

Information Anywhere Suite

Afaria Security Manager for Handhelds and Laptops

KEY FEATURES

- Security and Management from a single console
- High performance on-the-fly file decryption for Windows Mobile Handheld devices and laptops
- Full disk encryption for laptops
- Unattended Computer reboot
- Kill Pill for Windows Mobile
- Block rogue devices access from Microsoft Exchange email
- Email and PIM encryption on handhelds
- Encrypt and share removable storage media for laptops
- Support for smart card and token-based authentication products for laptops
- Temporary password recovery
- Windows handheld and laptop support
- Administrator password control
- Full protection from the latest mobile threats, via automatic virus definition updates

AFARIA SECURITY MANAGER

Mobile users face an extremely vulnerable computing environment where security gaps can exist. Handheld devices and laptops can be lost or stolen, the risk of intrusion is high, and security controls are inconsistent at best and often unenforceable. Additionally, government and industry regulations regarding data privacy and encryption are becoming stricter, and can even result in fines for noncompliance. It is imperative that organizations manage and protect sensitive information, and enforce security centrally, rather than leaving the burden of security to the mobile device end user.

Afaria Security Manager offers unique handheld and laptop security functionality from a single console. It enables IT to manage security requirements centrally, such as enforcing power-on password, encryption of data, updating signature files and antivirus engines, and managing the configuration of the device. Coupled with Afaria's robust management capabilities, IT is able to increase the efficiency of managing any mobile deployment while ensuring security policies are enforced and devices remain updated.

Afaria is a key component of the Information Anywhere Suite, which addresses converging IT requirements by offering a secure and scalable mobile software platform.

Password Protection

Password protection is the first step toward securing data on mobile devices. Afaria Security Manager offers IT the ability to centrally define, control and enforce end user password requirements.

- Power on password capability requires a user to enter a password each time the device is cycled on
- Device "lock down" after a predefined number of failed password entry attempts
- Device reset, encrypted data deletion or complete device disablement may be enforced by IT after failed password entry attempts
- Alphanumeric and/or character based passwords may be used
- Variable frequency of password change requirements
- Remote password retrieval by IT is possible in the case of a forgotten password

On-Device Data Encryption

Afaria Security Manager gives users and IT high performance piece of mind by offering the ability to encrypt data that resides on devices. In the case of a lost or stolen device, data is protected through strong encryption, rendering the device unusable. Through the Afaria Security Manager console, IT can select what data to encrypt and when it should be encrypted. Removable storage medium, such as compact flash cards and SD cards, can also be encrypted.

- For Window Mobile handhelds, on-demand data decryption decrypts only the requested data instead of decrypting the complete contents of the device leading to improved user experience through faster recall of information and greater battery life.
- Full disk encryption for Win32 laptops
- Encryption for both device and over-the-air transmissions
- Encrypt removable storage media

Policy Management

Security policies are easily managed and enforced from a central location, simplifying management of a diverse set of frontline users, applications and devices.

- Security policies are created and controlled by IT from a central console
- Policy changes are automatically updated on the device during a connection with the Afaria server
- Ensures antivirus definition files and firewalls are configured correctly and operating normally
- Easily and remotely track and report on the status of security installations and encryption

Reports and Data Logging

Key to any corporate security effort and policy is the ability to log and report all security activity occurring on remote devices, as well as being able to pull and deliver detailed reports for any exceptions, violation of company security policy and devices entering and leaving service.

- Generate reports by device type, groups or user type
- Password entry failure and redeployment of new policy upon reconnection
- Status of client delivered to handheld devices

SECURITY MANAGER FOR HANDHELD DEVICES

Password & Data Encryption

Afaria Security Manager gives users and IT high performance piece of mind by offering the ability to encrypt data that resides on devices. In the case of a lost or stolen device, data is protected through strong encryption, rendering the device unusable. Through the Afaria Security Manager console and using flexible file folder encryption, IT can select what data to encrypt and when it should be encrypted. Removable storage medium, such as compact flash cards and SD cards, can also be encrypted.

- For Window Mobile handhelds, on-demand data decryption decrypts only the requested data instead of decrypting the complete contents of the device leading to improved user experience through faster recall of information and greater battery life.
- FIPS 140-2 certified modules
- Temporary password recovery for lost or forgotten passwords
- Interoperable with GPS devices. Administrators can allow the GPS application remain in the foreground, even when handheld is in a locked state
- Helps meet governmental regulations such as HIPAA and Sarbanes-Oxley
- Option to encrypt PIM data, company specific data, or data stored on external media

Data Fading

Afaria Security Manager allows an IT administrator to lock, wipe or reset a device that has not communicated with the corporate network or Afaria server after a predetermined number of days.

- Automatically renders a device unusable, eliminating manual IT intervention for lost or stolen devices
- Options setting fully configurable by IT

Remote Kill

When a device is lost or stolen, the risk of data loss increases is untenable. Fines may be imposed and company reputation can be irreparably damaged, so IT needs the ability to ensure data does not land in the wrong hands.

