brivo

# Brivo Smart Home Security and Compliance

## A DETAILED REVIEW OF ASSURED CONTROL

## Notice

Users are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Brivo product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Brivo and its affiliates, suppliers or licensors. Information in this document is subject to change without notice and does not represent a commitment on the part of Brivo Systems LLC. For the most up-to-date information, visit www.brivo.com

Brivo products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of Brivo to its users are controlled by Brivo agreements, and this document is not part of, nor does it modify, any agreement between Brivo and its users.

This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of Brivo Systems LLC. The information contained within this document or within the product itself is considered the exclusive property of Brivo Systems LLC. All information in this document or within the hardware and software products themselves is protected by the copyright and/or other intellectual property laws of the United States.

# Table of Contents


**Notice** 2
**Table of Contents** 3
**Overview** 4
**Shared Responsibility** 5
**Reseller's Responsibility** 6
**User's Responsibility** 7
**Brivo's Responsibility** 8
Brivo's 8
Third Parties 8
**Brivo Smart Home Architecture** 9
**Brivo Smart Home Account Management** 10
Gateways 10
**Device Control Process** 11
**Third Party Integrations** 11
API Services 11
**Cloud Computing Security** 12
Data at Rest 12
Resilient Design 12
Continous Monitoring 13
Vulnerability Scanning 13
System Maintenance/Patching 13
Multi-Tenancy 13
**Network Security** 13
Web Application Firewall (WAF) 13
Intrusion Detection System (IDS) 14
Office Network 14
Remote Work 14
**Gateway Security** 14
Networking 15
Data in Motion 15
Portal Administration Interface 15
**System Data Flows** 16
Components and Support Processes 16
**Smart Home Portal Security Features** 17
Administration Authentication 17
Logging & Reporting 17
TLS 17
Cookies & Sessions 17
**Software Development Life Cycle (SDLC)** 18
Dependency 18
Secure Development 18
Change Control Process 18
Application Vulnerability Scanning 19
Penetration Testing 19
**Mobile Application Security** 19
Cloud Security 19
Brivo Mobile Pass (BMP) 19
**Security Policies** 20
Access Control 20
Supply Chain Risk Management 20
Security Training 20
**Physical Securities** 21
Data Centers 21
Offices 21
Privacy 21
**Additional References** 22

# Overview

## Introduction

As a provider of physical security services, we at Brivo believe that information security is of paramount importance to maintaining the safety and security of your facilities, and the privacy of your data. That's why information security has been a consideration since day one.

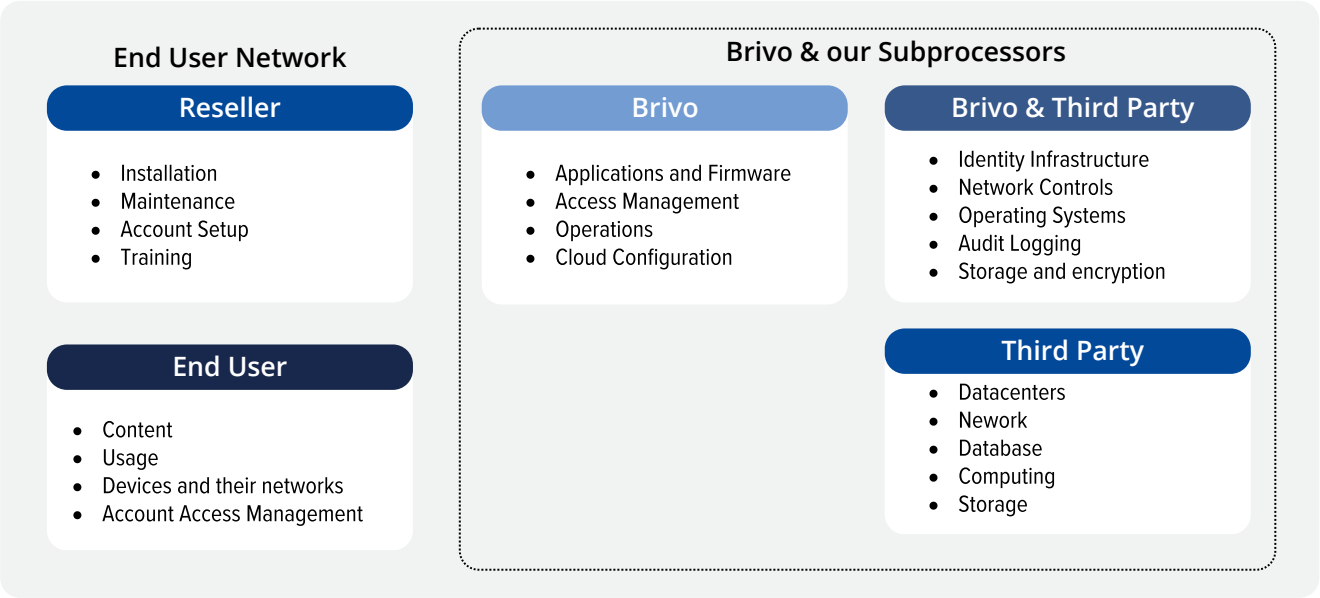
Brivo looks at security holistically in our technology, people and processes. We use guidance from industry best practices, applicable publications, and international regulatory requirements to employ a defense-in-depth strategy for the controls in our security framework.

## Assumptions

Some security features in this paper are not available on outdated hardware or firmware, this paper will call out those features so that users can request hardware and firmware updates. If your gateway needs a hardware or firmware update, contact your Brivo authorized reseller. This paper is primarily intended for IT professionals familiar with computer networks and information security.

