

## Secure Web Portal Access Platform.

### Introduction

SentryCom **Secure Web Portal** Access Platform enables Extended Enterprise businesses by ensuring the right people have access to the right information, while safeguarding critical data and confidential assets from unauthorized use.

### Highlights

Users are authenticated through a unique scalable 2-tier, malware-resilient 2-tier or 3-tier client-server architecture, which includes Voice Authentication and a proprietary combination of hardware and software identifiers.

**Secure Web Portal Access Platform** delivers a complete security architecture that includes the four A's of business risk management: Authentication, Authorization, Administration, and Audit. Using the four A's our clients are able to build a solid security architecture.

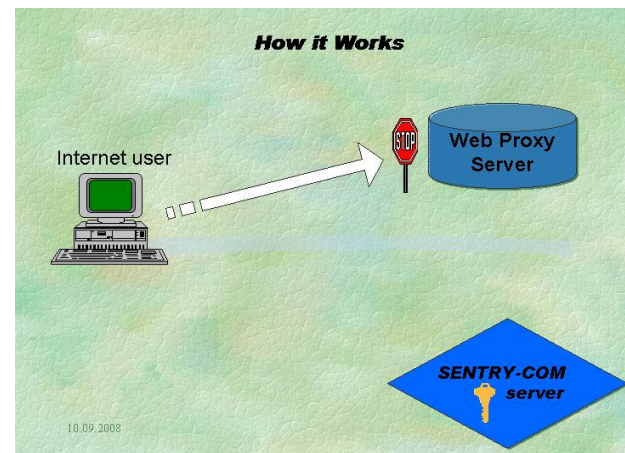
### Benefits

- Software-only PC-based VoiceShield® solution exceeds US NIST Level 4 open network e-authentication requirements.
- Authentication on demand

- Malware resiliency
- Live Voice Authentication engine
- No need for expensive dedicated hardware and network infrastructure
- Easy deployment
- Seamless integration with any Web platform
- Full set of admin, logging and audit tools

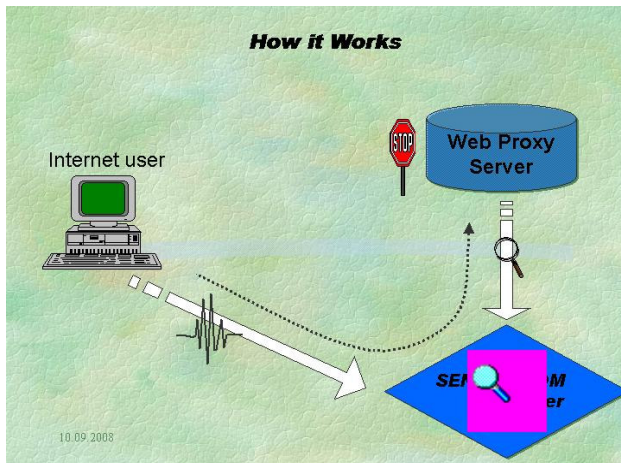
### How it Works

Internet/Intranet users requesting access to Web Portal resource URL are required perform strong authentication vs. SentryCom MACS - Managed Authentication & Crypto Server. On submission – they are redirected seamlessly to **MACS** Authentication server, which acts as a gateway to existing infrastructure.

