Faith Group

alcatraz ai

AlcatrazAI “The Rock”

JULY 2024

Table of Contents

Introduction

AlcatrazAI manufactures AI-driven facial recognition credential devices that are system agnostic. These devices utilize a person's face as their credential without the need to store images or templates on an enterprise's existing access control or IDMS server. This is enabled either by utilizing their cloud service or through the use of an on-premises management server. The system is GDPR, BIPA, and CCPA compliant because it does not use direct images of individuals but uses a checksum-based algorithm which is compiled from the original enrollment image. The architecture allows for enrollment at any reader or through the use of a mobile device making this stage of implementation very user friendly. The system only requires a category cable for network connectivity at the edge device and does not require any additional cabling to the access control system making it a great fit for augmenting or enhancing existing systems.

Problem

Biometric credential readers of all modalities (Facial, Palm, Iris, Fingerprint, Hand Geometry) have all traditionally had challenges related to the capture of initial credentials and repeatability of valid reads over time. As time goes on users frequently must update their saved valid credentials or experience a high occurrence of failed reads on devices. Some of these challenges relate to the modality being utilized and the role of the person using the device for example fingerprint readers get dirty and fingerprints of individuals who work with paper or cash tend to get worn or altered quickly. Faith Group is setting up a pilot in our Innovation Lab to validate ease of configuration and set-up, user enrollment, integration with Access Control systems and reliability of the solution.

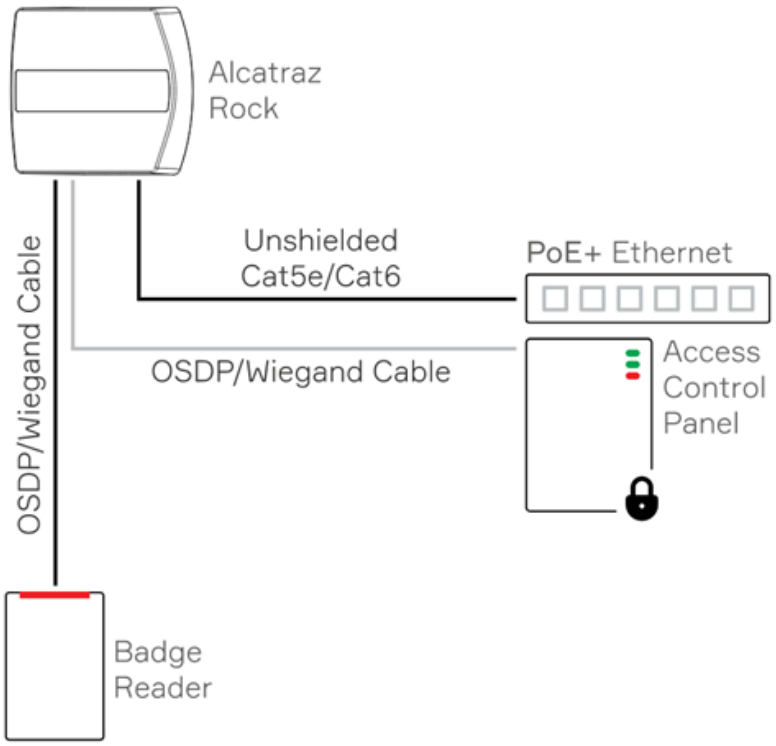
Testing Environment, Tools & Strategy

Testing took place at Faith Group's headquarters in St. Louis, MO. The initial testing was conducted in our lab environment utilizing the following equipment:

- Genetec Head-end Access Control Software
  - Running on HP hyper Converged Hardware
  - Virtual Machine
- Lenel Access Controller and Reader boards
- Life Safety Power Supply's
- Cisco 3850 Network Switch with POE
- HID RP40 Credential reader
  - OSDP2
- AlcatrazAI "The Rock"

The unit was installed per diagram below in accordance with manufacturer's instructions.

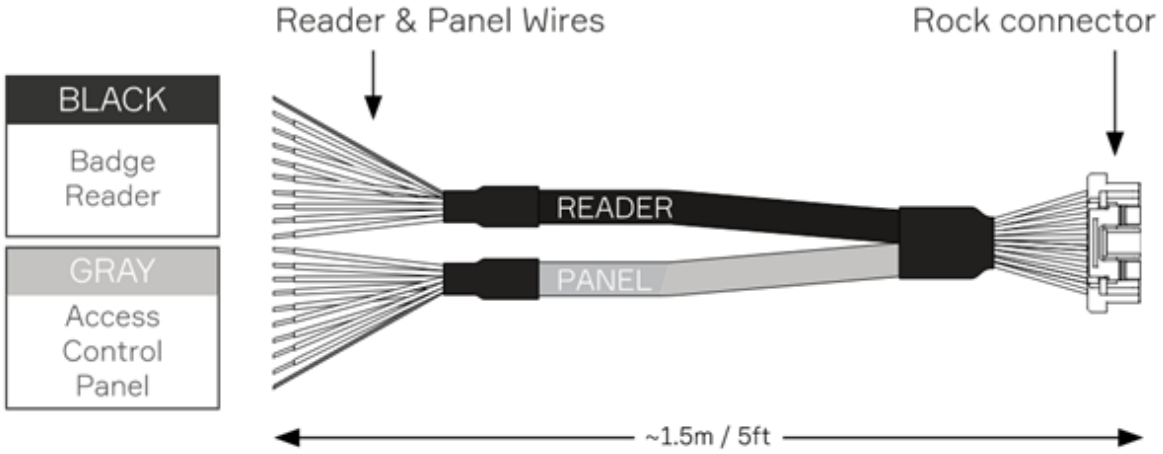
Connection Overview



Testing Environment, Tools & Strategy

The following wiring harness provided with the unit was used for the installation

