

# SentriNET

Fingerprint Authentication to Windows Networks

Password overload and password management is a burgeoning problem of today. The number of passwords the average employee has to remember is spiralling out of control, whether it is to log-on to the business network, a laptop loaded with sensitive information or to the many applications organisations typically use.

Maintaining security and controlling access to IT systems and applications through the use of passwords has been both a burden and an inconvenience to users and IT staff - the conventional security controls based on usernames and passwords consume inordinate amounts of IT Departments time.

SentriNET, from BMS Biometrics, is an off-the-shelf solution which allows a person's fingerprint to be used to authenticate their identity when accessing Microsoft Windows networks.

SentriNET offers the stability to implement and enforce a corporate security policy, integrating with Active Directory (AD) for the enrolment of users and the storage of templates. BMS has been delivering secure Network log-on with SentriNET solutions for the past decade.

SentriNET is used across many industries and private and public sector organisations including the NHS, Banks, the Police, Security and Educational establishments.



Tim O'Neill, Assistant Director for IT at the Security Industry Authority (SIA) said,

*"the SIA chose biometric authentication from BMS over passwords for a number of reasons including:*

- ✓ *Security – the technology provides strong authentication, encryption and access control. People don't have to remember passwords, or share them, or need to write them down for fear of forgetting them*
- ✓ *cost saving – we have made large savings on help-desk calls and IT support, as people no longer forget their passwords"*

## Secure Fingerprint Network Log-on

A person's fingerprint is totally unique to them and it will never change. SentriNET uses a unique algorithm to convert the visual fingerprint into digital form. This algorithmic number—up to 250 characters—cannot be used to recreate an impression of the fingerprint elsewhere. It is a number that only SentriNET can read.

SentriNET does not store a copy of the fingerprint, so it is impossible to reverse engineer a fingerprint from SentriNET. This is important when considering the possible civil liberty implications of using fingerprint technology.

## Key Features:

- Fingerprints cannot be forgotten, copied, transferred or stolen.
- Faster, easier and more secure network and workstation access control.
- The cost of password administration is drastically reduced.
- SentriNET uses Microsoft user management tools for enrolment.
- Easy to install and deploy, with minimum training required.

**BMS**

# because it's got to be you...

The result of the authentication process is a secure, faster, easier and more auditable network log-on. It is no longer necessary to enforce regular password changes, because fingerprints cannot be forgotten, copied, transferred or stolen.

Businesses, hospitals and government agencies have found that the return on investment from biometric solutions is high when they are used to deter identity theft and preserve resources.

SentriNET biometric authentication software offers:

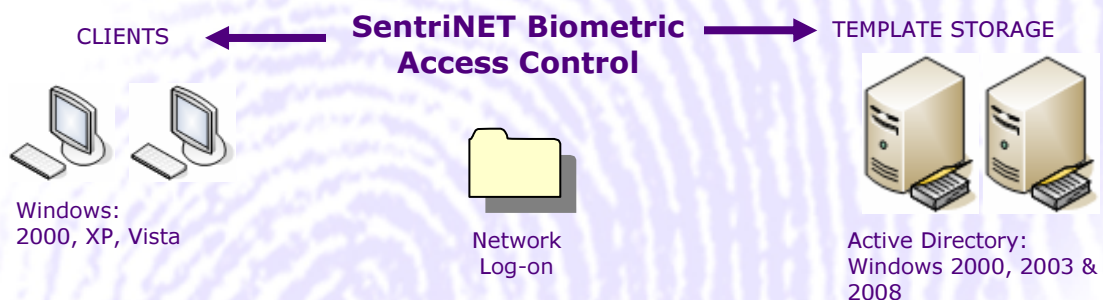
- The ability to implement and enforce a corporate security policy
- Secure enterprise network log-on and access control, both local and remote
- Low cost, easy deployment by administrators and fast, convenient logon for end users
- Cost savings due to elimination of network password management
- Outstanding value, rapid payback and high ROI

Unlike other biometric security products, SentriNET removes the need for any additional authentication servers and links directly into an already operational Windows network with little or no disturbance to the network infrastructure.

The benefits of using SentriNET over traditional passwords are clear:-

- Fingerprints cannot be forgotten, copied, transferred or stolen
- Faster, easier and more secure network
- SentriNET, is unique in it's class and at this time, has no direct competitor.
- The cost of password administration is dramatically reduced
- SentriNET uses Microsoft user management tools for enrolment
- Easy to install and deploy, with minimum training required
- Common biometric devices can be used with standard PCSC compliant smart cards or USB tokens to protect access to credentials such as digital certificates
- Works with VPN solutions for mobile users accessing enterprise networks via the Internet
- Supports a range of industry leading fingerprint scanners
- Works with both the Authentec and UPEK chipsets, which are currently incorporated within laptops from HP, IBM, Lenovo, Fujitsu and Toshiba

By using SentriNET an organisation can know with certainty who is logging onto the corporate network and accessing sensitive information.



**Business Management Services (UK) Ltd, BMS House, 10 Churchill Park,  
Private Road Number 2, Colwick, Nottingham, NG4 2HF**

Tel: 0115 965 8400  
Website: [www.ithealth.co.uk](http://www.ithealth.co.uk)

Fax: 0115 987 3202  
email: [info@ithealth.co.uk](mailto:info@ithealth.co.uk)

**BMS**