Swift Sensors Advanced Security Protocols

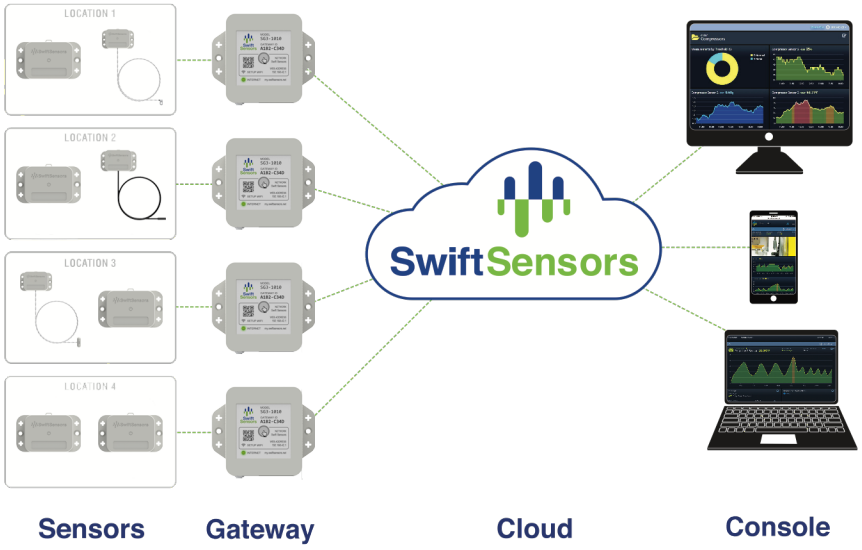
The Swift Sensors cloud-based service is designed with advanced technologies to keep your monitoring system safe and secure. This document describes the relevant aspects of the service, software, and hardware as they relate to security.

SwiftSensors

Swift Sensors | 4611 Bee Caves Road, Suite 100 | Austin, Texas 78746 | www.swiftsensors.com | +1 512 256 7552

Cloud-Based Architecture

The Swift Sensors Cloud system is built by industry experts with extensive experience in corporate network security implementing best practices according to the ISO/IEC 27001 security standard. The cloud-based architecture eliminates ongoing server, storage, and software maintenance. This means that the sensor system is always up to date, regardless of project or enterprise size, and the customer does not have to worry about applying security patches to client software.



Data Storage

The Swift Sensors Cloud stores two types of data: relational data and time-series data. Relational data is stored in a relational database cluster hosted by AWS and consists of metadata about the Swift Sensors hardware, other entities created by the customer in the Swift Sensors Console such as custom dashboards and thresholds, and the relationships among the various entities. Timeseries data is stored in a time-series database cluster hosted by InfluxDB that captures the history of time-stamped measurement values as reported by the sensors. Data at rest is not encrypted with the exception of user passwords, which are stored in a hashed and salted format.

Swift Sensors | 4611 Bee Caves Road, Suite 100 | Austin, Texas 78746 | www.swiftsensors.com | +1 512 256 7552

Data Security

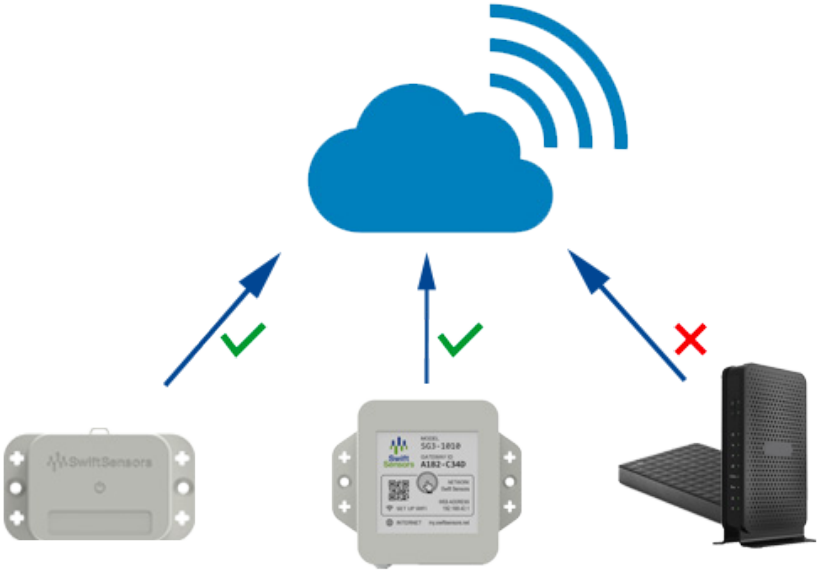
All data between Swift Sensors Gateways and the Swift Sensors Cloud is encrypted utilizing 256-bit AES encryption and then securely transmitted over Secure Sockets Layer (SSL) on port 443. Sensor to Gateway encryption is now at the forefront of our design with Swift Sensors Series 3. With 128-bit AES encryption between the sensor and gateway, your data is protected throughout your entire sensor system.*

