mSecure PDA Release Notes for 4.3

mSecure PDA employs technology supplied by a third-party provider—Credant Technologies—to secure data on devices. The product used is *Credant Mobile Guardian (CMG) Shield*. Information from Credant Technologies is incorporated into this mSecure PDA release notes document.

Supported Devices

- Palm devices running Palm OS 5.x with at least 4 MB of RAM and 2 MB free main memory
- Pocket PC 2003/2005 devices, with 3 MB free main memory
- Smartphone 2003/2005 devices with 1.5 MB free main memory

In this release, all previously supported Palm OS 4.x and earlier devices are now officially unsupported.

New Support and Functionality

Pocket PC Enhancements

- New Windows Mobile 5 encryption policies—Mail Encryption and PIM Encryption—provide on-the-fly AES 128 encryption of mail and PIM data
- New supported Pocket PC 2003 devices include the i-mate JAM
- New supported Windows Mobile 5 devices include: the Dell Axim X51v; HP iPAQ models 2190, 2490, 2790 and 6900 series; the Sprint PPC-6700; the T-Mobile MDA Vario; Palm Treo 700w; Cingular 8125; Verizon XV6700; Vodafone 1640; i-mate JASJAR and K-JAM; the Qtek 9100
- The cryptographic libraries used by the Pocket PC now take full advantage of the Intel IPP version 4.1 libraries. The integration of these libraries means that full advantage is taken of the encryption hardware acceleration and extended battery life of Intel processors on mobile devices
- If **Encrypt mail and mail attachments (AES 128)** and/or **Encrypt calendar, contacts and tasks (AES 128)** is ticked on the **PPC Encryption Options** screen of the mSecure PDA wizard, mSecure PDA creates an encrypted folder for mail and/or PIM data. Calculation of this folder's maximum size has been optimized to address larger PIM databases: see below for more details
- Hard-reset functionality (for the *Access Code Failure Action* value) has been enabled for Windows Mobile 5 AKU2 devices

Smartphone Enhancements

- New supported devices include the Windows Mobile 5 Cingular 2125and the Motorola Q
  NB: Data encryption is not yet available for these devices.

Palm Enhancements

- FIPS 140-2 validation has been received for Palm OS
- New supported devices include the LifeDrive, Tungsten E2, Tungsten T5, Tungsten X, Tungsten Z22 and Palm TX

mCenter Enhancements

- The ***** character can be used as a wildcard when specifying databases to be encrypted on Pocket PCs.

Fixes

Pocket PC Fixes

Previous versions for Windows Mobile 5 were beta releases and the fixes below represent flaws in that code which are now fixed:

- When mSecure PDA is installed, Letter Recognizer techniques requiring two strokes now work
- If Windows Mobile 5 encryption is enabled (Mail Encryption and/or PIM Encryption), the device's radio stack (which enables voice and data control and data transmission) is no longer disabled, and the phone can now be used
- Idle Time before Lock Action now properly considers touch screen activity and is now properly enforced on all supported Windows Mobile 5 devices
- A Windows Mobile 5 device running mSecure PDA no longer allows limited access to SMS messaging while locked
- When an encrypted SMS message is opened, its full text is now visible on Windows Mobile 5 devices
- Error 608 no longer appears on Windows Mobile 5 phone devices during ActiveSync
- On the Treo 700w, the message and Device Code on the manual authentication screen now display properly
- The *Turn phone off* menu option now works properly on the i-mate JASJAR
- During a phone call on a locked i-mate K-JAM, mSecure PDA now properly allows the phone application to be in the foreground
- mSecure PDA now installs properly on the Cingular SX66
- On the Cingular SX66, the *Today* screen is no longer accessible for 15-20 seconds during mSecure PDA startup
- HTC Windows Mobile 5 devices no longer occasionally lock up after being left overnight.

