Feenics

Cyber Security Hardening Guide

HOW FEENICS PROTECTS THE DATA AND INTEGRITY OF TRANSACTIONS

keep™ by FEENICS

FEENICS, INC. | 301-2310 St. Laurent Blvd., Ottawa, Ontario K1G 5H9 | (855) 333-6427 | www.feenics.com

Contents

‘Keep Secure’

How Feenics protects the data and security of transactions

For those who are new to cloud computing, the term “cloud” can sometimes bring concerns regarding digital security. What they may not know is that when using the appropriate methods and technology, cloud-based access control solutions are safer than ever before. In addition, cloud solutions bring more cyber security and resiliency than traditional legacy on-premise systems.

The Feenics Philosophy

Feenics approaches data security and data access in a multi-layered design philosophy. We followed what Microsoft refers to as SD3+C. Secure by Design, Secure by Default, Secure in Deployment and Communications. Keep was designed from the ground up to be a cloud based product and that requirement dictates that software security is paramount.

Roles-based User Rights

Roles-based user rights provides users to specifics areas of the software or partitions based on login permissions set by the administrator to accomplish the tasks assigned to that user’s rights. A user may have different rights in different parts of the enterprise. For example, a user may be able to enroll new card holders for the Ottawa office, but not the Baltimore office or not have access to specific features of the software, such as visitor management or badge creation.

No Default Passwords

An often-over-looked security vulnerability is default passwords. Many systems contain them and many never get changed. A quick internet search for “default passwords” under a specific access control product will turn up the factory default, which also means that a perpetrator looking to get into the system will do the same. Keep uses no default usernames and passwords. Each hosted by Feenics system is issued with a unique password. This is really the first step in designing with both human nature in mind and our secure by design philosophy.

Security Levels

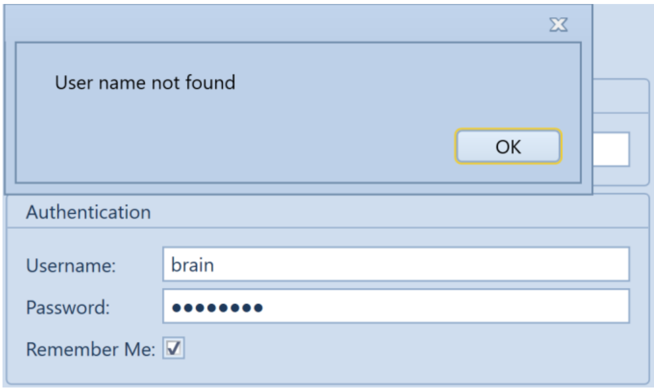
Keep allows administrators to set a Security Level that will dictate how much information is returned to a user attempting to login if that attempt is invalid.

For example, in a lower security environment, if the name ‘brain’ instead of ‘brian’, the user gets “User name not found” as we can see in Figure 1 to the right.

At a <u>High Security</u> level, if the user spelled their username incorrectly, they would just receive an ‘Invalid Logon’ as Feenics would not give a potential hacker any extra information on why they can’t access the system. This helps limit phishing attempts and brute force attacks.

This is the first step in protecting your logon process.

