Building Optimization Broker SaaS Security and Compliance

SAAS Security Compliance

Updated: April 2022

Overview

The WennSoft solution is a SAAS (Software as a service) solution. SAAS is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. WennSoft utilizes Amazon Web Services (AWS) to host our software solution. Since none of the software is hosted at WennSoft facilities, we will defer to certain security processes, disaster recovery/business continuity processes, and certifications maintained and achieved by AWS. A current and more detailed explanation and description of AWS Cloud Security can be reviewed at https://aws.amazon.com/security.

Physical and Logical Security of the Servers and Hosting Facility

AWS Security Responsibilities

Amazon Web Services is responsible for protecting the global infrastructure that runs all the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS's number one priority, and while you can't visit AWS data centers or offices to see this protection firsthand, AWS provides several reports from third-party auditors who have verified compliance with a variety of computer security standards and regulations. For more information, visit aws.amazon.com/compliance[1].

Note that in addition to protecting this global infrastructure, AWS is responsible for the security configuration of its products that are considered managed services. For these services, AWS will handle basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

Physical and Environmental Security

AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

1 http://aws.amazon.com/compliance

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems. Power1

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Network Security

The AWS network has been architected to permit WennSoft to select the level of security and resiliency appropriate for our workload. To enable WennSoft to build geographically dispersed, fault-tolerant web architectures with cloud resources, AWS has implemented a world-class network infrastructure that is carefully monitored and managed.

Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

ACLs, or traffic flow policies, are established on each managed interface, which manages and enforces the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS’s ACL- Manage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.

Secure Access Points

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic.

These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows you to establish a secure communication session with your storage or compute instances within AWS. To support customers with FIPS cryptographic requirements, the SSL-terminating load balancers in AWS GovCloud (US) are FIPS 140-2-compliant.

In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices.

Transmission Protection

You can connect to an AWS access point via HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

The AWS network provides significant protection against traditional network security issues including Distributed Denial of Service (DDoS) attacks, Main in the Middle (MITM) attacks, IP spoofing, Port Scanning, Packet sniffing by other tenants. In addition to monitoring, regular vulnerability scans are performed on the host operating system, web application, and databases in the AWS environment using a variety of tools.

WennSoft Security Policies for AWS

Security for access to AWS is controlled by the primary account ID through the WennSoft Director of IT. All passwords must be changed every 90 days, password length must be a minimum of 8, password makeup requires the following: at least one uppercase letter, at least one lowercase letter, at least one number, and require at least one non-alphanumeric character, and the last four passwords are remembered. Multi-factor authentication (MFA) is also required once a user logs into AWS. Utilizing MFA provides another method of access control in which a user is granted access only after successfully presenting several pieces of evidence to the authentication process. In this case, something they know (userid and password) and something they have (a validated authentication device such as a cellphone/mobile device).

Access to actual server instances on AWS is secured through the following means: non-standard ports, SSL, proxy services, user-specific IDs, access/traffic logging, and firewall rules that only allow specific IP addresses to be granted access.

Backup and Recovery and Fault-Tolerance

Fault-Tolerant Design

Amazon’s infrastructure has a high level of availability and provides you with the capability to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in

lower-risk flood plains (specific flood zone categorization varies by region). In addition to utilizing discrete uninterruptible power supply (UPS) and onsite backup generators, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

Backups and Recovery

WennSoft utilizes Amazon Relational Database Services (Amazon RDS). Amazon RDS manages the database instance on WennSoft's behalf by performing backups, handling failover, and maintaining the database software. Turned on by default, the automated backup feature of Amazon RDS enables point-in-time recovery for WennSoft's DB Instance. Amazon RDS backs up the database and transaction logs and stores both for a 7-day retention period. This allows us to restore our DB Instance to any second during the retention period, up to the last 5 minutes.

The BOB Application server is backed up on a weekly basis utilizing the CloudRanger service. Backups are retained for 1 month.