Smartphone Fixes

Previous versions for Windows Mobile 5 were beta releases and the fixes below represent flaws in that code which are now fixed:

- The T-Mobile Vario no longer freezes when the *Home* button is selected
- A *Lock Device on Power Off* setting of *True* is now properly enforced on a T-Mobile Vario

Palm Fixes

- On Handspring Treos, ListType lists (used for entering accented characters and symbols) in mSecure PDA no longer display asterisks rather than special characters, so you no longer need to ask users to avoid accented characters and symbols in their domain passwords
- On the Palm OS 5 Set PIM Password dialog, the *Unassign* button properly disables this password without deleting any password-protected data, and it no longer displays the *Forgot Password* message when tapped
- By default, the Kyocera 7135 (Verizon) displays *Setup* (prompting the user to tap in various locations to calibrate the touch screens) following each soft reset. When this happens, mSecure PDA now installs properly
- When a DateBk5 reminder displays on a Treo 650 running mSecure PDA, the device no longer stays awake until the DateBk5 reminder is acknowledged
- When you set *Bluetooth Enabled* to *False* on a Tungsten E2, the device no longer displays a fatal error
- Now if a Treo 650's Bluetooth radio is on when a *Bluetooth Enabled* value of *False* is implemented, mSecure PDA turns if off
- The *Databases to Exclude from Encryption* policy is now properly enforced
- There is no longer a restriction when upgrading a policy via HotSync.
- Cyclic resets no longer occur in some circumstances when installing mSecure PDA.
- Tungsten E memory utilization enhancement should now prevent lockups after logoff.
- Treo 650 should no longer experience flashing screens after mNotes replication.

Workarounds & Known Issues

Pocket PC Workarounds

- If the keyboard panel is blocking a PIN screen on an iPAQ, from mSecure PDA's menu, tap *About*, and then tap *OK*
- On an iPAQ h4355, a hard reset initiated by mSecure PDA hangs the device. To work around this issue, soft-reset the device
- An *Infrared Enabled* policy setting of *False* does not take effect until the second soft reset following its delivery. To work around this issue, following a policy update, soft-reset the device again
- Currently, if *Power Off Time before User Logoff* has a non-zero value, a PPC running mSecure PDA wakes up at the Power Off Time and stays awake until the device is powered off again, or its user unlocks it. You can work around this issue and avoid draining the battery as follows: tap *Start* > *Settings*, and then tap the *System* tab. Tap *Power*, and then tap the *Advanced* tab. Under *On external power*, select the *Turn off device if not used for* check box (this is not the default setting)
- Currently, you cannot successfully move an existing encrypted folder across volumes (from main memory to a storage card, or vice versa) using the *Encrypted Folder Path* policy. Attempting this results in the existing encrypted folder being unmounted (and therefore inaccessible) and a new, empty encrypted folder being created in the new location. To work around this issue, change the policy back to its previous value
- Currently, an iPAQ 6515 does not immediately log off, after the number of minutes specified in *Power Off Time before User Logoff*. To partially work around this issue, be sure *Lock Device on Power Off* is *True*
- Currently, mSecure PDA does not respond to the Treo 700w's OK/ Close keyboard button. To work around this issue, use the center navigation button instead
- Currently, following authentication on a Treo 700w, the *Today* screen does not automatically gain focus, so the device's 5-way navigation cannot be used. To work around this issue, tap the *Today* screen
- When an *Access Code Failure Action* value of *Hard Reset* takes effect on a Qtek 9100 or an i-mate K-JAM, currently the device enters a soft-reset loop. To work around this issue, manually hard-reset the device
- On the T-Mobile MDA 4, the UI will occasionally lock up after data is decrypted. To work around the issue soft-reset the device

Pocket PC Known Issues

- A *Network Device Enabled* setting of *False* currently blocks network devices on the iPAQ 6315 silently (that is, mSecure PDA does not display a notification for the user)
- The *PIM Encryption* policy for Windows Mobile 5 devices is implemented via a SecurePIM vault. The vault cannot currently be resized. As this is by design, there are no plans to make any changes
- A *Network Device Enabled* policy of *False* is not currently enforced on the i-mate JAM
- Currently, keypad lock is not supported on the Treo 700w
- When screen orientation on the Cingular 8125 is toggled from horizontal to vertical (or vice versa) while mSecure PDA is open, mSecure PDA currently does not refresh to match
- On Windows Mobile 5 devices, uninstalling mSecure PDA prevents connection to a PC using ActiveSync. Hard reset the device. This will be addressed in a future hotfix.
- If no master password is specified, a device can enter a soft reset loop if mSecure PDA is uninstalled. Hard reset the device.
- Bluetooth and WiFi-disabled polices are not currently implemented on HTC Wizard devices (i-mate K-Jam etc.)
- Dell X51 devices occasionally experience a black & white screen when left overnight.

