FREEDOM ACCESS CONTROL
Rethinking Physical Access Control
Every year enterprises spend millions of dollars purchasing proprietary access control systems based on a 20-year-old architecture. These systems typically have high support and replacement costs, limited functionality around IT security operations and an increasing number of security vulnerabilities due to their legacy architectures. What’s needed is a new approach to access control that can easily integrate with IT infrastructure, leverage advanced cloud computing methodologies, enable virtualization and mobility, and minimize threats from cyber-attacks.

Viscount breaks this paradigm from both a technology and deployment model, thereby enabling a unique opportunity to move physical access control out of the realm of “facilities” and into the enterprise IT infrastructure where it is more easily managed by IT security managers and CSOs.

What this means.

Freedom “looks and acts” like most IT enterprise security application unlike the traditional access control “systems”. Because Freedom is built on the same security paradigms used in the logical/ID management side of the enterprise – we “provision doors” the way they provision other IT assets – it allows Freedom to fit into their overall logical/ID security strategies in a more “harmonious and unified” deployment. In effect, what Freedom does is take “doors” out of the realm of physical barriers and turn them into another IT asset that is provisioned based on identities, policies and attributes instead of departments and physical location. A customer can now for the first time seamlessly unify the physical/logical and now cyber security strategies and more fully leverage their investment in IT infrastructure and resources.
LESS COST PER DOOR — There are no control panels, associated labor or third-party hardware needed since the system can run on any server environment (conventional servers, virtual servers, private/public cloud or on a Freedom CUBE). The entire client architecture is 100% web-based which reduces installation and expansion costs, annual maintenance resulting in a substantially lower total cost of ownership.

CYBER SECURED — Card holder records, configuration parameters and card reader event history reside within Freedom's software. All this data is protected behind IT managed servers and is not exposed in local control panels.

SOFTWARE-CENTRICITY — Freedom works with applications that run on virtual machines, in a cloud environment or on physical servers. It can also integrate with hardware solutions that conduct authentication, authorization and portal control.

NET-CENTRICITY — Engineered for networking beyond internal communication among core PACS components, Freedom utilizes real-time data to obtain situational awareness relating to asset protection, apply policy-based control measures in response to threat and operations conditions, and share information with subscribed stakeholders (people, systems or devices). This helps to support planned organizational responses for maintaining personnel safety and asset security.

SERVER-BASED REAL-TIME ACCESS DECISIONS — A high-speed, server-based decision engine makes access decisions on role, policy and attribute information. This information is gathered in real-time and provides immediate status information such as threat levels, personnel presence/location data, access zone compromises and environmental safety conditions.

SIMPLY SCALABLE — The solution provides scalability for additional server applications. Freedom can run on a single server, on a virtual machine in a data center or the cloud, and provides high availability and tiered redundancy in the same way that Amazon, eBay, Facebook, Twitter and YouTube deploy their massively-scaled high-performance systems.

IT-FRIENDLY — Easily conforming to an IT department's technology roadmap, policies and practices, Freedom minimizes risk with redundancy policies, auto-failover and network path outage solutions.

ICAM-FRIENDLY — Enabling a unified physical and logical identity and access management, and common credentialing, through native support for corporate directory and identity management system integration, and for online authentication systems.

STANDARDS-BASED — Freedom allows users to configure system integration via established standards rather than vendor-specific APIs and SDKs.

SMART-CARD-FRIENDLY — Providing direct support (no third-party devices or middleware) for digital certificate-based authentication, including all levels of U.S. federal PIV Card (FIPS-201) and corporate PIV-I identity authentication assurance. Freedom also includes support for all of the capabilities in NIST 800-116, having passed rigorous federal testing to appear on the FIPS-201 Approved Product List.

MOBILE-DEVICE-FRIENDLY — Access Freedom anywhere. All functionality, including the attributes of presence and location, are available on a mobile device. Users can perform real-time device authentication and acceptance.

N-FACTOR AUTHENTICATION CAPABLE — Freedom supports configurable authentication requirements and is based on a combination factors including location, biometrics, personal knowledge, physical tokens, real-time digital tokens and behavior. The system allows escalation or relaxation of the n-factor count requirement based upon threat level and other conditions.

BROAD AUTHENTICATION TECHNOLOGY SUPPORT — Freedom accommodates a full spectrum of card-readers, cards and electronic credentials, and especially native support for credential technologies with high-security features like challenge/response protocols and biometrics.
The above architecture and deployment of the Freedom Enterprise solution allows up to 300 doors spread over multiple sites, with up to 50 database replications. The solution is scalable up to 50 locations, including the main administration site.
FLEXIBLE AND EASY TO OPERATE
There are no limits to schedules, access groups, controlled areas, business partitions or the number of users. Assigning access privileges along with start and expiry dates is extremely simple with Freedom’s web-based interface. Deploy Freedom in the following scenarios:

- On dedicated servers
- On Viscount Freedom CUBEs
- On a ‘virtualized’ server environment
- Within a private cloud
- Within a hosted or third party cloud

INSTANTLY CHANGE PRIVILEGES BASED ON THREAT LEVEL
A change in threat level will instantly cause a local or global change of access privileges. Administrators can apply rules to specific events to ensure that access to specific areas is monitored and restricted.

