

Wizcon Supervisor 9.4

Enhanced security and traceability in mission critical processes

User, Data and Process Security as top priorities

In today's modern world – and more acutely since the events of September 11, 2001 – security is crucial in almost all human activities, whether in the production of food, beverages or pharmaceuticals, industry, manufacturing, water and power utilities, government and public buildings, etc. Processes must be safeguarded from acts of terrorism, sabotage, vandalism, misconduct, accidents, or simple human error.

Anywhere computers are used, system threats abound:

- Internal threats: identity theft (e.g. use of others' passwords), rights theft (e.g. execution of forbidden activities), etc.
- External threats: data theft (e.g. spying, sniffing, forgery), identity theft (e.g. password theft), etc.

For security and protection, business owners, government officials and families rely on well-designed systems and trusted methods to provide:

- Traceability
- Process safety
- System integrity
- Human health and safety
- Homeland security

With **Wizcon Supervisor 9.4**, ELUTIONS introduces revolutionary new ways of handling person, asset and system security:

- Strong authentication: providing secure login of Wizcon users.
- Station access restriction: providing or denying access of certain Wizcon stations to certain named users or groups, and at certain times.
- Data protection: ensuring integrity of the Wizcon databases.

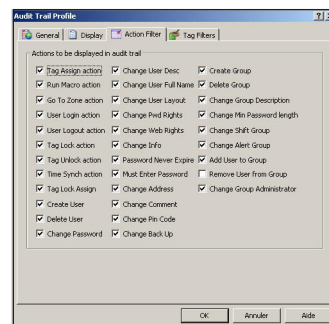
Security in Wizcon applications is based on several core guiding philosophies:

- Every user is authenticated and has specific rights (strong authentication)
- Information is protected and encrypted (data protection)
- Every user action is logged (audit trail)

Audit Trail

Wizcon Supervisor's Audit Trail, which enables development of applications that comply with FDA 21CFR Part 11 security standards, has been enhanced and the number of traceable actions has been quadrupled to a total of 33 possibilities:

- User actions: Changing tag value, Running a macro, Going to a zone, User login...
- User management actions: Creating a user, Deleting a user, Changing a user password...
- Group management actions: Creating a group, Deleting a group, Changing a group description...

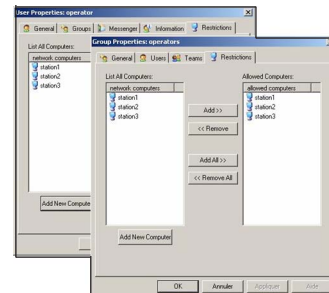


Audit Trail profile configuration

Station Access Restriction

Wizcon Supervisor 9.4 enables granting or revoking access to a specific Wizcon station, at specific times:

- Secure Wizcon network
- User restriction
- Group restriction
- Manual restriction list
- Shift management



User and Group restriction lists

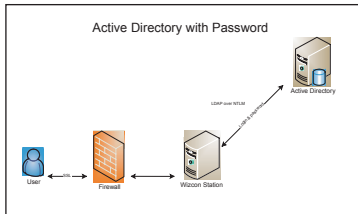
Data Protection

Wizcon Supervisor 9.4 enables protecting Wizcon's core databases:

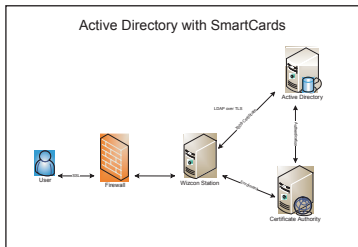
- User Management
- Tag and Alarm definitions

The content of the databases is protected using sophisticated encryption algorithms so that it can only be modified from within Wizcon Supervisor. If, at start-up, Wizcon detects that an external program has changed the code, a system alarm is generated. This ensures integrity of the Wizcon databases, and enables strict compliance with FDA 21CFR 11 system security rules.

Enhanced security and traceability in mission critical processes



Active Directory with Password



Active Directory with SmartCard + PIN code

Centralized user management using LDAP with Active Directory

Wizcon supports Microsoft's Active Directory structure for centralized user management (Windows 2000 Server and 2003 Server). Wizcon Supervisor's User Management system can thus rely on a centralized Active Directory using the industry-standard LDAP protocol.