# Shared Responsibility

**Figure 1: Shared Responsibility Diagram**




As with all cloud solutions, responsibilities for the confidentiality, integrity, and availability of the Brivo Access system are shared to ensure that all data is secure in creation, transport, storage, and deletion. These responsibilities are tracked in the Brivo shared responsibility model seen here.

**To summarize:**

- Resellers are responsible for the secure installation of Brivo integrated hardware, secure initial account setup, and security training of the users.
- Users are responsible for the security in their accounts, their networks, and the physical security of the devices at their facilities.
- Brivo is responsible for the security of the systems and services we provide including handling data securely, building secure applications/firmware, and configuring our third party service providers using security best practices.
- Brivo shares responsibility for the security of our systems and services with our third party providers which provide cloud services to Brivo such as identity infrastructure, network controls, operating systems patching, audit logging, and data storage and encryption.
- Our third party providers are responsible for the security of our datacenter facilities and infrastructure hardware.
- Some customers will not engage with a reseller but may perform self-serviced installation and setup. In this case, the responsibilities of the reseller are to be borne by the customer / user but may be supported and assisted by the Brivo Customer Success team and / or Brivo authorized installers.

# Reseller's Responsibilities

1. **Selecting the right install location and pairing devices:**
   a. Central location to all devices.
   b. Near an outside wall or window (to help with the cellular backup connection).
   c. Lower visibility area.
   d. Near the router if possible, as a wired Ethernet connection is most reliable.
   e. Pair devices to the gateway in the proper sequence to ensure efficient z-wave network communication. (Repeaters, thermostats, other devices with repeater functionality, locks, and then sensors or non-repeating devices).
   f. After pairing all devices, confirm using the gateway page network graph that the z-wave mesh network has been created in an efficient manner.

**2. Securing network access:**
   a. Hardware should be placed on the end user's Local Area Network (LAN) or corporate Wide Area Network (WAN) and secured using Access Control Lists (ACLs) to prevent unauthorized network access.
   b. ACLs should be set to deny all except for TCP port 443 (HTTPS) outbound to the Brivo IP space: 64.35.160.0/20 or the following domains: c2.brivo.com, b2.brivo.com, g4data-prod.brivo.com, g4cmd-prod.brivo.com.

**3. Administrator authentication:**
   a. Always use a unique username and password for each administrator.
   b. Recommend that the administrator uses a password manager to generate and store strong passwords.
   c. Remind administrators to never share their passwords with anyone.
   d. Fine tune permissions for each administrator role based on the least privilege principle, where they only have the minimum permissions needed to do their job.
   e. Ensure that there is at least one backup administrator with access and training for each task in the system.
   f. Administrator accounts intended to be used for API access should be properly named as such and should not be used to log in to the web portal or mobile app.

**4. Monitor the system:**
   a. Assist the customer in properly setting up and configuring rules and email notifications for events and alerts to the correct personnel.
   b. Train administrator on how to review activity reports/audit log periodically to ensure there hasn't been any suspicious activity.

**5. Perform periodic maintenance:**
   a. Check Brivo release notes periodically for new features, bug fixes, etc and install firmware updates as needed. Release notes can be found by going on our support website: https://support.brivo.com/.
   b. Verify account, billing, and administrator contact information regularly.
   c. Test backup power supplies/batteries regularly.

For more details and instructions on installation, refer to the appropriate installation manual on our website.

# Users' Responsibilities

**Users are in charge of:**

1. Policies and Processes - Users are responsible for maintaining formal policies that provide guidance for information security within the organization and the supporting IT environment.
2. Incident Reporting - Users are responsible for communicating any identified security violations to Brivo on a timely basis, as necessary.
3. Monitoring - Users are responsible for ensuring appropriate notifications are configured in the system with updated contact information to support monitoring and incident response procedures.
4. User Devices and Networks - Users must ensure that their devices and networks which connect to Brivo systems are secure and hardened.
5. Mobile Device Security - Users are responsible for enforcing lock screens and optional biometric settings on mobile devices with Brivo mobile applications installed.
6. Credential Management - User entities are responsible for enforcing strong passwords for administrator access to their account. User entities are responsible for ensuring that personnel are not sharing their credentials with others, including passwords, etc.
7. Privilege Management - Users are responsible for ensuring only authorized personnel have access rights within their accounts commensurate with their job responsibilities.
8. Exported Data Security - Users are responsible for adequately securing data contained in any output reports provided by Brivo, including appropriateness of individuals accessing the output reports and storage/disposal of the output reports.
9. Exported Data Retention & Disposal -Users are responsible for retaining and disposing of output reports in accordance with their data retention and disposal policies.
10. Physical Security - User entities are responsible for ensuring physical security and environmental controls for Brivo hardware installed at their locations meet business continuity objectives. User entities are responsible for installing devices in a secured manner such that tampering is made difficult.
11. Network Security - User entities are responsible for implementing network access controls to restrict outside access to hardware installed on their networks.
12. Supply Chain Risk Management - User entities are responsible for evaluating vendors for risk prior to authorizing third-party integrations with their Brivo account.
13. Usage of Brivo Systems - Users must follow their own security program and our Terms of Use when using Brivo systems.
14. Legal Requirements - Users must follow all applicable legal requirements such as getting consent before putting sensitive data into our system and they must maintain the accuracy of that data. Users must be able to complete data subject's rights requests such as the rights to request their information, modify their information, delete their information, etc.

