



Microsoft[®] Messaging & Security Feature Pack

Mobile access to Microsoft Exchange Inbox, Calendar, Contacts, and Tasks through Windows Mobile[®] powered devices is enhanced by the new messaging and security capabilities of Microsoft's second release of Windows Mobile 5.0 (AKU2). Used in combination with Exchange Server 2003 Service Pack 2 (SP2), the Messaging & Security Feature Pack (MSFP) allows organizations to enforce power-on password and basic security controls on Windows Mobile 5.0 AKU2 devices and even provides an over-the-air device wipe capability. Although MSFP is a solid step forward in device protection, it lacks a number of features that many companies require for complete protection and legislative compliance. This technical brief provides an overview of key MSFP features and describes how CREDANT Mobile Guardian complements MSFP to provide enterprises a more comprehensive data security solution.

Overview

Microsoft's MSFP allows Exchange administrators to specify security policies and to send and enforce those policies over-the-air once a user connects to the Exchange Server and signs in.

To take advantage of the new capabilities provided by MSFP an organization must do three things:

1. upgrade their existing Exchange environment to Exchange Server 2003 SP2;
2. configure Exchange ActiveSync[®] to run in their environment; and
3. upgrade Windows Mobile 5.0 devices to MSFP (AKU2) or purchase new devices that are running AKU2. Note: the most comprehensive list of AKU2 devices can be found on Microsoft's web site. Users should contact their carrier or device manufacturer to find out if their particular device is compatible with MSFP features.

Messaging & Security Feature Pack

The Microsoft Messaging & Security Feature Pack for Windows[®] Mobile 5.0 works with Microsoft Exchange Server 2003 SP2 to deliver a direct, scalable and cost-effective mobile messaging solution.

This solution enables business users to easily stay connected to their Microsoft Office Outlook[®] Mobile information while on the go and helps businesses to better protect device data.

- Keep your Calendar, Contacts, Tasks, and Inbox up-to-date using Direct Push Technology. Plus, you can now browse your corporate address book over-the-air with Exchange 2003 SP2.
- Better protect device data and manage devices using the Feature Pack and Exchange 2003 SP2. With this combination, IT administrators can remotely manage and enforce select corporate IT policies over-the-air via the Exchange 2003 SP2 console. Businesses can mandate policies like requiring PIN passwords for every device.
- Deploy scalable, cost-effective mobile messaging solutions and reduce the need to pay for an additional third party server product and client access license fees by using existing Exchange 2003 SP2 investments.

Source:

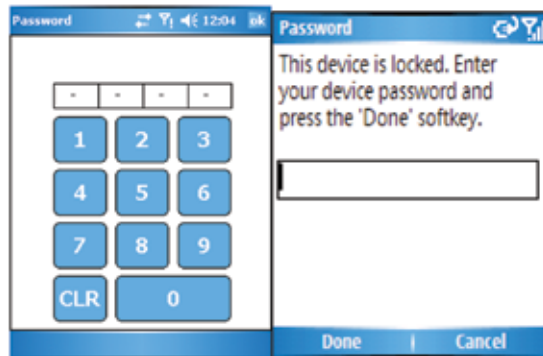
<http://www.microsoft.com/windowsmobile/business/5/default.mspx>

Overview (cont.)

MSFP Security Policy Options

As Windows Mobile 5.0 devices connect with Exchange Server 2003 SP2¹ to synchronize via Exchange ActiveSync, administrators can define and enforce the following security policies at the Exchange 2003 SP2 console:

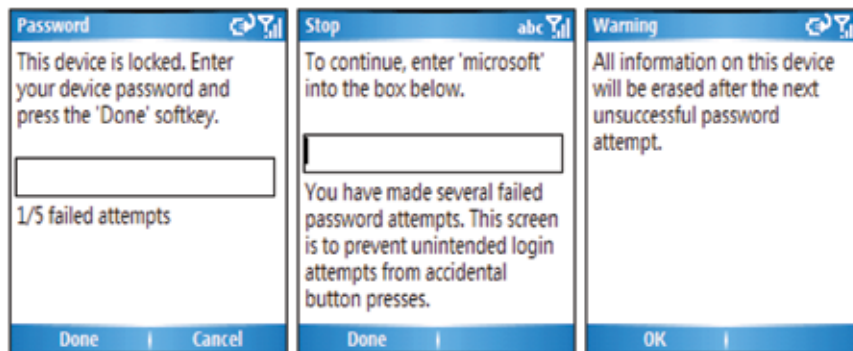
Minimum password length (characters) — specifies the required length of the user’s device password. While the default setting is 4 characters, password length can be 4 to 18 characters.



Password require both numbers and letters — requires that users choose a password with both numbers and letters. This option is not selected by default.

Inactivity time (minutes) — specifies whether users log on to their devices after a specified number of inactive minutes. This option is not selected by default. If selected, the default setting is 5 minutes.

Wipe device after failed (attempts) — specifies whether the device memory is wiped after multiple failed log-on attempts. This option, which initiates a hard reset on the device, is not selected by default. If selected, the default setting is 8 attempts.



¹ List of available policies taken from http://www.microsoft.com/technet/itsolutions/mobile/deploy/msfp_6.msp

Overview (cont.)