Wiring Harness Connections



Initial Testing

Initial testing took place over 1 month. During this test, the reader was connected to our test system as shown above. Selected users were enrolled via the auto-enrollment feature and the unit was used to control one door. It was recorded that it took an average of 4-5 access events for the enrollment process to be complete. This was tracked via the unit's online web admin page. After enrollment was completed, the auto-enrollment feature was disabled, and the unit was used as the primary means of credential verification for access to the door. During this testing authorized and unauthorized users were presented to the

Supplemental Testing

Supplemental testing has taken place over the last year and a half. During this testing, the reader was relocated to the main office entry door at the Saint Louis office and connected to the production Genetec access control system in the same manner it was connected to the initial test system. Auto-enrollment was enabled on the unit however no staff was notified of the reader or its usage. Over the course of two weeks, users entered the office utilizing their badges and at the conclusion of this time, all office staff were actively enrolled in the system. At this time staff were notified and asked to report any issues with access using only the biometric reader.

Results

Initial Testing Results

- Auto-enrollment took place in 4 – 5 access events which is in line with manufacturers documentation
- Unit required no direct integration or programming on the access control system to function properly
- After 1 month all enrolled users still were granted access when presenting their face as a biometric token
- Unit logged all access events as did the access control system head-end
  - Should be noted that the access control system cannot differentiate between the facial biometric reader valid read and a valid card read at the associated reader
- System also logged instances of tailgating and cross-traffic events internally in its logs
  - These events were not forwarded to the ACS head end during this initial testing.
- There were no recorded instances of false positive reads during the testing period. (ie the system never

Supplemental Testing Results

- Auto-enrollment took place in 4 – 5 access events which is in line with manufacturers documentation
- Unit required no direct integration or programming on the access control system to function properly
- After 485 days all enrolled users still are granted access when presenting their face as a biometric token
- Unit logged all access events as did the access control system head-end
  - Should be noted that the access control system cannot differentiate between the facial biometric reader valid read and a valid card read at the associated reader
- System also logged instances of tailgating and cross-traffic events internally in its logs
  - These events were not forwarded to the ACS head end during this initial testing.
- There were no recorded instances of false positive reads during the testing period. (ie the system never granted access to an unauthorized/unbadged person)
- Despite being listed as an indoor reader this installation is outside under an overhang and functions reliably
  - The only noted deficiency is during periods of intense direct sunlight behind the individual being read, the unit has some challenges and will sometimes need to be shaded to function properly. Given the unit is not rated to be used in this environment this is not a manufacturer or equipment issue.

Conclusion

The AlcatrazAI Rock Facial Biometric reader performs as advertised by the manufacturer. It has proven to be rugged and reliable providing repeatable outcomes over extended periods of use. We have not experienced any false positive events in either testing application. The unit was easy to install and works properly with no integrations needed making it a great solution for enhancing or retrofitting into existing access control solutions.

Recommendations, Limitations & Opportunities

One notable limitation for the AlcatrazAI Rock Facial Biometric reader is that currently, only the indoor model is available. An outdoor model is scheduled for release 3rd quarter 2024. The outdoor model is supposed to address backlighting issues, and weather resistance and incorporates a built-in intercom. Faith Group is looking forward to testing the outdoor model soon.

Faith Group

About Us

Faith Group LLC was established in 2004 as a full-service women-owned consulting and engineering firm specializing in the planning and design of security, IT, audiovisual, safety, operational, and building systems for aviation, transit & rail, federal, state & local government, education, and commercial clients. The firm's mission focuses on helping clients unfold the complex issues surrounding continued operational changes, including those brought about by new technology development, federal regulation, and customer service opportunities.

The firm provides a full-range of services that include developing security and IT master plans, system design documents, requests for proposals, system testing, construction phase services, and commissioning. Since its inception, Faith Group has provided these services for more than 300 clients and more than 1,200 projects across North America and internationally. In addition to providing quality systems engineering, Faith Group focuses on planning for the operational and business processes that must be identified prior to designing and applying security and technology to a facilities' environment. By working with clients up front in this critical part of the process, Faith Group provides "as-is" and "to-be" business analysis coupled with sound engineering practices in order to meet the varied needs of their clients. At the core, Faith Group helps clients develop a new vision for the future and the tools required to help the client meet their new agenda.

Faith Group is comprised of more than 100 highly skilled professionals, most with more than 20 years of hands-on experience ranging from all aspects of operations to security, IT, safety and command control systems planning and design. Faith Group is headquartered in St. Louis, MO with regional offices in Atlanta, Dallas, Ft. Myers (FL), Minneapolis, Nashville, Philadelphia, Los Angeles, and Washington DC.

Faith Group is WBE/SBE certified with several different agencies.

HAVE QUESTIONS?

Joe Fallon
Director of Security & Construction Services
joef@faithgroupllc.com

Cary Gulsby
Professional Services Manager
cary.gulsby@faithgroupllc.com

Marcus Anderson
Security Systems Specialist
marcus.anderson@faithgroupllc.com

Cory Mayes
Lab Infrastructure Lead
cory.mayes@faithgroupllc.com