Freedom Access Control

Rethinking Physical Access Control

- **SOFTWARE-DEFINED PHYSICAL SECURITY PERIMETER**
  Eliminates complex control panel configurations and replaces them with technology that communicates over encrypted IP-network protocols
- **HIGHLY SECURE AND RELIABLE**
  Uses advanced encryption technology to eradicate security vulnerabilities
- **OPEN PLATFORM DESIGN**
  Enables rapid,cost-efficient integration to any relevant infrastructure
- **ACCESSIBLE ANYTIME, ANYWHERE**
  Monitor and grant access 24/7 via any web browser
- **MEETING FICAM COMPLIANCE**
  Fully compliant with the U.S. government's FIPS-201 and HSPD-12

Freedom Access Control by Identiv is a feature-rich, server-based physical access control system (PACS) software application that communicates over IP on an existing or dedicated IT network infrastructure. Freedom Encryption Bridge connects the door hardware to the IT network and provides encrypted communication to servers. All system configuration, administration, and monitoring are performed using a common web browser. Simplified architecture reduces system complexity and lowers the total cost of ownership (TOC). Centralized databases can operate independently or be connected to an identity management system (IDMS), such as Active Directory, unifying physical access control and logical security management within the IT infrastructure.

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. 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.

An IT Approach to Access Control

Less Cost Per Door — Very little labor or third-party hardware needed since the system can run on any server environment (conventional servers, virtual servers, private/public cloud, or Freedom CUBE) and the entire client architecture is 100% web-based, reducing installation, expansion, and annual maintenance costs, resulting in a substantially lower TOC

Cyber-Secure — Cardholder records, configuration parameters, and card reader event history reside within the software, protected behind IT-managed servers and not exposed through proprietary networks

Software-Centricity — Works with applications that run on virtual machines, in a cloud environment, or on physical servers, while also integrating with hardware solutions that conduct authentication, authorization, and portal control

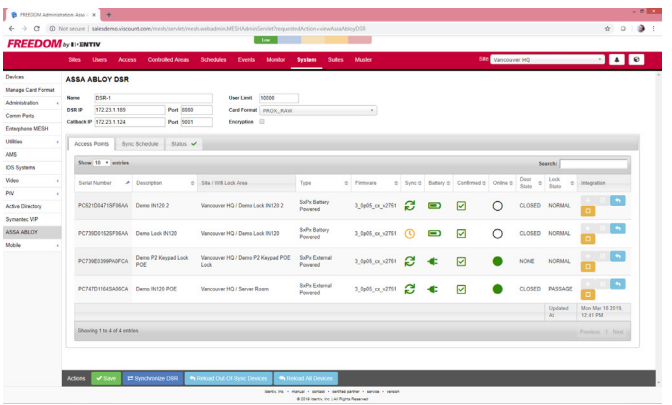
Net-Centricity — Engineered for networking beyond internal communication among core PACS components and utilizes real-time data to obtain situational awareness relating to asset protection, apply policy-based control measures in response to threat and operations conditions, and share information with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

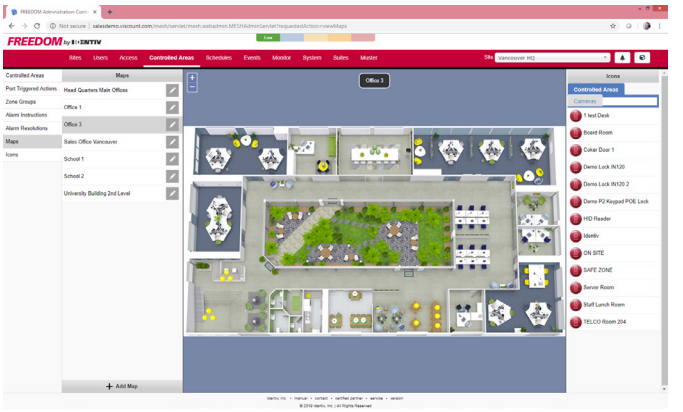
Server-Based Real-Time Access Decisions — A high-speed, server-based decision engine makes access decisions on role, policy, and attribute information, gathered in real-time and providing immediate status information such as threat levels, personnel presence/location data, access zone compromises, and environmental safety conditions

Simply Scalable — Allows scalability for additional server applications, running 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 conforms to an IT department's technology roadmap, policies, and practices, minimizing risk with redundancy policies, auto-failover, and network path outage solutions

Unified Security — Enabling unified physical and logical identity and access management and common credentialing through native support for corporate directory and IDMS integration and for online authentication systems





Standards-Based — Allows users to configure system integration via established standards rather than vendor-specific APIs and SDKs