Incident Handling

Incidents are submitted to the WennSoft support team via email (support@wennsoft.com), phone (262- 317-3800), or web portal (https://www.wennsoft.com/wsportal). Each incident is logged, categorized by product, and prioritized based on impact and urgency. WennSoft Support then employs various methods of troubleshooting to determine the root cause for issues. If necessary, issues are escalated internally or externally for additional assessment or resolution. Service Level Agreements (SLA's) are determined by the support package purchased by the customer.

Logs of security attacks and NDA's

Security Logs

As important as credentials and encrypted endpoints are for preventing security problems, logs are just as crucial for understanding events after a problem has occurred. And to be effective as a security tool, a log must include not just a list of what happened and when, but also identify the source. To help with after-the-fact investigations and near-real-time intrusion detection, AWS CloudTrail provides a log of all requests for AWS resources within our environment. For each event, we can see what service was accessed, what action was performed, and who made the request. CloudTrail captures information about every API call to every AWS resource being used, including sign-in events.

Non-Disclosure Agreements

Non-disclosure agreements (NDA) and licensing agreements between WennSoft and our customers are normally signed during the sales process and purchase process. If WennSoft's records indicate these documents have not been signed when a customer decides to subscribe to WennSoft's SAAS solutions, the appropriate documents will be provided for authorized signatures.

Process Compliance

AWS's ISO 27001 certificate is located at https://aws.amazon.com/compliance/iso-certified/.

SOC Cloud compliance information is located at https://aws.amazon.com/compliance/soc-faqs/.

Reference: Security, Identity & Compliance | AWS Architecture Center (amazon.com)[2] (May 2021)

ISO Certified (amazon.com)[3]

Security

Updated: April 2022

Traditional BAS Security Approach

Traditional building automation systems (BAS) and non-Cloud analytics solutions require installers or end-users to deploy their server solutions within a corporate network. While there is nothing inherently insecure about deploying vendor solutions within corporate networks, there is an increased responsibility taken on by the installer and end-user to ensure that the solutions are deployed in a secure manner. This includes taking responsibility for:

- SSL certificate management
- Network access management (Public and Private)
- Database management
- Application maintenance
- Operating system maintenance
- Hypervisor maintenance
- Physical security to data centers

When a vendor system is deployed, specifically in the building automation and analytics space, the expectation of the vendor and end-user is that the system is available from any location and any device. This is typically accomplished in one of two ways:

- VPN Access
- Exposing the application to the internet with a public IP address

Once the solution is exposed to the internet with a public address, that solution is now a target for attackers to leverage as a penetration point into the corporate network. While some attacks target applications like building automation and analytics systems, the attackers are typically more interested in corporate information that is placed behind the firewall with no direct access from the internet.

Traditional building automation systems (BAS) and non-Cloud analytics solutions, that require top-to-bottom management by vendors and end-users, are more susceptible to cyber-attacks.

Building Optimization Broker Security Approach

To address the security weaknesses in traditional BAS models, WennSoft® has architected the Building Optimization Broker solution in a significantly different manner:

Fully Managed Cloud Services

- The Building Optimization Broker application service is deployed in a fully managed cloud in AWS
- The Building Optimization Broker database server is deployed in a fully managed cloud in AWS

2 https://aws.amazon.com/architecture/security-identity-compliance/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type=*all&awsf.methodology=*all

3 https://aws.amazon.com/compliance/iso-certified/

AWS (Amazon) Handles	WennSoft® Handles
Operating System maintenance (Database)	Operating System maintenance (Application Servers)
Hypervisor maintenance	Network access management (Public and Private)
Physical security to data centers	Database management
	Application maintenance

SSL Communications between Clients and Server/Database

- Building Optimization Broker MiniAgents communicate with the Building Optimization Broker database and application server using SSL
    - The Building Optimization Broker Desktop Application communicates with the Building Optimization Broker database and application server using SSL

Proprietary Communications Protocol

Our “mLink” protocol employs a proprietary messaging system that only WennSoft® devices and applications are able to decrypt.

