

## Brivo® Information Security

**Overview:** This application note explains how Brivo Systems achieves its high standards for information security for both its Internet-based service and the wireless networking component.

### Introduction

Application and data security have been engineered into Brivo services since day one, both at our central hosting site and in our fielded hardware. Our information security technologies and practices are built on the same tools and principles that guard financial data at the biggest online brokerages and financial institutions.

Data is always encrypted when it leaves or enters our servers, so that our customers can be sure that no one can intercept it and use it for unauthorized purposes. And, while resident on our production servers, data is partitioned to private storage repositories, out of reach from the Internet and even from Brivo's own internal corporate network.

### Brivo Data Center Security

Brivo's servers for the ACS service are physically hosted at one of Qwest's secure, guarded, 24x7 facilities with strict physical access controls, which means that no unauthorized personnel can gain access to our equipment. The site is also equipped with the latest fire detection and control technology, as well as redundant, diesel-backed uninterruptible power supplies.

### Internet Server Security

As recommended by best practices in the field of information security, Brivo uses a multi-layered approach to providing for the security of its servers and the confidentiality of the information they hold.

The first layer of security is provided by dedicated, redundant firewalls that screen out all Internet traffic except for legitimate requests to access one of the front-end Web servers that Brivo operates for its ACS service.

A second layer of security, specifically designed to protect against common denial of service (DOS) attempts, is provided by a set of switches that detect these attacks and shunt the traffic before it can affect the quality of service provided by our Web servers.

Brivo uses highly rated operating systems on all of its servers, which provides for insurance against many of the security holes that affect other brands of operating system. Brivo further "hardens" its servers through a rigorous set of policies that restrict services and ports, restrict user IDs and passwords, and require application of all of the latest security-related operating system patches from our vendors.



The Oracle software that drives our database servers is known to be among the most secure database applications available on the market today. Data stored in our application database is segmented from all corporate activities, as are the rest of our servers, for maximum security and data privacy.

### **Encryption of Data**

Brivo employs industry-standard encryption techniques for all the communications channels we use. On both the control panel and browser interfaces into our data center, this means 128-bit SSL — the same that banks, e-commerce, and brokerage sites use to protect your financial data.

### **Account Security**

Customer accounts on Brivo's ACS application are protected by logon/password pairs that are exchanged with our server within an SSL session, so that no one can "snoop" your identity or password when you log onto the application.

For security reasons, Brivo does not employ "cookies" that allow a user to automatically log on, as is common practice with lower security applications and many e-commerce sites. Cookies are, however, temporarily used to maintain certain session information, but they have no validity outside the context of a current session, and cannot be used at a later time to gain access to the system in the event that a customer's computer experiences a security violation (e.g., loss or theft).

### **Information Security Policies**

And we haven't forgotten the human side of security, either. Our corporate information policies are based on the best practices of financial institutions and managed service providers, and are vetted by industry experts to ensure that they are always complete and up-to-date. Included in our policies is an information security training curriculum that all new employees must undergo upon arrival at the company, with periodic retraining and updates for existing employees.

### **Information Security Audits**

Brivo undergoes periodic audits of its information security policies and system configuration to ensure compliance with stated information security policies.

### **Custom Solutions**

Contact us if you need a custom solution beyond those described above.