the AUX outputs or RS 485 connections.

Last modified: 21 June 2023

RC-04 End of Life support

This is where we will document the RC-04 EOL information and help to provide answers to commonly asked questions.

Last modified: 24 June 2026

ISONAS RC04 vs. Schlage Reader Controller

The ISONAS RC04 and the Schlage Reader Controller (RC11, RC15, RCK15) differ in communication, wiring, supported credentials, and rule behavior. Review the comparison below before mixing device types on the same tenant.

[INSERT IMAGE: ISONAS RC04]	*[INSERT IMAGE: Schlage Reader Controller (RC11 / RC15 / RCK15)]*
ISONAS RC04	**Schlage Reader Controller (RC11, RC15, RCK15)**

Device Comparison

Attribute	ISONAS RC04	Schlage Reader Controller
Communication Ports	55533 TCP/IP	80 (http) & 443 (https)
Communication Speed	10 Mbps (100 Mbps with Coldfire firmware 78.04+)	10/100 Mbps
Host URL	`isonas.pureaccesscloud.com`	WSS/CA via `cloud-iot.isonas.com/engage`
Commissioning	Via MAC address in Access Point Settings and the ISONAS Configuration Tool	Via the Engage Mobile App
Pigtail	8-pin connector	12-pin connector
Wiring Differences	DPS: Blue to Brown; REX: Green to Brown	DPS: Blue to Black; REX: Green to Black; AUX: Gray to Black
Door Sense	N.C. contacts only	N.C. or N.O. contacts (configurable)
REX	Configurable as REX or AUX; N.O. contacts only; unlocks in lockdown with Coldfire firmware 78.05+	Configurable Off/Admit/Report Only; N.O. or N.C. contacts; always unlocks in lockdown
AUX	N/A	Configurable Off/Admit/Report Only; N.O. or N.C. contacts

Attribute	ISONAS RC04	Schlage Reader Controller
Supported Physical Credential Formats	ISONAS Proprietary Prox, ISONAS DESFire EV2, plus one additional bitmasked prox format	ISONAS Prox formats plus 26A, 28G, 28H, 32K, 32X, 33D, 34N, 34S, 35C, 35X, 36B, 36C, 36L, 36M, 36X, 37B, 37H, 37P, 37X, 40X, 48X
Supported 13.56MHz Smart Credentials	ISONAS DESFire EV2/EV3 (encrypted, MCT models); other smart credentials read CSN only	Schlage MIFARE Classic EV1, MIFARE Plus, DESFire EV1/EV3; ISONAS DESFire EV2*/EV3* (*requires configuration card)
Supported Mobile Credential	ISONAS Pure Mobile	Schlage Mobile Access Credential
Credential Enrollment	Presentation (bitmask-based) or manual (badge ID only)	Presentation (select format) or manual (facility code + badge ID)
Credential Time Limit	Resolution to the minute	Resolution to the hour
Credential Count Limit	Offline approvals deducted from total on reconnect	Offline approvals deducted from total on reconnect
Toggle	Based on the last toggle event; changes the access point’s command state	Based on the current latch state only; command state unaffected
Credential ADA Relock Delay	Not supported	Configurable 1–255 second global delay
Host Based Credential Properties	Toggle, Count Limit, Time Limit	Count Limit
Rule End Times	Ends at the end of the specified end time	Ends at the start of the specified end time
Auto-Unlock w/ Badge Rules	One rule per device; specified user(s) start it by presenting a credential	Uses “First Person In” setting; any user with Grant Access permission can start it
Holiday Events	Works with Weekly Rules to suspend or activate a rule during the holiday period	Not available on Engage-linked tenants; use daily Lock/Unlock/Lock Down events instead
Custom Rules	“A user’s card is accepted” does not fire on toggle approvals	“A user’s card is accepted” fires on toggle approvals
Host Based	Admit, Lockdown, Schedule,	Admit, Lockdown, Schedule, Unlocked, Lock, Clear

