



NMS for PDA

IT Security that doesn't get in the way

New Media Security provides security solutions to protect your organisation's data when it is at its most vulnerable - on mobile devices such as PDAs, Laptops, Tablet PCs, and also in emails and on CDs and DVDs.

Our software solutions prevent unauthorised access to sensitive information by using a combination of user authentication, such as a strong password, and data encryption.

NMS software protects the mobile enterprise while being:

- **Easy to use for the end user.** There is nothing to learn or remember to do.
- **Easy for the IT Dept.** Management tools make it easy to deploy, manage and recover users remotely
- **Cost-effective.** Enables your organisation to use technology to the full without worry, and with reduced support and Help Desk costs.

Other NMS products

As well as NMS for PC we offer:

- **NMS for PC**
Protects laptops, desktop PCs and XP Tablets.
- **NMS nCode**
Creates encrypted CDs, DVDs and email attachments.

Securing the mobile enterprise

NMS for PDA™ provides security for the professional and enterprise PDA user. It prevents unauthorized use of Pocket PC PDAs and protects sensitive data from risk of compromise in the event that a PDA is lost or stolen.



NMS for PDA Highlights

NMS for PDA protects data with a secure login password and by strongly encrypting all data held on removable media, and in persistent storage.

Before data can be accessed, users must identify themselves to the PDA by entering a password in the login screen that appears on power-up. Repeated entry of an invalid password causes the delay between login attempts to double. Data on storage cards, and in persistent storage is encrypted to prevent it from being read in another PDA. When the user logs in and accesses the data, it is automatically decrypted in the background.

The security settings can only be accessed with a separate Manager password, and allow a PDA administrator to change the login settings, set password policy, control the use of Bluetooth and Infrared ports, and control whether and under what conditions the PDA is automatically wiped of all data. The policy for encrypting storage cards can be set to always, or never encrypt, or to allow the user to choose whether or not to encrypt a storage card when it is inserted into the device. A similar control governs whether persistent storage is encrypted. Management tools supplied with the Enterprise Edition allow the security policy to be pre-configured without intervention from the user.

What NMS for PDA does

NMS for PDA helps you keep sensitive data and files on Pocket PC-based PDAs secure from unauthorised users, should your PDA or storage cards be lost or stolen, and fall into the wrong hands. It does this in two ways:

Secure authentication. A password that can be up to 25 characters and contain numbers and letters is much stronger than using a four-digit PIN. The user password is also required when connecting the PDA to a PC. As well as a user password, there is a Manager password that allows the management functions to be configured.

Encryption. All data stored on memory cards, and in persistent storage is held encrypted if required. If the PDA is stolen and hard reset, memory cards and files in persistent storage cannot be read. Encryption and decryption is transparent to the authorised user and occurs on-the-fly.

More than just encryption

NMS for PDA is the only security software currently available for Pocket PC PDAs that features all these key benefits:

- Protects all data with a strong user authentication password, not just a PIN.
- Encrypts all data, in real-time, on all removable media such as Compact Flash cards, SD-cards and micro drives.
- Encrypts data in persistent storage.
- Secures the ActiveSync connection to the PC with the NMS password. Allows secure temporary authorisation to connect to plain PDAs, and data on protected PDAs cannot be copied to unauthorised PCs.
- Controls the use of Bluetooth and Infrared ports.
- Can be set to wipe all PDA data under three conditions: if the PDA becomes locked, (after a number of wrong passwords have been entered), or is not used or docked for a specified number of days.
- A Manager password, separate from the User password protects security policy. Only PDA Administrators can set or change login settings, control password policy and encryption settings.
- Allows you to securely restore the installation and security settings of NMS for PDA after the PDA has been hard reset, or after all battery power has been lost. This makes it possible to have a secure encrypted backup and restore of data.

Some features Windows Mobile 2003 editions only.

Tools for managing Enterprise security

The Management tools that make up the Central Management System are designed for automating deployment and allowing management of PDAs from a central location:

- **Mass Deployment.** Allows easy deployment across an entire organisation. The Mass Deployment tool creates a known security set-up for distribution to end-users via email, CD, Intranet, etc. In this way, an organisation can enforce its PDA security policy without having to rely on the end-user, or recall every PDA to base.

The Mass Deployment tool provides a simple method of allowing NMS-protected PDAs to dock to more than one PC. It can also be used to deploy to PDAs that never dock to host PCs.

- **Remote Recovery.** Allows for the remote recovery from forgotten passwords or locked PDAs, using a once-only challenge response unlock mechanism that doesn't need to be physically or electronically connected to the PDA.

Allows secure remote recovery from a Dead PDA. Data and NMS installation can be restored securely without the need for a physical or electronic connection to the PDA.



24 Monument Road
Weybridge
KT13 8QX
United Kingdom

T: +44 (0)1932 854 968
F: +44 (0)1932 855 783
E: sales@NewMediaSecurity.com
W: www.NewMediaSecurity.com