OUTPUT MAPPING: ONE CARD PRESENTATION CAN AFFECT ALL DOORS
Presentation of a card to a card reader, or simply an activation of an emergency push button, can affect as many output relays as necessary. This means that one card read can lock, unlock or lockdown an entire building or floor. A card reader can also be set-up as a switch. One card can then activate a relay or multiple relays, to control lights or other third party devices.

LOGICAL STATEMENTS APPLIED TO INPUTS
It is easy to set-up sophisticated logic to control output events. Multiple inputs, such as door sensors or emergency buttons, can be programmed to automatically create outputs, such as alarms or activate third party devices.

VIRTUAL MUSTERING—PROVIDING SAFETY IN EMERGENCY SITUATIONS
Upon a forced evacuation event, Freedom provides multiple ‘who is missing’, muster reports. There is no need to run to a muster station; just present a card to any reader in the safe zone.

TELEPHONE ENTRY — ENTERPHONE VISITOR MANAGEMENT
Freedom offers seamless integration with Viscount’s Enterphone Telephone Entry. Freedom can centrally manage one panel or network multiple Enterphone panels for more complex and integrated visitor management and card access applications.

RETRO-FIT WITHOUT DISRUPTION
When retrofitting a legacy access control system to Freedom, disruption is kept to a minimum and the implementation can be done in stages. Customers can usually keep their existing cards, readers, wiring, power supplies and cabinets. As a result, Freedom ensures exceptional value as a customer can utilize much of the past capital investment.

VIDEO INTEGRATION
Freedom offers seamless video integration with access control. Video integration allows the access control system to monitor both physical access control and surveillance video from a single point of administration, as well as link specific access control events such as forced entries, invalid presented credentials, and door held open events to live video. Freedom supports integration with several leading VMS platforms to offer the best solution for the customer. Learn more at www.viscount.com/technologypartners.
ACTIVE DIRECTORY AS A PHYSICAL SECURITY SYSTEM

An Active Directory structure is a hierarchical framework of objects. Each object represents a single entity — whether a user, a computer, a printer, or a group — and its attributes. In general, there is no difference between an Active Directory object and a physical security object. In physical security typical entities would be users and devices (door readers, elevators, and locking hardware).

In Active Directory an object is uniquely identified by its name and has a set of attributes — the characteristics and information that the object can contain — defined by a schema, which also determines the kinds of objects that can be stored in Active Directory. So, for physical security the objects and attributes will be contained within a physical security schema extension within Active Directory. The first advantage of the unified platform is the elimination of a separate user database of physical security. As shown in Figure 1 below, Freedom Active Directory reads existing users from the Active Directory.

Unlike other Active Directory based physical access control systems, Freedom Active Directory does not duplicate nor making data association on users.

WHAT MAKES FREEDOM ACTIVE DIRECTORY ARCHITECTURE UNIQUE?

Unlike traditional Integration design where Active Directory data objects are mapped and imported into Access Control System’s proprietary database; Viscount’s unique solution is built around Active Directory Lightweight Directory Services (ADLDS). Freedom Access Control data is stored in an independent custom ADLDS partition within the directory. Our data objects such as schedules, roles, and devices are simply extensions to existing Active Directory Infrastructure. This approach makes our data highly compatible and consistent with domain-wide directory services, yet it does not affect any Directory Schemas that are crucial to IT operations.

With ADLDS’s multi-master update and replication capabilities; Viscount’s Freedom Access Control System becomes a highly effective and scalable distributed service with the enterprise.

- The domain controller is a Windows server that is promoted as a domain controller, and runs the Freedom software.
- When you make a change in active directory it using the existing active directory replication to push an ADLDS instance to each site.
- At every card scan, it checks with active directory to check the state of the user.
- No server to server replication, it links directly on site with your active directory.
- Freedom Admin Web interface is written in .Net, and runs on the PACS domain controller.

Viscount sees the future of physical security as one in which card readers and sensors will simply be managed devices within an IT platform and user databases will be managed within the framework of existing logical security databases.

For large Enterprises, further integration with XACML, SAML, and SPML policy servers will allow physical security policies to be written and enforced from the enterprise access control policy store. This is simply not possible with today’s technology that is based upon proprietary control panels.

For end users, this represents a more sensible and much more affordable approach to physical security. This new architecture represents a fundamental change to the decades old model of proprietary software and control panels. System integrators can now provide physical security as a software application using the customer’s existing IT infrastructure and within the framework of overall identity management applications and policies. The leading initiative in this area is the US Federal Government through FIPS 201. In essence, the US Government through FIPS 201 has endeavored to create a common credential for both physical and logical security.

