

Avert™

Access Control

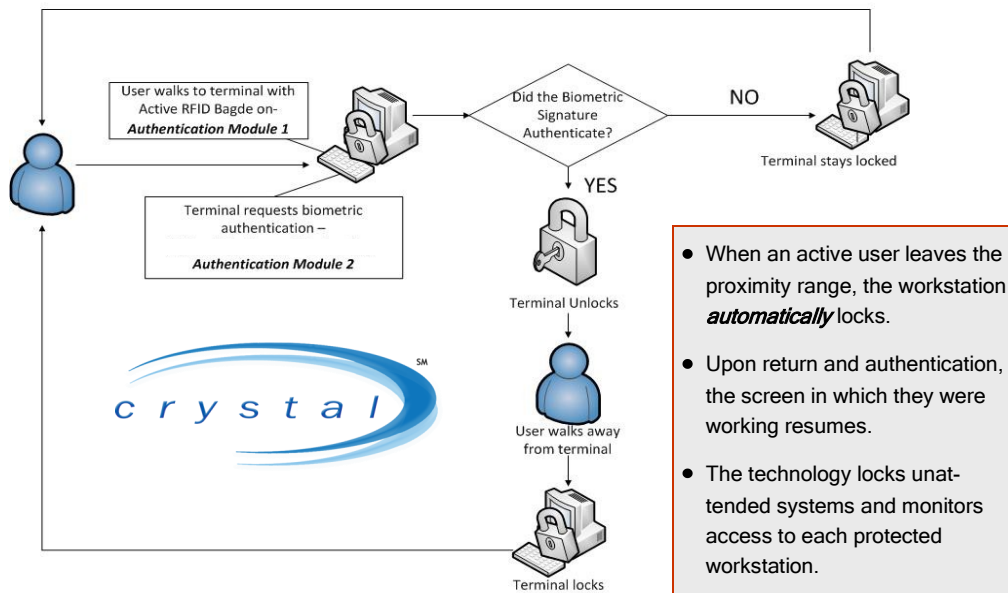
Automatically Locks Unattended Systems and Eliminates Unauthorized Access

Crystal IT Delivers Next Generation Enterprise Access Control and Password Management

Internal breaches are exponentially surpassing external threats for companies and governments worldwide. Crystal IT, Inc. provides clients with a non-intrusive endpoint security module to control access to individual workstations. In addition, our enterprise-level central management appliance controls each integrated workstation so IT staff have the ability to administer and monitor each and every authorized user access. Best of all, it is transparent to the user, prevents unauthorized access to proprietary information and intellectual property, and eliminates passwords - all while reducing administrative costs associated with help-desk support calls—averaging savings of up to \$380 per user per year.

How Does Avert™ Access Control work?

The dual authentication endpoint security module is a stand-alone component to prevent unauthorized access to individual workstations. Multiple modules seamlessly integrate with the access control central management appliance offering a dynamic solution for enterprise-level demands.



Avert™ Access Control specific components:

Access Control Endpoint Security Module

Once installed on the computer, RFID badges are assigned to individual users and the user biometric signature is scanned. Identification is captured, encrypted, assigned, and stored along with the user badge information. When an active user leaves the proximity range, the session is terminated and the workstation locks. Upon return and authentication, the previous screen reappears without interruption. If a different authorized user approaches the workstation in the interim and authenticates their presence with a authorized biometric signature, the previous user is then logged out, and the computer will log on the new user.

Access Control Central Management Appliance

As a stand-alone appliance, this component integrates each of the workstations containing endpoint security modules into one seamless solution providing your IT staff control over user access. This server appliance stores all configuration information including biometric signatures and RF proximity badge data for each user on the Domain level and makes it available anywhere on the network—as long as the workstation is a member of the domain and contains an access control endpoint module. Event logs detailing workstation usage are created, stored, and may be printed for management reporting purposes.