Smartphone Known Issues

- mSecure PDA encryption policies for Windows Mobile 5, Mail Encryption and PIM Encryption, are not available for Smartphone. As this is by design, there are no plans to make any changes
- An *Infrared Enabled* policy of *False* is not currently enforced on the Motorola Q

Palm Workarounds

- If you soft-reset from the Network Preference Panel, and the *Network Device Enabled* policy is set to *False*, when you authenticate, mSecure PDA displays the message “You do not have permission to open this application.” When you tap *OK*, the message appears again. Workaround: if this happens, press a hardware button to start an application other than Preferences. (After this happens, you cannot access Preferences until your *Network Device Enabled* policy is set to *True*.)
- When you upgrade mSecure PDA from one version to another, the device normally soft-resets. Occasionally this soft reset is unsuccessful, and the screen goes blank. To work around this issue, soft-reset again
- Currently, non-emergency phone calls cannot be successfully placed from a locked CDMA Treo 600. To work around this issue, unlock the device before placing a non-emergency phone call
- Following a hard reset of a Treo 600 initiated by mSecure PDA, the device is calibrated incorrectly. To work around this issue, manually hard-reset the device
- Installing mSecure PDA on a Treo 650 changes a privacy setting of *Mask Records* to *Show Records*. To work around this issue, following installation, mask records again
- Currently, you cannot save a contact after completing a phone call on a locked Treo 650. To work around this issue, unlock the device before working with Contacts

Palm Known Issues

- The following policies are not yet supported for Palm OS 5 devices (although they can be seen in the policy viewer on these devices): *Infrared Enabled*, *Network Device Enabled*. mSecure PDA for Palm OS 5 does not yet support restriction of infrared beaming or network devices

Software and Hardware Compatibility

mSecure PDA has been tested against the supported device list. Credant Technologies have tested mSecure PDA for compatibility with mSuite, and have performed tests on the relevant hardware. Where appropriate, Credant Technologies have reported problems found during testing to other vendors.

Any Palm software that does not handle errors gracefully (for example, an error writing to a disabled external storage card) may begin to report fatal exceptions once Credant Mobile Guardian Shield is installed. A soft reset usually clears the exception, but it is likely to recur under the same circumstances. If this happens, check whether an upgrade for your third-party software is available.

Dell Axim x51 & x51v

It is recommended that any Dell Axim is running the latest ROM version. We will be unable to support issues on devices that are not running the latest available ROM. The Dell Axim X50/51 may show only a Black/White screen when activated from a sleep state whilst in its cradle.

This issue has been reported to Dell and appears on their support site http://support.dell.com/support/topics/global.aspx/support/dsn/en/document?docid=0BD5B8650D525766E0401E0A55177F46&c=us&l=en&s=gen

The A06 ROM addresses a lot of issues with the device itself, which in turn should address some issues when using mSecurePDA. On Dell's Web site, the latest ROM may be labeled as A01 however, once downloaded, it should list itself as A06. This is likely a simple mislabelling on the Dell support Web site.

http://support.dell.com/support/downloads/download.aspx?c=us&cs=04&l=en&s=bsd&releaseid=R114959&SystemID=PDA_AXIM_X51&os=PPM&osl=en&deviceid=7643&devlib=0&typecnt=1&vercnt=2&formatcnt=1&libid=7&fileid=151479

It's recommended you update to this ROM, at the very least the device itself is more stable.

Using Backup Software

Credant Mobile Guardian Shield for Pocket PC is fully compatible with Sprite's Pocket Backup version 2.2 and higher. You can use this product to create a full device backup from which you can restore.

Otherwise, there are several Credant Mobile Guardian Shield files that, for security reasons, cannot be backed up. For more detailed information about backups, see the Installation Guide.

Using Silver Screen Application Launcher

Silver Screen application launcher (for Palm devices) is blocked from accessing the Credant Mobile Guardian Shield application icons.

Using InoculateIT

InoculateIT virus-scanning software from Computer Associates does not run on Palm devices that have Credant Mobile Guardian Shield installed.