# Brivo' Responsibilities

**Brivo is responsible for:**

- Policies and Procedures - Brivo is responsible for maintaining an information security management system (ISMS) that is compliant with AICPA's Trust Services Criteria (TSC) for SOC 2 and ISO27001.
- Brivo applications and firmware development and security - We ensure that we are building our systems with privacy and security as a priority.
- Internal access management - Brivo securely manages privileged access credentials for sensitive systems. System owners audit and manage the privileges of administrators so that we provide the minimum permissions necessary. Access is removed within 24 hours of a change of employment.
- Operations - Brivo is responsible for patching, monitoring, and responding to any incidents with our systems 24/7. Brivo is responsible for communicating any planned downtime due to maintenance or unplanned outages to our users through our status page: https://status.brivo.com.
- Cloud Configuration - Brivo must use security best practices and cloud hosting provider recommendations to configure our cloud hosted environments.
- Legal Requirements - Brivo is responsible for ensuring we meet legal and regulatory requirements such as privacy and security laws.

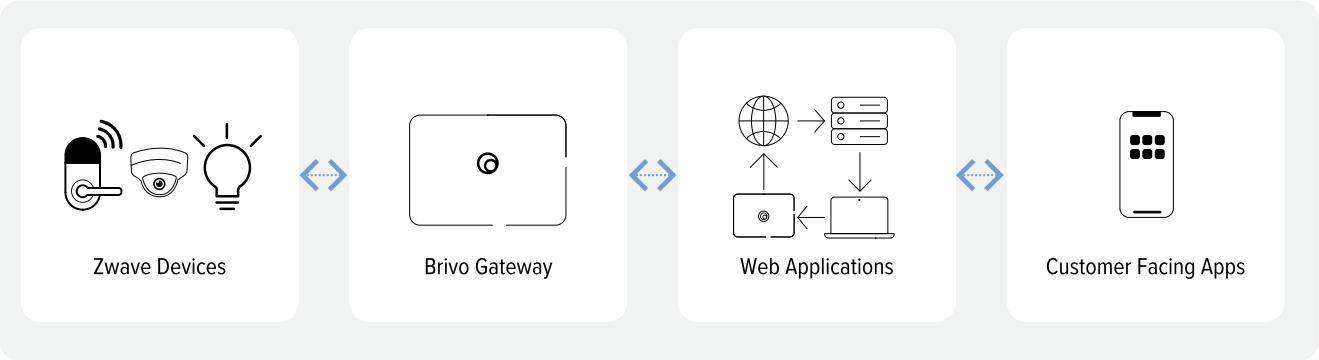
**Brivo and Third Party Responsibilities:**

- Brivo and our sub processing third parties have the following responsibilities:
- Identity Infrastructure - Brivo engineering teams configure an identity infrastructure with a third party provider for users to authenticate into Brivo systems.
- Network Controls - Brivo must design a secure and highly available network architecture using our cloud providers. Our cloud providers manage the networking for our serverless applications.
- Operating Systems maintenance - Brivo must select and install operating systems for our virtual servers and containers.
- Audit Logging - Brivo must provide logging for Users to audit activity in Brivo systems. Our cloud providers must provide logging for Brivonians to audit activity in our cloud accounts. We must perform that auditing regularly.
- Storage and Encryption - You must be sure to store Brivo data on approved, secured Brivo-issued devices and you must use the provided procedures, VPN, and encryption when transmitting data. Our cloud providers are responsible for Brivo cloud encryption.
- Datacenter Infrastructure - Our third party cloud providers are solely responsible for the maintenance, resiliency, and security of Brivo cloud datacenter facilities and the hardware within.

# Brivo Smart Home Architecture

**Figure 2: Brivo Smart Home System Overview**

Brivo Smart Home is a Software as a Service (SaaS) primarily targeted at commercial and multi-unit residential properties with employee, resident, and property managers for whom access needs to be regulated and recorded. A cloud hosted system such as Brivo Smart Home is an excellent fit to meet prospective tenants through self-guided tours, control smart lights, thermostats, and sensors to save energy and costs. Brivo Smart Home features keyless entry with smart locks and mobile access control to allow residents to manage visitors from one geographically distributed app.




As shown above in Figure 2, there are four major components to the operation of the Brivo Smart Home service:

1. Brivo Smart Home application (available via web browser or mobile application).
2. Gateway installed on customer network; network communications via wired ethernet, WiFi and 4G cellular.
3. Z Wave Connections to z wave devices.
4. Brivo services are hosted with major cloud service providers.

These components share data across multiple platforms and networks in order to manage residents' experience and deliver smart home automations like, control your lights and temperature from your phone, get alerts for leaks, and open doors, manage and grant visitors, staff, maintenance and delivery access, and other services such as software updates to the gateway.

Gateways are networked to the cloud through wired or wireless connection. Wired options include a built-in Ethernet port for connection to a corporate LAN, or broadband modem, or any other IP-based networking technology with connectivity to the Internet. Wireless networking options include a cellular network router or wi-fi adapter that comes with or is built into the gateway.
The gateway automatically uses the strongest connectivity which provides a highly reliable solution for any connectivity scenario.

# Brivo Smart Home Account Management

The access control life cycle begins with an administrator logging into the Brivo Smart Home website or Brivo Smart Home App and setting up users, groups, credentials, schedules, and other security policy elements that dictate who has permission to enter which facilities at which times. Any activity in a Smart Home account performed by an administrator is logged in the journal report.

Administrators can also issue Brivo Smart Home credentials to users. The user will need to install and activate the Brivo Smart Home App on their mobile device, then they can use an Internet connected device or Brivo Smart Home portal to control compatible devices such as smart locks, thermostats, lights, plugs and water sensors.

