



## Portable Security

### FlashID™

Handy, strong authentication

FlashID is an innovative product that intelligently transforms the standard USB storage device (USB flash drive, USB key, USB disk, USB memory, thumbdrive) into a security token, which can then be used in any application where two-factor authentication is required.

FlashID binds the user's identity to a standard USB storage device, transforming the commonly used USB flash drive into a hardware security token. With FlashID, users have to provide both the USB key device itself and the USB key password in order to gain access to protected resources, such as Windows Logon, Remote Desktop, VPN and Web applications.

**FlashID provides a more cost effective authentication solution than the conventional dedicated hardware token.**

### KEY FEATURES

#### Reliable

FlashID smartly binds the user's identity to the hardware of the USB key device and securely locks the user's information with strong encryption and the USB key hardware fingerprint, making it a secure and reliable hardware security token.

#### Portable

FlashID does not require end users to install any software onto their PCs or laptops. Users can simply plug their USB keys into any computer, and will be immediately authenticated by the FlashID system.

#### Flexible

FlashID can be optionally configured to block the USB flash drive or any removable media drive from user access, protecting organisations from data leakage.



### KEY BENEFITS

#### Two-Factor Authentication

FlashID helps enable organizations to replace insecure static password authentication with a strong two-factor authentication. Protected by FlashID, users have to provide both the USB key device (what you have) and the USB key password (what you know) in order to gain local and remote access to corporate networks or websites.

#### Multi-Application Support

FlashID can be used to protect virtually any application that requires strong authentication, including Windows local/network logon, remote desktop logon, VPN remote access and web-based applications such as Outlook Web Access, Citrix Web Interface etc.



#### User Friendly

For consumers, by using USB key as a hardware security token, users do not need to install new hardware. USB key is small and portable, and is commonly used by a majority of computer user.

#### Cost Effective

For businesses, the main advantage over existing hardware token-based authentication solutions is that they do not need to bear the expense of stocking and supplying tokens to its users but can simply advise customers to buy a USB flash disk in whatever capacity they like.