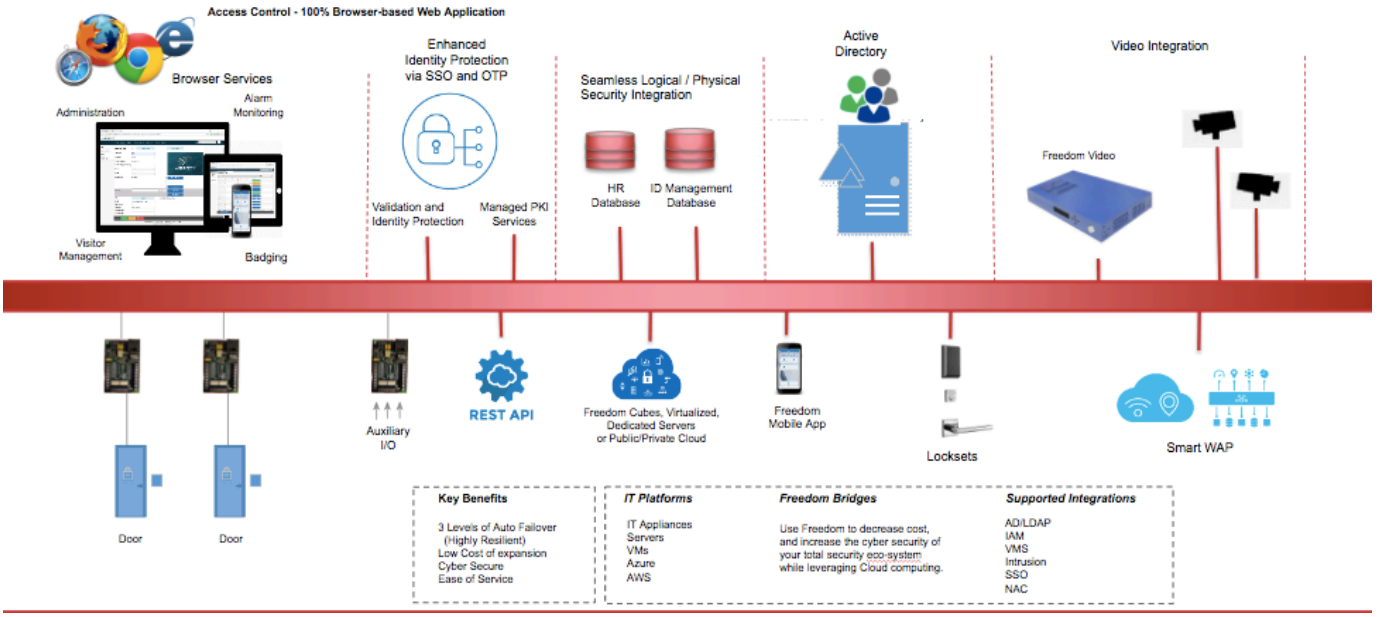
U.S. Government Approved — Providing direct support (no third-party devices or middleware) for digital certificate-based authentication, including all levels of U.S. federal PIV Card (FIPS-201) and corporate PIV-I identity authentication assurance, and all of the capabilities in NIST 800-116 (appearing on the FIPS-201 Approved Product List)

Mobile Device Friendly — All functionality, including the attributes of presence and location, is available on a mobile device and users can perform real-time device authentication and acceptance

N-Factor Authentication Capable — Supports configurable authentication requirements, is based on a combination of factors, including location, biometrics, personal knowledge, physical tokens, real-time digital tokens, and behavior, and allows escalation or relaxation of the n-factor count requirement based upon threat level and other conditions

Broad Authentication Technology Support — Accommodates a full spectrum of card-readers, cards, and electronic credentials, including native support for credential technologies with high-security features, like challenge/response protocols and biometrics

HOW IT WORKS



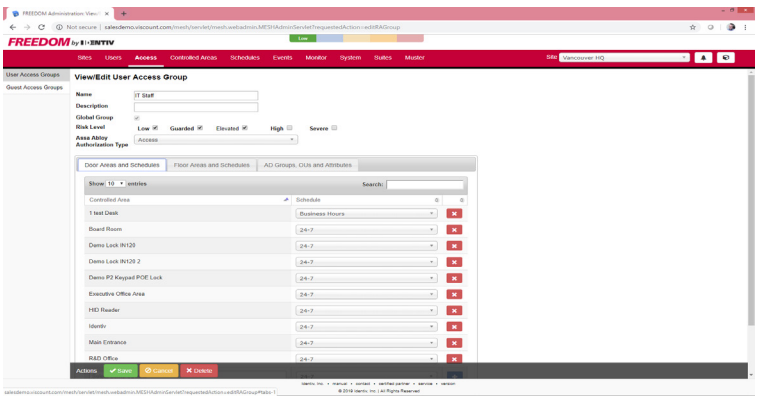
INNOVATIVE SOFTWARE FEATURES

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.