## Gateways

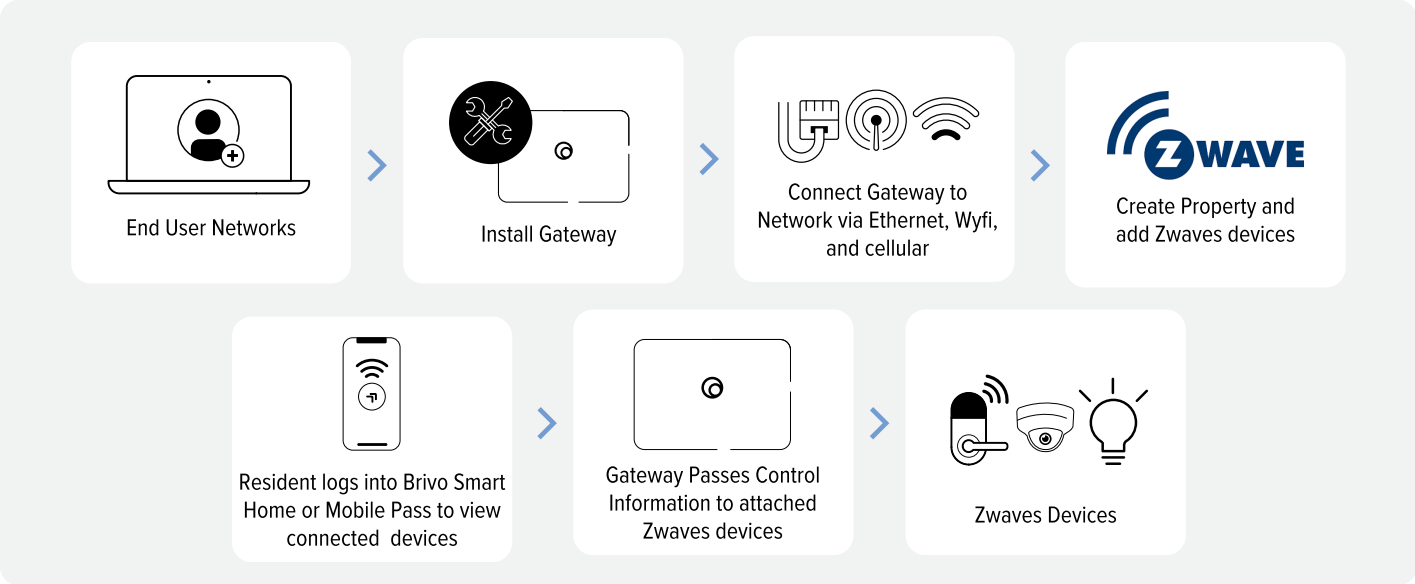
The Brivo Gateway serves as the nerve center of your home automation system and ties all of your devices together.The Brivo gateway is a tri-band (wired ethernet, WiFi and 4G cellular) communications device that connects the Brivo cloud platform to compatible devices like smart locks, thermostats, lights and water sensors. The gateway automatically uses the strongest connectivity channel which provides a highly reliable solution for any connectivity scenario. It is the automation hub that serves as the one solution for unifying smart home devices and controlling them from a single location.

The Brivo gateway utilizes the Z-wave protocol to interact with smart devices. Z-wave protocol is one of the more widely used options in home automation due to its superior range. Z-wave is completely wireless and operates at a low radio frequency, which means it will not interfere with Wi-Fi signals, mobile phones or microwave ovens. Z-wave creates a mesh network that allows signals to hop from one device to another, and each network can support multiple devices including smart light and plugs, door and window sensors, door locks, thermostats and leak sensors.

The account data is stored in Brivo's cloud data platform. The gateway, upon initial connection, will download the data file to approve or deny users as the administrator has programmed. The gateway will establish a connection channel with the server and check regularly for new account data. If changes are made to devices in the Smart Home account, an update is pushed to the gateway from the server using the pre-existing channel or upon the next Gateway connection.

# Device Control Process

**Figure 3: Brivo Smart Home System Overview**




When a resident logs into their Brivo Smart Home account, they are able to access all their connected smart home devices. The app will send control commands to the gateway, and the gateway will in turn forward the corresponding z-wave commands to the devices. Device status and events will be forwarded from the gateway to the Brivo cloud and viewable through the Smart Home app. Since the gateway is a tri-band (wired via ethernet, WiFi and 4G cellular) it automatically uses the strongest connectivity channel which provides a highly reliable solution for any connectivity scenario.

# Third Party Integrations

Brivo Smart Home offers third party integrations with other systems in one of two ways. Customized synchronized code that runs inside the smarthome system where Brivo writes the code and through API integrations.

## API Services

Brivo offers API services for third-party integrations. Brivo API uses rotating token authentication for account access. We are working on implementing OAuth2 three-legged authorization workflow in the near future. Account administrators are provided the ability to selectively enable/disable API connections to their Brivo Smart Home account. All communications via the API are HTTPS using TLS 1.2 or higher. For more technical information on Brivo API, visit our documentation (Brivo Smart Home API Documentation).

# Cloud Computing Security

Brivo Smart Home is delivered as a multi-tenant model using secure logical controls to separate customer data. Brivo leverages AWS hosting services and other third party solutions for a secure and resilient solution. AWS has a comprehensive security program that Brivo evaluates continually as part of its supply chain risk management program. AWS publicly provides details on their security program and data centers which you can find on their website (https://aws.amazon.com) including:

1. AWS Security Overview
2. AWS Data Centers
3. AWS Compliance Programs

Brivo understands that by using AWS, we must maintain and secure our resources as part of the AWS shared responsibility model. Brivo implements a security program specific to these resources including access control, secure network configuration, continuous monitoring, firewalls, IDS and system configuration/patching. More details on how we do this will be covered in this paper.