Figure 1: Low Security Level Setting



User name not found

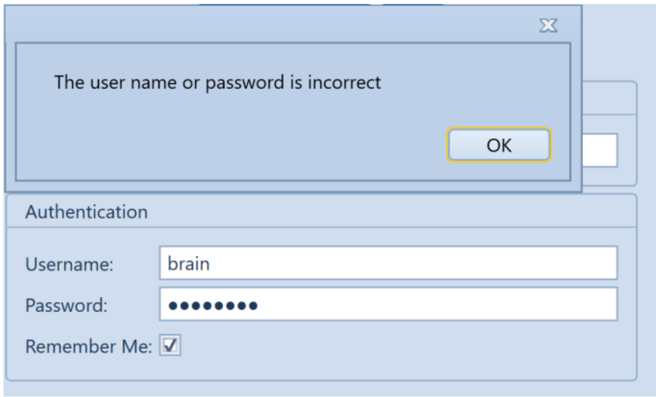
Authentication

Username: brain

Password: ●●●●●●●●

Remember Me: ☑

Figure 2: High Security Level Setting



The user name or password is incorrect

Authentication

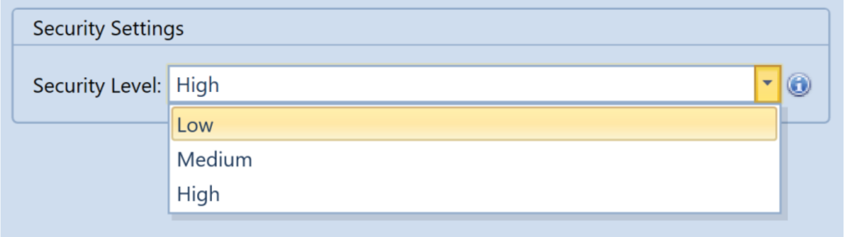
Username: brain

Password: ●●●●●●●●●

Remember Me: ☑

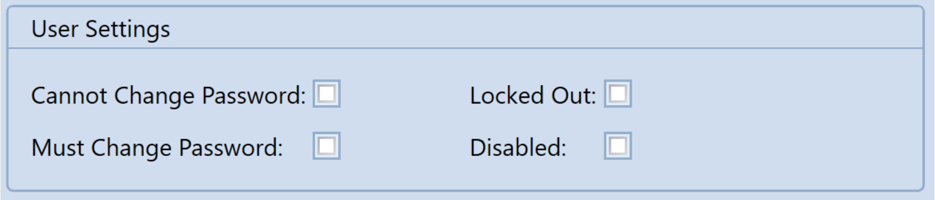
Password Requirements

Keep allows system administrators to enforce varying degrees of password strength to meet organization requirements. Administrators can also require that system users must change their passwords every so many days.



Security Settings

Security Level: High



User Settings

Cannot Change Password: □

Locked Out: □

Must Change Password: □

Disabled: □

Two Factor Authentication (TFA)

Often administrators following best practices in password security require that all system users accessing company IT resources must use so called strong passwords. Strong passwords are typically 8 characters or more and include both alpha-numeric text and special characters.

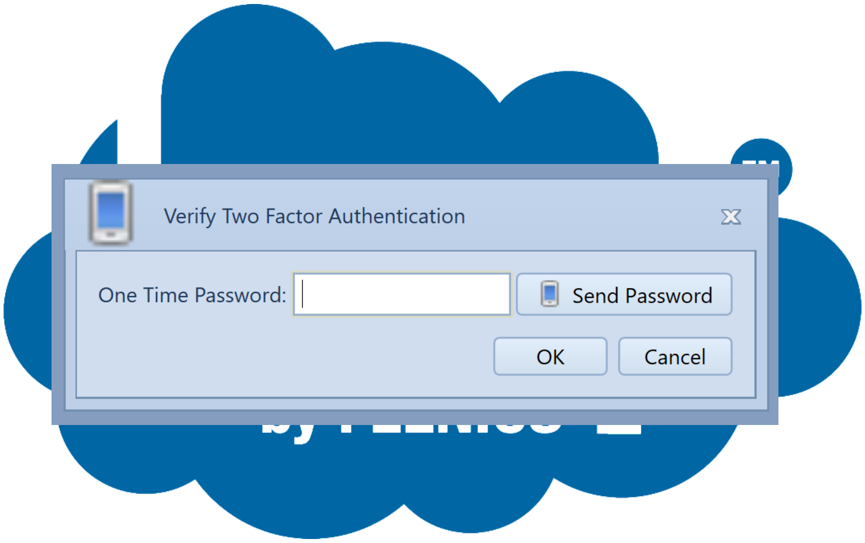
However, they run into the unexpected roadblock of basic human behavior. That system users often feel overwhelmed by the number and length of the passwords they have to remember and how often they must be changed. This leads to system users recycling the same password for different systems or the computer monitor with several yellow Post-It notes stuck to the side, each with a username and password for a system. A frustrated user has now circumvented a best practice and created gaping holes in IT security.

Feenics supports two factor authentications. Two Factor Authentication not only provides unrivaled security in the access control space, it can also help to both mitigate and even prevent system users from creating security vulnerabilities. Two Factor authentication helps you get past this be requiring the extra code that is specific to users and devices and is updated every 30 seconds.

