alcatraz ai

Alcatraz AI
Autonomous Access Control
Information Security Guide

Table of Contents

Purpose of this document:

The purpose of this document is to provide information required for a successful Information Security Review. The system architecture of the Alcatraz AI solutions: Cloud-Hosted and On-Premise, along with the network requirements are included.

Alcatraz Overview:

We enable our customers to make their buildings more safe and secure while bringing a frictionless experience to the user. The Alcatraz solution is scalable, fast, easy to integrate and works with existing access control systems. Our technology leverages artificial intelligence to make powerful real-time decisions at the edge. Whether the Rock is cloud-hosted or on-premise, the Rock provides capabilities to enroll effortlessly and is easily configurable in a number of mode's to meet the security needs of your organization. Our mission is to accelerate adoption of facial identity while staying focused on simplicity, security and privacy.

Alcatraz Company Privacy Policy:

Alcatraz values the privacy of our users and individuals in the environments in which our products operate. The Alcatraz platform is not designed for covert surveillance. The system provides configurable image and data retention settings to allow customers to comply with corporate governance and local legislation. The collection of enrollment data for the Alcatraz platform requires the user to interact with the Alcatraz hardware installed in the field. The system uses this data to create a profile that is fused with a user's badge data for identity authentication. The Alcatraz profile does not include information such as name, birthdate, email address, etc. Profiles can be deleted at any time. All logs, configurations and profiles are encrypted using industry best practices including AES-256 encryption.

The Alcatraz Administration Portal collects personally identifiable information from its registered users. This may include company email address, name, company physical address, and company telephone number, only for users that have created accounts in the Alcatraz platform. Information about the computer hardware and software used to access the Alcatraz platform is automatically collected by Alcatraz. This information includes: IP address, browser type, domain names, access times, and referring website addresses. This information is used by Alcatraz for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of the Alcatraz Administration Portal.

The Rock does not store or collect personally identifiable information such as names, birthdates, etc.

Enrollment with the Rock creates biometric profiles that are anonymous.

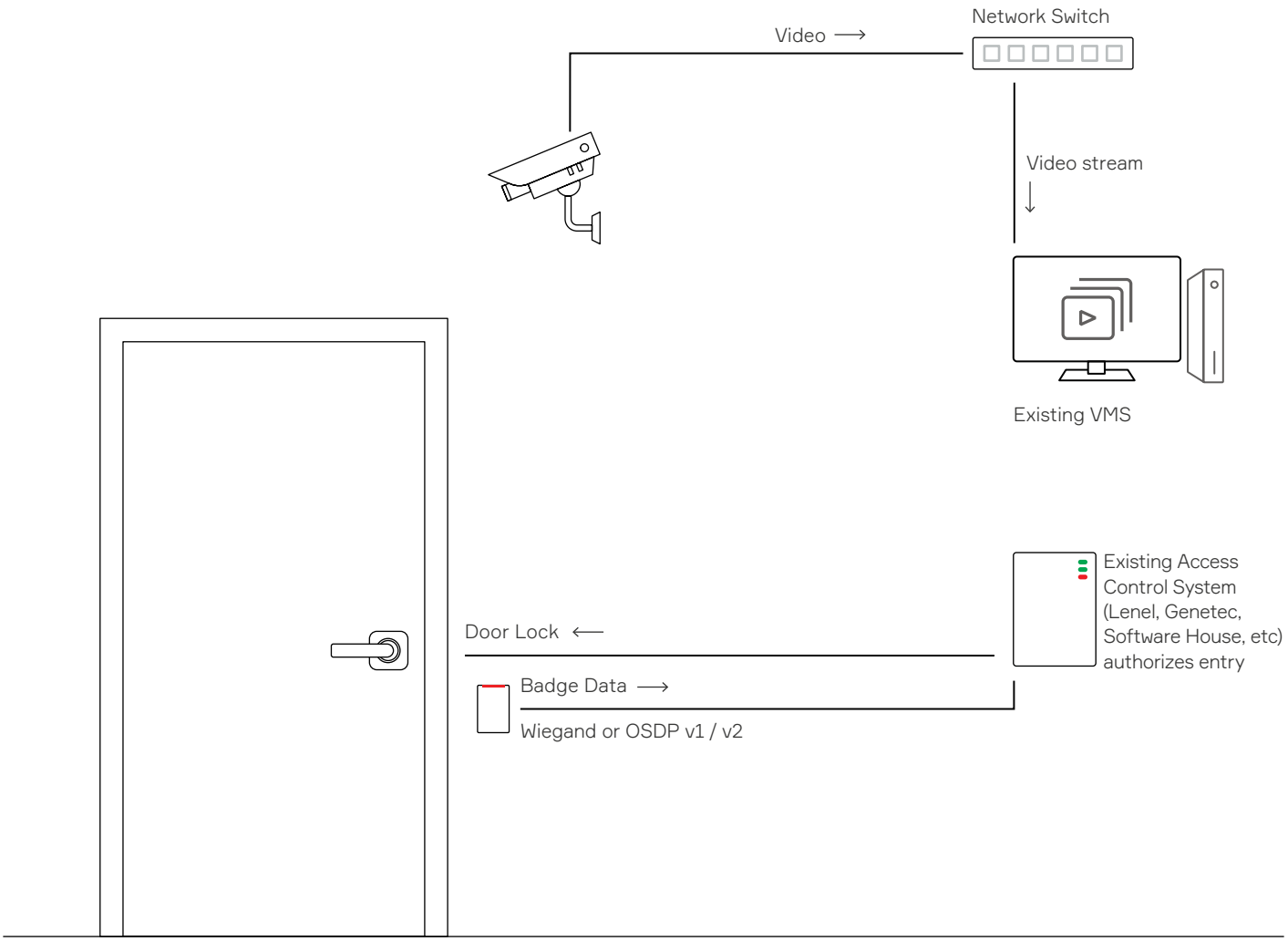
For all deployments, data is secured from end to end.

