

## Authenex HDLock™ for Toshiba Notebooks

Authenex HDLock is optimized to protect Toshiba notebooks using strong two-factor authentication and AES (Advanced Encryption Standard) to encrypt and secure the contents of the notebook's hard drive. The Authenex A-Key® acts as the key to your notebook; without it, the hard drive remains encrypted and inaccessible to anyone else.

### Two-Factor Authentication

Two-factor authentication is a security method that restricts access to a specific resource or device by requiring two factors of identification: something you have (a hardware token or card), and something you know (a password or PIN). A very common example of two-factor authentication is the process used by bank ATM machines that require both an ATM card and PIN number before granting access to a particular user. The two factors of authentication required by HDLock are the Authenex A-Key and the user's unique password. The A-Key conducts true Challenge-Response sequences directly with the encryption engine and does not require PKI.

### 128-Bit AES Encryption

HDLock uses the U.S. government standard AES to encrypt the contents of the notebook hard drive. Once encrypted, the contents of the hard drive cannot be decrypted until the user re-inserts the original A-Key and password.

### Using HDLock

Once logged on to the notebook, HDLock is designed to allow Toshiba notebook users work without interruption. All encryption and decryption processes occur on the fly – and are transparent to the user. Upon hibernation, shut down or removal of the A-Key, the hard drive becomes “locked” and the encrypted contents become inaccessible to anyone but the owner of the unique A-Key and password with which the drive was encrypted – even if the hard drive is removed from the notebook. The only way to unlock and view the hard drive data is for the HDLock user to once again login using their A-Key and password.

### Optional Password and Token Recovery

HDLock includes a simple registration and recovery option in the event a user loses their A-Key or password. If a registered user loses or forgets their A-Key, they may visit the support section of the Authenex website and pass the question and answer recovery process to receive a “soft” key. This soft key can then be used to temporarily login to the notebook until the next time the A-Key is used. The soft key will expire when the A-Key is used to login again.



*Toshiba Tecra® M3 Notebook*

### Multiple Languages Available

For companies with global needs, HDLock is available in English and Japanese. The program has multi-language capabilities and functions alongside localized versions of Microsoft Windows. HDLock will be made available in more languages in the future.

### The HDLock Management Server

Our Management Server feature offers greater flexibility in managing HDLock user accounts and recovery for ease of deployment and administration for enterprises. This feature allows for a simple web method of recovery in the event an A-Key is lost or misplaced. A three-step question and answer process generates a soft key that can be used to access an encrypted hard drive. Also included are reporting capabilities to show active and inactive A-Keys.

Since employees travel with important, and often confidential, data on their Toshiba notebooks, protected information must always be accessible. In the event of a lost token while on the

## The HDLock Management Server (Continued)

road, our management server ensures that a company has control of its recovery options for that user. Designated administrators manage account profiles and allow for recovery to be conducted over any browser and Internet connection.

## Authenex HDLock Benefits

---

- Protects Toshiba notebooks that are unattended, lost or stolen
- Secures the contents of the notebook's hard drive
- Allows users to work without interruption
- Uses powerful AES-based encryption algorithm and two-factor authentication
- Includes the Authenex A-Key token
- Does not require PKI
- Allows use of the same A-Key with multiple Authenex e-Security applications
- Recovery procedure for lost A-Keys and passwords
- Management Server feature offering greater flexibility for recovery options

## The Authenex Suite Of Applications

---

The A-Key was designed to support a full compliment of security needs – leveraging the entire suite of applications available through Authenex. These solutions include: strong authentication for VPN, LAN and web access, file encryption, secure file exchange, strong web access control, and more. This allows administrators to add security solutions as requirements grow and change – adding applications without having to replace A-Keys. The A-Key is also available in several models allowing for combined authentication methods, such as full on-board PKI, Challenge-Response and One-Time Password.

## System Requirements:

---

- Windows XP Home or XP Professional
  - English Edition
  - NTFS
- Windows XP Tablet Edition 2004 or 2005
  - English Edition
  - NTFS
- CD-ROM Drive
- 256MB RAM
- 200 MB Free hard disk space (for installation only)
- USB (Universal Serial Bus) 1.1 or above
- Internet Connectivity is required for A-Key registration and recovery functions (unless deploying the management server)

## Management Server Specifications:

---

- Microsoft Windows Server 2003 Standard Edition
- Microsoft Windows 2000 Server Service Pack 3 or higher
- 256MB RAM
- 100 MB of free hard disk space
- One 10Base-T/100Base-Tx Ethernet network adapter
- One USB port must be available (version 1.1 or above)

---

© 2005 Authenex, Inc. All rights reserved. Authenex, A-Key, HDLock, and associated logos are registered or unregistered trademarks of Authenex, Inc. All other registered or unregistered trademarks are the property of their respective owners.

Authenex®

Corporate Headquarters  
1489 Salmon Way  
Hayward, CA 94544  
tel: +1 510 324 0230  
fax: +1 510 324 0251  
www.authenex.com