Using Fireviewer

Fireviewer, from Firepad, Inc., does not run on Palm devices that have *Network Device Enabled* set to *False*. Fireviewer attempts to access the network library.

Either with or without Credant Mobile Guardian Shield installed, Fireviewer sometimes displays a fatal stack overflow error during HotSync's Cleaning up phase.

Using Hacks and Utilities

Credant Mobile Guardian Shield does not support hacks or utilities that alter device manufacturers' performance specifications. For example, the AfterBurner hack adjusts the clock speed of a device's processor, affecting the results of certain math operations. Because some of these math operations are required for encryption and decryption, using this hack could easily lead to data corruption.

Using ePocrates Rx Pro

Because its databases contain only formulary reference information, if your organization uses ePocrates Rx Pro, we recommend that you exclude these databases from encryption using the *Databases to Exclude from Encryption* policy:

- druginteractions-nc-2
- drugs-nc-2
- pricing-nc-2
- clinical-nc-2
- strings-nc-2
- groupid-nc-2
- eula-nc-2
- formdetails-nc-2
- classes-nc-2
- abbreviations-nc-2
- p002-nc-2
- p011-nc-2
- p120-nc-2
- altclin-nc-2
- prostrings-nc-2
- formstatus-nc-2
- utilities-nc-2
- clientnames-nc-2
- lasths-nc-2
- duse-nc-2
- PrefsDB
- cfg-nc-2
- formsortorder-nc-2
- SmshEULA-nc-2
- sort-nc-2
- version-nc-2
- status-nc-2

Palm OS Debugger

For security reasons, the Palm OS debugger is disabled on Palm devices running Credant Mobile Guardian Shield. It is still available, however, via the Palm OS Emulator.

Chapura Pocket Mirror 2.0.5

Due to instability in the Palm USB driver, Credant Mobile Guardian Shield is incompatible with some back versions of Chapura Pocket Mirror (for example, version 2.0.5). This results in the Gatekeeper workstation rebooting during HotSync synchronization. You can work around this issue by upgrading to Chapura Pocket Mirror 3.0.2 or 3.1.3. You can download an update from http://www.chapura.com/pm_standard.php.

Dell Axim-ActiveSync 3.7 Compatibility

While using Credant Mobile Guardian Shield, you may encounter the Dell Axim-ActiveSync 3.7 compatibility issue. You may want to upgrade to ActiveSync 3.7.1. For more information about this issue, see Dell's Community Forum: http://delltalk.us.dell.com/supportforums/ board?board.id=aximactivesync

Hard-reset Recovery on iPAQs

On some iPAQ devices with older ROMs, when *Hard Reset Recovery Enabled* is *True* and an SD card is in the device when it's hard-reset, Credant Mobile Guardian Shield is unable to recover immediately due to a ROM bug. Although the primary purpose of this feature is to protect the device against unauthorized users, an authorized user can work around this issue by removing the SD card, and hard-resetting the device again.

We have seen this on an iPAQ 5555 with ROM version 1.00.10 or 1.00.13, an iPAQ 1945 with ROM version 1.00, an iPAQ 3870 with ROM version 2.15.12, an iPAQ 5550 with ROM version 1.00.13, an iPAQ 4155 with ROM version 1.00.07, an iPAQ 3850 with ROM version 1.15.04, and an iPAQ 3835 with ROM version 1.20.21. You can address this issue by updating iPAQs that have ROM updates available prior to installing Credant Mobile Guardian Shield. You can find information about available updates for a particular device series at http:// www.hp.com in the Software and Drivers area (check the device series' BIOS category for a ROM Update).

You can also help ensure this policy is enforced by asking users to remove SD cards from iPAQs whenever they're not in use, particularly when devices are at high risk of being lost or stolen (for example, when traveling).

Treo 600 Phone Notifications

If a new voicemail or missed call notification appears on an unlocked Treo 600, the device does not power off in response to either native or Credant Mobile Guardian Shield idle timers. Be aware that not dismissing these dialogs could drain the device's battery. We have reported this issue to PalmSource. (Since these devices are now end-of-line, this is no longer relevant.)