The Rock is not designed for surveillance and does not collect data for non-enrolled users.

Data is encrypted using AES-256 encryption.

Deletion of profiles can be performed at any time.

Your Existing Security Infrastructure



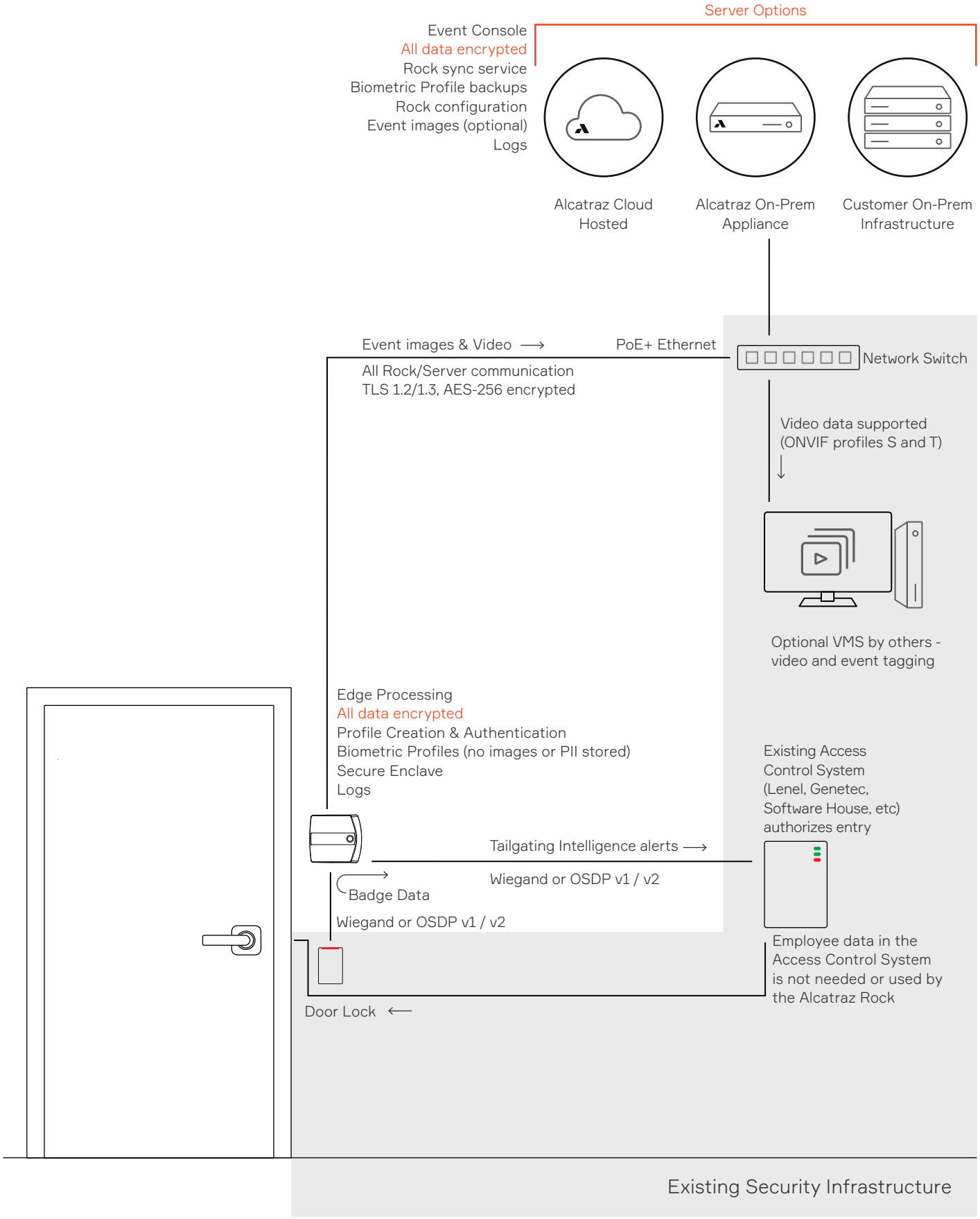
Existing Security Infrastructure

Your company's Access Control System determines who is authorized to access facilities. Commonly the system includes the access control panel and a badge reader. A user must provide their credentials, by swiping their badge which will be verified with an access control list, and thereby granting or denying the user access. The access control system ultimately controls the unlocking of the door.

A Video Management System (VMS) may be connected to the ACS to stream video, view events and alarms sent by the ACS.