An authenticator can be attached to the login of any user for an added layer of security. User accounts are linked with the authenticator company of choice which generates a one-time token with an expiration. Users must provide this code upon entering their username and password. Now a perpetrator would need three things to access the system:

1. Your username
2. Your password
3. Your device

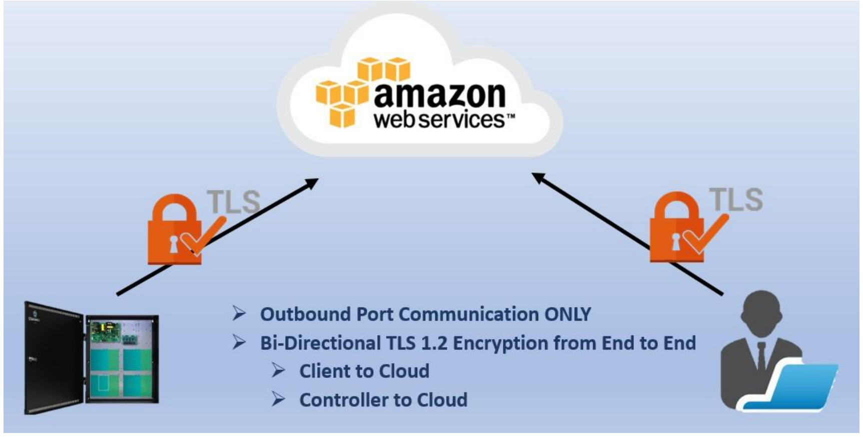
Note: Keep's two factor authentication follows the IETF RCC 6238 for Time Base One Time Password Algorithm. Many applications such as Google Authenticator, Duo, AWS and LastPass, all support this standard.



Data Encryption

Feenics protects the transmission of data between the client and the cloud based server using modern TLS 1.2 encryption. This same technology is used to secure credit card information, social security numbers, and login credentials. TLS 1.2 is essentially the next step in the evolution of encryption and has replaced SSL.

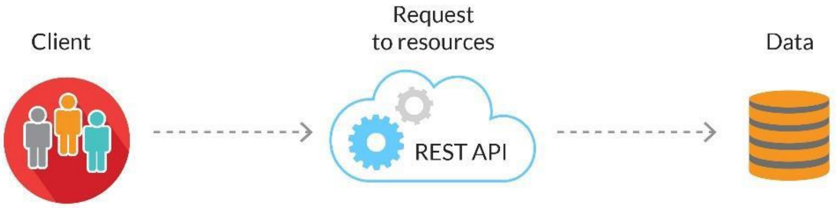
All data in transit (moving from or to AWS) is protected by TLS 1.2 encryption while data at rest (once the data reaches AWS' servers) is protected with server-side encryption (SSE).



- Outbound Port Communication ONLY
- Bi-Directional TLS 1.2 Encryption from End to End
  - Client to Cloud
  - Controller to Cloud

No accessibility to the Database

The is ZERO access to the database. All activity related to the database must pass through Feenics RESTful API. The MongoDB resides on its replica sets behind AWS' firewalls in an encrypted state.



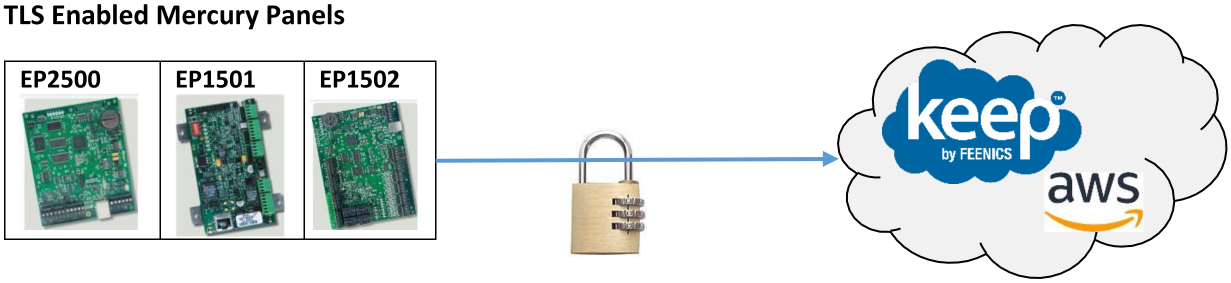
Audit Logs

User activity audit logs are first class citizen with the rest of the event pipeline. Alerts can be generated (email, SMS, mobile, WebHooks) for data modification just as for door access. For example, send the user a text after two successive failed login attempts.