AES encryption is common across the IT industry and is considered very strong by today's security standards.

*Swift Sensor measurement readings are also safe from manual manipulation from within the cloud software. The Swift Sensors Console does not allow any data to be manipulated or changed.

Connections to the Swift Sensors Cloud

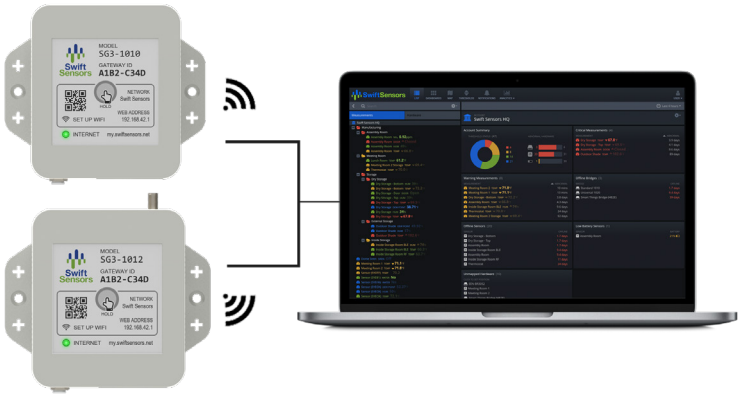
The Swift Sensors Cloud accepts connections only from two entities: Sensor data uploads from legitimate Swift Sensors gateways and valid API access requests from the Swift Sensors Console or a third-party app. All other connections to the Swift Sensors Cloud are rejected. Deprecated gateways can be blacklisted and automatically shut down by the Swift Sensors Cloud.



Cloud-Based Architecture

The Swift Sensors gateway is designed to periodically initiate a connection exclusively to the Swift Sensors Cloud to securely transmit sensor data. The gateway can operate inside firewalled networks as long as the firewall rules do not prevent the gateway from reaching out over port 443 to the external IP address resolved by “hub.swiftsensors.net“.

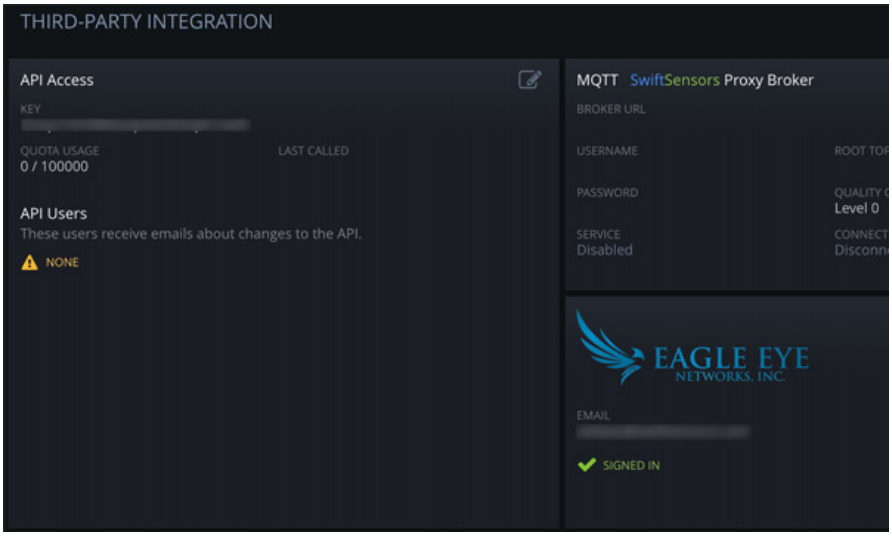
The gateway is designed not to accept incoming connections, except during the limited hotspot mode used for WiFi configuration. When the gateway is unable to reach “hub.swiftsensors.net“, the gateway will assume that internet access is not available and switch to hotspot mode to serve up the Wi-Fi Configuration page used to configure or reconfigure the gateway’s WiFi credentials to give the customer an opportunity to restore internet access using WiFi.