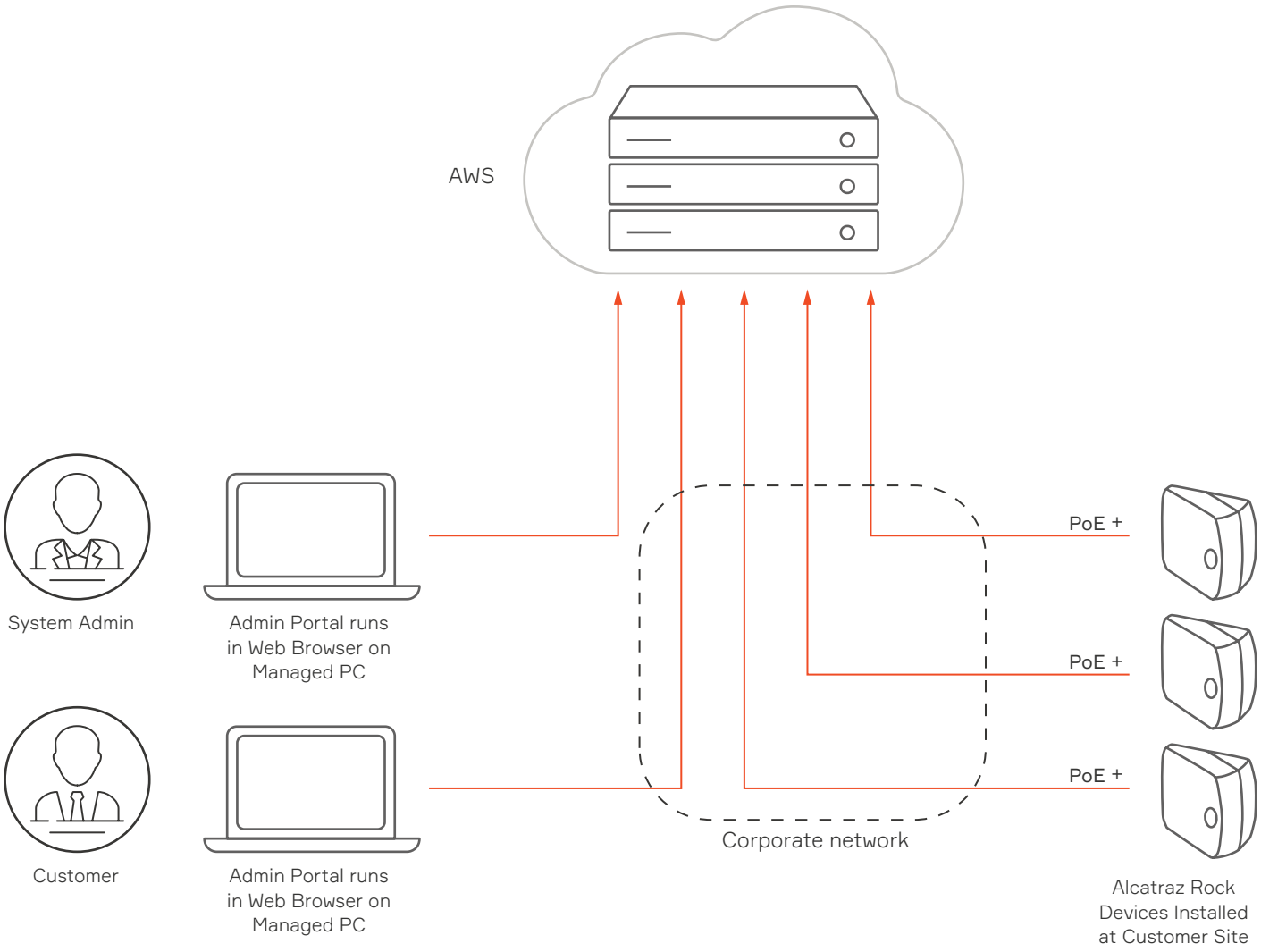
Wiegand and OSDP (Open Supervised Device Protocol) are both communication protocols that are used to connect devices in access control systems. Communicating badge numbers, LED control, and tamper are examples of functions over these protocols. There are some notable differences between connecting by Wiegand vs. OSDP. Wiring for Wiegand requires at minimum 5 wires and additional wires for more functionality whereas OSDP requires 4 wires to provide the same functionality as Wiegand setups. Wiegand communication is uni-directional vs. bidirectional for OSDP). So whether your current system is using Wiegand or OSDP, the Rock supports both protocols for communication between the badge reader and Rock as well as between the Rock and ACS panel.

How your Access Control System works with the Alcatraz Rock



Cloud Hosted System

The Alcatraz Cloud-Hosted system includes one or more Rocks and a customer provided computer for accessing the Alcatraz Admin Portal.



Platform Architecture: AWS Containers
Device OS: Custom Linux Derivative
Encryption: AES-256
Security Protocol: TLS 1.2
Rock Power: PoE+ (802.3at Type 2) 30W