Refresh settings on the device (hours) — specifies how often an administrator sends a provision request to devices. This option is not selected by default. If selected, the default setting is every 24 hours.

Allow access to devices that do not fully support password settings — allows devices that do not fully support the device security settings to synchronize with the Exchange Server. This option is not selected by default.

Remote Wipe — enabled through the Microsoft Exchange ActiveSync Mobile Web Administration tool, this is a tool created apart from MSFP so that non-Exchange Administrators or Help Desk staff could be delegated the right to manage devices. Additional information can be found at <http://msexchange.com/archive/2005/07/07/407416.aspx>.

The screenshot shows the 'Remote Device Wipe' interface. At the top, it says 'Use this page to manage user's devices. You can initiate remote wipe for specific devices and also cleanup device partnerships.' Below this is a search box for 'Enter the mailbox name to lookup list of devices' with 'Sync1' entered. The user account information is: 'User Account: Sync1, Mailbox Server: SALT1, Smtip Address: Sync1@salt1dom.extest.microsoft.com'. The main part of the interface is a table with columns: Device Id, Type, Status, and Action.

Device Id	Type	Status	Action
Device1	SmartPhone	OK	[Wipe] [Delete]
setup	SmartPhone	OK	[Wipe] [Delete]
Device2	SmartPhone	OK	[Wipe] [Delete]
Dummy	PocketPC	OK	[Wipe] [Delete]
Device123	PocketPC	OK	[Wipe] [Delete]
Device3	PocketPC	OK	[Wipe] [Delete]
NKHMGPEDA	PocketPC	OK	[Wipe] [Delete]
blah1	PocketPC	OK	[Wipe] [Delete]
NSFJITNAA	PocketPC	Wipe initiated 2/4/2005 7:30:15 PM	[Cancel Wipe] [Delete]
Device2	PocketPC	OK	[Wipe] [Delete]
Device1	PocketPC	Wipe initiated 12/31/1600 10:00:00 PM Sent to device 2/7/2005 9:58:45 PM Device acknowledged 2/7/2005 9:58:45 PM Wipe operation completed successfully!	[Cancel Wipe] [Delete]

MSFP Interoperability with CMG Shield

The CMG Shield for Windows Mobile 5.0 is interoperable with the MSFP. CREDANT testing has determined that when the CMG Shield is deployed on an MSFP device, the CREDANT security policies take precedence, meaning that all CREDANT password, encryption and device authorization policies are enforced by the CMG Shield. Furthermore, Exchange Server 2003 SP2 recognizes devices with the CMG Shield as being secure and will allow the Exchange ActiveSync session to continue. Testing has also determined that the MSFP remote wipe feature works on MSFP devices protected by the CMG Shield.

How CREDANT Mobile Guardian Enhances MSFP

CREDANT Mobile Guardian, when used in conjunction with the MSFP, delivers the following benefits:

- Security and control for **all** mobile device platforms throughout the organization — Windows Mobile 2003, Windows Mobile 5, Windows, Symbian, Palm, RIM, and removable media. *NOTE: because Windows Mobile 2003, Symbian and Palm now have Exchange ActiveSync capabilities built in to the base operating system, protecting only Windows Mobile 5.0 devices alone does not guarantee protection of all of your sensitive data.*

MSFP provides power-on password controls for only Windows Mobile 5.0 devices running AKU2 through Exchange Server 2003 SP2. Exchange accounts for approximately 50% of today's corporate e-mail and messaging market, and since Microsoft believes that only 25% of Exchange users have upgraded to SP2 to date, MSFP therefore addresses only about 12.5%. CMG, however, addresses 100% of this market, because it works independent of the messaging solution and OS version, providing advanced security controls for all mobile device platforms across the enterprise.

- Complete mobile security life cycle management — detection, encryption, management, and support from one central web-based administration console.
- Centrally available mobile inventory and audit information for compliance and enforcement.
- Other CMG security controls include:
 - FIPS 140-2 validated encryption of sensitive data on the device (e-mail and contacts) and on removable media.
 - Complete range of advanced device controls for restricting and protecting devices against vulnerabilities (e.g. Bluetooth, IR, Network, etc.).
 - Self-service PIN/password reset (connected/disconnected).
 - Forgotten PIN/password recovery — secure Help Desk recovery (whether connected or disconnected).
 - Device synchronization control to prevent users from synchronizing data to non-trusted machines.
 - Complete phone usability while device is in a locked state — accept and place incoming/outgoing calls.

Summary

The addition of CREDANT Mobile Guardian to an organization using Windows Mobile 5.0 SP2 and MSFP delivers a more thorough mobile data protection and control solution for the entire mobile infrastructure. This combination allows for enterprises to take full advantage of Microsoft's messaging and security features. Furthermore, CREDANT Mobile Guardian protects and controls all mobile device platforms throughout the organization — Windows Mobile 2003, Windows Mobile 5, Windows, Symbian®, Palm®, RIM, and removable media.

CREDANT Technologies	15303 Dallas Parkway, Suite 1420, Addison, Texas 75001 USA	866-CREDANT (273-3268) or 972-458-5400	www.credant.com	info@credant.com
----------------------	--	---	-----------------	------------------