Connections from Apps Using API Access

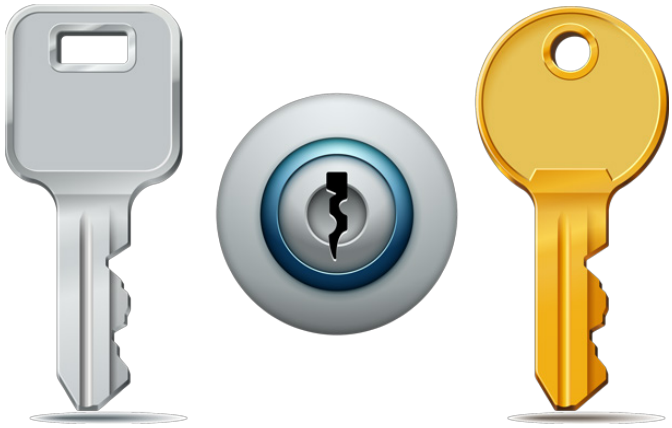
Swift Sensors provides an application programming interface (API) to allow third-party developers to create custom applications that communicate directly with the Swift Sensors Cloud servers. The same API is used by the Swift Sensors Console. The Swift Sensors API adheres to the REST standard for organizing all API endpoints to make the endpoints easier to manage and secure.

Upon request, API access is granted to customers using a unique 32-character alpha-numeric API key tied to the customer’s account. This key can be re-generated at any time if it ever becomes compromised.



Authorization Token

To establish a connection with the Swift Sensors Cloud and create a user session, an application must submit a valid API key, username, and password for a user on the same account. The server will respond with an authorization token that must be included in all subsequent data requests. The authorization token is unique for the user session and cannot be reused by another user agent. The authorization token expires in 24 hours. Before the token expires, a new refresh token can be generated using the original token without having to re-enter user credentials to extend the lifetime of the user session beyond the original 24 hour period.



Access Control

Swift Sensors offers two primary methods for controlling access to Swift Sensors data and commands: **role-based access control** and **account hierarchy-based access contro**l. Combining these methods of access control provides a wide range of flexibility suitable for organizations of all shapes and sizes. These access control methods are explained below.

Role-Based Access Control (RBAC)

The Swift Sensors Cloud service implements role-based access control (RBAC). User access to data and commands depends on the role of the user used to generate the session token. From Multi-Account Administrator to Reader, these different roles offer various levels of interaction that can aid in the workflow within your facility.

No user can change their own role. No user can elevate the role of another user to a role with more privileges than their own role. By default, the first user on the account has the highest role of Multi-Account Admin, and that user can invite additional users to join the account with a role of the first-user's choosing. If the first user creates additional Multi-Account Admins or Admins, those users can also invite additional users to join the account since all Admins have user management privileges.

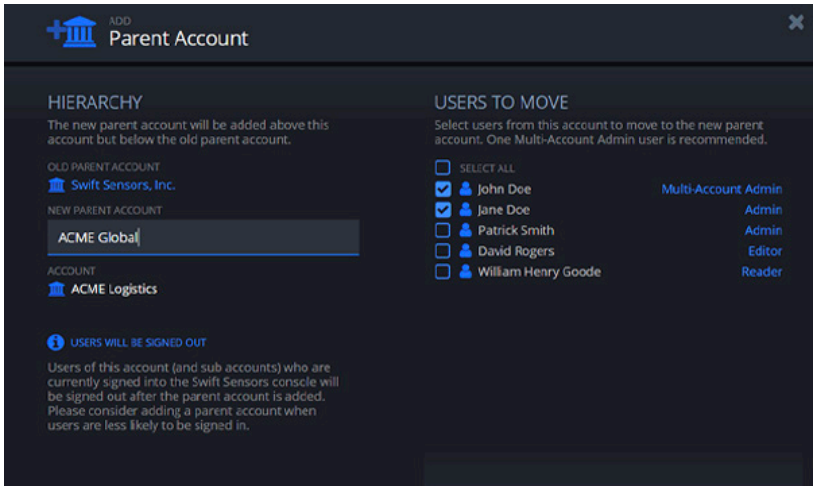
Role Definitions

Reader – Browse the list, dashboards, map, thresholds, and notifications in read-only mode, and build reports.
Editor – Reader privileges plus management of the list, dashboard, thresholds, notifications and deleting empty gateways.
Admin – Editor privileges plus management of users, WiFi settings, and deleting sensors.
Multi-Account Reader – Reader privileges on the home account and all sub-accounts.
Multi-Account Editor – Editor privileges on the home account and all sub-accounts.
Multi-Account Admin – Admin privileges on the home account and all sub-accounts, plus management of Multi-Account Admin users.