Freedom's software-defined perimeter aligns with migration from hardware-driven to software-driven architecture embraced by IT infrastructure providers.

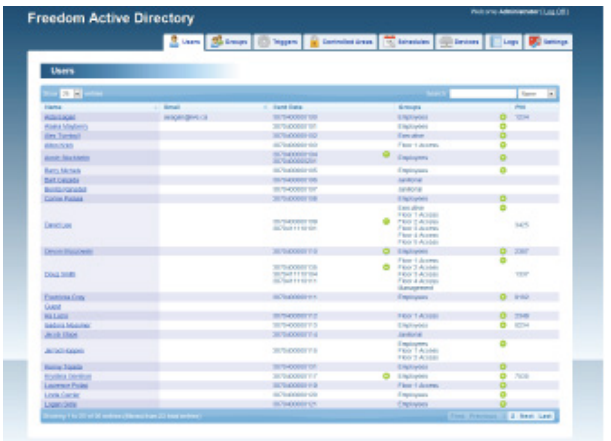
- There are no limits to schedules, access groups, controlled areas, business partitions, or number of users
- Privileges can be instantly changed based on threat levels
- Presentation of a card to a card reader, or simply an activation of an emergency push button, can affect as many output relays as necessary
- Multiple inputs, such as door sensors or emergency buttons, can be programmed to automatically create outputs, such as alarms or activate third-party devices
- Upon a forced evacuation event, provides multiple "who is missing" muster reports
- Integrates seamlessly with Enterphone Telephone Entry by Identiv
- When retrofitting a legacy access control system, disruption is kept to a minimum and the implementation can be done in stages
- Supports integration with several leading video management system (VMS) platforms

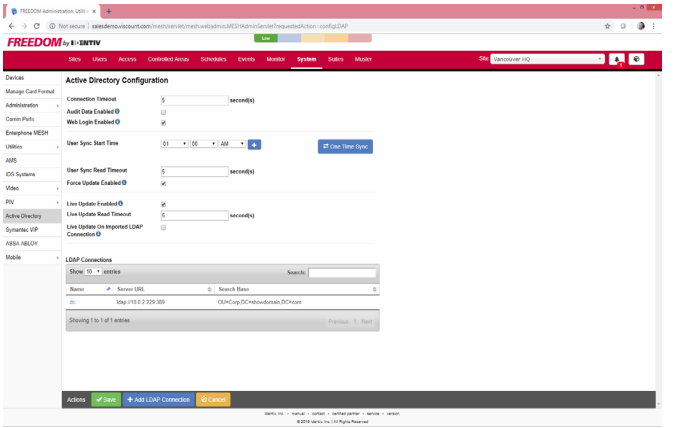


ACTIVE DIRECTORY AS A PHYSICAL SECURITY SYSTEM

With Freedom, we can leverage existing Active Directory (AD) infrastructures to manage authentication and authorization of card user populations. We do this by syncing user accounts between OUs and Groups in AD doors privileges in Freedom. Typical objects and attributes to map and synchronize are users and devices (door readers, elevators, and locking hardware). The advantage of a unified platform is the elimination of a dedicated user database of physical security.

- When a change is made in AD, it gets replicated to Freedom
- The current validity of a user and their door access is managed in AD
- Links directly on-site with preferred AD catalog





Managing PACS within a Virtual Server Environment

Freedom is a PACS that is VMware-ready for deployment in a virtual server environment, eliminating the need to maintain a 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
- Unified physical and logical security
- Browser-based web application
- Secure, Linux operating system
- Peer-to-peer directory synchronization

Ordering Information

Contact your Identiv Regional Sales Manager or email sales@identiv.com.

Identiv (NASDAQ: INVE) is a global provider of physical security and secure identification. Identiv's products, software, systems, and services address the markets for physical and logical access control, video analytics and a wide range of RFID-enabled applications. Customers in the government, enterprise, consumer, education, healthcare, and banking, retail, and transportation sectors rely on Identiv's access and identification solutions. Identiv's mission is to secure the connected physical world: from perimeter to desktop access, and from the world of physical things to the Internet of Everything.

Identiv has offices worldwide. Addresses and phone numbers are listed at identiv.com/contact. For more information, visit identiv.com or email sales@identiv.com.