Transport Layer Security (TLS)

Feenics can encrypt the data being transmitted from the hardware controllers to the cloud using TLS 1.2 encryption on Mercury panels. Many other access control providers offer some sort of panel encryption but it is often very cumbersome to setup. It is often very difficult to setup for the integrator which means it becomes costlier to the customer and we see that human nature again gets in the way. A justification is made that the risk of someone eavesdropping on your hardware communication is low and not worth the cost to implement. Feenics addresses this by using TLS encryption on the Mercury panel which is a simple checkbox for the integrator. Feenics cloud based servers then automatically negotiate that encryption.

TLS Enabled Mercury Panels



TLS allows for asymmetric sharing of symmetric keys for AES 128 Encryption. It works similarly to SSL except that it uses a By Protocol connection rather than By Port. This means that connections are first initiated to the server by an insecure broadcast and then switch to secured communications once the handshake has been established. TLS 1.2 is the latest and most secure version that is implemented across devices. Using TLS Keep encrypts the transfer of data from the client to the server, as well as the controller to the server.

Mercury's Series 3 'Red' boards

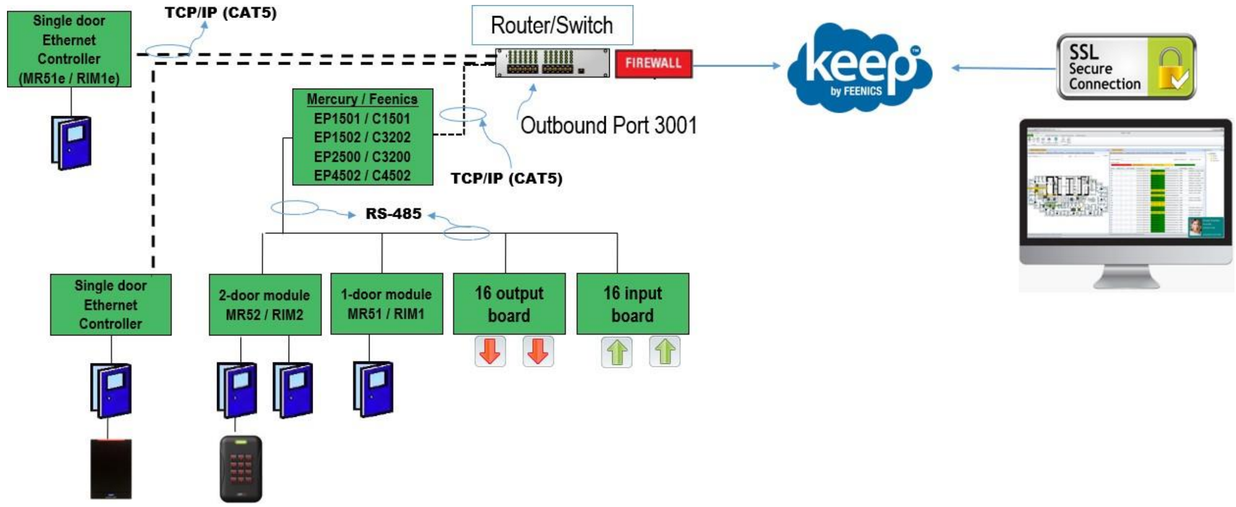
Mercury's introduction of the series 3 downstream modules also enhances additional security functionality at the field level with the following:

- Enhanced Cyber Security capabilities
  - SAM Chip – Encrypted storage of data and keys
  - RS485 communications (MSP1) encrypted by default
  - AES256 encryption (LP series controllers in July, 2018)
- Full OSDP Support (SIA Link)

Communication Ports

The following outbound ports must be opened to effectively communicate between Keep and its connected devices:

3001 – Mercury Controllers to Cloud (Outbound only)
443 – Client to Server (Outbound only)



Keep only uses outbound ports, meaning that an IT director will never have to open inbound ports on their network. This helps keep customer networks safe. All communications originate from inside the customer firewall. Once the cloud-based server answers, two-way communication is initialized.

Veracode

Feenics has entered a contractual agreement with Veracode, who is owned by CA Technologies. With each software release, Feenics submits our code to Veracode for both static and dynamic code analysis. Veracode looks for all cyber security vulnerabilities that they can find and produces a report to Feenics detailing all low, medium, and high threats. The goal was to instill confidence that Feenics is doing everything possible to maintain the integrity of Keep while protecting the customer from any outside influences that could cause a breach or cyber-attack to the end user.