With these different levels of administration, the assurance of reliability, control and access is defined strictly by you. Utilizing each role can aid in the workflow and efficiency of your facility.

Account Hierarchy-Based Access Control

Swift Sensors supports nested account hierarchies. This means that accounts can have sub-accounts, which themselves can have sub-accounts, and so on. Users with multi-account roles have access to data on their account and any descendant sub-accounts, but cannot access data on the parent or ancestor accounts, if such accounts exist. This access includes notifications, so multi-account users can choose to receive notifications for hardware or measurements located in one or more sub-accounts. Sub-accounts can be managed only by multi-account users and only within the scope of the user's account branch.



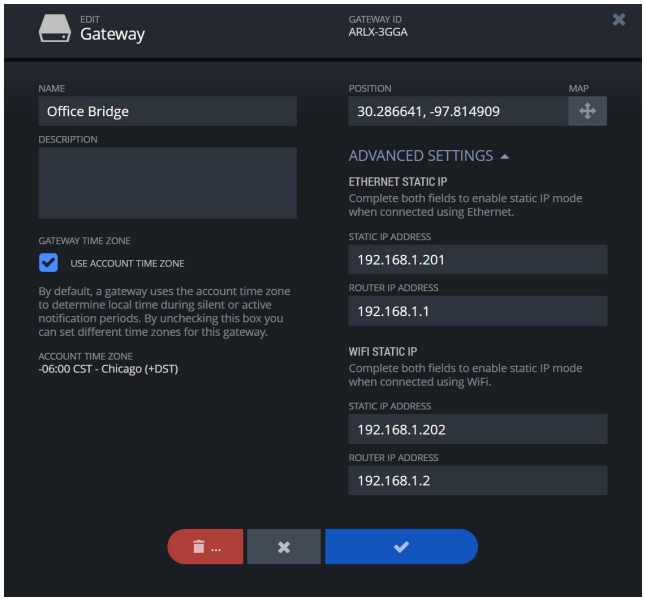
Swift Sensors Cloud-Based Console

The Swift Sensors Console is the command and control center for the entire distributed sensing system. Designed as a responsive web app running in a browser in full-screen mode, the Console is the primary consumer of the Swift Sensors API described below, and therefore benefits from all the security measures and access controls enforced by the API. Since the Console is served up from the Cloud, it is always up to date with the latest security enhancements and bug fixes. When the Swift Sensors Cloud software is updated, the Console web app is able to update itself without user intervention even while the user is already signed-in.