## Data at Rest

All Brivo cloud data stores are encrypted at rest. Brivo uses the industry standard AES-256 encryption algorithm to encrypt the data at rest for our databases. Data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. All data is stored within the contiguous United States.

## Resilient Design

To provide high availability of our services, Brivo uses a modern, resilient design of our applications and services.

Brivo Smart Home utilizes serverless functionality and resilience as built by AWS. Brivo Smart Home is run on highly available, fault-tolerant infrastructure spread across multiple availability zones. AWS manages all the administration, maintenance, and patches of the infrastructure without any impact to Brivo Smart Home availability. Serverless enables Brivo Smart Home to have continuous scaling of our application by running event triggered code in parallel, and processing each event individually.

Brivo API, web services and other systems that support Brivo Smart Home are elastic container based applications. Brivo replicates services across three availability zones in AWS Northern Virginia, United States region. This enables Brivo to release updates to services seamlessly and to provide services in the event of an AWS availability zone outage. Backup snapshots of our database are performed daily. We maintain some resources in the Oregon, United States region as a warm disaster recovery site. Brivo annually updates and tests our processes and backups restoration in our QA environment to ensure efficient incident response and disaster recovery.

Brivo Smart Home gateways at customers location will cache up to 2.5GB of log files that include event data among other data at all times. Log files are rotated once they reach 512MB. There are a maximum of 5 log files stored at any time. Brivo believes in transparency as part of building trust with its users. We announce status updates for any planned or unplanned downtime publicly on our status page (https://status.brivo.com/).

## Continuous Monitoring

Brivo has a suite of tools fine tuned by our operations staff to monitor critical systems. These tools create baselines for system performance and alert staff when performance is abnormal. These alerts could signal an upcoming service disruption, or a potential security event. We have staff on call 24/7 to respond to these alerts with procedures for activating incident response and disaster recovery plans.

## Vulnerability Scanning

Brivo uses vulnerability scanning tools to assess our environment. These tools automatically update their signatures and scans systems daily to potentially identify any flaws in their configuration or installed operating system and services. The tool alerts our security and operations teams on new vulnerabilities for investigation and remediation.

## System Maintenance/Patching

For the Brivo Smart Home application, Brivo performs patching periodically in order to keep systems up to date and reduce vulnerabilities. In the event of a high risk patch identified by a security advisory or vulnerability scan, we create a mitigation plan, test the proposed mitigation in a non-production environment and, if no issues arise, deploy those updates to production with no downtime.

## Multi-Tenancy

For the Brivo Smart Home application, Brivo logically separates customer accounts within the database. When an account is created, it is tied to a unique identifier that is hidden to the end-user. When any action is done on an account, the unique identifier and valid credentials are needed. Brivo Smart Home administrators can be granted different levels of privileges for reading, modifying, or deleting user groups or sites within the account.

# Network Security

Brivo configures logical networks in AWS using built-in security features. Environments are logically separated through the use of different AWS accounts, security groups, and subnetting. Security groups are configured with a white list of ports and IPs to ensure that only the ports absolutely necessary for providing services are open. AWS provides secure network hardware and automatic encryption of all traffic on the AWS global and regional networks between AWS secured facilities.

## Web Application Firewall (WAF)

FBrivo uses a Web Application Firewall (WAF) in addition to the built in network security features to additionally monitor and restrict traffic flowing to AWS resources. The WAF is set up with rules to deny traffic that is from known bad reputation IP addresses.

### Intrusion Detection System (IDS)

Brivo uses an AWS featured partner to provide an Intrusion Detection System (IDS), web application security event detection (passive WAF), security event log aggregation, and a team of security experts that provide 24x7x365 threat monitoring and tuning. These services alert the security and operations teams when any potential incidents such as suspicious network traffic is detected. Detection is both anomaly-based and signature-based. Potential incidents are investigated by the Brivo team to rule out false positives. All true positives are added to Access Control Lists (ACLs) in the WAF to block.

### Office Network

Brivo's HQ office networks use logical separation of departments through subnetting. Network firewalls only authorize the ports necessary to provide services. For resiliency, Brivo utilizes two different Internet providers. All necessary devices are connected to a battery backup and surge protection. Network devices are in a physically secured server room to prevent non-authorized employees or visitors from accessing devices. Brivo has backup air conditioning in the event of HVAC failure. In the event of a disaster, employees are able to work from home to continue maintaining services and providing support to end users.

### Remote Work

Brivo employees and contractors must use a Brivo-managed VPN to access network resources when remote and some sensitive systems when on location. Use of this VPN allows another layer of access control, logging, and encryption for employee network traffic.

## Gateway Security

The Brivo Smart Home Gateway (BSHG) is the brain of the Brivo Smart Home system and the most important device. The Gateway serves as the nerve center of your home automation system and ties all of your devices together.

A gateway is dedicated hardware containing a microprocessor, memory, and I/O interfaces that utilizes the z-wave protocol to interact with smart devices. Z-wave protocol is one of the more widely used options in home automation due to its superior range. Z-wave is completely wireless and operates at a low radio frequency, which means it will not interfere with Wi-Fi signals, mobile phones or microwave ovens. Brivo has designed and manufactured several models of the gateway which differ in capacity, communication options, and features.