- Send a "kill device" command to completely disable Windows Mobile devices
- Ability for the Help Desk to kill a lost or stolen device
- Options include hard reset of device, or deletion of data on external storage media

Email Interoperability

Afaria Security Manager for Handhelds is fully interoperable with iAnywhere's OneBridge wireless email solution and Microsoft Exchange. Full interoperability ensures data is always secure by allowing a device to receive email even when it is in a locked state, and by encrypting PIM databases.

- Protects sensitive corporate email and company contact information
- Enforces mandatory encryption of sensitive information
- Receive email and PIM data, even when device is locked

Antivirus & Firewall

Mobile threats have escalated from simply a lost or stolen device scenario to more sophisticated, invisible attacks designed to either cause irreparable harm to your mobile device or intercept sensitive company data.

- Full protection from the latest mobile threats, via automatic virus definition updates
- Real-time Monitor scans any file received via SMS, MMS, Bluetooth, WiFi, infrared, or desktop sync
- Inbound and outbound traffic monitoring
- "Black list" filtering of mobile spam and unwanted calls

SECURITY MANAGER FOR LAPTOP AND TABLET PC'S

Password & Data Encryption

Perhaps the most important element of laptop data protection is the ability to protect all the data that exists on the hard drive. That's Afaria offers a comprehensive approach to laptop security.

- Full disk encryption protects all data on the machine
- Multi user and administrator support for each protected laptop
- Easy administrative decommissioning process for laptops
- Encrypt and share removable storage media for laptops

- Support for smart card and token-based authentication products for laptops
- Win 32 two factor authentication using Security Manager and a USB token. In boot-time the clients prompts for insertion of token or smartcard, and authenticates user credentials before the operating system loads.

Unattended Reboot

Unattended reboot allows administrators to securely bypass the pre boot authentication, on Win 32 computers, based upon a preset time window. This proves valuable when you would like to encrypt both mobile and LAN base machines. Administrators can easily manage updates to LAN based machines while protecting them with full disk encryption

- Specify an exact time window that a reboot is allowed
- Able to set up repeat windows such as weekly, monthly... to conform to standard update schedules
- Add custom messages to display to the user during unattended reboot procedure
- User can bypass unattended reboot by entering in credentials if they log on during a window

Multiple User/Administrator

The multiple user feature provides the ability for separate users to authenticate on the same laptop or tablet computer using unique log on credentials. Administrators can create their own account in the Afaria client installation process so all machines will have an administrative log in. This means that the user's credentials do not need to be compromised for administrators to manage the device.

Afaria Security Manager for laptops can support multiple Security Manager Administrators and clients. Administrators have the rights to add and remove users, change policy settings, and decommission clients.

- Users can be easily added using a simple GUI
- Administrators have the ability to create/delete/modify user accounts
- Multiple users or administrators per computer
- Standard users do not have access to administrative options
- Allows administrators access to computers without requiring the users credentials

Decommissioning Utility

Administrators can securely wipe all pre-boot data contained on laptop or tablet PC's, allowing it to be decommissioned, reassigned or resold with confidence that the data on the machine will not be accessible.

- Third party data erasure services are not needed.
- Process is accomplished in one easy step
- Corporate policy frequently required decommission prior to a laptop or tablet is discarded, sold or turned in at the end of a lease

AFARIA AS A SECURE INFRASTRUCTURE

Backup Manager

The information your remote workers gather and use in the course of serving customers is an important corporate asset. Ensuring that this data is backed up and rapidly recoverable is both a high priority and a challenge. Your mobile users are often too busy serving clients to remember to back up their data; even if they did remember, most are intermittently connected, often over low-bandwidth connections. Even if they wanted to back up data it would be a time-consuming and inefficient process. Instead, a centralized and automated process is the way to ensure that important information is always available.

Afaria Backup Manager makes the data archiving and recovery process simple for individual users and effective for the larger organization. It backs up frontline workers' critical business data and documents, ensuring their availability to both the frontline employee and the company, even if the device is lost, damaged or stolen. Archived data, applications and hardware configurations can be quickly restored to any system or device that has been lost or damaged.

- Archive data, applications and hardware configurations to a centralized location
- Back up information on a scheduled basis without user involvement
- Efficiently retrieve data using techniques that minimize connection times
- Remotely download lost data, applications and settings to replacement devices

Patch Management

Afaria Patch Manager supports the latest patch technology from Microsoft for laptops, which can push out patches for Microsoft products such as Exchange 2003 and Office 2003, and supports automatic installation of service pack updates.