Learn more about the Console at www.swiftsensors.com/products/console

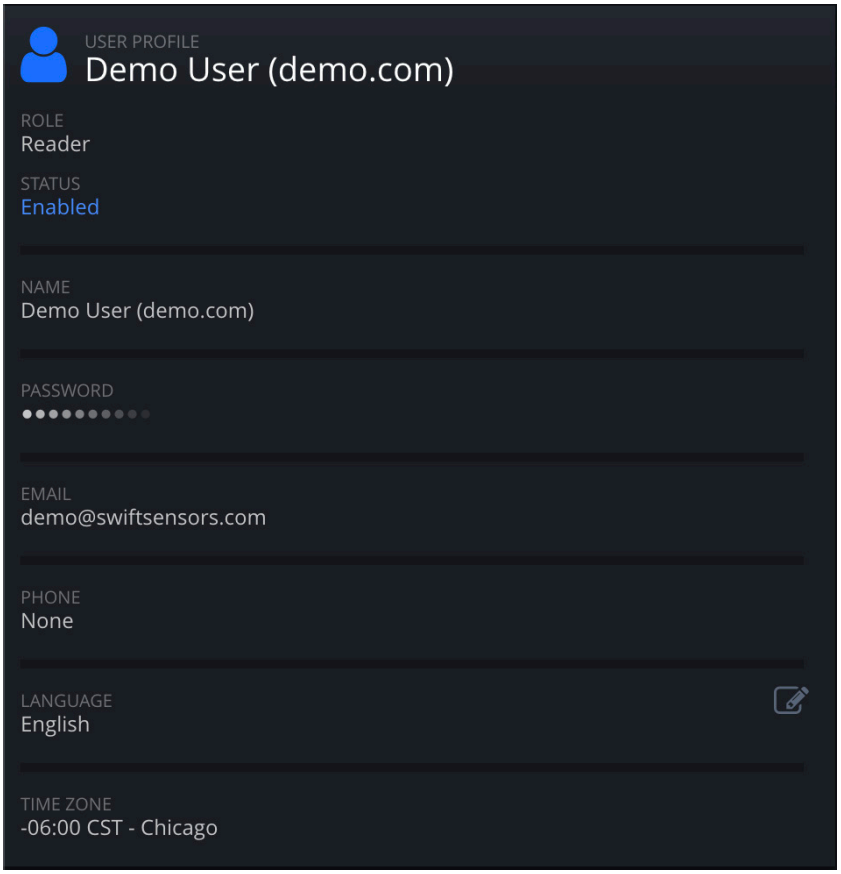
Linking Hardware to Account

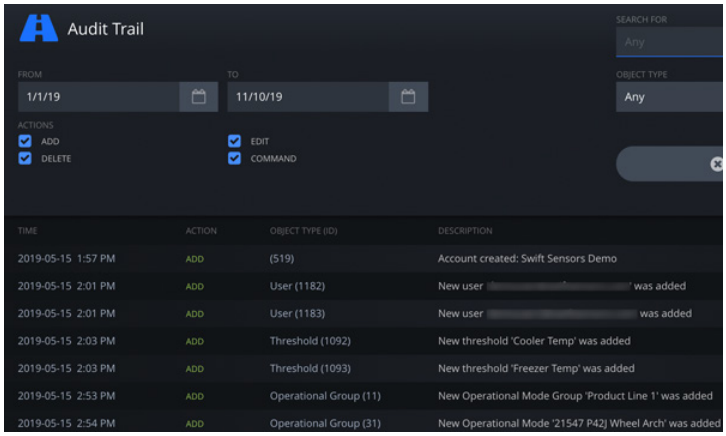
Once a new gateway is added to an account, the gateway becomes permanently linked to that account and can transmit sensor data only to that account until it is deleted or migrated to another account. Likewise, once a new sensor is detected by a gateway on the account, that sensor becomes permanently linked to that account and can transmit sensor data only to that account using any gateway linked to that account unless the sensor is deleted or migrated to another account. If a sensor that has already been linked to one account tries to communicate with a gateway linked to another account, the gateway linked to the other account will refuse to connect to that sensor, and no sensor data will be collected until a gateway linked to the same account as the sensor comes in range of the sensor.



User Passwords, Emails, and Phone Numbers

The Swift Sensors Cloud supports very strong user passwords with a length of up to 255 characters. User passwords are always transmitted to the Swift Sensors Cloud while the connection is encrypted. Finally, user passwords are always stored in a hashed and salted format to protect the user. Changes to user emails are protected by a verification process that emails a verification link to the new email address with a special verification key embedded in the link. The email change only takes effect when the user clicks on the verification link and then enters their user credentials on the email verification page of the Swift Sensors Console. Changes to user phone numbers are protected by a verification process that sends an SMS text message with a verification code to the new phone number. The phone number change only takes effect when the user enters the verification code while signed into the Swift Sensors Console.





Audit Trail

All user actions are audited and stored in the audit trail history for each account. Audited information includes the user id, user email, timestamp, type of action, type and the id of the object acted upon, and a description of the action taken. This creates a permanent record of all user activity for each customer account.

Two-Factor Authentication

The Swift Sensors Cloud Console supports and provides users with the option to enable two-factor authentication. With two-factor authentication, users gain an additional level of security with their personal account data and sensor measurements. When a user enables two-factor authentication, our server will alert the account owner via text message that two-factor authentication has been enabled on the account. Once enabled, any login attempt will now be prompted with a one-time password request window. Our servers will then send a unique, six-digit one-time password through text message to the selected user's phone number associated with the account. A user is able to select 'Trust this Device' which allows for the selected device to bypass the authentication request window for 30 days.