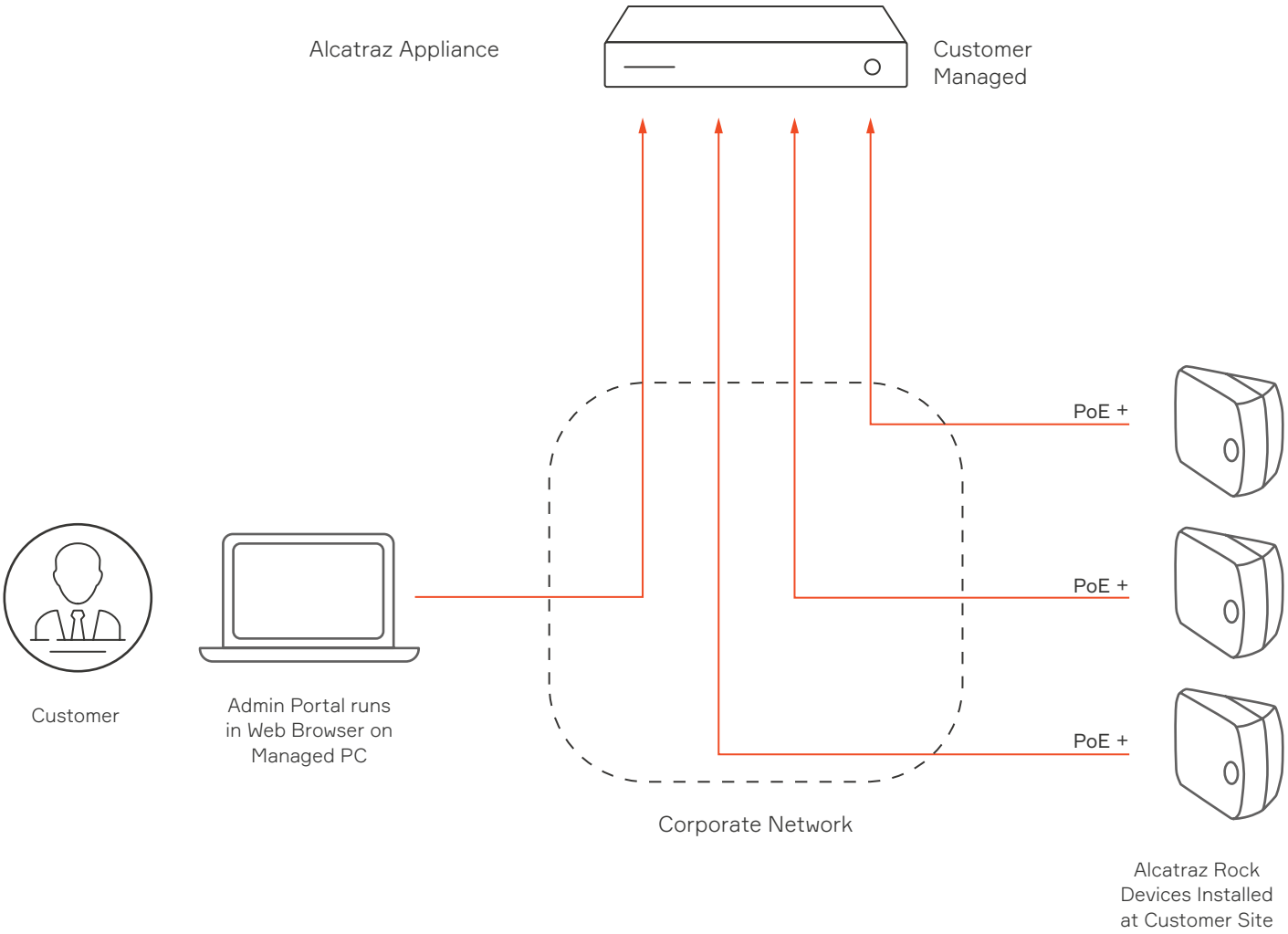
Cloud Hosted Network Requirements

1. If you have Captive Portal Login, it must be disabled.
2. Whitelist the urls given by Alcatraz AI with specific instance name
   - https://platform.<YourCloudInstance>.alcatraz.ai
   - https://devices.<YourCloudInstance>.alcatraz.ai
   - Unless **Your Cloud Instance** name has been provided by Alcatraz AI, the Alcatraz AI Cloud info is as follows for whitelisting:
     Whitelist the Cloud URLs
     – https://platform.us.alcatraz.ai
     – https://devices.us.alcatraz.ai
     OR Cloud IPs
     – 3.23.74.102
     – 3.140.166.106
3. These ports are required to be opened. These are outbound only from the Rock.