Utilizing Biometrics and Active RFID Technologies to Secure Individual Workstations with Administrative Rights



Avert™ Access Control

- Two Factor Authentication
- Prevents Unauthorized Access to Your Computer
- Controls Access and Security to Network
- Instantaneously Locks Computer System when User Walks Away
- Automatically Generates Passwords for the User
- Eliminates IT Help Desk Password-Related Calls
- Maintains Access Controls through Central Administrative Appliance
- Operates on a Non-intrusive RF Frequency within any Healthcare Setting
- Protects Corporate, Employee, Customer and Patient Data
- Secures Intellectual Property and Proprietary Information
- Meets and Exceeds Regulatory Compliance
- Reduces Risks Associated with Hiring Contractors, Temporary Employees, and Maintenance Staff

Features and Benefits of *Avert*™ Access Control

Easy Installation and Deployment

By utilizing the central management server, enterprise-wide installation can easily be accomplished to set-up, activate, and capture each user's credentials within a matter of minutes optimizing an efficient deployment.

Improves Employee Productivity

Employees are no longer responsible for creating, managing and maintaining passwords. Now, their focus remains on each task at hand restoring time spent on password issues to productivity.

Enforces Corporate Protocol

Corporate protocol is enforced when employees no longer rely on physical documentation to remember passwords.

Enterprise-Wide Universal Single-Sign On

Each authorized user's biometric signature provides initial workstation access as well as authorizing access for all subsequent applications requiring credentials for entry.

Enhances Industry Compliance

Avert™ Access Control meets and exceeds compliance with HIPAA, the Sarbanes-Oxley Act, and the Gramm Leach Bliley Act.

Non-Disruptive Updates

Automatically and effectively receive software updates and periodic maintenance through the access control central management server – avoiding potential disruption to your organization and unnecessary access to your internal data and network infrastructure.

Reduces In-House IT Support Expenses

Help desk support calls are dramatically decreased. *Avert*™ Access Control eliminates passwords from the user experience, thus doing away with expenses associated with lost, stolen or changing passwords.

Assists with Forensic Research

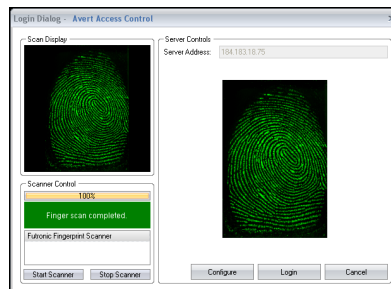
Because each user's biometric signature is stored each and every time an endpoint secured workstation is accessed, precise details of each log-on event are recorded. Should an authorized user access files that they shouldn't, their biometric signature identifies them as the individual that accessed the sensitive information.

Multiple User Access Control

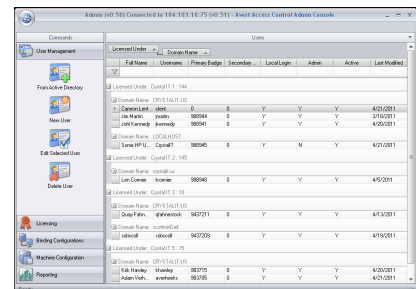
Avert™ Access Control allows multiple employees access control capabilities on each individual workstation module.



Screenshot: RFID Badge Recognized; User Submitting Biometric Pattern.



Screenshot: Administrator Login Through Central Administration.



Screenshot: Server Administration Application.



Meeting the New Standard for AC²

AC² protocol dictates that an access control solution actively distinguish, in real time, the difference between a user's presence and absence at a terminal and then lock the system based upon identifying that the user is away and the system is unattended. This eliminates the risk of significant exposure by ensuring that unattended systems, their sessions and applications are never left open and unsecured.

There is a significant and distinct difference between AC² and past generation access control protocol. Most solutions only *grant* access based upon credentials approved exclusively at initial logon without providing any further ongoing supervision to validate and ensure authorized activity within the session. AC² compliant solutions consistently monitor the entire user session and actively *control* access throughout that session, locking the system automatically and without user intervention should that user leave the proximity of the system. This protocol presents a dynamic security layer that older, non-AC² solutions lack, which oversees and manages user sessions in real time.