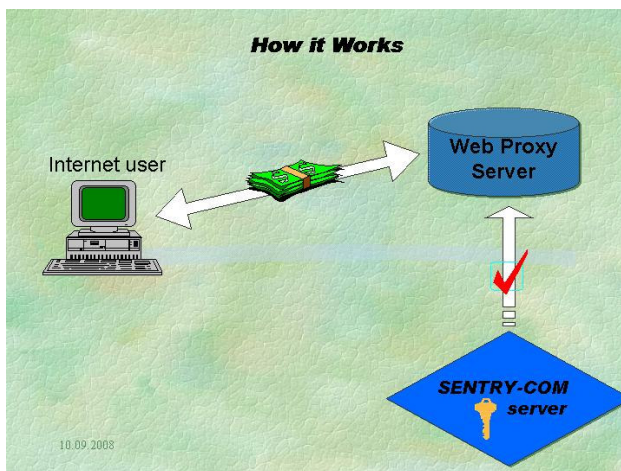


# Secure Web Portal Access Platform.

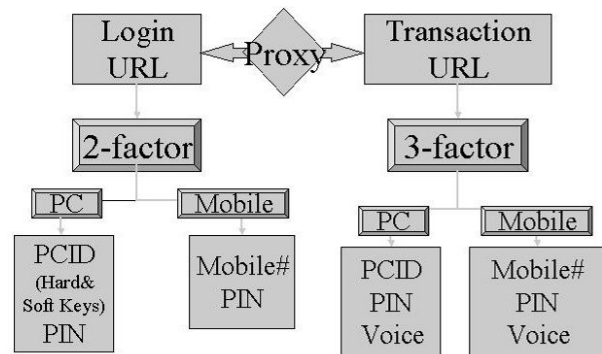
The strength of the requested authentication is to be determined by Enterprise and may be changed according to their security /convenience preferences and can be configured on demand. To ensure the highest level of security during the authentication process, a users identity is verified using his PC hardware/software key, PIN number and Biometric Voiceprint authentication. Alternatively, while roaming, the user's identity can be verified using mobile phone number, PIN number and Biometric Voiceprint authentication.



Upon successful Verification, users are granted access to URL and can proceed with their work.



The system allows a choice between 2-factor (in cases that malware is not an issue) , malware-resilient 2-factor and highest security 3-factor (including voiceprint) authentication. Using Proxy Server one can write simple rules specifying which URL access is protected by 2-factor For example 2-factor for login URL and 3-factor authentication, for business transaction URL.



## System Requirements

**Web-Site integration:** Web proxy server

**MACS Server Software** (if installed internally):  
Win 2003, 2008 server  
MS SQL 2005 server

**Client Software:** Win2000, XP, Vista, 7

**Browser:** IE 6.0 , 7.0 , 8.0

- No microphone is needed for 2-factor authentication.
- Built-in laptop microphone is sufficient for malware-resilient 2-factor authentication.
- Headset Microphone is required for Voice Biometrics 3-factor authentication.

### Clientless – using mobile phone:

If installed internally - IVR with Voice XML support is required for clientless mobile phone .

# Secure Web Portal Access Platform.

## Integration with Existing Enterprise Infrastructure.

This product operates side-by-side and on-top of existing infrastructure. The typical usage is outlined below:

1. Existing Web Portal is integrated with IAM (Identity and Access Management) platform. Login is protected by username & fixed password. Administrator may add to log-in URL a rule requesting 2-factor strong authentication as described above.

2. Existing Web Portal is integrated with IAM (Identity and Access Management) platform. Login is protected by username & OTP generated by SentryCom MACS, following 2-factor strong authentication, see relevant product sheet or :

<http://www.sentry-com.net/VoiceReset.html>

There is no need for additional log-in rule.

3. Specific sensitive URL access may require additional Strong Authentication, with variable strength according to circumstance. Existing IAM do not provide such functionality.

Administrator may add to this URL a rule requesting 3-factor strong authentication as described above.

## About SentryCom

SentryCom's mission is to deliver malware-resilient reliable, cost-effective and easy to use strong authentication and crypto solutions to secure critical data within and beyond extended enterprise.

SentryCom products and technology are protected by US patents **7,689,832**, **5,913,196** and **6,510,415**.

## Contact

**SentryCom Ltd.**

**POB 56263**

**Haifa 34989**

**Israel**

**Tel: +972-4-8342392**

**Fax : +972 -3-7255867**

**E-mail: [info@sentry-com.net](mailto:info@sentry-com.net)**

**Web Site: [www.sentry-com.net](http://www.sentry-com.net)**