MiniAgent Client Certificates

All MiniAgents are configured with a client certificate to identify it as a WennSoft MiniAgent. This ensures that Building Optimization Broker can only talk to our MiniAgents and nothing else.

Outbound Only Ports for On-Premises Components (MiniAgent and Building Optimization Broker Desktop)

Instead of exposing the Building Optimization Broker MiniAgent to the internet, which would mark the MiniAgent as a potential penetration point into the corporate network, the MiniAgent sits securely behind a firewall and only requires outbound ports for communication with the Building Optimization Broker database and application server.

By employing the above security features Building Optimization Broker allows vendors and end-users to:

- Remove the need to handle top-to-bottom management and maintenance of the solution
- Securely access live and historic building automation data without exposing those systems to the internet

With the Building Optimization Broker tunneling feature, WennSoft provides vendors and end-users access to the building automation system in a manner significantly more secure than the required exposing of other vendor solutions to the internet.

By architecting WennSoft cloud solutions in the manner described above, a cyber-attack would be near impossible, and minimizes potential impact to vendors, building owners, tenants, and their end-users.

Security FAQs

Updated: April 2022

Overview

This document provides answers to common network and security questions about the Building Optimization Broker from WennSoft™.

If there are additional questions that are not covered in this document, please contact a sales representative from WennSoft.

General Security

How do you get data from a sensor/endpoint and into AWS? What level of encryption are you using? If VPN, please reference a standard.

All data is sent from the MiniAgent to the AWS Database via SSL. The SSL Cipher used is ECDHE-RSA-AES256-GCM-SHA384. The data collected from the BAS uses BACnet or oBIX and the level of security is dependent on the level of security set up by the controls installer.

How do you authenticate the connections to the endpoints from AWS to prevent rogue systems from feeding data?

The WennSoft MiniAgent uses a specific set of credentials set up by WennSoft and AWS to authenticate to the Database and store the data. All communications are secured via the SSL connection discussed above.

What security controls are in place to manage communications between the endpoints and the gateway device?

We use security groups within an AWS VPC to limit what connections can be made to the database. This is secured not only through firewall protections, but SSL and login credentials as well.

What security controls are in place to lock the gateway down to again protect customers and our systems & interests?

Our MiniAgent only uses outbound ports to AWS, uses SSL to communicate to AWS resources, and each agent has a client certificate for the server to verify the agent is legitimate.

How is patching handled?

We push automatic updates down to all MiniAgents and server patching is handled via a maintenance schedule.

Are there any communication/workflows that are bidirectional to customer equipment from the gateway?

Yes, the MiniAgent can receive requests to activate/adjust points in the BAS, but this must be configured by the installer of Building Optimization Broker. The communication from the configuration software to AWS is all SSL encrypted and locked down through login credentials. All communication between AWS and the MiniAgent is SSL encrypted and secured as described above.

How are ports filtered and managed?

AWS ports are filtered and managed by AWS security groups, OS Firewall rules, and Network ACLs. Ports on the customer's site where the MiniAgent reside are filtered and managed by their IT provider.

Do the gateways accept ANY information from external networks through the customer connections? For example, is the endpoint EVER routable to the Internet? How do you ensure this independent of customer network configurations?

It is recommended that the MiniAgent be placed behind a firewall with no inbound ports opened and routed to the MiniAgent. With that said, if the MiniAgent is exposed to the web via an inbound firewall port and public IP the device could accept requests, but the requests would need to conform to the Building Optimization Broker proprietary protocol and would require the SSL encryption to be deciphered.

What is the name and address of the location where the data will physically reside?

Amazon Web Services Northern Virginia Region, there are 6 data centers, and the data will be spread across them all. Amazon does not provide us with addresses for the data centers.

Does the application encrypt data before sending it over the internet or an open network?

Data is not encrypted at rest but is encrypted in transit.

Can the vendor supply the CPU chassis serial number and hard drive serial number for the hardware that will be utilized?

No, data is hosted in AWS, and we have no access to the physical hardware, nor do we know what physical machines at AWS our applications are running on.