VERACODE

ca technologies VERACODE
VERIFIED
STANDARD

In April 2018, the API for Keep passed the stringent year-long process of becoming Verified, Veracode's vulnerability compliance assessment. Feenics is now listed on Veracode's, Verified directory.

Stay Up to Date

Feenics utilizes Amazon Web Services (AWS) as its hosted environment. AWS is the largest datacenter provider in the world. Utilizing AWS adds layers of redundancy and security that most standard users could never afford on their own. The AWS EC2 instances that we use include their own SLAs and guaranties.

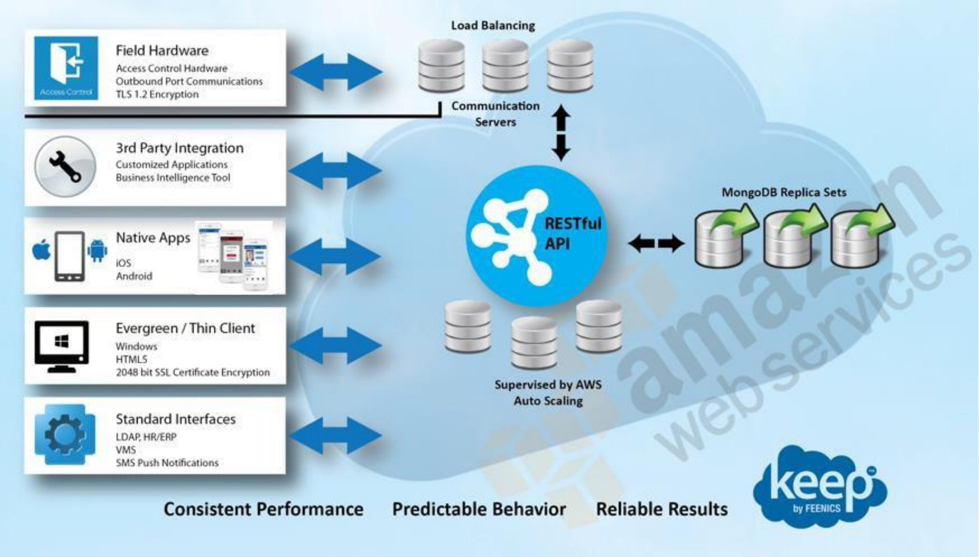
When Feenics hosts customer systems in AWS, the following are provided:

1. Full backups every 24 hours for point in time recovery.
    a. Mongo Database replica sets running on a minimum of three redundant servers.
2. Monthly software updates. This could be new features/functionality, patches or fixes. Remember that access to buildings is not impacted by software updates.
    a. Updates frequently include simple training videos on new features and improvements in the system.
3. Elastic Block Storage – data is written to multiple availability zones for redundancy.
4. All operating systems, database, webserver and application patching and updates.
5. Maintain all services that facilitate communications

RESTful API Architecture

While the user's experience resides at the interface, Keep's engine is built on a RESTful API, or common language for all developers. Keep is 100% open for developers to allow other integrations to interoperate with the platform. There is no direct access to the MongoDB. Everything MUST go through the API.

Feenics employs the power of AWS' load balancing at the communication servers to meet the demands of the API calls to maintain optimum performance, and auto scaling, to allow expansion for the customer based on growth. Horizontal scaling allows peak transactional moments to occur, without the need to increase hardware requirements of the actual servers (RAM, memory, HDD capacity), or vertical scaling, which is what occurs on traditional on premise configurations.


Field Hardware
Access Control
Access Control Hardware
Outbound Port Communications
TLS 1.2 Encryption
3rd Party Integration
Customized Applications
Business Intelligence Tool
Native Apps
iOS
Android
Evergreen / Thin Client
Windows
HTML5
2048 bit SSL Certificate Encryption
Standard Interfaces
LDAP, HR/ERP
VMS
SMS Push Notifications
Load Balancing
Communication Servers
RESTful API
MongoDB Replica Sets
Supervised by AWS Auto Scaling
amazon web services
Consistent Performance
Predictable Behavior
Reliable Results
keep by FEENICS