The Freedom Active Directory schema and IP Encryption bridge architecture provides a platform for full and seamless audits and compliance through the unification of logical and physical logs and the ability to create direct relationships between logical and physical security functions.
The Freedom access control system is a feature-rich, server-based software application that communicates over IP on an existing or dedicated IT network infrastructure. A Freedom Encryption Bridge connects the door hardware to the IT network and provides encrypted communication to servers. All system configuration, administration and monitoring is performed using a common web browser. Simplified architecture reduces system complexity and lowers the total cost of ownership.

Centralized databases can operate independently or be connected to an IDMS (identity management system), such as Active Directory, unifying physical access control and logical security management within the IT infrastructure.

- Complex control panel hardware configurations are replaced with compact, energy efficient Freedom Bridge devices, which communicate between door hardware and the Freedom server using encrypted IP network protocols.
- Simplified architecture installation ensures rapid deployment with minimal training requirements.
- System configuration, administration and monitoring are all performed using a web-based user interface.

The Freedom Bridge enables a powerful new way to deploy an access control system.

Freedom is typically installed on an existing network. Fault tolerance and resiliency strategies that ensure network security and reliability, automatically apply to Freedom. The Freedom architecture offers risk mitigation for every scenario. Application and database servers operate virtually or on dedicated hardware with redundant power supplies, network connections and hard drive storage. Synchronized redundant servers can be implemented across the network to mitigate both server and network failure. Every Freedom Bridge can establish and maintain communication with up to three different servers, automatically switching to another available server, if required.

Manage Physical Access Control within a Virtual Server Environment
Freedom Virtual is a physical access control system (PACS) that is VMware Ready for deployment in a virtual server environment, eliminating the need to maintain separate, stand-alone server(s) or dedicated network appliance(s). Freedom's innovative access control solution is designed for organizations that have migrated their IT infrastructure to a secure, private cloud environment, allowing them to maintain enterprise-grade physical security without the risk of storing sensitive information on a shared server hosted in a public cloud.

Integrated Access Control Virtual Platform
Freedom Virtual is a web-based, access control application that leverages an open architecture, integrates identity management and video surveillance and achieves the highest level of scalability with a significantly lower cost of ownership. Freedom Virtual is available through either a perpetual or subscription licensing scheme.

Unified Physical and Logical Security
Freedom Virtual allows organizations to seamlessly integrate IT and physical security systems, such as Identity Access Management (IAM), Security Information and Event Management (SIEM), Physical Security Information Management (PSIM) and HR systems to correlate physical and logical security event information, monitor alarms and rapidly respond to threats.

Browser-Based Web Application
Freedom Virtual is accessible anytime, anywhere from any standard web browser. Manage employee facility access privileges quickly and easily from any location without being tied to a dedicated client workstation or paying for individual software licenses per user.

Secure, Linux Operating System
Freedom Virtual ships pre-installed with a secure, open-source, Linux operating system (OS), which significantly reduces the risk of virus attacks, frees administrators from installing Windows security patches and ongoing anti-virus updates and eliminates the cost of operating system licenses and upgrade fees.

Peer-to-Peer Directory Synchronization
Freedom integrates with an organization's existing Identity Management system or HR employee database, without requiring duplicate data entry or ongoing maintenance. Identities, roles and policies are synchronized across all Freedom network appliances and door controllers in real-time so security settings are always updated and never outdated.
WHY CHOOSE FREEDOM?

**PANEL-LESS ARCHITECTURE**
Freedom eliminates complex and costly control panel configurations and replaces them with technology that communicates over encrypted IP-network protocols.

**HIGHLY SECURE AND RELIABLE**
Freedom uses advanced encryption technology to eradicate security vulnerabilities. Its built-in resiliency allows the solution to be deployed across unlimited devices without fear of failure.

**OPEN PLATFORM DESIGN**
Freedom’s advanced design enables rapid and cost-efficient integration to any relevant infrastructure. Simply use any application program interface (API) or software development kit (SDK) to integrate and deploy.

**ACCESSIBLE ANYTIME, ANYWHERE**
Unlike legacy client/server based access control systems, Freedom is accessible 24/7 via any web browser. Monitor and grant access from anywhere at anytime.

**MEETING FICAM COMPLIANCE**
Freedom easily adheres to corporate security and IT-based policies. It is fully compliant with the U.S. Government’s FIPS-201 standard and HSPD-12 initiative.

ABOUT VISCOUNT
Viscount is the leading provider of next generation, IT-centric access control and identity management applications. Viscount’s Freedom application platform allows seamless unification of the physical and digital security worlds by replacing discrete, self-contained systems with an integrated security system that is sophisticated enough to protect today’s critical business assets, and flexible enough to keep up with the evolving IT infrastructures of government and private organizations. For more information please visit: www.viscount.com.