Blue Nomad BackupBuddy

Blue Nomad's BackupBuddy backs up Credant Mobile Guardian Shield properly, but cannot restore it. This happens because BackupBuddy uses the Exchange Manager, which cannot handle large segments (which our application has), to restore. We have reported this issue to Blue Nomad.

SMS Messages on Treos

On some Treo devices with older ROMs, SMS messaging causes the device to soft-reset, or locks the device at a white screen, requiring a soft reset to recover.

We have seen this on a Sprint Treo 600 with ROM version 1.0. You can address this issue by updating Treos that have ROM updates available prior to installing Credant Mobile Guardian Shield.

Smartphones with OS Version 4.20 and Previous

The following issues occur on all Smartphones running OS version 4.20 and previous (Smartphone 2003 First Edition). If you experience one of these issues, check whether the device's manufacturer has a ROM update to

OS version 4.21 (Smartphone 2003 Second Edition) or later available. Such an update addresses all of these issues:

- If an application specified in the *Restricted Applications* policy is uninstalled and reinstalled, it is no longer restricted
- When a policy update is delivered, a manual soft reset is required in order for the update to take effect

Sierra Wireless's Voq Professional Phone

The following issues occur on Sierra Wireless Voq Professional Phones running Smartphone 2003 First Edition. If you experience either of the following issues, you can download from Sierra Wireless's site updated software (release 2.1 or later) that addresses them, as well as upgrading your phone to Smartphone 2003 Second Edition:

- When the *Automatic keypad lock on device lock* check box is selected, Sierra Wireless's Voq Professional Phone's keypad does not lock when the device locks
- Due to Sierra Wireless's Voq Professional Phone's sending an incorrect notification when it's operating on battery power and its backlight dims, the *Lock Device on Power Off* policy can take effect prematurely when this device is operating on battery power

Samsung i600 Smartphone

Due to the Samsung i600's reprogramming of the END key, when the *Automatic keypad lock on device lock* check box is selected, the i600's keypad does not lock when the device locks.

FileZ

Credant Mobile Guardian Shield is currently incompatible with nosleep software's freeware FileZ file manager utility on all Palm devices.

palmOne's Palm Security

Credant Mobile Guardian Shield is currently incompatible with palmOne's add-on Palm Security (but is compatible with built-in or native Palm Security from PalmSource).

Windows Mobile 5 AKU2

An *Access Code Failure Action* value of *Hard Reset* takes effect only on Windows Mobile 5 devices where Windows Mobile Adaptation Kit Update 2 (AKU2) has been applied. If you're using this policy setting, we recommend upgrading your Windows Mobile 5 devices to AKU2.

Windows Mobile 5 Smartphone Speed

According to eWeek.com, Windows Mobile 5 Smartphones may, "for no apparent reason, begin to operate very slowly, or just as suddenly speed up to a sprint..." For more information, see the complete article at http://www.eweek.com/article2/0,1895,1950685,00.asp

McAfee VirusScan PDA with a Storage Card

If a Pocket PC has a storage card inserted, and McAfee VirusScan PDA attempts to scan the card while Credant Mobile Guardian Shield and the device are locked, the inability to access the card is not handled gracefully and VirusScan freezes. If this happens, power the device off, soft-reset, and remove and replace the card.

Getting Technical Support

When you contact CommonTime Customer Support, please be ready with information from the following list that is relevant to the issue you're experiencing:

- Version information for relevant Credant Mobile Guardian Shield components: you can find Credant Mobile Guardian Shield's version number and build date on a Pocket PC, Smartphone and Palm from Credant Mobile Guardian Shield's menu and selecting *About*
- Operating system and ROM version for the device on which the relevant Credant Mobile Guardian Shield component(s) are running:
  - For a Pocket PC device, you can find the OS version number as follows: tap *Start*, and then tap *Settings*. From the *System* tab, tap the *About* icon, and (if necessary) tap the *Version* tab. The OS version information appears
  - For a Smartphone device, you can find the OS version number as follows: press *Start* > *Settings* > *About*. The OS version information appears
  - For a Palm device, you can find the OS version number as follows: start the Application Launcher. From the *App* menu, tap *Info*, and then tap the *Version* button. The OS/version information appears at the top of the screen
- The device manufacturer(s) and model(s)
- Peripherals in use, eg. storage cards, etc.
- The version(s) of ActiveSync and/or HotSync (Palm Desktop) employed, if applicable
- The version of mSuite: in the Admin Console, click the **Help** menu, select **About mSuite Administration Console** and look under **Version**
- How the mSecure PDA policy was delivered, i.e. wirelessly or over the cradle
- You may need to send policy settings to Customer Support: rebuild the problematic mSecure PDA policy and, in most cases, do a search for *mSecurePDAPolicy*.xml* under *C:\Documents and Settings\<name of user currently logged in>\Local Settings\Temp.* Email the appropriate file to Customer Support
- For synchronization issues, please refer to the relevant user guide