## Networking

The Brivo Smart Home Gateway (BSHG) initiates the communication with the Brivo Portal. The MQTT protocol is used to communicate between the Gateways and Brivo cloud services. IP addresses are assigned by the customer's network provider when communicating over wired/Wi-Fi. When communicating over cellular connection, the gateway communicates through a Virtual Private Network. This means that the gateway will operate with routers and firewalls configured to use Network Address Translation (NAT).

The Brivo Smart Home Gateway (BSHG) requires outbound HTTPS traffic (TCP port 1883/8883) open to connect to Brivo MQTT brokers.

## Data in Motion

The Brivo Smart Home Gateway (BSHG) will only respond to commands/requests that are initiated by the portal over MQTT.

All of the Brivo Smart Home Gateways (BSHG) exchange credential and event information with the Brivo data center. Brivo uses digital certificates described by the ANSI X.509 specification for public key infrastructure (PKI) systems. For the Brivo Smart Home Gateway (BSHG), Brivo acts as its own CA because it can guarantee a physical chain of custody during the installation of certificates into Brivo Smart Home Gateway (BSHG) during our manufacturing process, and because there are no third parties communicating with those gateways who need to be part of the authentication process.

The Brivo Smart Home Gateway (BSHG) communicates via TLS with SHA256 with RSA Encryption. The gateways establish a TLS session with Brivo before exchanging information. When establishing a TLS session, the gateway and the portal validate each others' certificate to authenticate their identity.

*Some older firmware or hardware models do not support these levels of encryption.*

## Portal Administration Interface

**Brivo Install App**

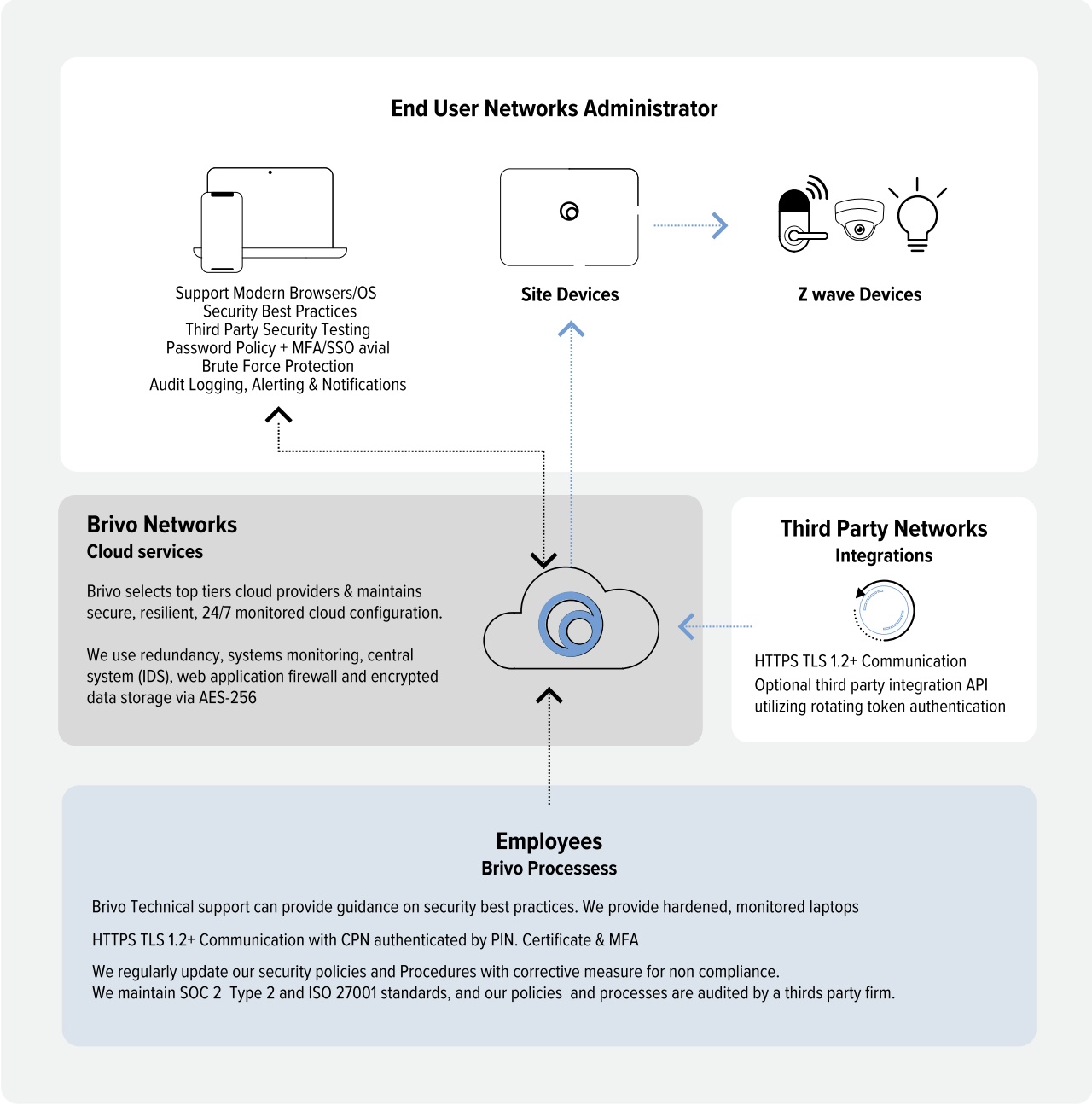
The Brivo Install App is only accessible by Brivo Certified Installers, and it uses Bluetooth connection to the gateway. This interface allows authorized installers to verify the signal strength of Cellular/Wifi networks, and generic system health information and set up WiFi credentials on the gateway. It does not allow for opening of doors or manipulation of devices.