Attribute	ISONAS RC04	Schlage Reader Controller
Commands	Unlocked	Tamper
Global Re-Lock Time	Supported	Not supported
Forced Door Alerts	No history event; “Unauthorized Open” alert only	“Forced Door Alert” history event plus “Unauthorized Open” alert
Active Directory	Syncs users, credentials, and user groups	Syncs users and user groups only (Engage-linked tenants)

A device can only support one DESFire type at a time. Switching a device back to its default configuration to restore Schlage DESFire compatibility is a paid service. —

! Once a tenant is linked with Engage, credential enrollment changes — presentation enrollment must happen at a Schlage Reader Controller, and existing credentials must be migrated or re-enrolled before they work at Schlage devices

- An RC04 pigtail-to-SRC adapter cable is available: P/N 47609539 – RC04 to SRC Adapter Cable.
- Active Directory integration is available only for RMR and 51+ door licenses.

Confirm the credential format and enrollment method match the target device type before deploying a mixed ISONAS and Schlage environment.

Last modified: 9 July 2026

Considerations when Linking

Linking Pure Access Cloud with Engage

To add supported Schlage devices (**RC11**, **RC15**, **RCK15**, **LE**, **LEB**, **NDE**, **NDEB**) to a Pure Access Cloud tenant, link the tenant with Engage first. Linking changes how the tenant handles credentials, enrollment, and several rule types — review the sections below before linking.

Commissioning Hardware

- Schlage devices commission to an Engage site created within the Pure Access Cloud account.

- Legacy Isonas **RC-04** and **IP Bridges** continue to commission directly to Pure Access Cloud through the Isonas configuration tool.

Credential Changes After Linking

Schlage devices don't read credential data the same way Isonas devices do, so credential enrollment changes to comply with Schlage requirements. As a result, existing credentials — except Isonas Pure Mobile and Key Pins — move into an **Unknown Format** state. They continue to work with Isonas devices but must be migrated or re-enrolled before they'll work with compatible Schlage devices.

Credential Migration

Migration converts existing credential data into the format required by Schlage devices, and requires the credential's format to be known and entered. See `Migrating Credentials (Legacy to Engage)` for the procedure. [MISSING: link URL to this manual section]

- If migration fails, decline the credential at a Schlage Reader Controller to collect the necessary read data, then retry.
- If migration fails again, re-enroll the credential so it works with compatible Schlage devices.
- If a newly introduced credential format requires a bitmask change, push the updated bitmask to legacy Isonas hardware so it can continue reading it.

Credential Enrollment Methods

Method	Requirements
Presentation Enrollment	Performed only at a Schlage Reader Controller; requires the correct credential format to be entered. If you add only Schlage Wi-Fi devices (**NDE**, **LE**) to a tenant with existing Isonas devices, presentation enrollment is no longer available at that tenant.
Manual Enrollment	Requires the correct credential format, facility code, and hotstamp badge ID. Facility code is not required for Isonas Proprietary Prox, Isonas DESFire EV2, Isonas HID, Isonas Mobile, or Schlage Mobile credentials.

Supported Credential Formats and Parity

When running Isonas and Schlage devices in the same tenant, use a credential format supported by both, and make sure the bitmask is set correctly on Isonas devices.

Hardware	Format support
Legacy Isonas	3 message formats: Isonas proximity/smart credentials by default (no bitmask required); one custom format requiring a bitmask; HID/Isonas-compatible credentials using the **ISONAS** bitmask

Hardware	Format support
RC-04	setting under **Settings > Credentials**.
Schlage **RC** / **NDEB** / **LEB**	Up to 24 total formats — the same 3 Isonas formats plus 21 additional 125kHz Prox and 13.56MHz smart credential formats.

For 13.56MHz smart credentials across an installation that includes Isonas devices, use Isonas DESFire — it's the only smart credential format Isonas devices can read via secure sector (encrypted) reading.