Appendix 1: List of Devices Supported by mSecure PDA

Palm 5.0	Windows Mobile 2003	Smartphone 2003	Windows Mobile 5
Palm LifeDrive *	Audiovox PPC 6600 (Sprint/Verizon)	AudioVox SMT5600 (Cingular)	Cingular 8125
Palm Treo 600 (Cingular, Sprint, T-Mobile, VZW)	Dell Axim X3	iMate Smartphone2	Dell Axim X51v
Palm Treo 650 (Cingular, Sprint, VZW, & ROWdy)	Dell Axim X3i	iMate SP3i	HP iPaq hx2190
Palm Tungsten C	Dell Axim X50	Motorola MPx220 (Cingular)	HP iPaq hx2490
Palm Tungsten E	HP iPaq rz1710	Samsung SCH-i600 (Sprint/VZW)	HP iPaq hx2790
Palm Tungsten E2 **	HP iPaq 194x	**Windows Mobile 5 Smartphone**	Sprint PPC 6700
Palm Tungsten T	HP iPaq 221x	Cingular 2125 ***	T-Mobile Vario
Palm Tungsten T2	HP iPaq 415x	Motorola Q ***	Verizon Treo 700W
Palm Tungsten T3	HP iPaq 435x		Verizon VX6700
Palm Tungsten T5	HP iPaq 555x		Vodafone v1640
Palm Tungsten T/X *	HP iPaq 631x		i-mate JASJAR
Palm Z22 ***	HP iPaq 6340		i-mate K-JAM
Palm Zire 71	HP iPaq 6365		HP iPAQ 6900
Palm Zire 72	HP iPaq hw651x		Qtek 9100
	HP iPaq hx21xx		
	HP iPaq hx24xx		
	HP iPaq hx27xx		
	HP iPaq hx47xx		
	iMate JAM		

	iMate PDA2K		
	Intermec 740		
	Siemens SX66 (Cingular)		
	Toshiba PPC e755		
	Toshiba PPC e800		

Legend:

* - Not fully certified
** - May have memory-related issues due to limited device capabilities
*** - Encryption not yet supported

Appendix 2 - Windows Mobile 5 Encryption Policies Are True

More details:

a. mSecure PDA checks the current size of all mail and/or PIM data to be encrypted.
b. If the current size is less than 3 MB, mSecure PDA checks whether 3 MB of free space is available. If the current size is more than 3 MB, mSecure PDA checks whether free space equal to the current size of the data is available. If this amount of free space is not available, mSecure PDA does not encrypt any mail or PIM data.
c. A new device registry setting allows you to determine the amount of growth to allow for (\SOFTWARE\Credant Technologies\UserData\PIMPercent). If the registry setting is 5 or less, mSecure PDA creates an encrypted folder consisting of the amount of free space from the last step, plus 5% of all remaining free space. If it's 80 or more, mSecure PDA adds 80% of all remaining free space. If the registry entry does not exist, mSecure PDA adds 10% of all remaining free space.

If mSecure PDA ever needs to decrypt this data as a result of a Current Shield State policy change to *Uninstall & Decrypt*, it must have an equivalent amount of free space in main memory in order to decrypt all the mail and/or PIM data. If there is insufficient free space to decrypt, currently the encrypted data is deleted.

The registry setting should only be modified under the guidance of CommonTime Customer Support. It determines the size of the encrypted folder. Note, however, that the size can't be changed after the folder is created: if it is necessary to change the default behavior, the registry setting must be present before the mail/PIM encryption policy is applied. In practice this means creating an mControl device package with the appropriate registry entry and ensuring that it is deployed before mSecure PDA.