Is the application HIPAA compliant?

No

Are you compatible with 3rd party encryption?

Contact your WennSoft sales representative. They will work our technical team to confirm compatibility or will schedule time to perform a compatibility certification.

Will you utilize any subcontractors to develop, deliver, support, or process the product or service?

Yes

Has the vendor, product, or service (including subcontractors relevant to this project) been involved in, included with, part of, affiliated with, or in any way connected to, or a target or victim of a data breach or security incident?

No

Hosted Environment: Physical Security

Does a third party host the platform?

Yes, Amazon Web Services. SOC1, SOC,2, and SOC3 reports are available. For us to send the SOC reports an NDA between the customer and Amazon must be in place.

Are documented security policies and procedures in place to guide personnel in granting, controlling, and monitoring physical access to the data center facility?

Yes

Is written documentation and supervisor approval needed to add, modify, and/or terminate access privileges?

Yes

Does corporate security management perform a review of badge access privileges and physical keys on a periodic basis to help ensure that access privileges are current?

Yes

Are digital surveillance cameras in place throughout the data center facility to monitor activity?

Yes

Is the data center facility monitored 24 hours per day?

Yes

Is physical hardware maintained behind locked server racks and cages?

Yes

Hosted Environment: System Administrative Security

Are system access privileges of terminated employees revoked as a component of the employee termination process?

Yes

Are strong password controls for access to systems in place?

Yes

Is a Privileged Access Management system in place for administrative access (e.g. password vaulting and activity recording)?

Yes

Are vendor-recommended security patches applied in a timely fashion?

Yes, all database security patches are applied by Amazon. For application servers, they are applied as required.

Is intrusion detection/prevention monitoring in place?

Yes

Web Hosted Application Security

Please describe how authentication to the web application is secured (e.g. two-factor authentication, password) in a comment.

Username/Password Combination

Please describe how user accounts are provisioned (e.g. separate database, integrated with on-premise application, integrated with customer enterprise directory).

Application database in AWS

Network Data Requirements

What are the network bandwidth requirements?

The bandwidth requirements and frequency depend on trend interval and object counts configured by the user in the WennSoft Building Optimization Broker software. Building Optimization Broker requires ~25 bytes per object that is trended. If you trend 2,000 objects 4x per hour it's roughly 200kB per hour.

Software updates range in size, but are typically applied once per month and are roughly 8MB.

Are there any load balancing requirements?

No

Are there any layer 2 or layer 3 adjacency requirements?

No

Are there any DNS requirements?

Yes, the MiniAgent installed on-site and the Building Optimization Broker website will require DNS to access the cloud services for Building Optimization Broker.

Are there any POE requirements? If yes, please list the power draw per type of devices to be deployed.

No

What are the per-device overall network throughput projections?

The bandwidth requirements and frequency depend on trend interval and object counts configured by the user in the WennSoft Building Optimization Broker software. Building Optimization Broker requires ~25 bytes per object that is trended. If you trend 2,000 objects 4x per hour it's roughly 200kB per hour.

Software updates range in size, but are typically applied once per month and are roughly 8MB.

If we do network maintenance during our standard Sunday 2 am to 4 am maintenance window, will your application be ok?

Yes

Does this solution need to be able to access public internet?

Yes

Are there any wireless requirements?

No

What are the make, model, and relevant network specifications for each model of hardware that will be deployed?

Embedded Linux device, Model Number MA-001. Network Specs: 100 Mbps Ethernet.

What are the security and/or firewall requirements for this request?

The Building Optimization Broker MiniAgent (physical data pump) will need to be installed on the local network with access to the Building Automation System (BAS). The MiniAgent will require 4-outbound ports (5432, 57000, 57001, and a Custom Port assigned when contract is signed) for connectivity to the WennSoft Cloud.

How many connections to the internet are required?

One (1) internet connection is required per MiniAgent. A MiniAgent is required per Building Automation System connection.

What are the IP requirements?

Private Static IP per MiniAgent