Ports Required for Rock		
TCP 443	UI and Events	Outbound from Rock to Alcatraz AI Cloud
TCP 3310	Data Sync	
TCP 8443	Device On-boarding and Updates	
UDP 53	DNS	Outbound from Rock to DNS Server
UDP 123	NTP	Outbound from Rock to NTP Server
Ports for ACS Integration		
TCP 3033	ACS Integration only (optional)	Outbound from ACS Integration Server to Alcatraz AI Cloud
Ports for ONVIF		
TCP 80	ONVIF Agent	Inbound to the Rock from the VMS
TCP 554	RTSP Streaming	
UDP 554	RTSP Streaming	
UDP 3792	ONVIF Discovery	
Other Multicast Ports as defined by the VMS		

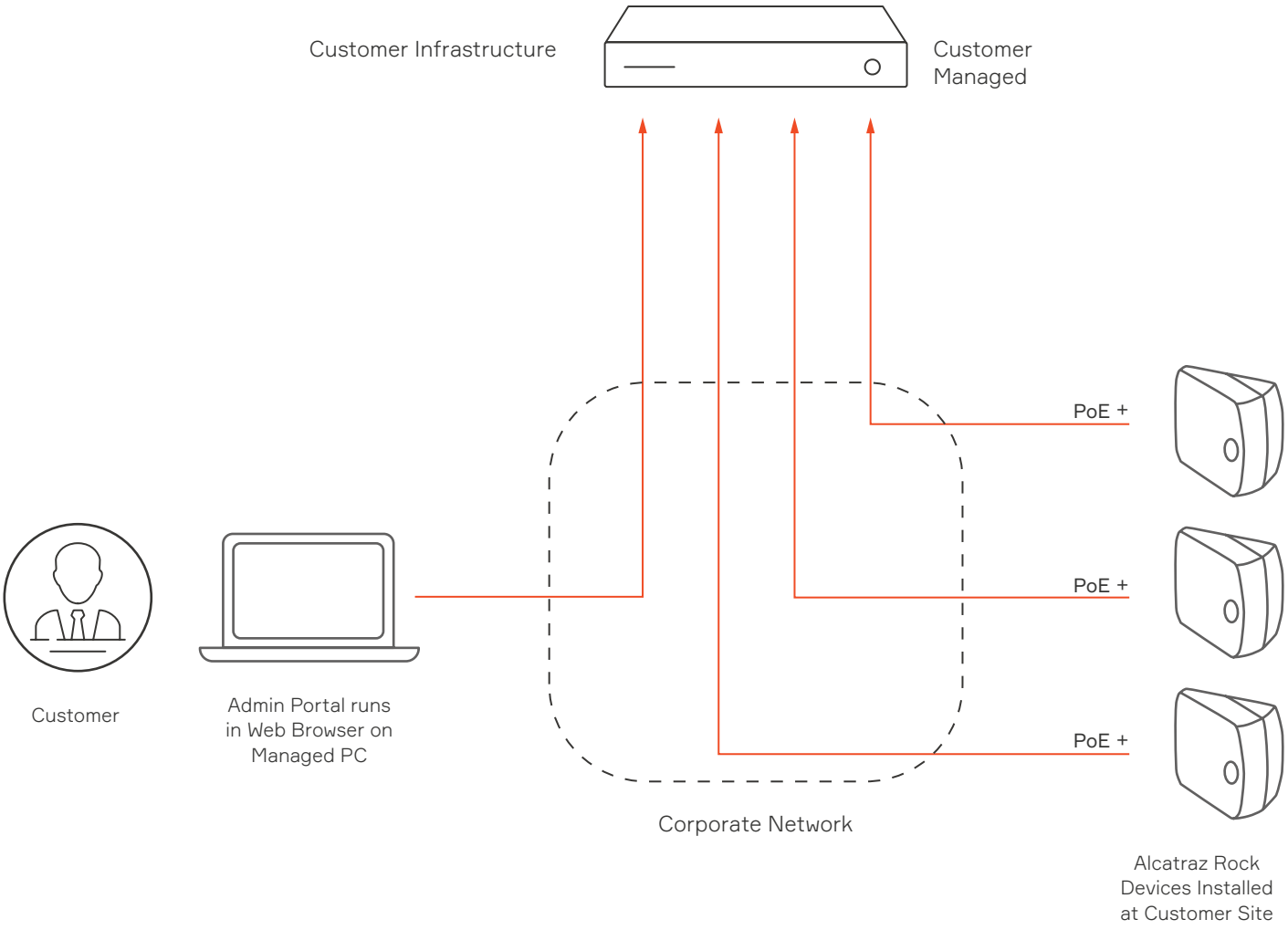
On-Prem System

The on-prem system includes either the Alcatraz AI appliance or a customer provided server installed with the Alcatraz AI software package, one or more Rocks, and a customer provided computer for accessing the Alcatraz AI Admin Portal.



Server OS: Windows Server 2019 Essentials
Platform Architecture: Natively pre-built and running Windows Services
Device OS: Custom Linux Derivative
Encryption: AES-256
Security Protocol: TLS 1.3
Rock Power: PoE+ (802.3at Type 2) 30W

Customer Provided Infrastructure



Server OS: Windows Server 2019, CentOS 8 & RHEL 8
Platform Architecture: Natively pre-built Services
Device OS: Custom Linux Derivative
Encryption: AES-256
Security Protocol: TLS 1.2/1.3
Rock Power: PoE+ (802.3at Type 2) 30W

On-Prem Network Requirements

If ALL components are not on the same subnet, the following ports must be open to the on-prem appliance:

1. Whitelist the urls for specific Alcatraz Platform server.
   - https://<ip address>
2. These ports are required to be opened. These are outbound from the Rock.

Ports Required for Rock		
TCP 443	UI and Events	Outbound from Rock to the Alcatraz Platform
TCP 3310	Data Sync	
TCP 8443	Device On-boarding and Updates	
UDP 53	DNS	Outbound from Rock to DNS Server
UDP 123	NTP	Outbound from Rock to NTP Server
Ports for ACS Integration		