# System Data Flows

## Brivo System Components and Support Processes

The following diagram depicts the data flows between major system components and the layered protections provided for each element.

**Figure 3. Brivo System Components and Support Processes**



# Smart Home Portal Security Features

## Administrator Authentication

An administrator is a Brivo Smart Home user with privileges to sign in to the Brivo Smart Home application and observe or make changes to an account that controls one or more sites. Brivo authenticates administrators by an email address and password.

The password policy is the following:

- Passwords may be between 8 and 128 characters in length and must contain Lower case (a-z), upper case (A-Z) and numbers (0-9) or special characters.
- Passwords cannot be any of the previous 5 passwords.
- Passwords cannot be on a common password list,
- Passwords cannot be any personal information such as the user's full name and email or the first part of it, i.e., firstpart@email.com.
- Passwords cannot be compromised credentials from a third party data breach.

Brivo is working on implementing a two-factor authentication method for Smart Home Portal.

## Logging & Reporting

Administrator activity is logged in the Journal in Brivo Smart Home. This includes activity when Brivo customer support is asked to log into an account to assist in troubleshooting.

All device/gateway events are logged in the database and central logging system. Users with sufficient permissions can view/download the logs from the smart home portal. Brivo Smart Home also can provide email and text message notifications of a wide range of events.

All data is retained per the Terms of Use for Brivo Services (https://www.brivo.com/terms-of-use-brivo-services/).

## TLS

Brivo Smart Home uses TLS to secure data in motion. Our services prioritize negotiation to secure TLS ciphers for all modern browsers. We recommend users to keep their browsers updated to get the best possible TLS encryption options. We continually monitor for new TLS configuration best practices, and create action plans to implement them as they become available.

## Cookies & Sessions

Brivo Smart Home uses sticky sessions to maintain state information and provide a continuous experience to clients. To use sticky sessions, the clients must support cookies. Cookies have the secure flag enabled so they are transmitted via HTTPS.
Regardless of activity, users have to reset their web and mobile login passwords every 90 days.

# Software Development Life Cycle (SDLC) Security

Brivo uses security best practices throughout the Software Development Life Cycle (SDLC). This means that security is included throughout phases of development and deployment.

## Dependency

All the backend software dependencies are up to date and on the latest Long Term Support versions.

## Secure Development

Brivo engineers are provided a secure development training curriculum specific to the programming language they use. Every engineer is required to complete their curriculum. This program trains on the OWASP Top 10 vulnerabilities and how to mitigate them through secure coding practices. Engineers have a plugin in their integrated development environment (IDE) to highlight security best practices or vulnerabilities that need to be remediated inline as they are writing code. Engineers can also create a sandbox on their machine to perform static application security scans on files they are working on so they can remediate any flaws before submitting a release for QA. The security team and management track the progress of training and results of sandbox scans.

## Change Control Process

The development, QA and production environments are logically separated in the cloud. In order to submit any releases to QA or production environments, Brivo has a change control process to ensure that every release meets the criteria as set forth by management. This process requires every release to be documented with changes before submitting to the QA environment.

Once in the QA environment, the release is tested through automated tools and manual input. Those results and the documentation must be approved by an engineering director prior to being released to production and the approval is documented.

Releasing to production generally does not cause any outage of services due to the resilient design of our environment, however if any outage is planned, our Status Page (https://status.brivo.com) will be updated with a maintenance notification 24 hours prior to the release. Once deployed, regression testing is performed and any issues are resolved by either roll back or roll forward as determined by the engineering team.

## Application Vulnerability Scanning

Brivo uses static analysis, source component analysis, and dynamic analysis to identify any vulnerabilities within Brivo Smart Home and our supporting services.
Static analysis scans are done automatically with every build of our applications. Static analysis tests the application's source code for any vulnerabilities including OWASP Top 10, CVEs, etc.

Source component analysis is built into our static analysis scans and reviews the usage of third-party libraries to check their version and licensing which it checks against a constantly updated vulnerability database to determine if the libraries have any known vulnerabilities.

Dynamic analysis is done weekly in production. Dynamic analysis is an automated testing that crawls the website to potentially identify or exploit any vulnerabilities.

## Penetration Testing

Brivo has contracted a well established third-party provider to conduct annual penetration tests. These tests aim to discover vulnerabilities and exploit these vulnerabilities to gain unauthorized access to data or systems. Any results received are prioritized by our engineering teams for remediation and followup testing is performed by the third-party provider. The goal is to have no vulnerabilities after remediation.

# Mobile Applications Security

Our mobile applications use the same SDLC security mechanisms as stated above.

## Cloud Security

Brivo leverages Google Firebase for our mobile application functionality. Google has a comprehensive security program that Brivo evaluates continually as part of its supply chain risk management program. Google publicly provides details on their security and privacy program centers which you can find on their website (https://firebase.google.com/support/privacy/).

All data at rest in the cloud is encrypted with standard AES256 encryption algorithm.

## Brivo Mobile Pass (BMP)

The BMP application is an optional virtual credential for residents to operate smart devices via an internet connection. When an invite for residents is sent via the portal, residents receive an email through which they create an account. Once the account is created, they can use it to login to Brivo Mobile Pass (BMP) or BSH. The mobile app will control smart devices to which the user has valid, active permissions.