Benefits of using Active Directory with Wizcon user management:

- User Management is centralized on an IT Server
- Users and Passwords are managed by the IT department
- There is no redundant User Management
- Achieve tighter integration with Microsoft's User Management, allowing simpler Maintenance for the IT Department and more efficient enterprise-wide management.

Strong Authentication

Three possible authentication factors can protect unauthorized login to a high-security application:

- What I know (password)
- What I have (smartcard, token)
- What I am (fingerprint)

Adding any or both of the latter two points provides strong authentication via secure login.

Smartcard-based Strong Authentication

Wizcon Supervisor 9.4 now supports smartcard secure login:

- Based on Microsoft PKI architecture: secure architecture involving X509 certificate to authenticate users against Active Directory
- Using TLS authentication and encryption: strong encryption mechanisms ensuring data security and user identity
- Native support of Aladdin eToken products: low cost and secure USB tokens or smartcards

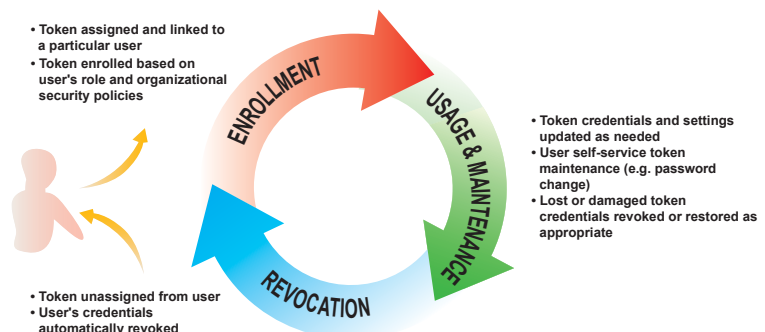
Benefits of smartcard-based authentication:

- Compatible with existing IT system: using smartcards fully compliant with smartcard standards such as PKCS, LDAP, X509...
- User-friendly: simply plug-in token and enter PIN code to authenticate
- Web-enabled: PKCS supported by Wizcon Web clients, using Certificate authentication and strong data encryption

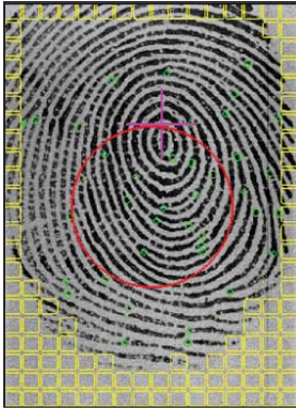


Smartcard-based authentication for Wizcon Supervisor 9.4 uses field-proven Aladdin USB eToken

The Token Life Cycle



**Enhanced security
and traceability
in mission critical
processes**



Biometry-based authentication for Wizcon Supervisor 9.4 is based on NEC Positive Identification, one of the world's fastest and most widely used biometric identification algorithms in service at Japanese government authorities for more than 25 years

Biometry-based Strong Authentication

Wizcon Supervisor 9.4 now supports biometric secure login:

- Based on biometry world leader NEC technology: the world's fastest and most widely used biometric identification algorithms (>50% worldwide market share)
 - Number 1 in NIST FpVTE03
 - Number 1 in NIST SDK Speed test 2006 (1:N)
- 1:1 Authentication or 1:N Identification: with multiple-factor authentication to improve security
- Multiple reader compatibility: supports several high-quality fingerprint scanners

Wizcon Biometry solution architecture:

- Wizcon PID (Positive Identification) Enrollment License(s)
 - Used once to enroll new users' fingerprints into Wizcon User Management
- Wizcon PID (Positive Identification) Verification License(s)
 - Used always and at all Wizcon stations to log into application
- Fingerprint Scanner(s)
 - Used once to enroll fingerprints into Wizcon User Management
 - Used always and at all Wizcon stations to log into application

Key features of Wizcon Biometry solution:

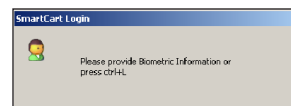
- Security solution is fully integrated in **Wizcon Supervisor 9.4**
- Provides either 1:1 Authentication or 1:N Identification
- Software: best of class technology from the world's biometric leader
- Hardware: multiple devices certified, for various uses and providing various levels of quality, durability, price

Benefits of biometry-based authentication:

- Strong authentication mechanism with 2-factor or 3-factor authentication: the user is the password
- User-friendly: simply place finger on the reader
- State-of-the-art technology

Main benefits of Wizcon Biometry solution:

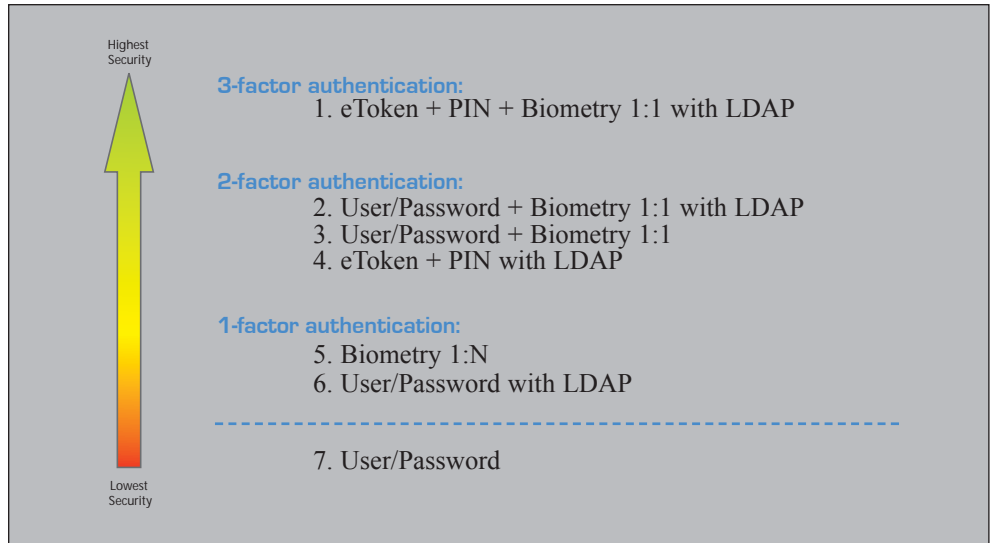
- Provides enhanced secure login for all Wizcon users in any circumstance
- Open: several non-proprietary scanners supported
- Easy to buy: single supplier offers whole solution
- Easy to deploy: plug & play, USB or Ethernet
- Easy to maintain: durable, easily replaced
- Scalable: easily add new users, scanners



Biometry-based authentication on Wizcon Supervisor 9.4 is extremely simple to deploy and to use

Enhanced security and traceability in mission critical processes

Strong authentication - Increasing Security Level



Enhanced Security in Wizcon - Features

Strong authentication topologies

- User/Password: station and Web, standard in Wizcon
- Enterprise User Management: station and Web, with connection to enterprise network and Active Directory
- Secure login with eToken: station and Web, with connection to enterprise network and Active Directory
- Secure login with Biometry: station only (not on Web), with or without connection to enterprise network and Active Directory

Feature	Options								
	Wizcon 9.3	Wizcon 9.4	Comments	LDAP Enrollment	LDAP Client(s)	eToken Enrollment	eToken USB key(s)	Biometry Enrollment	Biometry Client(s)
Custom password policy	✓	✓							
Fine grain authorization management	✓	✓							
Secure Web connection through SSL	✓	✓	(Web only)						
Audit Trail	✓	✓	Extended!						
Station access restriction		✓	New!						
Data protection		✓	New!						
User authentication:									
- Standard User/Password	✓	✓							
- Enterprise User Management		✓	New!	✓	(✓)				
- Secure login with eToken		✓	New!	✓	(✓)	✓	✓		
- Secure login with Biometry		✓	New! (station only)					✓	(✓)
- Secure login with multi-factor authentication		✓	New!	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)

Note: All features available on Wizcon station and on Web except as noted.

When selecting the appropriate mix of standard features, options and hardware, Wizcon Supervisor helps build security into any mission-critical application.