- Isonas IP Bridges require R1 readers with the bitmask set to **ISONAS**.
- Schlage Reader Controllers read Isonas DESFire using the **CE-5901-0402** configuration card. Schlage devices can only read one DESFire version at a time — reconfigured for Isonas DESFire, they can't also read Schlage DESFire unless returned to default configuration, which is a paid service (ship-in or on-site visit).

Mobile Credentials

Credential	Compatible hardware
Isonas Pure Mobile	RC-04 Reader Controllers and IP Bridges equipped with Isonas R1 readers.
Schlage Mobile	Schlage Reader Controllers, Bluetooth-enabled NDEB/LEB Wi-Fi locks, and IP Bridges with MTB readers. Requires **Schlage Compatibility Mode** enabled on the corresponding IP Bridge access point in Pure Access Cloud device settings.

Both mobile ID apps can be installed on the same phone and tied to the same cardholder record. Select the app that matches the reader or controller model at each door.

Behavior Differences After Linking with Engage

Setting	Behavior with Schlage devices
Credential Time Limit	Resolves to the hour, not the minute. A 9:40–11:15 window approves the credential between 9:00 and 11:00.
Credential Count Limit	Not updated in real time for Wi-Fi locks (LE/NDE), which don't maintain a persistent connection to Pure Access.
Global	Does not currently apply to Schlage devices.

Setting	Behavior with Schlage devices
Re-lock Time	
AUX outputs / RS-485	Schlage RC adds a separate AUX input, two AUX outputs, and an RS-485 connection, but Pure Access Cloud does not currently support the AUX outputs or RS-485 connection. [ASSUMED: verify this is still accurate]

Auto-Unlock with Badge (“First Person In”)

Auto-Unlock w/Badge rules are configured differently with Schlage devices, using a feature called **First Person In**. Enable it under **Auto-Unlock** rules in the Schlage Reader Controller’s device settings. Any user with **Grant Access** permission at the access point during the auto-unlock window can start the unlock by presenting a valid credential.

Holiday Events

Schlage Reader Controllers don’t support single events running longer than 24 hours, so Holiday Events are not available on Engage-linked tenants. NDEB and LEB locks don’t support the holiday feature at all.

Use Lock, Unlock, and Lock Down events instead. For periods beyond 24 hours, create an individual event for each day.

Only a Lock Down event overrides a Grant Access weekly rule — during Lock Down, access is limited to users who both have permission via an existing weekly rule **and** hold a credential with the **Master Bypass** special property. Alternatively, temporarily deactivate the weekly rule and reactivate it afterward.

Active Directory

Once a tenant is linked with Engage, Active Directory can no longer sync credential data — only users and user groups. Active Directory integration requires an RMR or 51+ door license.

Hardware Differences: RC-04 vs. Schlage RC

The RC-04 uses an 8-wire pigtail; the Schlage RC uses a 12-wire pigtail. [ASSUMED: confirm whether an adapter cable has since been released — as of the source material, one was still in development.]

Using the Engage Mobile App

Use the Engage mobile app for:

- Commissioning Schlage RC devices and offline devices (NDE, LE, etc.)
- Schlage device network configuration
- Updating Schlage offline devices from the server outside their scheduled check-in window

Manage all users, device settings, and rules in Pure Access Cloud — everything except the tasks above, which must be done in physical proximity to the device.

Additional Resources

- `Linking to Engage` — Pure Access Manual section on how to link a tenant with Engage. [MISSING: link URL]
- `Adding a Schlage device using ENGAGE` — Pure Access Manual section on commissioning Schlage devices. [MISSING: link URL]
- `Migrating Credentials (Legacy to Engage)` — Pure Access Manual section on credential migration. [MISSING: link URL]
- “Expanding Your Pure Access Cloud Business with Schlage’s Wi-Fi Locks” — video overview of linking a tenant with Engage. [MISSING: link URL]
- “Making the Transition to Isonas Pure Access Cloud 4.0” — video for Isonas-only (RC-03/RC-04/IP Bridge) customers evaluating the move. [MISSING: link URL]

Last modified: 9 July 2026