- All updates are backed up with detailed log files and reports, ensuring full compliance with existing corporate policies
 - Supports dynamic bandwidth throttling and segmented delivery to deliver large updates such as a new service packs
- Allows IT to download patches in specific languages which saves time and disk space

CLIENT DEPLOYMENT AND DEVICE REMEDIATION

Over-the-air Client Deployment

Afaria Security Manager enables over-the-air deployment, allowing administrators and end-users to simply and easily leverage existing wireless connections to automatically download and install Afaria Security Manager client software on mobile devices.

- Client can be deployed wirelessly, eliminating the need for desktop sync
- Download client via a clickable URL is sent to the user via an SMS message
- Device specific client creation wizard creates the smallest installation size image, saving download time and disk space

Access Control

Access Control provides a new way for customers to detect and prevent rogue Window Mobile devices from connecting to your corporate Microsoft Exchange email servers. Working with Microsoft Exchange Serve, Access Control functionality detects when devices are attempting to synchronize with an Exchange server and blocks their access if they are not properly managed and secured by the Afaria server. With this capability companies can ensure that the devices requesting synchronization access to your Exchange Server are fully under IT's control

- Device white listing features allows devices to synchronize with the Exchange Server even if the device does not meet current security policies
- Device black listing allows IT to "permanently" disallow a device access to the Exchange Server
- Allows for frequent device changes by executives
- Protects Exchange email and PIM data

Secure Architecture

The Afaria server delivers enterprise performance with minimal maintenance and cost, while seamlessly integrating into the IT infrastructure.

- Seamless integration with SQL Anywhere database from iAnywhere, providing the convenience of a single-vendor solution
- Provides integration with key directory technologies, such as NT and LDAP-compatible directories
- Will run on Microsoft SQL Server and Oracle
- A web based console supports Microsoft .NET technologies, allowing system administration and control of business and IT information
- A broad range of connectivity options are supported, such as TCP/IP over wireless or wired connections, dial-up remote access connections (RAS),WAN, and high-speed LAN connections
- Also supported are HTTP and HTTPS to allow users to connect over the Internet and have a secure access point through corporate firewalls
- The Afaria server runs on Windows Server 2003 Standard or Enterprise with service pack, or Windows 2000 Server or Advanced Server with Service Pack 4

SYBASE IANYWHERE - STRATEGIC MOBILE SOFTWARE PLATFORM

The Information Anywhere suite is a secure, scalable mobile software platform that addresses the converging IT requirements of enterprises today. By combining email/messaging, mobile device management, enterprise-to-edge security and back-office application extension capabilities, Information Anywhere enables organizations to empower employees to do the work they need to do anywhere, at anytime, on any device. Built from the inception to address the unique characteristics of frontline environments, Information Anywhere ensures that mobilized applications are as secure, reliable and available as those that run within the data center. Backed by more than 20 years of expertise in solving mobile deployment challenges, Information Anywhere allows organizations to integrate, extend and leverage investments in their existing IT infrastructure when developing a mobile strategy.

For more information, please visit: <http://www.sybase.com/products/mobileenterprise>

ABOUT IANYWHERE

iAnywhere, a subsidiary of Sybase, Inc. (NYSE:SY), enables success at the front lines of business. The company holds worldwide market leadership positions in mobile and embedded databases, mobile management and security, mobile middleware and synchronization, and Bluetooth® and infrared protocol technologies. Sybase iAnywhere plays an important role in the Sybase Unwired Enterprise strategy, which focuses on managing and mobilizing information from the data center to the point of action. Tens of millions of mobile devices and over 20,000 customers and partners rely on the company's "Always Available" technologies, including SQL Anywhere and its Information Anywhere suite.

IANYWHERE SOLUTIONS, INC.
WORLDWIDE HEADQUARTERS
ONE SYBASE DRIVE
DUBLIN, CA 94568-7902
U.S.A.

FOR GENERAL INFORMATION:
CONTACT_US@IANYWHERE.COM
NORTH AMERICA
T 1-800-801-2069
1-519-883-6898

FOR SPECIFIC REGIONAL PRODUCT
INFORMATION:
EUROPE, MIDDLE EAST, AFRICA
+44 1628 597 100
ASIA PACIFIC
+852 2506 8700
JAPAN
+81 3 5544 6400
BENELUX
+31 (0)30 - 247 8444
FRANCE
+33 (0) 1 41 90 41 90
GERMANY
+49 (0) 7032 / 798 - 0
UNITED KINGDOM
+44 (0) 1628 597100

IANYWHERE SOLUTIONS IS A SUBSIDIARY OF SYBASE, INC. COPYRIGHT © 2008 IANYWHERE SOLUTIONS, INC. ALL RIGHTS RESERVED. IANYWHERE, ONEBRIDGE, SYBASE, AND THE SYBASE LOGO ARE TRADEMARKS OF SYBASE, INC. OR ITS SUBSIDIARIES. ALL OTHER TRADEMARKS ARE PROPERTIES OF THEIR RESPECTIVE OWNERS. ® INDICATES REGISTRATION IN THE UNITED STATES OF AMERICA. LOXXXX-0608