TCP 3033	ACS Integration only (optional)	Outbound from ACS Integration Server to the Alcatraz Platform
Ports for ONVIF		
TCP 80	ONVIF Agent	Inbound to the Rock from the VMS
TCP 554	RTSP Streaming	
UDP 554	RTSP Streaming	
UDP 3792	ONVIF Discovery	
Other Multicast Ports as defined by the VMS		

Custom Configuration

NTP server access is required and provided by customer.
If customer cannot provide, the Alcatraz AI platform can be setup to provide NTP services as an option.

System requirements

Max Rock Quantity	Processor	Memory	Storage	Network
50	Intel® Core i3 10105 3.7GHz, 6M cache, 4C/8T or better	8GB or better	512 GB Hard Drive	100 Mbps or better
200	Intel® Core i3 10305 3.8GHz, 8M cache, 4C/8T or better	8GB or better	1 TB Hard Drive	1000 Mbps or better
500	Intel® Core i5 10505 3.2GHz, 12M cache, 6C/12T or better	16GB or better	2 TB Hard Drive	1000 Mbps or better
> 500	Contact Alcatraz AI for details.			

Cloud Alliance CAIQ Questionnaire:

Provided upon request

The Consensus Assessments Initiative Questionnaire (CAIQ) v4.0.2 offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services, providing security control transparency. It provides a set of Yes/No questions a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix (CCM). It is created and maintained by the Cloud Security Alliance (CSA) whose members include companies such as Accenture, Adobe, Atlassian, Dell, Dropbox, Google, HP, IBM, McAfee, Microsoft, Oracle, Raytheon, etc.

3rd Party Pen Test Security Assessment:

Carve Systems was engaged to assess the Alcatraz components for threats. Further info on the successfully completed audit can be requested.

Alcatraz Certifications:

Alcatraz incorporates the highest of standards in designing our platform which is why we seek certification from a variety of professional organizations. We have been certified by national and international testing standards.

FC CE ISO 27001 ISO 27017 ISO 27018

ETL LISTED Intertek GDPR CCPA NDAA COMPLIANT

581-0014-00-07