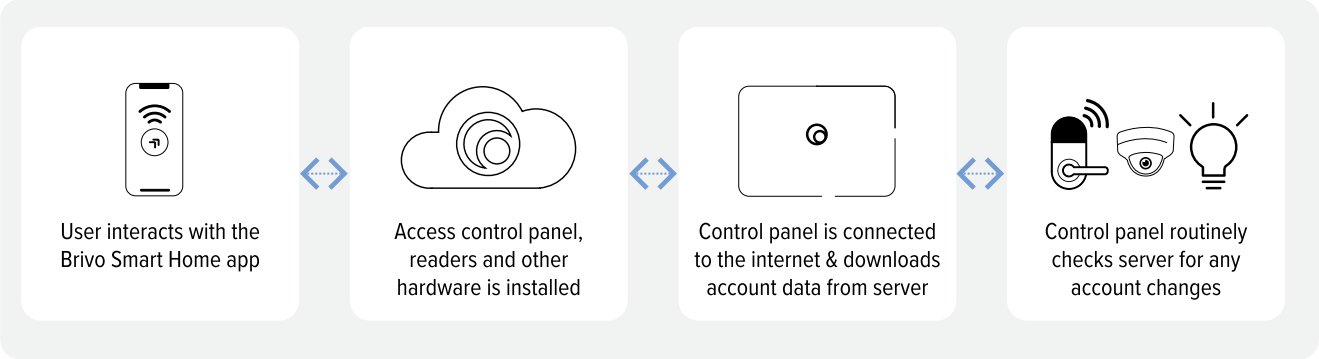



**Figure 4. Brivo Mobile Pass App Standard Internet Unlock Flow**

# Security Policies

## Access Control

The Brivo policy around access control requires access to be granted using role based and least privilege principles. Prior to granting any access, Brivo employees are screened in an interview process, undergo a background check, sign confidentiality clauses, acknowledge the employee handbook, and complete security awareness training. Sensitive systems access is reviewed quarterly by the IST to prevent access creep. Access is revoked immediately upon termination. Brivo requires the use of two-factor authentication and single-sign on (SSO) where available.

The password policy requires passwords to be at least 8 characters in length and must contain at least 2 of the following 4 categories: Lower Case, Upper Case, Digit, Non-Alphanumeric. Password hygiene training is available for all employees and included in security awareness training. Brivo system administrators are required to change default passwords on all systems to passwords that meet the requirements in this policy.

Customer support teams perform authentication for callers using probing questions and/or an email from the account on file to verify the caller identity prior to divulging any information or performing any actions on an account.

## Supply Chain Risk Management

Brivo uses an IT supplier policy to govern the selection and analysis of vendors in the supply chain. Any vendors that may have access to sensitive data are assessed for security best practices. The security team will review the documentation for the vendor such as audit reports, white papers, and any other security-related material the vendor provides annually. If any concerns are identified, then the security team reaches out to the vendor for clarification/remediation.

## Security Training

Brivo provides security training for employees including targeted role-based training and a security awareness program for all employees that is attended during onboarding and annually thereafter. The Security Awareness program includes, but is not limited to, physical security, safety, account management, social engineering attacks, data classification and information handling, security policies, and how to report security events. The training is updated annually and delivered annually via a training system with a test to assess comprehension. Employees are tested continuously with simulated phishing emails and provided additional training on social engineering attacks as needed.

Brivo provides supplemental role-based training for our Sales, Marketing, Engineering, and Customer Care teams. These teams have different security responsibilities such as secure development, account handling, and customer data.

# Physical Security

## Data Centers

Brivo data centers are managed by AWS. AWS publicly provides details on their security program and data centers which you can find on their website (https://aws.amazon.com) including:

1. AWS Security Overview
2. AWS Data Centers
3. AWS Compliance Programs

## Offices

Brivo offices are secured at the building and office level with access control systems. Brivo employees are granted access control cards with the minimum access needed to perform their duties. Brivo uses difficult to reproduce smart cards to access secured areas. Cameras are installed in the offices and monitored for all access points and secured areas. Security guards monitor and patrol the building and surrounding premises.

Visitors are required to sign in and are not granted access to office areas unless escorted by an authorized Brivo employee. Visitors are granted unique visitor badges which they must have visible on their person while on the premises. These badges are returned when they leave.

## Privacy

Brivo values the privacy of our end users and we are transparent with our privacy policy. For our privacy policy in regards to business practices and the use of the Brivo website, please review our Privacy Policy as found on our website (www.brivo.com/privacy/). For the specific privacy policy surrounding the use of Brivo services, please see our Services Privacy Statement as found on our website (https://www.brivo.com/services-privacy/).

Brivo complies with the requirements in GDPR, CCPA, and the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Our Privacy Shield listing is available to the public for review on the Privacy Shield website (https://www.privacyshield.gov/).

Brivo has entered into a number of Data Processing Agreements that include the EU standard contractual clauses in accordance with Article 26(2) of Directive 95/46/EC of the GDPR.

If you have questions regarding Brivo Privacy Policies or if you need to request access to or update, change or removal of personal information that we control, you can do so by contacting:

Brivo Privacy Officer
Brivo Systems LLC
7700 Old Georgetown Road, Suite 300
Bethesda MD, 20814 USA
privacy@brivo.com

# Additional References

While this paper is intended to be a stand-alone document, you may have additional interest in either the Brivo system or some aspects of information security discussed. Additional references such as installation manuals, networking manuals, and data sheets can be found in our Partner Resource Library (https://resources.brivo.com/technical-documentation). You may send any security questionnaires or requests for information to our sales team (sales@brivo.com).

## Revision Table

| Version | Date | Author | Content |
|---|---|---|---|
| 1.0 | 12/08/2022 | LMW | Original document |
| 1.1 | 08/31/2023 | LMW | Updated diagrams and added shared responsibility matrix |